وزارة التعليم العالي و البحث العلمي

جامعة العربي التبسي – تبسة -

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة ضمن متطلبات لنيل شهادة ماستر تخصص قانون جنائي

الإرهاب الإلكتروني

"دراسة مقارنة في القانون الجزائري والمقارن"

إعداد الطالبة:

حلايمية سليمة

إشراف الأستاذ الدكتور:

دلول الطاهر

الاسم واللقب	الرتبة العلمية	الصفة في البحث
فرحي ربيعة	أستاذ مساعد " أ"	رئيسا
دلول الطاهر	أستاذ التعليم العالي	مشرفا ومقررا
أحمد بومعزة نبيلة	أستاذ مساعد " أ"	ممتحنا

السنة الجامعية: 2017/2016

"الكلية لا تتحمل أي مسؤولية على ما يرد في هذه المذكرة من آراء"

شكر وعرفان

أتقدم بالشكر إلى الأستاذ والدكتور "**دلول الطاهر**" على صبره وتحمله وتعاونه معي لأجل إنجاز مذكرة لنيل شهادة ماستر حقوق تخصص قانون جنائي كما أتقدم بالشكر إلى الأستاذة "فرحي ربيعة" والأستاذة "**أحمد بوعزة نبيلة**" على مجهوداتهم المقدمة وأتقدم بالشكر إلى كافة عمال المكتبة الجامعية "تبسة" لتعاونهم معي ببعض المراجع.

كما أتقدم بالشكر إلى كافة أساتذة كلية الحقوق والعلوم السياسية جامعة تبسة.

الإهداء

أبي والدي الغالي الذي أوصلني إلى بر الأمان وحتمت عليه الأقدار أن يفارقني.

أبي الروح التي تبقى إلى النهاية في جسدي

أهدي عملي هذا

إلى أمي الحبيبة... أسأل الله أن يشفيها ويمتعها بالصحة والعافية.

إلى إخوتي وأخواتي وأزواجهم كل باسمه.

إلى أبنت أخي نعمة المثابرة والمجتهدة وأتمنى لها النجاح في شهادة البكالوريا وإلى ابن أخي كمال "أيهم عبد الحبيب المدعو طالب".

وإلى إبنتي أخي رياض "التوءم تسنيم وسجود".

إلى أيمن ونورهان ورفيدة.

إلى آية وأحلام وأتمنى لهما النجاح والتوفيق.

مقدمة

مقدمة:

يعد الإرهاب الإلكتروني من أخطر أنواع الإرهاب في العصر الحاضر، نظرا لاتساع نطاق استخدام التكنولوجيا الحديثة في العالم ويعتمد الإرهاب الإلكتروني على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الآخرين وإلحاق الضرر بهم أو تهديدهم. حيث يقوم مستخدمه بعمله الإرهابي وهو في منزله، أو مكتبة، أو حتى في غرفته.

حقا أصبح الإرهاب الإلكتروني هاجسا يخيف العالم الذي يتعرض لهجمات الإرهابيين عبر التكنولوجيا الحديثة وبث أفكارهم المسمومة ومما يزيد الأمر صعوبة أن التقدم التكنولوجي لا يتوقف لحظة، لذا يصعب على الأفراد مواجهة هذه العمليات الإرهابية.

أهمية الدراسة:

تبرز أهمية هذا البحث لحداثة موضوعه الإرهاب الإلكتروني وندرة الكتابات عنه كما يستمد هذا البحث أهميته كذلك من خطورة التهديد الإرهابي على الأمن العالمي بوجه عام والتهديد الإلكتروني لهذا الإرهاب على وجه الخصوص لاسيما مع صعوبة الكشف عن مرتكبيه.

ونظرا للتطور الهائل الذي يشهده العالم، وما يترتب عليه من إدخال التقنية الحديثة في كافة المجالات، بحيث أصبحت مكافحة تمويل تلك الجماعات تتطلب توافر قوى بشرية ذات مواصفات وسمات خاصة من حيث الإلمام بالمعلومات والقدرة على التعامل مع أجهزة الحاسب الآلي وشبكات الانترنت والآلات والأجهزة الحديثة، إلى جانب مكافحة الجرائم ذات الصلة، مثل جرائم المعلوماتية وغيرها من الجرائم التي تمخض عنها عصر التقنية الرقمية، ولذلك لم تخف دول العالم قلقها من احتمالات استخدام التنظيمات الإرهابية لشبكة الانترنت واستغلال إمكاناتها في تفعيل أنشطة تلك الجماعات.

تكمن أهمية هذه الدراسة في التجربة العربية وعلى رأسها تجربة المملكة العربية السعودية كتجربة في مجال مواجهة عمليات تمويل الجماعات المتطرفة إلكترونيا عبر شبكة الانترنت من الإجراءات الوقائية أمنا وقانونا.

دوافع اختيار الموضوع:

يمكن أن ندرج في هذا الصدد نوعين جوهريين من الدوافع منها الدوافع الشخصية والنوع الثاني الدوافع الموضوعية:

1- **الدوافع الشخصية:** وتتمثل في الاهتمام الشخصي لهذا الموضوع وبما أنه أي الإرهاب الإلكتروني يتصف بجميع الظواهر الإجرامية:

أولا: ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق:

إن الشبكات مصممة في الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها رغبة في التوسع وتسهيل دخول المستخدمين وتحتوي الأنظمة الالكترونية والشبكات المعلوماتية على ثغرات معلوماتية ويمكن للمنظمات الإرهابية استغلال هذه الثغرات في التسلل إلى البني المعلوماتية التحتية' وممارسة العمليات التخريبية والإرهابية.

ثانيا: غياب الحدود الجغرافية وتدني مستوى المخاطرة :

إن غياب الحدود المكانية في الشبكة المعلوماتية بالإضافة إلى عدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة يعد فرصة مناسبة للإرهابيين حيث يستطيع محترف الحاسوب أن يقدم نفسه بالهوية والصفة التي يرغب بها أو يتخفى تحت شخصية وهمية، ومن ثمة يشن هجومه الالكتروني وهو مسترخي في منزله من دون مباشرة، وبعيدا عن أعين الناظرين.

ثالثا: صعوبة اكتشاف واثبات الجريمة الإرهابية

في كثير من أنواع الجرائم المعلوماتية لا يعلم بوقوع الجريمة أصلا وخاصة في مجال جرائم الاختراق، وهذا ما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته، كما أن صعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الالكتروني لأنها تعطي المجرم أملا في الإفلات من العقوبة.

خامسا: الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية

إن الفراغ التنظيمي والقانوني لدى بعض المجتمعات العالمية حول الجرائم المعلوماتية والإرهاب الالكتروني يعتبر من الأسباب الرئيسية في انتشار الإرهاب الالكتروني وكذلك لو وجدت قوانين تجريمية متكاملة فان المجرم يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة ثم يقوم بشن هجومه الإرهابي على بلد أخر فيه قوانين

صارمة، وهنا نثار مشكلة تنازع القوانين والقانون الواجب التطبيق كما أن عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على الشبكة.

2- **الدوافع الموضوعية:** وتتمثل في الإقبال المتزايد على استخدام الحواسيب الآلية وشبكة الانترنت وما ينتج عنها من مساوئ وسلبيات أي تؤثر سلبا على المستوى دول العالم داخليا وخارجيا منها العديد من الدوافع المتنوعة

أولا: الدوافع الفكرية: تتنوع الدوافع الفكرية المؤدية لظاهرة الإرهاب ويمكن بيان أهمها فيما يلي:

1- الفراغ الفكري، والجهل بقواعد الدين الحنيف، وآدابه وسلوكه.

2- الفهم الخاطئ للدين ومبادئه وأحكامه، وسوء تفسيره واعتماد الشباب بعضهم على بعض دون الرجوع إلى العلماء، يقول ابن مسعود " لا يزال الناس بخير ما اخذ العلم عن أكابرهم وعن أمنائهم وعلمائهم فإذا أخذوه عن صغارهم وشرارهم هليكوا"

ثانيا: الدوافع السياسية: إن من ابرز الأسباب والدوافع السياسية لظاهرة الإرهاب الإلكتروني ما يأتي:

1- السياسات الغير العادلة التي تنتهجها بعض الدول ضد مواطنيها، وانتهاك حقوقه وتلبية متطلبات التوازن الاجتماعي، وانعدام تفعيل دور مؤسسات المجتمع المدني.

2- الإحباط السياسي، فان كثير من البلدان العربية والسياسية لم تكتفي بتهميش الجماعات الإسلامية، بل وقفت في وجهها، وتصدت لأربابها وحصر نشاطها، وجمدت أعضاءها، حتى في بعض البلدان التي تدعي الديمقراطية وحرية الرأي وهذا من شانه أن يوحد المنظمات السرية، وردود الأفعال الغاضبة التي لا تجد ما تصيب فيه غضبها سوا الإرهاب.

3- ما تعانيه بعض المجتمعات الدولية من ظلم واضطهاد واحتلال، وسيطرة استعمارية وانتهاك صارخ للحقوق والحرمان، وسلب للأموال والمقدرات وخرق للقوانين والمواثيق الدولية، مما دفع تلك الشعوب للتطرف.

ثالثا: الأسباب الاقتصادية والاجتماعية:

- إن الجماعات الإرهابية تتركز في محافظات تعاني من أوضاع اجتماعية واقتصادية متدهورة نسبيا قياسا إلى المحافظات، وفي قرى تعاني من نقص الخدمات بمعناها العام وفي أحياء، ومناطق عشوائية تعاني من كافة أنواع المشكلات الاقتصادية والاجتماعية

المتطورة إن الأوضاع الاقتصادية الصعبة تخلق بيئة مولدة للإرهاب، فالبطالة والتضخم وتدني مستويات المعيشة وعدم التناسب بين الأجور والأسعار وتفاقم مشكلات الإسكان والصحة والمواصلات تدفع قطاعا واسعا من الشباب إلى الاتجاه من التدين الذي يعد سمة أساسية للشعب المصري إلى التطرف حيث توجد نوعا من التنفيس عن طاقته المكبوتة.

غير إن الأوضاع الاقتصادية لا تؤدي وحدها إلى الاتجاه نحو الأعمال الإرهابية فاقتران تلك الأوضاع بظروف اجتماعية أخرى هو الذي يدفع إلى ذلك الاتجاه.

إن من أهم الدوافع الاقتصادية المؤدية إلى تفشي ظاهرة الإرهاب ما يلي:

تفاقم المشكلات والأزمات الاقتصادية في المجتمعات الدولية، بالإضافة إلى المتغيرات الاقتصادية العالمية، والاستقلال غير المشروع للموارد الاقتصادية لبلد معين.

عدم القدرة على إقامة تعاون دولي جدي من قبل الأمم المتحدة، وحسم المشكلات الاقتصادية الدولية وعدم قدرة المنظمة على إيجاد تنظيم عادل ودائم لعدد من المشكلات العالمية.

انتشار البطالة في المجتمع وزيادة العاطلين عن العمل وعدم توفر فرص للعمل، من أقوى العوامل المساهمة في امتهان الجريمة والاعتداء والسرقة وتفشي ظاهرة الإرهاب، فالناس يحركهم الجوع والفقر وعدم العمل ويسكتهم المال والعمل.

التقدم العلمي والتقني للأنظمة المصرفية العالمية أدى إلى سهولة انتقال الأموال وتحويلها بين جميع أرجاء العالم عن طريق الشبكة العالمية للمعلومات (الانترنت) مما ساعد المنظمات الإرهابية على استغلال الفرصة من اجل تحقيق أغراضهم غير المشروعة.

وتتعدد الأسباب الاجتماعية الداعية إلى ظهور الإرهاب ويمكن تصنيف أهمها:

التفكك الأسري والاجتماعي، مما يؤدي إلى أمراض الجنسية والانحراف والإجرام.

غياب التربية الحسنة الموجهة التي توجه الأشخاص لمكارم الأخلاق.

الإشكالية: بناءا على الخطة المنجزة يمكن طرح الإشكالية التالية:

ما مدى مواكبة التشريع الجزائري لمكافحة جريمة الإرهاب الإلكتروني مقارنة بالتشريعات الأخرى؟

المنهج المتبع:

بالنسبة للمناهج التي استعملتها في موضوع دراستي كانت متنوعة حسب طبيعة المادة العلمية فكان المنهج المقارن وذلك لمقارنة جريمة الإرهاب الإلكتروني بين مختلف

التشريعات سواء على المستوى الوطني الداخلي أو على المستوى الدولي أما المنهج الوصفي فكان ضروريا لوصف هذه الظاهرة ومختلف الجرائم التي تحدث عبر شبكة الانترنت أما المنهج التحليلي كان ضروريا لدراسة وتحليل المواد القانونية وتحليل الأحكام القضائية والأجهزة الدولية المختصة في مجال مكافحة جريمة الإرهاب الإلكتروني.

أهداف الدراسة:

1.تهدف هذه الدراسة إلى التعرف على طبيعة الإرهاب الإلكتروني وتحديد الخصائص وأساليب تلك الجرائم وطبيعتها القانونية.

2.تحديد طرق وأساليب تمويل الجماعات المتطرفة إلكترونيا عبر شبكة الانترنت.

3.عرض الجهود الدولية لمكافحة الإرهاب الإلكتروني وقمعه.

الدراسات السابقة:

لقد تناولت دراسات سابقة موضوع الإرهاب الإلكتروني في التشريع الجزائري والتشريع المقارن إلا أن المراجع والمؤلفات التي ألقت الضوء على عنوان بحثي ليست بالقدر الكافي ومن أهم الدراسات التي اعتمدت عليها " مصطفى محمد موسى بعنوان: الإرهاب الإلكتروني، وعلي مطر وعبد الله بن عبد العزيز بن فهد العجلان، وأطروحات ودكتوراه ورسائل ماجستير.

صعوبات البحث:

واجهتني في موضوع هذا البحث العديد من الصعوبات يمكن حصرها بالنقاط التالية:

- قلة وجود النصوص القانونية المتخصصة في جرائم الإرهاب الإلكتروني بالأخص في التشريع الجزائري ويتمثل في الفراغ والقصور التشريعي.
- نظرا لحداثة هذا الموضوع.

خطة الدراسة:

للإجابة على الإشكالية المطروحة قسمت موضوع دراستي إلى فصلين في الفصل الأول تناولت الإطار المفاهيمي لجريمة الإرهاب الإلكتروني للدراسة حيث قسمته إلى مبحثين حيث كان المبحث الأول ماهية الإرهاب الإلكتروني من حيث مفهومه وخصائصه ووسيلة ارتكاب جريمة الإرهاب الإلكتروني عبر الانترنت فيما تناولت في المبحث الثاني الأركان العامة لجريمة الإرهاب الإلكتروني حيث تناولت في المطلب الأول الركن الشرعي أما المطلب الثاني الركن المادي وتناولت في المطلب الثالث الركن المعنوي أما

الفصل الثاني فكان عنوانه الجهود الدولية لحماية ومكافحة جريمة الإرهاب الإلكتروني حيث تطرقت في المبحث الأول التعاون الدولي في مواجهة جرائم الإرهاب الإلكتروني وتطرقت إلى ثلاث مطالب المطلب الأول التشريعات على الصعيد الدولي، المطلب الثاني التعاون القضائي، المطلب الثالث الأجهزة المختصة في متابعة الجريمة الإلكترونية في التشريع الجزائري، أما المبحث الثاني فقد تطرقت فيه إلى دور المنظمات العالمية في مكافحة الإرهاب الإلكتروني وتطرقت فيه إلى ثلاث مطالب المطلب الأول دور المنظمات المتخصصة في مكافحة الإرهاب الإلكتروني، المطلب الثاني دور المنظمات الإقليمية في مجال مكافحة الإرهاب الإلكتروني، والمطلب الثالث دور الأمم المتحدة في مكافحة الإرهاب الإلكتروني.

الفصل الأول:

الإطار المفاهيمي لجريمة الإرهاب الإلكتروني

تمهيد وتقسيم:

أدى التطور التكنولوجي الكبير وبالتحديد في ظل ثورة المعلومات والمعرفة الرقمية وتطور وسائل الاتصال التقني والإلكتروني الحديث إلى استفادة الجماعات الإرهابية من مكتسبات هذه الثورة والمعرفة التقنية ووظيفتها لتحقيق أهدافها. ويمكن ارتكاب الجريمة الالكترونية من أقصى بقاع الأرض بنفس سهولة ارتكابها من أقرب مكان وقوعها كما أن رسالة واحدة تعزز ارتكاب جريمة إلكترونية يمكن تمريرها من خلال الكثير من مقدمي الخدمات في بلدان مختلفة ولها نظم مختلفة وعلى هذا الأساس سنطرق في المبحث الأول ماهية الإرهاب الإلكتروني حيث تناولت فيه مفهوم الإرهاب الإلكتروني وخصائصه ثم وسيلة ارتكاب جريمة الإرهاب الإلكتروني عبر الانترنت أما فيما يتعلق بالمبحث الثاني تناولت فيه الأركان العامة لجريمة الإرهاب الإلكتروني حيث تطرقت فيه إلى الركن الشرعي ثم إلى الركن المادي وإلى الركن المعنوي.

المبحث الأول: ماهية الإرهاب الالكتروني

إن أهم القضايا الحديثة على المستوى الدولي هو عدم وجود تعريف مانع وجامع متفق عليه من طرف المجتمع الدولي للإرهاب نظرا لتنوع أشكاله ومظاهره وتعدد أساليبه واختلاف وجهات النظر الدولية وبالتالي سيقوم الباحث ببيان تعريف الإرهاب كما ورد في بعض الاتفاقيات من خلال هذه التعريفات نستخلص تعريف للإرهاب الالكتروني[1] وانطلاقا من هنا قسمنا المبحث الأول إلى ثلاث مطالب:

المطلب الأول: مفهوم الإرهاب الإلكتروني، المطلب الثاني: خصائص جريمة الإرهاب الالكتروني، والمطلب الثالث: وسيلة ارتكاب جريمة الإرهاب الالكتروني عبر الانترنت

المطلب الأول: مفهوم الإرهاب الالكتروني

ينطلق مفهوم الإرهاب الالكتروني من مفهوم الإرهاب، وفي ضوء التعريفات السابقة يمكن تعريف الإرهاب الالكتروني بأنه: العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الالكترونية بشتى صنوف العدوان وصور الإفساد، فالإرهاب الالكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية من اجل تخويف أو ترويع الآخرين وإلحاق الضرر بهم أو تهديدهم.

[1]–أمير فرج يوسف.الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، الطبعة الأولى، الناشر مكتبة الوفاء القانونية،الإسكندرية –مصر،2011، ص–ص219–220.

الفرع الأول: تعريف الإرهاب

تجمع قواميس اللغة العربية على أن كلمة الإرهاب تعني الفزع والخوف والرعب وكلمة إرهاب مشتقة من الفعل المزيد، ويقال ارهب فلان أي خوفه وفزعه وهو نفس المعنى الذي يدل عليه الفعل المصفف –رهب– أما الفعل المجرد من نفس المادة وهو رهب يرهب رهبة ورهبا فيعني (خاف) مع تحرر واضطراب فيقال رهب الشيء رهبا رهبة أي خافه، وكذلك يستعمل الفعل ترهب بمعنى ترعد إذا كان متعديا فيقال ترهب فلانا: أي ترعبه وأرعبه وسترهبه أي أخافه وأفزعه وتنفصل الرهبة عن الخوف لدى بعض اللغويين لتعني طول الخوف واستحكامه بالنفس ومنها انطلقت تسمية الراهب الذي يديم الخوف.[1]

وفي المعاجم المترجمة إلى اللغتين الانجليزية والفرنسية ورد لفظ الإرهاب بدلالة المصطلحات terrorisme المشتقة من الفعل terror بما يفيد معنى الذعر والتخويف أو إشاعة الهلع ويتضح مما تقدم أن معاجم اللغة العربية، قد جعلت من الخوف والترويع مقصد أو معنى لعبارة الإرهاب وهو الأساس الذي انطلق منه واقره من تصدي لتعريف الإرهاب اصطلاحا على الرغم من اختلافهم في التفاصيل، الأمر الذي أفضى إلى عدم وجود مفهوم دولي موحد للإرهاب بصفة عامة والإرهاب بصفة خاصة وفي هذا السياق، كانت اتفاقية جنيف لقمع ومعاقبة الإرهاب لعام 1938م. سباقة في تعريف الإعمال الإرهابية على إنها"الأعمال الإجرامية الموجهة ضد دولة ما وتستهدف أو يقصد بها خلق حالة من الرعب في أذهان أشخاص معينين أو مجموعة من الأشخاص أو عامة الجمهور".[2]

عرف القانون التركي في مادته الأولى من قانون مكافحة الإرهاب: "كل فعل مرتكب من خلال نشر الخوف والرعب أو من خلال الفزع والإرغام أو التهديد من شخص أو أعضاء في منظمة، بغرض تغيير دستور الجمهورية أو النظام السياسي أو القانوني والاجتماعي أو الاقتصادي أو العلماني أو بهدف المساس بوحدة إقليم الدولة

[1]–د.محسن الحيدري، الإرهاب والعنف في ضوء القران والسنة والتاريخ والفقه المقارن.دون طبعة، دار الولاء، بيروت، 2010م، ص20.

[2]–حارث سليمان الفاروقي، المعجم القانوني، ط5.بيروت، مكتبة لبنان، 2003، ص290.

والأمة أو الإضعاف أو القضاء أو الاستيلاء على سلطة الدولة،....الحقوق والحريات الأساسية أو الإخلال بالأمن الداخلي والخارجي للدولة، أو الإخلال بالنظام العام والصحة العامة".[1]

وفي السياق كانت اتفاقية جنيف لقمع ومعاقبة الإرهاب 1937م سباقة في تعريف الأعمال الإرهابية "على أنها الأعمال الإجرامية الموجهة ضد دولة ما وتستهدف أو يقصد بها خلق حالة من الرعب في أذهان أشخاص معينين أو مجموعة من الأشخاص أو عامة الجمهور".[2]

وعرف مجلس الأمن الدولي الإرهاب بأنه " كل عمل جرمي ضد المدنيين بقصد التسبب بالوفاة أو بالجروح البليغة أو خذ الرهائن من اجل إثارة الرعب بين الناس أو إكراه حكومة أو منظمة دولية للقيام بعمل ما أو امتناع عنه، أو كل الأعمال الأخرى التي تشكل إساءات ضمن نطاق المعاهدات الدولية المتعلقة بالإرهاب والتي لا يمكن تبريرها بأي اعتبار سياسي أو فلسفي أو إيديولوجي أو عرفي أوديني فكان هذا التعريف مفرقا في التركيز على الوسائل المستخدمة في الفعل الإرهابي على سبيل الحصر والتحديد الذي لا يمكن الإرتكان إليه مستقبلا إذا ما برزت وسائل ومظاهر إرهابية مستحدثة ومن ذلك على سبيل المثل الإرهاب الإلكتروني والجرثومي الذي شهدنه الساحة الدولية في الوقت الراهن لتثبت عجز هذا التعريف عن الإحاطة بكل أنواع الإرهاب.[3]

وقريبا من التعاريف أعلاه جاءت الاتفاقية العربية لعام 1998م للإرهاب بأنه"كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه أو أعراضه يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إفشاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها أو تعريض احد الموارد للخطر فكان

---

[1]– مصطفى محمد موسى، الإرهاب الالكتروني: دراسة قانونية أمنية–نفسية–اجتماعية.الطبعة الأولى، مصر: دار الكتب، الوثائق القومية المصرية،2009، ص94.

[2]– المادة الأولى من اتفاقية جنيف لقمع الإرهاب لعام1937م.

[3]– قرار مجلس الأمن الدولي بالعدد 1566 لعام2004.

إطارا جامعا دون تفصيلات دقيقة لأهم آليات الإرهاب دون الإشارة الواضحة إلى غايته أو دوافعه أو حتى تبيان الصور الأخرى منه.[1]

وإذا كان تعريف الإرهاب بصورته العامة مجالا لاختلاف الرأي وتبيان الاجتهادات فان الوجه الجديد للإرهاب بصورته الرقمية قد استوعب مساحة اكبر من الجدل والاختلاف في التوصيف والتعريف بين الباحثين والمهتمين، فكان تعريف الأمم المتحدة في تشرين الأول/ أكتوبر 2016 للإرهاب الرقمي الأكثر هلامية وإجمالا في الدلالة والنطاق دون الاستغراق في التفصيل والآليات والمقاصد الإرهابية، وذلك حيث عرف الإرهاب الإلكتروني على انه استخدام الانترنت لنشر الأعمال الإرهابية.[2]

وفي الموسوعة الالكترونية جرى تعريف الإرهاب الإلكتروني بأنه" استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرفية أو دينية.[3]

وكان تعريف اللجنة الدولية للصليب الأحمر أكثر استرسالا في تقصي التفاصيل الفنية عند تعريفها للإرهاب الرقمي على انه" عمليات تشن ضد أو عبر حاسوب بواسطة تيار بيانات وتهدف إلى تحقيق أغراض منها اختراق النظام المعلوماتي أو جمع أو نقل أو تشفير أو تغيير البيانات أو التلاعب بها من قبل منفذ عمليات الاختراق واستخدام هذه الوسائل لتدمير أو تعطيل مجموعة متنوعة من الأهداف في العالم الحقيقي كالصناعات والبني الأساسية.[4] بيد إن الإرهاب الإلكتروني وفق رأي أخر هو "نشاط هجومي متعمد ذو دوافع سياسية بغرض التأثير على القرارات الحكومية أو الرأي العام باستخدام الحاسبات ووسائل الاتصال وعلى إنتاج ومعالجة وتخزين المعلومات أو تعطيل خدمات لينتج عنه ترويع وتخويف وتدمير للبنية التحتية الحيوية فكان هذا التعريف دقيقا جامعا

---

[1]– المادة الأولى من الاتفاقية العربية لمكافحة الإرهاب لعام 1998م.

[2]– علي مطر، الإرهاب الالكتروني في القانون الدولي، مقال منشور على موقع الشبكة الالكترونية بتاريخ 4 نوفمبر 2013 على الرابط:hhp://www.assakim.com/about.php

[3]– بن يحي، الطاهر ناعوس، مكافحة الإرهاب الالكتروني ضرورة بشرية وفريضة شرعية، ص6.

[4]– تقرير اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة الحادي والثلاثين، 2011، ص67.

لأغلب وسائل الإرهاب ومقاصده، على الرغم من اعقاله لإمكانية استخدام الشبكة الدولية للمعلومات كوسيلة للاتصال والتنسيق بين الإرهابيين أو حتى منطلقا لتنفيذ العمليات الإرهابية على ارض الواقع.[1]

الفرع الثاني: تعريف الإرهاب الإلكتروني.

يعد تعريف الإرهاب الإلكتروني بأنه: العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الفساد. فالإرهاب يعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الآخرين وإلحاق الضرر بهم أو تهديدهم.[2]

بالانتقال إلى ساحة الإرهاب الإلكتروني، ابرز أولا إشكالية تحديد مفهوم[3] العنف الممارس في الفضاء الافتراضي، ومدى صلته بالعنف المعرف في الواقع. وهنا إذا اعتمدنا تعريف غالتونغ للعنف ويمكننا تلخيصه بشكل عام على أنه الإهانات التي يمكن تجنبها الموجهة للاحتياجات الإنسانية الأساسية، وبشكل أهم للحياة والتي تخفض مستوى تلبية الاحتياجات الحقيقية إلى ما هو دون المستوى المحتمل والمتوقع، وبكلام أوضح، فكل فعل يمارس ضدنا، ويكون بالإمكان تجنبه، وتكون نتيجة حرماننا من تلبية الاحتياجات التي نتوقعها يدخل في خانة العنف.

---

[1]– عادل عبد الصادق، هل يمثل الإرهاب شكل جديدا من أشكال الصراع الدولي، ملف الأهرام الاستراتيجي، مركز الأهرام للدراسات السياسية الإستراتيجية أكتوبر 2010.

[2]- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية، والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص 219 ص 220.

[3]– رائد العدوان، توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، المعالجة الدولية لقضايا الإرهاب الإلكتروني، دون طبعة، الرياض، 2013، ص 7.

الإرهاب التخيلي

يعد الإرهاب التخيلي نوع فريد من الإرهاب، ويستخدم المكونات التخيلية، وهناك عددا من المصطلحات التي تستخدم وتتداخل في معانيها منها، الحرب الفضائية (cyber war) وحرب الشبكات (war net)، وحرب المعلومات (IWF)[1] والإرهاب القضائي (cyber terrorism).

ويعد تعريف دورثي دايينج من أكثر التعاريف الشائعة خاصة وإنها من أوائل الذي يستخدموا هذا المصطلح، وتعرف الإرهاب التخيلي على أنه "التقاء للإرهاب مع الفضاء التخيلي، وهو يعني التهديدات غير القانونية ضد الحاسبات والشبكات والمعلومات المخزنة، وذلك لإخافة أو إجبار الحكومات أو الناس لتعزيز أهداف سياسة أو اجتماعية، وهو العنف ضد الأفراد أو الممتلكات أو أنه مؤذ لدرجة كافية لخلق الخوف والتعديات المفضية للموت أو الإصابة أو الإنفجارات أو الخسارة الاقتصادية ما هي إلا أمثلة للتعديات على الإرهاب التخيلي ويمكن تصنيف الجمهور المستهدف في ثلاثة فئات هي: الأفراد والممتلكات والحكومات (denning 2000 :1).

ويعرفه **كولنز** (collins) بأنه "سوء الاستخدام المتعمد لنظام المعلومات الإلكتروني والشبكات، أو المكونات تجاه هدف يدم أو يسهل حملة إرهابية أو فعل إرهابي" (3: 199 white).

أما ستارك: فعرف الإرهاب التخيلي بأنه "الاستخدام العمد أو التهديد بالاستخدام للحرب التخيلية أو العنف التخيلي بأهداف سياسية، أو اجتماعية أو اقتصادية أو دينية من قبل جماعات مدعومة من الدولة أو جماعات غير حكومية، وذلك لإثارة الخوف والقلق والمعاناة لدى مجتمع مستهدف وذلك لعرقلة الأصول (الموجودات) العسكرية والمدنية (Stark 1999 :8-9).[2]

[1]- ذياب موسى البدانية، الانترنت والإرهاب، الإرهاب المعلوماتي، دون طبعة، القاهرة، 2008، ص 12.

[2]- ذياب موسى البدانية، المرجع السابق، ص 12.

ويعرفه بولييت "هجوم معد مسبق بدوافع سياسية ضد المعلومات ونظم الحاسب والبيانات والذي ينجم عنه عنف ضد أهداف غير قتالية من قبل مجموعات فرعية وعملاء سريون (clandestine) (Pollitt 2001).

ويعرفه فليممتج وستوهاي (Flemming stohi) بأنه "الإرهاب التخيلي أي فعل إرهاب يستخدم نظم المعلومات أو التقنية الإلكترونية (الحاسبات أو الشبكات) كوسيلة أو هدف" (Flemming stohi 2001 :31).

ومن أمثلة الإرهاب التخيلي:

- الدخول عن بعد لنظم التحكم في مصانع غذاء الأطفال لتغيير مستويات الحديد بهدف إمراض وقتل الأطفال.
- تعطيل البنوك وعمليات التحويل المالي مما يلحق الأذى بالاستثمار الأجنبي وبالثقة بالاستثمار عامة وإلحاق الأذى بالاقتصاد الوطني.
- مهاجمة نظم التحكم الوطني في الطيران لإحداث تصادم بين الطائرات.
- إدخال تعديلات عن معادلات صناعة الدواء لقتل الناس الذين يتناولون الدواء.
- تعديل ضغط الغاز عن بعد في أنابيب الغاز لتفجيرها.
- تعديل نظم السلامة في المصانع الكيماوية لإحداث أضرار بالناس.

Cyberterrorisme : Begrepet Cyberterrorisme ble frst bru kit det akademeske - miljo. Denning (1999 :69) skriver at det var barry collin som pci 1980. Tallet samkjorte begrepess mellon cyberspace og terrorisme. O'brien nusbaum (2000 :54) nevner ogsa at begrepet cyberterrorisme ertilskrevet barry collin.[1]

[1] - tonje grunnon, cyberterrorisme hovedoppgrave istatsvitenskap, universitete ioslo intitut for statsvi tenskap, varen, 2007, page 40.

الفرع الثالث: تعريف الإرهاب الإلكتروني في القانون الدولي.

يعتبر الإرهاب الإلكتروني عند علي مطر تهديدا قويا ومع أنه ليس بجديد، إلا أن استخدامه في المعارك من وراء البحر أصبح جديدا وهذا الإرهاب يتبلور بعد لكن يجب أن يؤخذ على محمل الجد وأن يتم الاستعداد لمواجهة، ويمكن أن يعرف الإرهاب بأنه استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، وأنه القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية.

وفي منتصف العقد الماضي، أنتبه الغرب إلى قضية الإرهاب الإلكتروني ومخاطره حيث قام الرئيس الأمريكي بيل كلينتون في العام 1996 بتشكيل لجنة حماية منشآت البنية التحتية الحساسة، وكان أو استنتاج لهذه الهيئة هو أن مصادر الطاقة الكهربائية والاتصالات، إضافة إلى شبكات الكمبيوتر ضرورية بشكل قاطع لنجاة الولايات المتحدة وبما أن هذه المنشآت تعتمد بشكل كبير على المعلومات الرقمية، فإنها ستكون الهدف لأية هجمات إرهابية تستهدف أمن الولايات المتحدة.

وفي أعقاب ذلك قامت كافة الولايات الحكومية في الولايات المتحدة بإنشاء هيئاتها ومراكزها الخاصة للتعامل مع احتمالات الإرهاب الإلكتروني فقامت وكالة الاستخبارات المركزية بإنشاء مركز المعلوماتية، ووظفت ألف من خبراء أمن المعلومات، وقوة ضاربة على مدى 24 ساعة لمواجهة الإرهاب الإلكتروني، وقامت القوات الجوية الأمريكية باتخاذ خطوات مماثلة ومثلها المباحث الفدرالية، كما تقوم قوات الأمن في أوروبا باتخاذ إجراءات مماثلة.[1]

ويقول التعريف الأمريكي المستخدم في الكليات الحربية لوزارة الحرب الأمريكي "إن الحرب الرقمية هي الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات. وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها" وتتضمن

[1] – http://ar.wikipedia.org/wiki.

العمليات الإلكترونية أنشطة مثل أمن العمليات والعمليات النفسية والخداع العسكري، الهجمات الفيزيائية والهجمات على شبكات الكمبيوتر.

ويعتبر الأوروبيون أن استخدام الإرهابيين للانترنت للاتصال في ما بينهم أو تبني أعمالهم أو لغايات الدعاية أو التمويل، إرهاب إلكتروني.

وقد عرفت الأمم المتحدة في تشرين الأول/ أكتوبر 2012 الإرهاب الإلكتروني بأنه: "استخدام الانترنت لنشر أعمال إرهابية"[1] ولقد رأينا لبقية إتمام استخدام الفيروسات ضد المنشئات النووية الإيرانية من قبل الاستخبارات الأمريكية وجهاز الموساد الصهيوني.

ويمكن أن يتم استخدام الإرهاب الإلكتروني في الحروب العسكرية من أجل السيطرة على معلومات، حيث يعتبر الجيش الأمريكي أن أكثر ما تتعرض له الولايات المتحدة من هجمات هو من قبل الصين وروسيا.

ويمكن شرح مفهوم "الإرهاب الإلكتروني" بأنه العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدولة أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه أو عرضه، أو عقله، أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الفساد.

وبذلك فقد أصبحت الجرائم تشكل خطرا كبيرا على استقرار الدول. وذلك بعد أن استطاع "الانترنت" اختراق جميع الحواجز والقيود لكي تسيطر على المجتمعات.

ولقد بات الإرهاب الإلكتروني "cyber terrorisme" يمثل تهديدا واضحا للأمن القومي للدول، حيث البنية التحتية لأغلب المجتمعات الحديثة تدار عن طريق أجهزة الحاسب الآلي والانترنت، ما يعرضها لهجمات متعددة من "الهاكر" و"المخترقين" بشكل عام ومع ذلك فليس هماك حتى الآن مفهوم دولي للإرهاب بصفة عامة والإرهاب بصفة خاصة،

[1] - http://www.sawtbeirut.com/breaking.

وليس هناك جهود واضحة حتى الآن لوضع تشريعات داخلية صارمة لمكافحة الجرائم التي تتعلق بالإرهاب الإلكتروني.

وعرف مجلس الأمن الدولي الإرهاب بأنه: "كل عمل جرمي ضد المدنيين بقصد التسبب بالوفاة أو بالجروح البليغة أو أخذ الرهائن من أجل إثارة الرعب بين الناس أو إكراه حكومة أو منضمة دولية للقيام بعمل ما أو الامتناع عنه، وكل الأعمال الأخرى تشكل إساءات ضمن نطاق المعاهدات الدولية المتعلقة بالإرهاب ووفقا لتعريفها، ولا يمكن تبريرها بأي اعتبار سياسي أو فلسفي أو أيديولوجي أو عرقي أو ديني.

ولكن الأمم المتحدة لم تعالج حتى الآن أية حالة يمكن الاستناد إليها في تعريف الإرهاب الإلكتروني وإمكانية التعامل معه من الناحية القانونية والجرمية، فالقانون الدولي لم يعط تعريف واضحا ومنهجيا معينا للتعامل مع هذا النوع الجديد من الإرهاب، علما أنه لحظ الإرهاب النووي وأصدر عدة قرارات يمكن الرجوع إليها، في حين أن الإرهاب الإلكتروني يمكن اعتباره أداة إرهابية مؤذية جدا ويمكن أن ينطبق التعريف الأول للإرهاب في بعض الأحيان على العناصر الجديدة والأشكال المتنوعة له.[1]

المطلب الثاني: خصائص جريمة الإرهاب الالكتروني

إن للجريمة الالكترونية خصائص كثيرة سنحاول حصرها وإبرازها ولقد أدى ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت إلى إضفاء مجموعة من الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية ويمكن إجمالها فيما يلي سنتناول الفرع الأول: الجريمة المعلوماتية متعددة الحدود (جريمة عابرة للحدود) أما الفرع الثاني سنتناول فيه: صعوبة اكتشاف الجريمة المعلوماتية، أما الفرع الثالث فيتمثل في صعوبة إثبات الجريمة المعلوماتية وأسلوب ارتكابها.[2]

[1] - http://www.sawtbeirut.com/breaking.

[2]– قورة نائلة، جرائم الحاسب الاقتصادية، دون طبعة، القاهرة: دار النهضة العربية،2004 ، ص47.

الفرع الأول: الجريمة المعلوماتية متعدية الحدود (عابرة للحدود)

المجتمع ألمعلوماتي لا يعترف بالحدود الجغرافية ولا يعيرها أي اهتمام فهو مجتمع متفتح عبر شبكات تخترق المكان والزمان دون أن تخضع لحرص الحدود فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل كميات كبيرة من المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها من نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال أدت إلى نتيجة تتمثل في أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد فالسهولة في حركة المعلومات عبر أنظمة وبرامج التقنية الحديثة جعل بالأماكن ارتكاب جريمة عن طريق الحاسوب موجودة في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى، هذه الخاصية التي تتميز به الجريمة المعلوماتية كونها جريمة عابرة للحدود خلفت العديد من المشاكل حول تحديد الدولة صاحب الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب التطبيق بالإضافة إلى إشكاليات تتعلق بإجراء الملاحقة[1] القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام، وتعتبر القضية المعروفة باسم مرض نقص المناعة المكتسبة من القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية، وتتخلص وقائع القضية التي وقعت عام 1989م في قيام احد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا إن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)، إذا كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على شاشة الحاسوب يقوم من خلالها بطلب مبلغ مالي يرسل على عنوان معين يتمكن المجني عليه من الحصول على مضاد الفيروس. وفي الثالث من فبراير من سنة 1990م تم إلقاء القبض على المتهم (جوزيف بوب) في ولاية (أوهايو) بالولايات المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب لتسليمه لها لمحاكمته أمام القضاء الانجليزي، حيث إن إرسال هذه البرامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي على تسليم المتهم،وتم توجيه إحدى عشر

[1]– ترجمة سامي الشورى، ubich sieber جرائم الكومبيوتر والجرائم الأخرى في مجال المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة: دار النهضة العربية،1993 ، ص58.

تهمة ابتزازا إليه وقعت معظمها في دول مختلفة إلا إن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية.[1] وإنها جزعة داخلية عندما تقع كاملة في نطاق إقليم دولة معينة، وجزعة دولية عندما تتعلق بالقانون الدولي أي عندما يكون أحد أطرافها شخص دوليا. على نحو ما حدث في التجسس الذي قامت به الولايات المتحدة الأمريكية عندما انتهكت أنظمة أعدائها الحاسوبية وذلك بواسطة أسلحة معلوماتية فتاكة أثناء القصف الجوي للحلف الأطلسي في كوسوفو. وقد تكون جريمة ذات بعد دولي، إذا اتفق المجتمع الدولي بمقتضى اتفاقية دولية بان جريمة دولية تشكل عدوانا على كل دولة، اوعندما ترتكب الجريمة داخل دولة معينة إلا أنها تمتد خارج إقليم تلك الدولة مثل جريمة ترويج المخدرات عبر الانترنت.[2]

الأولى: إنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية.

الثانية: إنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهم إعداد برنامج خبيث (فيروس).

ونتيجة لهذه الطبيعة الخاصة للجريمة المعلوماتية، ونظرا للخطورة التي تشكلها على المستوى الدولي، والخسائر التي تسبب بها ظهرت الأصوات الداعية إلى التعاون الدولي المكثف من اجل التصدي لهذه الجرائم والتعاون الدولي يتمثل في المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسيق يبين الدول الأعضاء، الأمر الذي يؤدي بالإيقاع بمجرمي المعلوماتية وتقديمهم للقضاء العادل.[3]

تكمن أهم المشاكل المتعلقة بالتعاون الدولي حول الجريمة المعلوماتية، وهي انه لا يوجد هناك مفهوم عام، مشترك بين الدول حول صور النشاط المؤدي أو المكون لهذه الجريمة بالإضافة إلى نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال في

---

[1]–حمزة بن عقون، السلوك الإجرامي للهجوم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، باتنة: جامعة الحاج لاخضر، 2011–2012، ص19.

[2]– محمد طارق عبد الرءوف الخن، جريمة الاحتيال عبر الانترنت، الأحكام الموضوعية والأحكام الإجرائية، الطبعة الأولى. منشورات الحلبي الحقوقية، بيروت–لبنان،2011، ص33.

[3]– حمزة بن عقون، المرجع السابق، ص–ص20–21.

تفكيك وتحليل عناصر الجريمة إن وجدت وجمع أدلة وبالتالي من اجل التصدي للإجرام المعلوماتي، لابد أن تعمل الدول في اتجاهين:

الأول: داخلي حيث تقوم الدول المختلفة ين القوانين الملائمة لمكافحة هذه الجرائم.[1]

الثانية: دولي عن طريق عقد الاتفاقيات الدولية حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تهدف إلى حماية المجتمع الدولي من نتائج وأثار هذه الجرائم.

الفرع الثاني: صعوبة اكتشاف الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصعوبة اكتشافها، وإذا ما اكتشفت فان ذلك يكون بمحضر الصدفة عادة، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجريمة قليلة إذا قورنت بما يتم اكتشافه مع الجرائم التقليدية.

ويمكن رد الأسباب التي تقف وراء صعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة إلى اثر خارجي بصورة مرئية، فلا يوجد جثث لقتلى ولا اثر للدماء كما أن المجرم يمكنه ارتكاب هذه الجريمة في دول و قارات مختلفة إذ إن الجريمة المعلوماتية كما سبق إنها جريمة عابرة للحدود وكذلك فان قدرة الجاني على تدمير دليل الإدانة في عمل من الثانية الواحدة يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم.

فالجرائم المعلوماتية في أكثر صورها خفية لا يلاحظها المجني عليه ولا يدري حتى بوقوعها والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في الذبذبات الالكترونية التي تسجل البيانات عن طريقها أمر ليس بالعسير في الكثير من الأحيان بحكم المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبها.[2]

[1]– نهلا عبد القادر المومني، الجرائم المعلوماتية، دون طبعة،عمان،2008 ، ص55

[2]–حمزة بن عقون، المرجع السابق، ص22.

ويكون للمجني عليه دورا أساسيا كذلك في صعوبة اكتشاف وتحديد نوع الجريمة المعلوماتية، حيث تحرص اغلب الجهات التي تتعرض أنظمتها المعلوماتية للقرصنة والانتهاك على عدم الكشف حتى بين موظفها عما تعرضت له وتكفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للأضرار بسمعتها ومكانتها وهز الثقة بكفاءتها، وتشير بعض التقديرات إلى أن ما يتراوح بين 20و25% من جرائم الحسابات لا يقم الإبلاغ عنها مطلقا، خشية الإساءة إلى سمعة المؤسسة أو المصنع. ويرى البعض أن المجني عليه كذلك دورا مثيرا للريبة في بعض الأحيان، فهو قد يشارك بطريقة غير مباشرة في ارتكاب الفعل، وذلك بسب وجوده في ظروف تجعل تعرضه للجريمة المعلوماتية امرأ مرتفعا بشكل كبير، ويرجع ذلك بشكل أساسي إلى القصور الأمني الذي يعتري الأنظمة المعلوماتية.[1]

ويبدو وان إحجام المجني عليه عن الإبلاغ عن وقوع الجرائم المعلوماتية أكثر وضوحا في المؤسسات المالية مثل البنوك والمؤسسات الادخارية ومؤسسات الافتراض والسمسرة، حيث تغش مجالس إدارتها من إن تؤدي الدعابة السلبية التي قد تنجم عن كشف هذه الجرائم، أو اتخاذ الإجراءات القضائية حيالها، إلى تضاؤل الثقة فيها بين المتعاملين معها،حيث إن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه.[2]

وهذا ما يؤثر بدوره على السياسة التي يمكن وضعها لمكافحتها، وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في الكشف عن هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي، ومن بين الاقتراحات التي طرحت لحمل المجني عليه للتعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بان تفرض النصوص المتعلقة بجرائم الحاسبات التزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل علمهم به من جرائم في هذا المجال مع تقرير خبراء على الإخلال بمبدأ الالتزام، غير أن هذا الاقتراح لقي رفضا، لأنه ليس من القبول تحويل المجني عليه إلى مرتكب الجريمة

[1]–نهلا عبد القادر المومني، المرجع السابق، ص55.

[2]–حمزة بن عقون، المرجع السابق ، ص22.

مما يزيد الأمر تعقيدا إن هؤلاء القراصنة لا يهاجمون من أجهزة الحاسب الخاصة بهم، إنما يدخلون إلى شبكات بعيدة عنهم ويهاجمون من خلالها.[1]

الفرع الثالث: صعوبة إثبات الجريمة المعلوماتية وأسلوب ارتكابها

1- صعوبة إثبات الجريمة المعلوماتية:

يعتبر اكتشاف الجريمة المعلوماتية أمر ليس بالهين والسهل ولكن حتى في حال اكتشافها والإبلاغ عنها، فان إثباتها أمر تحيط به الكثير من الصعاب فالجريمة المعلوماتية تتم في محيط غير تقليدي حيث تقع خارج أطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الأمور تزداد صعوبة وتعقيدا لدى سلطات الأمن وأجهزة التحري والتحقيق والملاحقة ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نهضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر محو الدليل وطمسه إلي من قبل المجرم أمرا في غاية البساطة والسهولة.[2]

وتجدر بنا الإشارة إلى أن وسائل المعاينة وطرقها التقليدية لا تفلح في غالب الأحيان في إثبات هذه الجريمة نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث، حيث تخلف أثار مادية تقوم عليها الأدلة، وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في كشف الجريمة الالكترونية، وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة الالكترونية تضاؤل ويتلاشى دوره في إظهار الحقائق المؤدية للأدلة والبراهين المطلوبة، ويرجع ذلك لسببين اثنين هما:

الأول: الجريمة المعلوماتية لا تخلف آثار مادية.

الثاني: إن كثير من الأشخاص يتعاقبون على مسرح الجريمة خلال فترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقق فيها،وهي مدة طويلة نسبيا، الأمر الذي يعطي مجالا

[1]-نهلا عبد القادر المومني، المرجع السابق، ص57.

[2]-حمزة بن عقون، المرجع السابق، ص58.

واسعا للجاني أو للآخرين أن يغيروا أو يتلفوا أو يعبثوا بالآثار المادية إن وجدت، الأمر الذي يورث الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية.[1]

ومن الأمور التي زادت الأمور تعقيدا وصعوبة نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء، فهذا الأمر يشكل عائقا أساسيا أمام الجريمة المعلوماتية، ذلك أن هذا النوع من الجرائم يتطلب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحظة في بيئة الحاسوب والانترنت، ونتيجة لنقص الخبرة وعدم إمكانية الشرطة في تقدير أهمية الجريمة المعلوماتية، فلا تبذل لكشف غموضها وضبط مرتكبها جهودا تتناسب وهذه الأهمية، بل إن المحقق قد يدمر الدليل لمحوه محتويات الاسطوانة الصلبة عن خطا منه وإهمال أو بالتعامل بخشونة مع الأقراص المرنة.[2]

وفي الأخير يمكن إثبات صعوبة الجريمة المعلوماتية في نقاط خمس وهي:

- إنها جريمة لا تترك اثر.

- إنها جريمة يصعب على المحقق التقليدي أن يفهم حدوها الإجرامية، وما تخلفه من أثار غير مرئية.

- إنها جريمة تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها.

2-أسلوب ارتكاب الجريمة المعلوماتية:

من خصائص الجريمة المعلوماتية أنها تبرر ذاتيتها بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعا من الجهد العضلي الذي يكون في صورة ممارسة العنف والإيذاء، كما هو الحال في جريمة القتل والاختطاف، أو في صورة الكسر وتقليد المفاتيح، هو كما الحال في جريمة السرقة [3].

[1]-نهلا عبد القادر المومني ، المرجع السابق، ص58.

[2]-حمزة بن عقون، المرجع السابق، ص24.

[3]-نهلا عبد القادر المومني، المرجع السابق، ص88.

... فان الجرائم المعلوماتية جرائم هادئة بطبيعتها لا تحتاج إلى العنف، بل كل ما يحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروع كما تحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت) مع وجود مجرم يوظف خبرته وقدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين كل ذلك يحتاج إلى سفك الدماء.

الفرع الرابع: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص

تتميز الجريمة المعلوماتية بأنها تتم عادة بتعاون أكثر من شخص على ارتكابها فغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت يقوم بالجانب التقني من المشروع الإجرامي، وشخص آخر من المحيط أو خارج المؤسسة المجني عليه لتغطية عملية التلاعب وتحويل المكاسب إليه، والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود منه لتسهيل إتمامها، وقد يكون اشتراكا ايجابيا وهو الغالب في الكثير من الجرائم ويتمثل في المساعدة الفنية والمادية.[1]

ومن خصوصية الجريمة المعلوماتية أيضا إن خصوصية مجرمي المعلوماتية انه يتصف بخصائص معينة تميزه عن المجرم الذي يرتكب الجرائم التقليدية (المجرم التقليدي)، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي أو معرفي للمجرم في عملية ارتكابها، فان الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم، والأشخاص الذين يقومون بارتكابها عادة يكونون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد ادني من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت، ومثال على ذلك فان الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الالكتروني غير المشروع للأموال يتطلب مهارة قدرة فنية وتقنية عالية جدا من قبل مرتكبيها كما أن البواعث على ارتكاب المجرم المعلوماتي لهذا النوع من الجرائم قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي.[2]

[1]–حمزة بن عقون، المرجع السابق، ص25.

[2]–حمزة بن عقون، نفس المرجع ، ص26.

1-يتميز الإرهاب الالكتروني أيضا بأنه عمل عدائي غير مشروع من حيث وسائل المستخدمة والأهداف المنشودة، إذ يشمل على تطوير وإرسال شفرات الحاسب الآلي والشبكة الدولية للمعلومات بغية تحديث أغراض عدة تتمثل في التدمير والأنقاض والتغيير التعطيل.

2-جرائم تقنية ناعمة، يعد الحاسب الآلي والشبكة الدولية للمعلومات الأداة الرئيسية في ارتكابها، مثلما يمكن اعتبار البرمجيات ونظم المعلومات الركن المعنوي لمثل هذا النوع من الجرائم.[1]

3-يعتمد الإرهاب الإلكتروني على خبرات وقدرات ذهنية ومهارات عالية في استخدام الحاسوب واختراق أنظمة الحماية المتوفرة، إذ أن مرتكب الإرهاب الالكتروني يكون في العادة ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه قدرة من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة والمعلوماتية.

4-جرائم عابرة للدول، يتسم الإرهاب الالكتروني بأنه جريمة عابرة للحدود نظرا لصعوبة كشف عملية الاختراق للبيانات واثبات الدليل على قيامها والقائمين عليها لتنفيذ أنشطة الإرهاب الإلكتروني باستخدام برامج وأدوات وحاسبات.[2]

المطلب الثالث: وسيلة ارتكاب جريمة الإرهاب الالكتروني عبر الانترنت

تتخذ وسائل تقنية المعلومات في عالمنا المعاصر عدة أنواع منها الوسائل المتصلة بموضوع الجريمة محل البحث وهي كل من الحاسب الآلي والانترنت.

الحاسب الآلي: لقد عرفه المشرع السعودي "بأنه جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي يحتوي نظام معالجة البيانات. أما الشبكة المعلوماتية فعرفها المشرع الإماراتي "إرتباط أكثر من وسيلة لتقنية المعلومات للحصول على المعلومات وتبادلها.

1- الارهاب والجرائم المعلوماتية، مجلة معلومات، المركز العربي للمعلومات، بيروت، 2010، تموز، العدد 80، ص100.

2-عفيفي كامل عفيفي، جرائم الكمبيوتر وتعرف المؤلف والمصنفات ودور الشرطة والقانون:دراسة مقارنة.دون طبعة، منشاة المعارف، الإسكندرية، دون سنة، ص21.

الفرع الأول: الاتصال والتنسيق بين الإرهابيين باستخدام الشبكة الدولية للمعلومات

تعد الشبكة الدولية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية إذ تتيح لهم حرية التواصل وتبادل المعلومات فيما بينها والتنسيق الشامل لشن هجمات إرهابية محددة في جو مريع وبعيد عن رقابة ومتابعة الأجهزة الأمنية وذلك باستخدام البريد الالكتروني آو المواقع والمنتديات وغرف الحوار الالكتروني إذ يمكن وضع وسائل مشفرة تأخذ طابعا لا يلفت الانتباه، ومن دون أن يشطر الإرهابي إلى الإفصاح عن هويته، كما أنها لا تترك آثرا واضحا يمكن أن يدل عليه، فضلا عن المزايا الأخرى التي توفرها هذه الوسائل الرقمية للتواصل من سرعة الاتصال وقلة تكلفته وإمكانية المناورة والتخفي عن ملاحقة الأجهزة الأمنية مقارنة بالوسائل الأخرى.[1]

والأكثر من ذلك فقد أسهمت هذه التقنية في تدفق الدعم والمساعدات إذ تتيح بواسطة الانترنت الوصول إلى جمهور ضخم من المانحين المحتملين وتسمح للأعضاء بالتنسيق سريعا مع اكبر عدد من الأتباع لضمان سريان سريع ومستمر للتعليمات يضمن أقصى درجات التنظيم لنشاطات المجموعات الإرهابية كما، وتجنيد الذين قد يتوزعون فوق رقعة جغرافية ضخمة، كما توفر منبر للدعاية.

وإذا كان الحصول على وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعبا، فان انتشار مواقع الانترنت، واستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين في الترويج لأفكارهم وكسب المؤيدين لهم أو حتى إبلاغ التعليمات والتدريبات لأنصارهم غدا سهلا وممكن حتى يضمنوا انتشارا أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن الوصول إليها، ومما يزيد من خطورة هذه المواقع، إن الجماعات الإرهابية أو المتطرفة تعتمد في خططها وأساليبها الإرهابية على طرف بسيطة تتيح للجميع الدخول المباشر إلى مواقع محجوبة عبر التصفح العادي أو عبر البرامج التبادلية، وهناك مواقع تنشر معلومات حساسة حول كيفية إعداد المتفجرات والمواد السامة وصناعة الصواعق بتفاصيل دقيقة ومكونات يمكن

[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 من 2 الى 4 يونيو 2008م.

الحصول على الكثير منها من أي مكان دون إثارة الرعية، ولا تقتصر خطورة توفر هذه المعلومات على الفئات الضالة بل يمكن إن تمهد الطريق لارتكاب الجرائم الفردية.[1]

الفرع الثاني: البريد الالكتروني[2]

البريد الالكتروني خدمة تسمح بتبادل الرسائل والمعلومات مع الآخرين عبر شبكة للمعلومات، وتعد هذه الخدمة من ابرز الخدمات التي تقدمها شبكة الانترنت لمن تمثله من سرعة في إيصال الرسالة وسهولة الاطلاع عليها في أي مكان، فلا ترتبط الرسالة الالكترونية المرسلة بمكان معين، بل يمكن الاطلاع عليها وقراءتها من أي مكان من العالم وعلى الرغم من أن البريد الالكتروني أصبح أكثر الوسائل استخداما في مختلف[3] القطاعات وخاصة قطاع الأعمال بكونه أكثر سهولة وأمنا وسرعة لإيصال الرسائل إلا انه يعد من أعظم الوسائل المستخدمة في الإرهاب الالكتروني ومن خلال استخدام البريد الالكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيرا من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الالكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها وبين القائمين بالعمليات الإرهابية والمخططين لها. وكذلك يقوم الإرهابيين باستغلال البريد الالكتروني في نشر أفكارهم و الترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر المراسلات الالكترونية.

وما يقوم به الإرهابيون أيضا اختراق البريد الالكتروني للآخرين وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية لقد نص الله –جل جلاله–عن التجسس، ونهت الشريعة الإسلامية عن الاطلاع على أسرار الناس وهتك حرماتهم.[4]

ففي الحديث أن النبي قال" انك إن اتبعت عورات المسلمين أفسدتهم أو كادت أن تفسدهم"

---

[1]– د.معتز محي الدين، الإرهاب وتكنولوجيا المعلومات، مقال منشور على مواقع مدارك الالكتروني، على الرابط: www.net neus delacls.help !/d :21

[2]- سايمون لوكن، التجارة عبر الانترنت، ترجمة يحي ديت ،الأفكار الدولية، نيويورك، 1999م، ص26.

[3]–انظر: عبد الرحيم صدق، الارهاب السياسي والقانون الجنائي، دار النهضة العربية القاهرة، 1985، ص81.

[4]–سورة الحجرات، الاية12.

واختراق البريد الالكتروني هو خرق لخصوصية الآخرين وهتك لحرماتهم وتجسس على معلوماتهم وبياناتهم التي لا يرغبون أن يطلع عليها غيرهم، وان النبي صلى الله عليه وسلم يقول "ولا تجسسوا ولا تجسسوا".

فالشريعة الإسلامية كفلت حفظ حقوق الشخصية للإنسان وحرمت الاعتداء عليها بغير حق، وهؤلاء الذين يعتدون على بيانات الآخرين ومعلوماتهم عبر اختراق رسائلهم البريدية الالكترونية آثمون لمخالفة أمر الشارع الحكيم ومستحقون للعقاب التعزيري الرادع لهم، ولابد من إشاعة هذا الحكيم بين الناس وتوعية المتعاملين بشبكة المعلومات العالمية (الانترنت) بخطورة انتهاك خصوصية الآخرين وحكم ذلك في الشريعة الإسلامية وان هذا الأمر مما استقرت الشريعة على تحريمه والنهي عنه وقد تضافرت نصوص الكتاب والسنة على حفظ حقوق الآخرين وعدم انتهاكها، بل قد نادت الدول إلى تحريم مخترقي البريد الالكتروني لما فيه من ضياع للحقوق واعتداء على خصوصيات الآخرين وأسرارهم، ولاسيما إذا كان ذلك لاستغلالها في الجرائم الإرهابية والعدوان على الآخرين واستثناء من ذلك فقد يكون التجسس مشروعا في أحوال معينة كالتجسس على المجرمين، فقد لا يعرفون إلا بطريق التجسس، وقد أجاز الفقهاء التجسس.[1]على اللصوص، وقطاع الطريق، وطلبهم بطريق التجسس.

أما الحاسوب الذي يتجسس على المسلمين فقد ذهب الحنيفة إلى أن يوجه عقوبة ويطالب حبسه حتى يحدث توبة وذهب المالكية إلى انه يقتل ولا يستتاب ولا دية لورثته كالمحارب لإضراره بالمسلمين وسعيه بالفساد في الأرض، وقيل يقتل إلا أن يتوب، وقيل يقتل إلا أن يعذر بجهل، وقيل يقتل إن كان معتادا لذلك.[2]

وذهب الشافعية إلى أن الجاسوس المسلم يعزر ولا يجوز قتله، وان كان ذا هيئة أي سلف كريم في خدمة الإسلام عفي عنه لحديث خاطب بن أبي بلتعة[3] وذهب الحنابلة إلى ان الجاسوس يقتل لضرره على المسلمين[4] وكذلك يجوز اختراق البريد الالكتروني للمجرمين

---

[1]–انظر: الخراج لابي يوسف205.

[2]–انظر: تبصرة الحكام لابن فرحون 1882م وتفسير القرطبي5218.

[3]– انظر: حاشية العليوبي2264.

[4]– حديث خاطب بن أبي بلتعه أخرجه البخاري، 1436، وأخرجه مسلم19414.

المفسدين في الأرض واللصوص وقطاع الطريق،لتتبعهم ومعرفة خططهم وأماكن وجودهم لقطع شرهم ودفع ضررهم عن المسلمين وهذا موافق لمقاصد الشريعة الإسلامية التي جاءت بحفظ الدين،العرض و المال و النفس والعقل.

الفرع الثالث: صور الإرهاب الالكتروني:

يستخدم الإرهابيون التقنية الالكترونية لتحقيق أغراضهم الخبيثة عدة استخدامات وتلك الصور التي يستخدم فيها الإرهابيون الانترنت والبريد الالكتروني ووسائل التواصل الاجتماعي للتخطيط وتنفيذ جرائمهم وهي كالأتي:

1-التحريض الصريح على الخروج على ولي الأمر المسلم عبر تلك المحروقات المستدارة بالدعوة إلى الخروج بالسنان.

2-التحريض على الخروج باللسان، بذكر مساوئ ولاة الأمور بتغريدات تصنع الجو المشحون وتهيج[1]

الضوضاء وإثارة السفهاء ولي الأمر المسلم على النظام العام في الدولة والتعبئة بذكر بعض مظاهر القصور في الدولة، مستغلين تعاطف الناس في قضاياهم عامة وحاجاتهم الدنيوية خاصة وجذبهم بعبارات براقة وأساليب حماسية عبر تغريدات وتدوير تغريدات.

3- تجنيد فكري للشباب والفتيات الأغرار بتلميع صور الخوارج المارقين، والتكفيريين المفسدين.

4-بث الإرهاب عقيدة وفكرا وسلوكا، بإنشاء مواقع الانترنت الخاصة بالجماعات الإرهابية لنشر عقيدة الخروج على الحكام المسلمين وتكفير من يحمل في أنظمة الحكومة الإسلامية القائمة.

5-بث المواد التي تخدم أهدافهم وفكرهم المرئية منها والمسموعة والمقروءة.

[1]-محمد بن عبد العزيز بن محمد العقيل، المرجع السابق، ص26.

6-الحصول على التمويل يتم استجداد العاطفيين من الناس باسم الدين والجهاد لدفع تبرعات مالية لأشخاص اعتباريين يمثلون وجهة لهؤلاء الإرهابيين ويتم ذلك عبر البريد الالكتروني بطريقة ماكرة تنطلي على المتبرعين.[1]

الفرع الرابع: اختراق المواقع الالكترونية وتدميرها

يشمل هذا السلوك، اختراق الواقع والأنظمة الالكترونية عبر الشبكة و السطو على محتوياتها أو تغييرها أو إحداث الضرر أو حتى تدميرها لتحقيق أهداف غير مشروعة

والمقصود بالتدمير هنا: "الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام إلي (sewer- PC.)، أو مجموعة نظم مترابطة شبكيا (مدمر لإغلاق المواقع الحيوية على الشبكات المعلوماتية، وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، ومحطات توليد الطاقة والماء، ومواقع الأسواق المالية،بحيث يؤدي توقفها عن العمل إلى تحقيق أثار تدميرية تفوق ما تحدثه القنابل المتفجرات من أثار.كما يمكن تصور هجوم الكتروني على احد المواقع الالكترونية بقصد الاستيلاء على محتوياتها والسيطرة والتحكم فيها ومن الوسائل المستخدمة حاليا لتدمير المواقع ضخ مئات الآلاف من الرسائل الالكترونية (mailese) من جهاز الحاسوب الخاص إلى المواقع بالمدمر المستهدف للتأثير على السعة التخزينية للموقع فنشكل هذه الكمية الهائلة من الرسائل الالكترونية ضغطا في النهاية يؤدي إلى تفجير الموقع العامل على الشبكة و تشتت البيانات المخزنة في الموقع فتنتقل في الجهاز المعتدي أو تمكنه.[2]

وتعد الفيروسات والديدان وسائل أخرى من أهم واخطر الوسائل المستخدمة في الاختراق والتدمير الإرهابي للمواقع ونظم المعلومات، والفيروسات عبارة عن برنامج حاسوبي خارجي صنع خصيصا للأضرار بنظام المعلومات والبيانات، ويقدر على التضاعف والانتشار[3] والانتقال من جهاز إلى أخر،إذ تحاول البرامج استغلال العيوب

[1]- محمد بن عبد العزيز بن محمد العقيل، نفس المرجع ، ص26.

[2]- سايمون كولن، المرجع السابق، ص26.

[3]- سراب تامر احمد، الهجمات على شبكات لحاسوب في القانون الدولي الإنساني، أطروحة الدكتوراه، جامعة النهرين، 2014، ص84.

الموجودة في البرامج الأخرى والأخطاء التي تقع فيها مستخدمو الحاسوب قبل الدخول إلى المواقع المصابة بالعدوى الفيروسية أو فتح مرفقات الرسائل البريدية.

ولفيروس الحاسب الآلي خصائص تتشابه إلى حد كبير مع الفيروس الطبيعي من نواح عدة منها، القدرة الفائقة على الانتشار والاختفاء والاختراق مثل الفيروس الطبيعي، كما انه القدرة على تغيير خصائص البرامج كما يقوم الفيروس الطبيعي بتغيير خصائص الخلايا المصابة وتتعدد أنواع واستخدامات الفيروسات سواء على مستوى الأهداف التي تنجزها ومنها على سبيل المثال(الاختراق، التدمير، الاحتيال، السرقة، التجسس) أو على مستوى الأضرار التي تلحقها بالنظام، بدءا من الأضرار اليسيرة إلى تدمير النظام بأكمله، ومنها ما يصيب نظاما الكترونيا محددا ومنها ما يكون واسع الانتشار والضرر وقدر المجلس الأوروبي تكلفة إصلاح الأضرار التي تسببها فيروسات المعلومات بنحو (12) مليار دولار أمريكي سنويا.[1]

أما الديدان فهي برامج صغيرة مستقرة قادرة على استنتاج نفسها ذاتيا باستغلال عيوب معروفة ثم تنتشر في النظام تمهيدا لتحقيق الأغراض التي صممت لها مثل تعطيل النظام أو قطع الاتصال بالشبكة أو سرقة بعض البيانات الخاصة، وتمتاز بسرعة الانتشار وصعوبة التخلص منها لقدرتها الفائقة على التناسخ والمراوغة وقد يقوم الإرهابيون بإنشاء ثغرة تسلل على غرار حصان طروادة باستخدام برنامج غير مرخص يضاف إلى برنامج ما، ليتمكن بعد ذلك بالولوج غير المرخص فيه إلى الشبكة أو البرامج .الحوسبي التي لا يسمح لهم بالدخول إليها بالأحوال الاعتيادية، تمهيدا للعبث فيه بالحذف والإضافة والتغيير بخصائص النظام كله فضلا عن التجسس.[2]

وقد يذهب الإرهابيون إلى ابعد من ذلك بزرع القنبلة المنطقية داخل النظام الالكتروني التي تكون عبارة عن برنامج حوسبي خبيث وخفي مصمم في وقت لاحق عند وقوع حدث معين أو حتى ظروف معينة، أو صورة تلحق الضرر أو حتى التوقيت للنظام أو

[1]– ريتشارد كلارك وروبرت نيك، حرب القضاء الالكتروني/التهديد الآلي للأمن القومي وكيفية التعامل معه، مركز الإمارات للدراسات الإستراتيجية، الإمارات العربية المتحدة، 2012، ص107.

[2]–محمود الرشيدي، العنف في جرائم الانترنت، الحماية والتامين، دون طبعة، الدار المصرية اللبنانية، القاهرة، 2011، ص–ص85–87.

الشبكة عن العمل أو حذف كل البيانات الموجودة فيها أو توجيه أوامر لمعدات الحاسوب لتقوم بشيء معين يؤدي إلى تدميرها.[1]

فالمتغيرات التقنية، وإلمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء (open source) سواء كان ذلك في مكونات نقطة الاتصال أو في النظم أو في الشبكة أو في البرمجة جعلت الحيلولة دون الاختراقات صعبة جدا، بالإضافة إلى أن هناك منظمات إرهابية يدخل من ضمن عملها ومسؤولياتها الرغبة في الاختراق وتدمير المواقع ومن المعلوم أن لدى المؤسسات من الإمكانات والقدرات ما ليس لدى الأفراد ويستطيع قراصنة الحاسب الآلي (hackers) التواصل إلى المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة.[2]

[1]–سراب تامر احمد، المرجع السابق، ص–ص86–87.

[2]– امير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، ص239.

المبحث الثاني: الأركان العامة لجريمة الإرهاب الإلكتروني

تتسم الجريمة الإرهابية بخصوصيتها وتستخدم للقوة والعنف والرعب بهدف التأثير والإثبات الجنائي هو نشاط إجرائي للوصول إلى اليقين القضائي[1] أما جرائم الإرهاب الإلكتروني فإن قواعد الإجراءات بشأن جرائم الكمبيوتر المتصلة بإجراءات الاستدلال والتحقيق والإثبات وإجراءات المحاكمة المتفقة مع طبيعة الاعتداءات في الدعوى التي تتعلق بجرائم الكمبيوتر حيث سنتناول في هذا المبحث ثلاث مطالب: المطلب الأول الركن الشرعي، المطلب الثاني الركن المادي، المطلب الثالث الركن المعنوي.

المطلب الأول: الركن الشرعي

القاعدة العامة بالنسبة لشرعية التجريم والعقاب حيث نصت الأولى من قانون العقوبات الجزائري "لا جريمة ولا عقوبة ولا تدابير أمن إلا بقانون".

وبالتالي يبقى الفعل مباحا ما لم ينص عليه في النصوص العقابية، حيث عرفت الجزائر أبشع صور الإرهاب، مما أدى بالسلطة التشريعية إلى سن قوانين تشريعية سواء بالنسبة لجرائم الإرهاب التقليدية، وجريمة الإرهاب الإلكتروني في التشريع الجزائري أو التشريع الإماراتي.

الفرع الأول: انطباق نصوص التجريم والعقاب في جريمة الإرهاب التقليدية:

تعد الجريمة فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدابير أمن فالجريمة بوجه عام كانت داخلية أو خارجية (دولية) قد يرتكبها شخص بمفرده وقد يساهم معه أشاخص آخرون في ارتكابها مع اختلاف المساهمة والجريمة العادية تختلف عن الجريمة الإرهابية وخصوصية هذه الجريمة تستخدم للقوم والعنف والرعب.

أ. **خضوع الفعل لنص التجريم:** بمعنى أنه لا يجوز اعتبار أي سلوك أو فعل ما لم ينص القانون على تجريمه ولا تعرض له عقوبة إلا إذا كان القانون يقرر له عقوبة جزائية

[1]- أمير فرج يوسف، المرجع السابق، ص239.

وبعبارة أخرى فإن الركن الشرعي وجود نص تشريعي يحدد الجزاء والمقرر لسلوك معين من عقوبة أو تدابير أمن وعليه فإن الركن الشرعي هو الذي يصفي وصف المشروعية.[1]

ب. النصوص العقابية في التشريع الجزائري بالنسبة للجرائم الإرهابية.

حيث يتم سن قوانين تشريعية المرسوم التشريعي 92- 03 المؤرخ في 1992/09/30[2] وصدور الأمر 10/95 المتضمن الجرائم الموصوفة بأفعال إرهابية وتخريبية إضافة إلى المواد 87 مكرر إلى المادة 87 مكرر 10 من الأمر رقم 11/95 المعدل والمتمم.[3]

ج. **النصوص العقابية للجريمة الإرهابية في التشريع الإماراتي:**

بصدور قانون جديد أصلح للمتهم تطبيقا لنص المادة 111 من الدستور الإماراتي فإن نصوص قانون العقوبات لا تعتبر نافذة الأمن تاريخ العمل بها الذي يبدأ بعد شهر من تاريخ نشرها في الجريدة الرسمية وتؤكد هذا الحكم المادة 12 "التي تقضي بأنه يعاقب على الجريمة طبقا للقانون النافذ وقت ارتكابها".[4]

الفرع الثاني: انطباق نصوص التجريم والعقاب على جريمة الإرهاب الإلكتروني.

حاولت قوانين العقوبات مواجهة الجرائم الإلكترونية بطرق التقليد كالجرائم الماسة بأمن الدولة.

إلا أنه يتبين من ذلك وجود قصور تشريعي لمواجهة هذا النوع من الجرائم التي ارتبطت بظهور أجهزة الكمبيوتر وفقا للقواعد العامة وبالتالي فالقانون الجنائي لا يتطور بنفس السرعة التي تطور بها التكنولوجيا.

- الحاجة لتدخل المشرع لمواجهة جريمة الإرهاب الإلكتروني:

---

[1]- المادة الأولى من الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، المعدل والمتمم.

[2]- المرسوم التشريعي 92- 03 المؤرخ في 1992/09/30.

[3]- الأمر رقم 11/95 المتضمن الجرائم الموصوفة بأفعال إرهابية وتخريبية المؤرخ في 25 فبراير 1995، المتضمن قانون العقوبات، المعدل والمتمم.

[4]- المادة 111 من الدستور الإماراتي.

تعد الجريمة الواقعة من نتائج التطور التكنولوجي أنها من المستجدات التي عجزت مواد القوانين العقابية التقليدية لذا اتسعت معظم التشريعات المتقدمة والدول العربية على المستوى الداخلي والخارجي لسن قوانين لمواجهة هذا النوع من الجرائم.

الفرع الثالث: النصوص العقابية لجريمة الإرهاب الإلكتروني في التشريع الجزائري:

لقد فرض المشرع الجزائري حماية جنائية على الحياة الخاصة للأفراد في القسم السابع مكرر بمحتوى المادة 394 مكرر إلى المادة 394 مكرر 7 بمقتضى القانون 04-15 المؤرخ في 2004/11/10 المعدل والمتمم والقانون 04/09 المؤرخ في 5 غشت 2009 المعدل والمتمم وكذلك القسم السابع من قانون العقوبات من القانون 16/02 المؤرخ في 22 يونيو 2016 المتضمن تعديل قانون العقوبات، الجريدة الرسمية، العدد 37 2016 في نص المادة 87 مكرر 11 حيث جرم المشرع الجزائري جريمة الإرهاب الإلكتروني في نص المادة 87 مكرر 11 من قانون العقوبات المعدل والمتمم "يعاقب بالسجن المؤقت من خمس (5)[1] سنوات إلى عشر سنوات وبغرامة مالية من 100.000 دج إلى 500.000 دج. كل جزائري أو أجنبي يقدم بالجزائر بطريقة شرعية أو غير شرعية، يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها.

يعاقب بنفس العقوبة لكل من:

- يوفر أو يجمع عمدا أموالا بأي وسيلة وبصورة مباشرة أو غير مباشرة بقصد استخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب الأفعال المذكورة في الفقرة الأولى من هذه المادة.

- قام عمدا بتمويل أو تنظيم فر أشخاص إلى دولة أخرى، بغرض ارتكاب أفعال إرهابية أو تدبيرها لإعداد لها المشاركة فيها أو التدريب عليها أو تسهيل ذلك السفر.

[1]- المادة 87 مكرر 11 من القانون 02/16 المؤرخ في 22 يونيو 2016، المتضمن تعديل قانون العقوبات، الجريدة الرسمية، العدد 37 ،المعدل والمتمم.

– يستخدم تكنولوجيا الإعلام والاتصال لارتكاب الأفعال المذكورة في هذه المادة.

• وكذلك المادة 87 مكرر 12 وقد أفرز ذلك ظهور المقاتلين الذين غالبا ما يجري تأطيرهم من قبل شبكات إجرامية لنشر أفكارهم المتطرفة.[1]

– المادة 394 مكرر 8 بمفهوم المادة 2 من القانون 09– 04 المؤرخ في 5 غشت 2009 للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المعدل والمتمم. وكذلك نصت المادة 394 مكرر 3. وكذلك الاتفاقية الدولية للإجرام المادة 2.

الفرع الرابع: النصوص العقابية لجريمة الإرهاب الإلكتروني في التشريع الإماراتي:

– حيث نص المشرع الإماراتي في المادة 26 من مرسوم بقانون 5 لسنة 2012 بشان جرائم تقنية المعلومات "يعاقب بالسجن مدة لا تقل من 5 سنوات والغرامة التي لا تقل عن مليون درهم ولا تجاوز ليون درهم كل من أنشأ أو أدار موقعا إلكترونيا أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات وذلك لجماعة إرهابية أو أي مجموعة أو جمعية أو منظمة غير مشروعة بقصد تسهيل الاتصال بقيادتها أو أعضائها أو لاستقطاب عضوية لها أو ترويع أو تجنيد أفكارها أو تمويل أنشطتها أو توفير المساعدة الفعلية لها بقصد نشر أساليب تصنيع الأجهزة الحارقة أو المتفجرات، أو أي أدوات أخرى تستخدم في الأعمال الإرهابية".[2]

– وكذلك تناول المشرع الجزائري نص المادة 394 مكرر 3 والاتفاقية الدولية للإجرام المادة 2.[3]

[1]– المادة 26 من مرسوم بقانون 5 لسنة 2012 بشان جرائم تقنية المعلومات.

[2]– المادة 394 مكرر 3 من القانون 04/15 المؤرخ في 10–11–2004 المتضمن قانون العقوبات المعدل والمتمم.

[3]– المادة 2 من الاتفاقية الدولية للإجرام.

المطلب الثاني: الركن المادي.

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة[1] والعلاقة السببية مع العلم أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة. ويقوم الركن المادي على صورتين أساسيتين الصورة الأولى وتتمثل في الاعتداء على نظام المعالجة الآلية وتحمل صورتين الأولى الدخول والبقاء غير المشروع في نظام المعالجة الآلية والصورة الثانية وهي ثلاثة أفعال وهي فعل الدخول والبقاء وعرقلة التعطيل أما الصورة الثانية متمثلة في فعل التزوير.

الفرع الأول: الصورة المشددة في التشريع الجزائري

نصت المادة 394 مكرر 3 "تضاعف العقوبات المنصوص عليها إذا استهدفت[2] الجريمة الدافع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد.

- حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق استهداف الدفاع الوطني والمؤسسات الخاضعة للقانون العام وبالتالي المساس بأمن الدولة.

- ونص المشرع الجزائري في المادة 394 مكرر 2/2 يجرم أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه الأفعال الواردة في القسم السابع مكرر من ق.ع.ج بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق... الخ.

- يثبت في نص المادة 394 مكرر 2/2 تصميم حيازة أو إفشاء أو توفير[3] أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم".

---

[1]– محمد أمين الرومي، جرائم الكمبيوتر والأنترنت، د ط، دار المطبوعات الجامعية، الإسكندرية – مصر، 2003، ص182.

[2]– المادة 394 مكرر 3 و 394 مكرر 2، قانون العقوبات الجزائري.

[3]– المادة 394 مكرر 2/2، من قانون العقوبات.

- ويبين أيضا في المادة 394 مكرر 4.

المشرع الإماراتي لمكافحة جرائم تقنية المعلومات: يمكن القول[1] أن المشرع الإماراتي حذا حذو المشرع الجزائري حيث عالج وواقف إنشاء موقع أو نشر معلومات مخلة بالآداب العامة عبر وسائل التقنية بمقتضى المادة 20 من القانون الاتحادي الإماراتي لمكافحة جرائم تقنية المعلومات رقم 2 لسنة 2006 على أن " كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل أو ترويج برامج وأفكار من شأنها الإخلال بالنظام العام أو الآداب العامة يعاقب بالحبس مدة لا تزيد على حمس سنوات".

والمصلحة المعتدى عليها محل الحماية القانونية هي حماية الحياة والآداب العامة من الإخلال بها وهذه المصلحة معنوية تغلب عليها الصفة العامة وليس الخاصة مما يجعلها من جرائم الخطر وليس الضرر يعني تتحقق الجريمة رغم إنتفاء تحقق الضرر.

الفرع الثاني: ارتكاب السلوك الجرمي:

لقد أورد المشرع الإماراتي صورتين للسلوك المكون للجريمة إذ أن تحقق أي منهما لقيام الجريمة بمقتضى المادة 20.

أ. إنشاء موقع إلكتروني: أن مكان إتاحة المعلومات على الشبكة المعلوماتية[2] وإذا لم يكن الموقع الإباحي متاحا على الشبكة المعلوماتية من خلال عنوان محدد فإنه لا تقع الجريمة وفق المادة 20 من القانون الإماراتي.

النشر يقصد به عرض الشيء على الجمهور أي عرضه على نظر العامة.

النتيجة: أن السلوك المتمثل بإنشاء موقع إلكتروني أو بنشر معلومات يجب أن ينصب موضوعه نحو الدعوة إلى تسهيل أو ترويج برامج يكون من شأنها إحداث نتيجة جرمية تتمثل بإخلال بالنظام العام.

---

[1]– المادة 20 من القانون الإتحادي الإماراتي.

[2]– نوفل علي عبد الله الصفو، جريمة إنشاء معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات دراسة مقارنة، دون طبعة، جامعة الموصل كلية الحقوق، العراق، ص 26.

ويتحقق الإخلال بالنظام العام عند القيام بفعل يمس أسس الكرامة للعامة وبهدم أركان حسن سلوكها.[1]

أما إذا كان الموقع الإلكتروني أو كانت المعلومات المنشورة على الشبكة المعلوماتية تنطوي على رسوم أو صور تمثل أوضاع جنسية فاحشة تدفع إلى الدعارة أو الفجور فعند ذلك نكون أمام جريمة التحريض على الدعارة أو الفجور متى توفر القصد الجنائي لدى الجاني وبالتالي تخضع الجريمة لنص المادة 13 من القانون الاتحادي لمكافحة جرائم تقنية المعلومات.

المشرع الجزائري أضاف جريمة أخرى وتتمثل في جريمة تجنيد الأشخاص[2] للقيام بأعمال إرهابية ويتمثل في السفر إلى الخارج وعاقبت المادة 87 مكرر 11 الجديدة على السفر من دولة إلى دولة أخرى بالنسبة لكل جزائري أو أجنبي مقيم في الجزائر بفرض ارتكاب أفعال إرهابية والإعداد لها أو المشاركة فيها أو التدريب عليها كما عاقبت نفس المادة على جمع الأموال بطريقة أو غير مباشرة بقصد استخدامها في تمويل سفر أشخاص لارتكاب أفعال إرهابية وتسهيل السفر وعاقبت أيضا المادة أيضا من يستخدم تكنولوجيا الإعلام والاتصال لارتكاب هذه الأفعال.

السلوك الإجرامي

استخدام تكنولوجيا الإعلام والاتصال لتجنيد وعاقبت المادة 87 مكرر 12 الجديد كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد أشخاص لمصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشتطها أو ينظم شؤونها أو يدعم أعمالها وأنشطتها أو ينشر أفكارها بصفة مباشرة أو غير مباشرة.

[1]– نوفل علي عبد الله الصفو، المرجع نفسه، ص 30.

[2]– المادة 87 مكرر 11 ومكرر 12، قانون العقوبات.

الفرع الثالث: النتيجة الجرمية.

النتيجة: أن السلوك المتمثل بإنشاء موقع إلكتروني أو بنشر معلومات يجب أن ينصب موضوعه نحو الدعوة إلى تسهيل أو ترويج برامج كون من شأنها إحداث نتيجة جرمية تتمثل بالإخلال بالنظام العام.

ويتحقق الإخلال بالنظام العام عند القيام بفعل يمس أسس الكرامة للعامة وبهدم أركان حسن سلوكها.[1]

أما إذا كان الموقع الإلكتروني أو كانت المعلومات المنشورة على الشبكة المعلوماتية تنطوي على رسوم أو صور تمثل أوضاع جنسية فاحشة تدفع إلى الدعارة أو الفجور فعند ذلك نكون أمام جريمة التحريض على الدعارة أو الفجور متى توفر القصد الجنائي لدى الجاني وبالتالي تخضع الجريمة لنص المادة 13 من القانون الإتحادي لمكافحة تقنية المعلومات.

– المشرع الجزائري أضاف جريمة أخرى وتتمثل في جريمة تجنيد الأشخاص[2] للقيام بأعمال إرهابية ويتمثل في السفر إلى الخارج وعاقبت المادة 87 مكرر 11 الجديدة على السفر من دولة إلى دولة أخرى بالنسبة لكل جزائري أو أجنبي مقيم في الجزائر بغرض ارتكاب أفعال إرهابية والإعداد لها أو المشاركة فيها أو التدريب عليها كما عاقبت نفس المادة على جمع الأموال بطريقة أو غير مباشرة بقصد استخدامها في تمويل سفر أشخاص لارتكاب أفعال إرهابية وتسهيل السفر وعاقبت أيضا المادة أيضا من يستخدم تكنولوجيا الإعلام والاتصال لارتكاب هذه الأفعال.

– **السلوك الإجرامي:** استخدام تكنولوجيا الإعلام والاتصال للتجنيد: وعاقبت المادة 87 مكرر 12 الجديد كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد أشخاص لمصالح

[1]– نوفل علي عبد الله الصفو، المرجع السابق، ص 30.

[2]– المادة 87 مكرر 11 ومكرر 12، قانون العقوبات.

إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها أو ينظم شؤونها أو يدعم أعمالها وأنشطتها أو ينشر أفكارها بصفة مباشرة أو غير مباشرة.

- **النتيجة الجرمية:** تعتبر النتيجة الجرمية الإرهابية كما هو الحال في جرائم القانون العام العنصر الثاني من عناصر الركن المادي.

أولا- حالة الخطر: وينشأ من ورائها ضرر ينال مصلحة محمية.

الفرع الرابع: العلاقة السببية

لكي يسأل الجاني عن النتيجة الضارة لقيام الركن المادي للجريمة لا بد أن يكون فعل الجاني وسلوكه الإجرامي هو السبب في إحداثها بمعنى أن تكون النتيجة مرتبطة بفعله وناتجة عنه فالعلاقة السببية هي الصلة التي تربط بين الفعل (السلوك) والنتيجة.

بل يلزم فضلا عن ذلك أن تتسنى هذه النتيجة إلى ذلك السلوك، أي أن يكون بينهما رابطة سببية.

إن البحث عن العلاقة السببية لا يثور بشأن كل جريمة ولكن يلزم أن تتحقق الشروط الآتية:

1-أن تكون بصدد جريمة ذات نتيجة.

2- أن ينفصل السلوك الإجرامي عن النتيجة فيلزم أن يتحقق فاصل زمني بين السلوك والنتيجة، أما إذا اتصلت النتيجة بالسلوك بغير فاصل زمني فإن البحث في علاقة سببية لا يكون له محل، وسلوك الجاني هو السبب الوحيد في حدوث النتيجة. إذ يتدخل عامل أجنبي أو أكثر مستقل عن النشاط المادي لفاعل يساهم معه في إحداث النتيجة أي المساهمة الجنائية لأجل إحداث نتيجة جرمية المعاقب عليها والتي ينتج عنها ضرر لأنها جريمة عمدية فنتيجتها دائما مقصودة.

المشرع الإماراتي: فقد نص في المادة 17 تحت البند 16: "كل من أنشأ موقعا أو نشر على الشبكة المعلوماتية بقصد الاتجار في الأشخاص أو تسهيل فيه يعاقب بالسجن المؤقت".[1]

المطلب الثالث: الركن المعنوي

بالنسبة للمشروع الجزائري للجريمة الإلكترونية يختلف باختلاف أشكالها وعليه ارتأينا التعرض للركن المعنوي لكل جريمة على حدى، حيث تناولت فيه ثلاث فروع:

الفرع الأول: جريمة الدخول والبقاء الغير المشروع داخل نظام المعالجة الآلية للمعطيات.

الفرع الثاني: جريمة الاعتداء على سير نظام المعالجة الآلية.

الفرع الثالث: وتناولت فيه المشرع الإماراتي.

الفرع الأول: جريمة الدخول والبقاء غير المشروع داخل نظام المعالجة الآلية[2] للمعطيات:

إن جريمة الدخول والبقاء غير المشروع هي جرائم عمدية تتطلب قصد جنائيا وذلك بنص المادة 394 مكرر من القانون رقم 15/04 المؤرخ في 10-11-2004 المتضمن قانون العقوبات المعدل والمتمم والتي عبرت عن القصد الجنائي بنصها" كل من يدخل أو يبقى عن طريق الغش وتعني هذه العبارة أن الفاعل كامل العلم بأن الدخول أو البقاء غير مشرع، كما نطرق المشرع الفرنسي في نص المادة 323/01 بعبارة Frauduleusement ولتوفير القصد الجنائي لا بد أن يكون الجاني محيطا علما بكافة عناصر الجريمة وله علم بأن الفعل الذي يقوم به ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات.

أما بالنسبة لنية الغش تبدو من خلال الغش الذي تم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام بالنسبة للبقاء.

---

[1]- قانون مكافحة جرائم تقنية المعلومات الإماراتي المادة 17 البند 16.

[2]– بعرة سعيدة، المرجع السابق، ص 60،61،62.

الفرع الثاني: جريمة الاعتداء على سير نظام المعالجة الآلية:

فهي جريمة عمدية لأن أفعال العرقلة والتعطيل من الأفعال العمدية وهذا ما يميز عن الاعتداء غير العمدي لسير النظام ويعتبر ظرف مشدد.

1- جريمة الاعتداءات العمدية على المعطيات: هذه الجريمة من جريمة عمدية فيما القصد الجنائي بعنصريه العلم والإدارة، فيجب أن تتجه إدارة الجاني إلى فعل الإدخال أو المحو أو التعديل ويجب أن يعلم الجاني أن نشاطه يترتب عليه التلاعب في المعطيات ويعلم أنه ليس له الحق في القيام بذلك بالإضافة إلى اتجاه إدارة الجاني إليه.

2- استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية: إن هذا الاستخدام متمثل في التصميم والبحث أو التجميع أو النشر أو الاتجار في معطيات مخزنة أو مرسلة عن طريق منظومة معلوماتية ويكون هذا الاستخدام عن طريق الغش.

الفرع الثالث: المشرع الإماراتي: بالنسبة للركن المعنوي: إن جريمة إنشاء موقع[1] أو نشر معلومات التي جاء بها المشرع الإماراتي هي من الجرائم العمدية ذات القصد الجنائي العام أي أن يكون الجاني عالما بأنه يقوم بإنشاء أو نشر معلومات تتضمن التسهيل أو الترويج للقيام بأفعال من شانها الإخلال بالنظام العام وإن تتصرف إرادته إلى ذلك. وهنا المشرع الإماراتي حذا حذو المشرع الجزائري.

عقوبة الجريمة: وعاقب المشرع الإماراتي وفق المادة 20 من يقوم بإنشاء موقع أو نشر معلومات من شأنها الإخلال بالنظام العام الحبس مدة لا تزيد عن خمس سنوات.

- **القصد الجنائي الخاص:** بأنه الغاية التي ترمي إليها فضلا عن كونه كامل الإرادة في مخالفة للقانون الجنائي.

[1]- نوفل علي عبد الله الصفو، المرجع السابق، ص 33.

الفصل الثاني:
الجهود الدولية لحماية ومكافحة جريمة الإرهاب الإلكتروني

تمهيد وتقسيم

أن من الآثار الرقمية التي يمكن تتبعها أو سريعة الزوال يستلزم اتخاذ إجراء سريع وهذا هو الحال حين يسعى المرء إلى منع ارتكاب جريمة في مرحلة التنفيذ مثل سن هجوم إلكتروني على بنية أساسية حرجة وهذا هو الحال أيضا حين يسعى المرء إلى جمع أدلة تتصل بجريمة ارتكبت مؤخرا ويتحدد فقط بالتطور التكنولوجي في استخدام الوسائل والتقنيات الحديثة وهي شبكة الانترنت وأصبح سلاحا تستخدمه الدول والجماعات والأفراد مستفيدة من التطور التقني والتكنولوجي لتحقيق أهدافها ومصالحها على حساب الأمن والسلام ولمحاولة القضاء على هذه الظاهرة ألا وهي ظاهرة الإرهاب الإلكتروني لا بد من تكاثف الجهود سواء على المستوى الداخلي أو الخارجي الدولي الأوروبي ومكافحة هذه الظاهرة لذا يمكن التطرق في المبحث الأول من هذا الفصل إلى التعاون الدولي في مواجهة جرائم الإرهاب الإلكتروني وتطرقت في المبحث الثاني إلى دور المنظمات العالمية في مكافحة الإرهاب الإلكتروني حيث تناولت فيه دور المنظمات المتخصصة في مكافحة الإرهاب الإلكتروني كذلك دور المنظمات الإقليمية في مجال مكافحة الإرهاب الإلكتروني ودور الأمم المتحدة في مكافحة الإرهاب الإلكتروني.

المبحث الأول: التعاون الدولي في مواجهة جرائم الإرهاب الإلكتروني.

يمكن ارتكاب الجريمة الإلكترونية من أقصى بقاع الأرض بنفس سهولة ارتكابها من أقرب مكان كما أن رسالة واحدة تعزز ارتكاب جريمة الإرهاب الإلكتروني يمكن تمريرها من خلال الكثيرين من مقدمي الخدمات في بلدان مختلفة لها نظم قانونية مختلفة كما أن الآثار الرقمية التي يمكن تتبعها تكون ضعيفة أو سريعة الزوال ولذا تستلزم اتخاذ إجراء سريع وهذا هو الحال تحديدا حين يسعى المرء إلى منع ارتكاب جريمة في مرحلة التنفيذ مثل شن هجوم إلكتروني على بنية أساسية حرجة وهذا هو الحال أيضا حتى يسعى المرء إلى جمع أدلة تتصل بجريمة ارتكبت مؤخرا وتصبح المهمة بالغة الصعوبة حتى يعبر الهجمة اختصاصات قضائية متعددة.[1]

المطلب الأول: التشريعات على الصعيد الدولي.

كانت الدول المتقدمة سباقة غلى مواجهة جرائم الانترنت سواء عن طريق سن التشريعات الجزائية الخاصة بهذه الجرائم، أو من خلال تعديل النصوص القائمة لتشمل هذا الإجرام المستحدث كما أن المشرع العربي لم يقف مكتوف الأيدي أمام هذه الظاهرة بل كانت هناك محاولات تشريعية في الدولة العربية لاستيعاب هذا النوع من الإجرام، وبناءا على ذلك سوف نلقي الضوء على هذه المواقف التشريعية على صعيد الدول الأجنبية وعلى صعيد الدول العربية.[2]

الفرع الأول: التشريعات على صعيد الدول العربية.

لقت محاولات المشرع العربي لمواجهة جرائم الحاسوب والانترنت حديثة نسبيا للمشروع العربي من التدخل لسن التشريعات الجزائية الكفيلة بمواجهة جميع جرائم المعلوماتية كما فعل المشرع العماني والسعودي والإماراتي والسوداني.

[1]– أمير فرج يوسف، مكافحة الإرهاب الإلكتروني في ظل ثقافة دول مجلس التعاون لمكافحة الإرهاب،د ط، دار الكتب والدراسات العربية الإسكندرية– مصر، 2011، ص 257.

[2]– محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 100 ص 102.

وتعد دولة سلطنة عمان أول دولة عربية تصدت لجرائم المعلوماتية من خلال إصدارها المرسوم السلطاني رقم 72/ 2001 المتضمن تعديل بعض أحكام قانون الجزاء العماني ليشمل جرائم الحاسوب فقد جرم هذا القانون العدد من هذه الجرائم ومنها الدخول غير المشروع إلى أنظمة الحاسوب، والالتقاط غير المشروع للمعلومات أو البيانات، وإتلاف أو محو البيانات والمعلومات كما جرم هذا القانون تزوير بطاقات الائتمان واستعمالها واستعمال البطاقة بعد انتهاء صلاحيتها أو إلغائها، أو استعمال البطاقة مع العلم بعدم وجود رصيد، واستعمال بطاقة الغير دون علمه، وغيرها من جرائم.[1]

أما المملكة العربية السعودية، فقد قامت في 31 آذار عام 2007 بإقرار نظام لمكافحة جرائم المعلوماتية وقد عاقب هذا النظام على العديد من الجرائم، ومنها على سبيل المثال:

- ✓ الدخول غير المشروع إلى منظومة معلوماتية لتهديد شخص أو ابتزازه.
- ✓ الاستيلاء على مال منقول أو سند أو توقيع على هذا السند أو انتحال صفة.
- ✓ الوصول دون وجه حق إلى بيانات بنكية أو ائتمانية أو أوراق مالية.
- ✓ إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو إعاقة الوصول إلى الخدمة.
- ✓ إنتاج ما من شأنه المساس بالنظام العام أو الآداب العامة أو حرمة الحياة الخاصة.

أما دولة الإمارات العربية المتحدة: فقد قامت بإصدار القانون الاتحادي رقم 02 لعام 2006 في شأن مكافحة جرائم تقنية المعلومات.

وفي السودان فقد تم إصدار قانون جرائم المعلوماتية لعام 2007 والحقيقة أن كلا من القانونيين الإماراتي والسوداني قد تضمنا أحكاما موضوعية تفصيلية لجرائم المعلوماتية، إلا أنهما لم يتضمنا الأحكام الإجرائية اللازمة لمكافحة هذا النوع من الجرائم كما برز بوضوح التشابه بين هذين القانونيين لجهة التقسيم.

[1]– محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 110 ص 113.

الوضع التشريعي في سوريا: وقد تضمنت هذه المشاريع نصوصا تجرم بعض الأفعال المخالفة لأحكامها والتي تدخل ضمن الجرائم المعلوماتية.

- **مشروع قانون مكافحة الجريمة الإلكترونية:**[1]

تم تشكيل لجنة من المختصين التقنيين والقانونيين لإعداد مشروع قانون مكافحة الجريمة الإلكترونية، وقد حاولت هذه اللجنة الاستفادة من القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات ومن التجارب التشريعية الأجنبية والعربية، إضافة إلى الاتفاقية الأوروبية لمكافحة الجريمة الافتراضية لعام 2001.

الفرع الثاني: التشريعات على صعيد الدول الأجنبية.

قام المشرع في كندا بتعديل القانون الجزائي الاتحادي في عام 1983 ليشمل جرائم الحاسوب والانترنت، حيث عاقبت 342 قانون عقوبات الكندي على الجرائم المتعلقة ببطاقات الائتمان، كتزويرها واستعمال البطاقات المزورة وغير ذلك.

ألمانيا: قانون العقوبات الألماني المادة (A/ 263) تتضمن تجريما للاحتيال المعلوماتي، حيث نصت على "أنه كل من يقوم بالحصول لنفسه أو لشخص آخر على منفعة مادية غير مشروعة والإضرار بممتلكات الغير عن الاستعمال الغير المصرح به للبيانات وعن التدخل غير المصرح به في عملية المعالجة ذاتها، يعاقب بالسجن لمدة لا تزيد عن 5 سنوات أو بالغرامة.

اليونان: المشرع اليوناني حذا حذو المشرع الألماني حيث أضاف لبعض المواد الخاصة بالجريمة المعلوماتية إلى قانون العقوبات اليوناني عام 1988 وسمحت المادة (A 386) من قانون العقوبات اليوناني بتجريم الاحتيال المعلوماتي.[2]

أما الدنمارك: قام المشرع يسن تشريع خاص لمكافحة جرائم الحاسوب والانترنت وشمل العديد من الجرائم.

[1]– محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 114 ص 115.

[2]– محمد طارق عبد الرؤوف الخن، نفس المرجع، ص 103.

أستراليا: ففي عام 1989 تم تعديل القانون الجزائي ليشمل جميع جرائم الحاسوب.

الفلبين: فقد تم إصدار تشريع يعاقب على القرصنة في عام 2000.

في **بلجيكا:** فقد صدر قانون حول الإجرام المعلوماتي في عام 2000.

أما في **سويسرا:** فقد جرم قانون العقوبات السويسري لعام 1995 الاحتيال المعلوماتي في المادة 147.[1]

كما قامت هولند وفلندا واليابان والمجر وبولندا بسن تشريعات جزائية بسن تشريعات جزائية لمواجهة جرائم الحاسوب والانترنت.

الولايات المتحدة الأمريكية: بعد قانون (فلوريدا) لجرائم الحاسوب في عام 1978 أول قانون في و.م.أ يخاطب الاحتيال على الحاسوب.

أما على الصعيد الفيدرالي فقد صدر عام 1984 قانون الاحتيال وسوء استخدام الكمبيوتر CFAA وتم تعديله في كل من سنة 1986 – 1988– 1990– 1994 وبعد ذلك تم تعديله.

أما في القوانين الإجرامية فهي منصوص عليها في الأقسام 2702/ 2701/ 2511/ 2703/ 2711/ 2705.

بريطانيا: قام المشرع البريطاني بإصدار قانون إساءة الكمبيوتر CAA لعام 1990 حيث قام بتجريم القرصنة، ويعد مرتكب لجريمة السرقة على التلاعب في البيانات من أجل الحصول على منفعة مالية فذهب إلى التوسيع في تفسير المادة 15 من القانون.

الفرع الثالث: الاتفاقية الأوروبية حول الجريمة الافتراضية (اتفاقية بودايست لعام 2001).

بتاريخ 2001/11/23 في بودايست (المجر) قامت ست وعشرون دولة أوروبية بالتوقيع على أول اتفاقية تكافح جرائم الانترنت كما قامت أربع دول من غير الأعضاء في

[1]- المادة 147 من قانون العقوبات السويسري، المتضمن الإحتيال المعلوماتي.

المجلس الأوروبي بالمشاركة في إعداد هذه الاتفاقية والتوقيع عليها أيضا، وهي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية المادة 36 من الاتفاقية وقد استغرقت المفاوضات بين الدول الموقعة على هذه الاتفاقية أربعة أعوام حتى تم التوصل إلى الصيغة النهائية المناسبة ورغم أن هذه الاتفاقية هي الأصل أوروبية الميلاد، إلا أنها دولية الطابع، لأنها مفتوحة أي تسمح بانضمام دول أخرى من غير المجموعة الأوروبية المادة (1748).

➢الأحكام الموضوعية: فيما يتعلق بالأحكام الموضوعية فقد تضمنت الاتفاقية أربع أطراف رئيسة لجرائم الحاسوب وطائفة خامسة تتعلق بقواعد المساهمة بالجريمة والعقوبات المفروضة لهذه الطوائف الأربعة وهذه الطوائف هي على النحو التالي:

الطائفة الأول: الجرائم التي تستهدف عناصر أمن المعلومات، وهي الجرائم ضد السرية والسلامة ووجود بيانات الحاسوب وتتمثل جريمة الدخول غير المشروع (المادة 02)، وجريمة المراقبة أو الاعتراض غير المشروع (المادة 03) وجريمة المراقبة أو الاعتراض غير المشروع (المادة 03) وجريمة التداخل أو التشويش على البيانات (المادة 04) وجريمة إتلاف أو تعديل نظام (المادة 05) وجريمة إساءة استخدام الأجهزة (المادة 06).

الطائفة الثانية: الجرائم المرتبطة بالحاسوب، وتشتمل التزوير المرتبط بالحاسوب (المادة 07)، والاحتيال المرتبط بالحاسوب (المادة 08).

الطائفة الثالثة: الجرائم المرتبطة بالمحتوى، وتشتمل جريمة واحدة، وهي جريمة دعارة الأطفال (المادة 09).

الطائفة الرابعة: الجرائم المرتبطة بحق المؤلف والحقوق المجاورة، وتشمل الجرائم التي تعد اعتداءا على المصنفات المحمية بحق المؤلف والحقوق المجاورة (المادة 10).[1]

[1]– محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 121 .

الطائفة الخامسة: المساهمة الجرمية والعقوبة، ويعالج هذا التفصيل الشروع والمساعدة والتحريض (المادة 11) ومسؤولية الأشخاص المعنوية (المادة 12)، ومعايير العقاب (المادة 13).

أما بالنسبة لجريمة الاحتيال فقد نصت عليه المادة (8) من الاتفاقية الأوروبية تحت عنوان الاحتيال المرتبط بالحاسوب حيث اعتبرت هذه المادة أن جريمة الاحتيال تقع عندما يقوم شخص عن قصد، ودون وجهة حق.

➢ الأحكام الإجرائية: نصت المواد من 14 حتى 21 من الاتفاقية الأوروبية على الأحكام الإجرائية لجرائم الحاسوب. وقد تضمنت هذه المواد إلزام كل طرف في هذه الاتفاقية بتهيئة تشريعه الداخلي لتقرير السلطات والإجراءات اللازمة في مجال التحقيق بالجرائم المنصوص عليها في الاتفاقية.

كما ألزمت هذه الاتفاقية الدول الأطراف عند سن تشريعاتها الداخلية المتعلقة بجرائم الحاسوب والانترنت أن تراعي الاتفاقيات الدولية لحقوق الإنسان مثل: الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية لعام 1950 والميثاق الدولي.[1]

أما فيما يتعلق بتفتيش وضبط البيانات المخزنة غي الحاسوب فقد أشارت المادة 19 من الاتفاقية على ضرورة أن يكون هناك نصوص تشريعية داخلية لدى الدول الأطراف.

- الاختصاص: أشارت المادة 22 من الاتفاقية إلى المعايير التي يجب على الدول الأطراف اعتمادها لتحرير الاختصاص القضائي حول الجرائم المقررة في هذه الاتفاقية المنصوص عليها في المواد من 2 إلى 11.

المطلب الثاني: التعاون القضائي.

فعالية التحقيق والملاحقة القضائية في الجرائم المتعلقة بالانترنت غالبا ما تقتض تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات المقدمة لتلك الخدمات حتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة

[1]– عمر يونس، الجرائم الناشئة عن استخدام الانترنت، الطبع الأولى، دار النهضة العربية، القاهرة، 2004، ص 89.

الاتصال بأجهزة الحاسب الآلي لتحديد مصدر الجريمة غالبا ما يتعين على أجهزة إنقاذ القانون الاعتماد على السجلات التاريخية التي تبين من أجريت تلك التوصيلات ومن أين ومن الذي أجراها.

الفرع الأول: ضرورة التعاون الأمني الدولي.

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من الأمن والنظام وتشكيل الجريمة إحدى القضايا الرسمية في الكير من دول وتشغيل إلى الحكومات والمختصين الأفراد على حد سواء ولقد أثبت الواقع العلمي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس المذهل في ميادين الحياة كافة فنتيجة هذا التطور في الاتصالات وتكنولوجيا المعلومات وظهور الانترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم المتعلقة بشبكة الانترنت ومي نوع من الجرائم[1] المعلوماتية التي باتت تشكل خطرا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحس بل تعدت إلى أمن البنى الأساسية الحرجة، ومع تمييزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي إذ يسمح بالاتصال المباشر بين أجهزة الشرطة وأجهزة شرطة دولة أخرى وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة فمن البديهي أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها لذا فإن التحقيقات في الجرائم المتعلقة بالحاسب الآلي وملاحقتها قضائيا تؤكد أهمية المساعدة القانونية المتبادلة بين الدول إذ يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود لأنها جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابعة لها بمعنى آخر أنه حتى ما فر المجرم خارج[2] حدود الدولة يقف جهاز الشرطي عاجزا. لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدولة المختلفة خاصة فيها.

---

[1]– أمير فرج يوسف، مكافحة الإرهاب الإلكتروني في ظل ثقافة دول مجلس التعاون لمكافحة الإرهاب، المرجع السابق، ص 258.

[2]– أمير فرج يوسف، المرجع نفسه، ص 258.

الفرع الثاني: جهود المنظمة الدولية للشرطة الجنائية (الأنتربول).

ترجع البدايات الأولية للتعاون الدولي الشرطي إلى عام 1904 عندما أبرمت الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض واليت نصت في مادتها الأولى على (تتعهد كل الحكومات المتعاقدة بإنشاء أو تعيين سلطة لجميع المعلومات الخاصة باستخدام الفتيات والنساء لغرض الدعارة في الخارج ولهذه السلطة الحق في أن تخاطب مباشرة لإدارة المماثلة لها في كل الدول الأطراف المتعاقدة). بعد ذلك أخذ التعاون الشرطي الدولي بأخذ صورة المؤشرات الدولية أولها وأسبقها تاريخيا كان مؤتمر موناكو 1914 والذي ضم رجال[1] الشرطة والقضاء والقانون من 14 دولة وذلك لوضع أسس التعاون الدولي ومناقشتها في بعض المسائل الشرطية لاسيما ما يتعلق بمدى إمكانية إنشاء مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين إلا أنه نتيجة لقيام الحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عملية تذكر وبنهاية عام 1923 نجح يوهانو سويرا مدير شرطة فينا في عقد مؤتمر دولي بعد الثاني على المستوى الدولي للشرطة الجنائية وذلك في 1923 ضم مندوبي 19 دولة وتمخض عنه ولادة اللجنة الدولية للشرطة الجنائية (ILPO) ويكون مقرها فينا وتعمل على التنسيق بين أجهزة الشرطة للتعاون في مكافحة الجريمة، إلا وانه باندلاع الحرب عام 1946 حيث عقد في بروكسل بلجيكا في 1946 مؤتمر دولي بهدف إحياء مبادئ التعاون الأمني ووضعها موضع التقيد بدعوى المفتش العام للشرطة البلجيكية.

وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة وقد مرت جهود المنظمة في هذا المجال بمراحل متعددة ونظرا لتنوع أنظمة الدول المختلفة كان هناك خيارات لأنظمة الاتصال داخل هذه الشبكة أولهما هو نموذج يخصص للدول المركزية وتجري الاتصالات العالمية للشرطة فيها من خلال الجمعية العامة واللجنة التنفيذية بوساطة السكرتارية العام والثاني للدول اللامركزية

[1]– أمير فرج يوسف، مكافحة الإرهاب الإلكتروني في ظل ثقافة دول مجلس التعاون لمكافحة الإرهاب، المرجع السابق، ص 259.

وتجري الاتصالات فيها مباشرة بين أجهزة الشرطة في الدول المختلفة وعلى غرار هذه المنظمة أنشأ المجلس الأوروبي في لكسمبورج عام 1991 شرطة أوروبية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة ولملاحقة الجناة في الجرائم العابرة للحدود منها بطبيعة الحال الجرائم المتعلقة بالانترنت أما على المستوى العربي نجد أن مجلس وزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية لتأمين التعاون بين أجهزة الشرطة في الدول الأعضاء وتنميته في مجال مكافحة الجريمة وملاحظة المجرمين في حدود القوانين والأنظمة المعمول بها دوليا.

الفرع الثالث: المساعدة القضائية.

الانترنت شبكة عالمية تمتاز بأنها دولية عابرة للحدود لا تعرف للحدود الجغرافية معنى وبالتالي فإن الجرائم المتصلة بها هي الأخرى عالمية وذات طابع دولي وأثرها يمتد لأكثر من دولة وتعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شانه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم وتتخذ المساعدة القضائية في المجال الجنائي صور عدة منها:

- **تبادل المعلومات:**[1]

وهو يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة مت عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم وقد يشمل التبادل السوابق القضائية للحياة. ولهذه الصورة المساعدة القضائية الدولية صدى كبير في كثير من الاتفاقيات كالبندين وزمن الفقرة (2) من المادة (1) من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية وهناك البند (أولا) من المادة (4) من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولية.

[1]– أمير فرج يوسف، مكافحة الإرهاب الإلكتروني في ظل ثقافة دول مجلس التعاون لمكافحة الإرهاب، المرجع السابق، ص 261 ص 262.

• **نقل الإجراءات:** ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة بالاتخاذ إجراءات جنائية وهي بصدد جريمة أو تكتب في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معنية من أهمها التجريم المزدوج ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات فضلا عن شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب غليها عن الجريمة نفسها وأيضا من الشروط الواجب توافرها أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان بحيث تؤدي دورا مهما في الوصول إلى الحقيقة[1] ولقد أقرت عدد من الاتفاقيات الدولية كمعاهدة الأمم المتحدة النموذجية واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، ومعاهدة مؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999.

• **الإنابة القضائية الدولية:** ويقصد بها طلب اتخاذ إجراءات قضائية من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك في الفصل في مسألة معروضة على الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى كسماع الشهود أو إجراء التفتيش وغيرها وعادة وكما هو معهود ترسل طلب الإجابة عبر القنوات الدبلوماسية.

يعد عامل السرعة في العوامل الرئيسية والمهمة في مكافحة الجرائم المتعلقة بالانترنت ولكون غالبية هذه الاتفاقيات صدرت في وقت لم تكن شبكة الانترنت قد ظهرت أو كانت موجودة ولكنها محدودة فإن تعديل هذه الاتفاقيات التقليدية المتعاون القضائي الدولي أصبح ضرورة ملحة لاسيما التطور الكبير في تكنولوجيا المعلومات والاتصالات لذلك أبرم عدد من الاتفاقيات الجديدة التي أسهمت في تقليل الوقت واختصار الإجراءات

[1]– أمير فرج يوسف، مكافحة الإرهاب الإلكتروني في ظل ثقافة دول مجلس التعاون لمكافحة الإرهاب، المرجع السابق، ص 263.

عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق مثال ذلك الاتفاقية الأمريكية الكندية التي تنص على تبادل المعلومات شفويا في حالة الاستعجال.[1]

المطلب الثالث: الأجهزة المختصة في متابعة الجريمة الإلكترونية في التشريع الجزائري والعربي.

وأنشئت بموجب القانون رقم 09- 04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المعدل والمتمم.[2]

حيث تعمل على تفعيل التعاون القضائي والأمني الدولي وإدارة تنسيق عمليات الوقاية ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية.

هناك حالات تسمح بمراقبة الاتصالات الإلكترونية لأغراض وقائية كالوقاية من جرائم الإرهاب والجرائم الماسة بأمن الدولة بإذن من النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة للتجديد.[3]

الفرع الأول: الهيئات القضائية الجزائية المتخصصة

- الأقطاب القضائية المتخصصة:

إنشاؤها: أنشئت بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية.[4]

تختص الجهات القضائية المختصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبق المواد 37- 329 – 40 قانون إجراءات جزائية.

---

[1]- أمير فرج يوسف، المرجع نفسه، ص 266.

[2]- سالم عبد الرزاق، ملتقى المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية بمحكمة سيدي محمد، ص 11.

[3]- القانون رقم 09- 04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المعدل والمتمم.

[4]- سالم عبد الرزاق، المرجع السابق، ص 12 ص 14.

اختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/06 المؤرخ في[1] 2006/1/5 إمكانية قيام اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام الاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09/04.[2]

الفرع الثاني: توسيع صلاحية الضبطية القضائية:

عند معاينة الجزائر الماسة بأنظمة المعالجة الآلية كما يمكن تمديد الاختصاص المحلي على كامل الإقليم الوطني المادة 1 قانون الإجراءات الجزائية.

- **أساليب التحري:** اعتراض المراسلات الإلكترونية المادة 65 مكرر من قانون إجراءات الجزائية، وبموجب القانون 06- 22 المؤرخ 2006/12/20 المعدل والمتمم.

- التسرب المادة 65 مكرر 11 القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.[3]

- تفتيش المنظومة المعلوماتية المادة 5 من القانون 09/ 04.

- حجز المعطيات المعلوماتية المادة 6 رقم 04/09.

- نسخ المعطيات على دعامة التخزين الإلكتروني.

- إمكانية منع الوصول إلى معطيات تحتويها المنظومة.

- منع الإطلاع على المعطيات التي يشكل محتواها جريمة.

---

[1]- المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/1/5

[2]– هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة، المعهد للأدلة الجنائية وعلم الإجرام، جامعة بسكرة كلية الحقوق، 2016، ص 3.

[3]- المادة 65 مكرر 11 القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

الفرع الثالث: المعهد الوطني للأدلة الجنائية وعلم الجرائم:

يتكون المعهد الوطني من إحدى عشرة دائرة متخصصة في مجالات مختلفة جميعها تتضمن إنجاز الخبرة، التكوين والتعليم تقديم المساعدة التقنية، تحليل وتقديم الدراسات في علم الجريمة، دائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة، تحليل وتقديم كل دليل رقمي وتماثلي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة، أفراد الدائرة يسهرون على تأمين اليقظة التكنولوجية من أجل تحسين المعارف، التقنيات والطرق المستعملة في مختلف الخبرات العلمية لإنجاز المهام المنوطة بها الدائرة إلى ثلاث مخابر: 1- مخبر الإعلام الآلي، 2- مخبر الفيديو، 3- مخبر الصوت.

الفرع الرابع: المديرية العامة للأمن الوطني والعربي:

1- جوانب التصدي للجريمة الإلكترونية: تصدت هذه المديرية للجريمة الإلكترونية من مختلف الجوانب منها: الجانب القانوني: والمتمثل في النصوص القانونية كقانون 22- 06 المؤرخ في 2006/02/10 والقانون 02- 06 والقانون 05/ 03 والقانون المدني، والقانون 04/ 09 المؤرخ في 2009/08/05.

الجانب التنظيمي: ويشتمل في التكوين المتواصل والتخصص والتكوين الأولي وتدعيم مخابر الشرطة، تدعيم المصالح الولائية للشرطة القضائية وتدعيم هيكلة مصالح الشرطة القضائية للتصدي للجريمة.[1]

الدول العربية:

- **مصر:** قامت أي جمهورية مصر العربية ببعض الجهات بمكافحة جرائم الانترنت، منها ما يعرف بالإدارة العامة للمباحث الأموال والإدارة العامة للتوثيق والمعلومات إلى جانب الأجهزة الحكومية، فقد تم تأسيس الجمعية المصرفية لمكافحة جرائم المعلوماتية والانترنت.

[1]- حملاوي عبد الرحمن، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجريمة الإلكترونية، جامعة محمد خيضر بسكرة، كلية الحقوق، 2016، ص 02.

- **الأردن:** قامت الأردن بإنشاء قسما خاصا بجرائم الحاسوب تابعا لمديرية الأمن ويختص بمختلف الجرائم للحاسوب والانترنت وفي عام 2006 تم تأسيس جمعية خاصة باسم "الجمعية الأردنية للحد من جرائم المعلوماتية والانترنت" مركزها عمان.

المبحث الثاني: دور المنظمات العالمية في مكافحة الإرهاب الإلكتروني.

تتقدم الأمم المتحدة قائمة المنظمات الدولية المعنية بمواجهة الإرهاب على اختلاف صنوفه[1] انبثقت منظمات عالمية أخرى أكثر تخصصا من أمثال (الإتحاد الدولي للاتصالات، والمنظمات العالمية للملكية الفكرية) لتكون سند الأمم المتحدة في مجال تخصصها الذي اتسع ليواجه المظاهر المستحدثة من الإرهاب الإلكتروني عبر الشبكة الدولية للمعلومات وهذا ما يستدعي تسليط الضوء على دور كل منها في مجال مكافحة الإرهاب وتناولت في هذا المبحث ثلاث مطالب المطلب الأول: دور المنظمات المتخصص في مكافحة الإرهاب الإلكتروني، المطلب الثاني: دور المنظمات الإقليمية في مجال مكافحة الإرهاب الإلكتروني، والمطلب الثالث: دور الأمم المتحدة في مكافحة الإرهاب.

المطلب الأول: دور المنظمات المتخصصة في مكافحة الإرهاب الإلكتروني.

ما يستدعي لتسليط الضوء على دور كل من مجال مكافحة الإرهاب وبما أن مكافحة الإرهاب لا يمكن دحره إلا بإتباع نهج شامل ومشاركة وتعاون فعليين من جانب كافة الدول والمنظمات الدولية في مكافحة الإرهاب الإلكتروني وتناولت فيه ثلاث فروع الفرع الأول الإتحاد الدولي للإتصالات.[2]
الفرع الثاني المنظمة العالمية للملكية الفكرية.

الفرع الأول: الإتحاد الدولي للاتصالات.

نشأ الإتحاد الدولي للاتصالات بمقتضى اتفاقية باريس عام 1865 تحت اسم (إتحاد التلغراف الدولي) قم عدل الاسم ليصبح (الإتحاد للاتصالات السلكية واللاسلكية)، وفي عام 1947 انظم الإتحاد إلى هيئة الأمم المتحدة وصار إحدى الوكالات المتخصصة في عمل الاتصالات المنضوية تحت مظلة الأمم المتحدة فأصبح بمثابة ملتقى دولي رئيس

[1]– كاظم مهدي النجار، الاتفاقيات الدولية ومكافحة الإرهاب، صحيفة النهار، بغداد، العدد 854، التاريخ: 24 آذار 2016.

[2]– خليل حسين، التنظيم الدولي، النظرية العامة والمنظمات العالمية، دون طبعة، دار المنهل اللبناني، بيروت، 2010، ص 394 ص 395.

لهذه الأنشطة، يضم في عضويته 482 عضوا من الشركات العلمية والصناعية العاملة بالقطاعيين العام والخاص، ومن المهام التي تضطلع من الإتحاد تعزيز التعاون الدولي للخدمات الهاتفية والسلكية واللاسلكية وتوسيع استخدامها بواسطة الجمهور وتطوير إمكانات الاتصالات السلكية واللاسلكية وتوزيع الموجات اللاسلكية، كما يقوم الإتحاد بتقديم التوصيات الخاصة والدراسات الفنية المتخصصة في الاتصالات اللاسلكية وجميع المعلومات ونشرها من أجل بناء قدرات الدول الأعضاء، ولاسيما البلدان النامية لتنسيق الاستراتيجيات الوطنية وحماية البنى التحتية للشبكات ضد المخاطر من خلال التوعية والتقييم الذاتي، وبناء القدرات وتوسيع المراقبة، والإنذار وقدرات الاستجابة للحوادث للدول والجهات المعنية. ويعمل الإتحاد بصورة وثيقة مع المنظمات الأخرى المعنية على وضع المعايير المتعلقة بالأمن المعلوماتي، إذ يقوم الإتحاد بالاشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصال كما تعاون الإتحاد الدولي مع مجلس أوروبا بإنجاز الاتفاقية الأوروبية حول الجريمة الإلكترونية من أجل الاستعانة بها في عملية وضع إطار قانوني دولي.[1]

وفي مسعى أكثر شمولا، ثم في المؤتمر الإقليمي حول الأمن الإلكتروني بالتعاون مع الإتحاد الدولي للاتصال في قطر في شباط من العام 2008 دعوى الدول لوضع وتنفيذ إطار وطني للأمن الإلكتروني وحماية البنية التحتية الحرجة للمعلومات والتي تعد بمثابة خطوة أولى في سبيل التصدي للتحديات التي تواجهها جراء اتصالها تكنولوجيا المعلومات والاتصال على صعيد آخر طالبت العالمية لمجتمع المعلومات في تونس في نوفمبر 2005 بأن ينسق الإتحاد الدولي للاتصالات آلية لبناء الثقة والأمن في مجال استخدام تكنولوجيا الاتصال والمعلومات عبر انطلاق برنامج الأمن الإلكتروني العالمي وهو إطار أعده الإتحاد الدولي للاتصالات بهدف اقتراح استراتيجيات للتواصل إلى حلول لتعزيز الثقة والأمن في مجتمع المعلومات، وتم لهذا الغرض تعيين فريق خبراء لإسداء المشورة

[1]– د. خليل حسين، مصدر سابق، ص 454 ص 455.

إلى الأمين العام للإتحاد بشأن المسائل المعقدة التي تكتنف موضوع الأمن السيبراني في خمسة مجالات هي الآتي:[1]

وفي مجال"التدابير التقنية والإجرامية" فيتم التركيز على التدابير الرئيسية الرامية إلى معالجة مواطن الضعف في منتجات البرمجيات، بما في ذلك خطط الاعتماد والبروتوكولات والمعايير وتضع "الهياكل التنظيمية" إطار العمل واستراتيجيات الاستجابة فيما يتعلق بمنع الهجمات السيبرانية وتتبعها والرد عليها وإدارة الأزمات المتعلقة بها. بما في ذلك حماية أنظمة البنية التحتية الحرجة للمعلومات.[2]

ويركز مجال بناء القدرات على وضع استراتيجيات لآليات بناء القدرات من أجل: زيادة الوعي، نقل الخبرة المتخصصة، تعزيز الأمن السيبراني في إطار برنامج السياسات العامة الوطنية.

ويهدف مجال "التعاون الدولي" إلى وضع إستراتيجية للتعاون والحوار والتنسيق على الصعيد الدولي في مجال التصدي للأخطار الإلكترونية.

الملاحظ مما تقدم انخراط الإتحاد الدولي للاتصالات في التفاصيل التقنية غير السياسية لمساعدة الدول والمنظمات والجهات المرتبطة بهذا الإتحاد في تهيئة وتطوير بنية المعلومات واستخداماتها المختلفة وتعزيز قدراتها في مجال أمن المعلومات لمواجهة الأخطار التي تخلفها محاولات إساءة استغلال هذه التقنيات من قبل بعض الجهات الإرهابية الدولية.

الفرع الثاني: المنظمة العالمية للملكية الفكرية.

في عام 1967 تم التوقيع في ستوكهولم في السويد على اتفاقية المنظمة العالمية للملكية الفكرية وأصبحت هذه المنظمة إحدى الوكالات المتخصصة التابعة للأمم المتحدة اعتبارا من السابع عشر من ديسمبر عام 1974 ومن أهدافها حماية الملكية الفكرية في

[1] - http//www.ituarabic.org/2008/c :p1doho.doha.déclaration

[2] – سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، دور المنظمات في مكافحة الإرهاب الإلكتروني، د ط، د د ن، د ب، د س، ص 26.

شتى أنحاء العالم عن طريق التعاون بين الدول الأعضاء والمنظمات الدولية الأخرى كما تعمل المنظمة على متابعة تنفيذ الاتفاقيات المتعلقة بالتصميمات الصناعية وتصنيف السلع التجارية وحماية الأعمال الإدارية والفنية وحقوق الإنتاج وتشجع المنظمة كذلك على توقيع معاهدات دولية جديدة والتنسيق بين التشريعات القومية والفنية للدول النامية بهدف حماية الملكية الفكرية وتنميتها وتغطية أوجه القصور في مجال التوثيق العلمي ونقل التقنية الحديثة.[1]

وبالرجوع إلى اتفاقية إنشاء هذه المنظمة تتضح غايات هذه المنظمة في دعم الملكية في جميع أنحاء العالم بجميع صورها (المصنفات الأدبية والفنية والعلمية والاختراعات) ومع تزايد الحاجة العالمية لحماية البرامج شكلت هذه المنظمة مجموعة عمل تضم عددا من الخبراء بهدف حماية برامج الحاسب الآلي وبعد سلسلة من الاجتماعات والدراسات حول الأساليب المثلى لحماية برامج الحاسوب ساد الاتجاه لدى أغلب الدول إلى الميل إلى خضوع برامج الحاسوب لقوانين حماية المؤلف وقد جاءت منظمة التجارة العالمية عام 1994 لتؤيد هذا التوجه وتستكمل طريقه من خلال إبرام الاتفاقية المتعلقة بمواصفات التجارة المرتبطة بحقوق الملكية الفكرية وما تفرضه من التزامات على الدول الأعضاء لفرض إجراءات تنفيذية وعقوبات جنائية لمواجهة أي اعتداء على حق المؤلف وخاصة القرصنة.

المطلب الثاني: دور المنظمات الإقليمية في مجال مكافحة الإرهاب الإلكتروني.

التحقت المنظمات الإقليمية بالجهود الدولية لمكافحة الإرهاب بعد الأمم المتحدة، وكان الإتحاد الأوروبي متصدرا في هذا الجانب بالنظر بالنضر لتقدم دولة في مجال تقنية المعلومات من جانب، ومشاركة هذه الدولة في الجهود الدولية الإرهاب تحت مظلة الأمم المتحدة مما جعلها هدفا للتنظيمات الإرهابية وكان التحاق سائر المنظمات الإقليمية متأخرة بهذه الجهود ولم يكن الإرهاب الإلكتروني في أجنداتها لمحدودية اعتمادها على الشبكة الدولية للمعلومات.[2]

[1]– طرق عزت رخا، المنظمات الدولية المعاصرة، دون طبعة، دار النهضة العربية، القاهرة، 2006، ص 214.

[2]– طارق عزت رخا، المرجع نفسه، ص 214.

الفرع الأول: جهود الجامعة العربية في مكافحة الإرهاب الإلكتروني.

عند مراجعة ميثاق جامعة الدول العربية بوصفه دستور هذه المنظمة، لا يمكن العثور فيه على ما يشير إلى الإرهاب وما يرتبط به من تفرعات[1] ومع ذلك فإن تأويل الدلالة العامة لبعض النصوص الواردة في هذا الميثاق، قد يخدم جهود مكافحة الإرهاب ومن ذلك ما جاء في المادة الثانية من الميثاق والتي أوضحت مقاصد هذه المنظمة في تحقيق التعاون بين الدول الأعضاء لصيانة استقلالها وسيادتها، والتي ستقاطع بالضرورة مع ما تنطوي عليه وسائل الإرهاب الإلكتروني من تجاوزات وإخلال لسلطة وسيادة الدول عبر التعرض لنظم المعلومات المرتبطة بالمؤسسات السيادية أو حتى إمكانية التحريض ضد النظام باستغلال وسائل التواصل الإلكتروني فضلا عن إمكانية استقلال المعلومات الحساسة وتوظيفها ضد مصالح الدولة العربية المستهدفة الأمر الذي يستدعي تعاون الدول العربية طبقا لهذه المادة لمواجهة مثل هذه الأنشطة الإرهابية عبر الفضاء الرقمي، وهو الاتجاه الذي أكدت الثالثة من الميثاق حينما خولت مجلس الجامعة، تقرير وسائل التعاون مع الهيئات الدولية التي قد تنشأ في المستقبل لكفالة الأمن والسلام، وإذا جاز اعتبار الاعتداء على نظم المعلومات التي تعتمدها المؤسسات الرسمية للدولة العربية ومحاولة تدميرها أو الإضرار بها وسرقة المعلومات أو حتى إشاعة الرعب والتحريض ضد النظام القائم التي تتم عبر آليات الإرهاب الإلكتروني من صور العدوان وفقا لقواعد القانون الدولي وميثاق الأمم المتحدة، فإن المادة السادسة من ميثاق الجامعة العربية قد أجازت الدول أو الدول التي وقع عليها أي اعتداء أو حتى خشي وقوعه، أن تطلب دعوة المجلس للانعقاد فورا ليقرر المجلس التدابير اللازمة لدفع هذا الاعتداء، ويصدر القرار بالاجتماع فإذا كان الاعتداء من إحدى دول الجامعة، لا يدخل في حساب الاجتماع رأي الدولة المعتدية، وبعيد عن أجواء الميثاق يلاحظ تأخر اهتمام جامعة الدول العربية على صعيد العمل الميداني حتى عام 1983 بدأت الجهود العربية المشتركة لمكافحة الإرهاب بالتواصل إلى الإستراتيجية الأمنية العربية التي أقرها مجلس وزراء الداخلية العرب والتي نصت على ضرورة الحفاظ على أمن الوطن العربي وحمايته من المحاولات العدوانية للإرهاب والتخريب الموجهة من الداخل والخارج، وفي إطار الخطة الأمنية العربية

[1]– سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، المرجع السابق، ص 30.

الأولى التي تشكلت لجنة الجرائم التي عرضت على مجلس وزراء الداخلية العرب في دورته السادسة بتاريخ: 1987/12/12 أصدرت قرار يقضي بتكليف الأمانة العامة لمجلس وزراء الداخلية العرب بإعداد مشروع إستراتيجية عربية لمكافحة الإرهاب بالتنسيق مع الأمانة العامة لجامعة الدول العربية.[1]

وفي مطلع 1988 أصدر مجلس وزراء الداخلية العرب قرارا ينص على تشكيل لجنة من ممثلي الدول العربية على مستوى الخبراء وبمشاركة الأمانة العامة لجامعة الدول العربية وأمانة مجلس وزراء الداخلية العرب لوضع تصور عربي لكيفية مواجهة ظاهرة الإرهاب، وبعد سلسلة من الاجتماعات التي عقدتها هذه اللجنة تم الانتهاء من الصياغة النهائية لمشروع الإستراتيجية العربية لمكافحة الإرهاب وإقرارها في الدورة الرابعة عشر لمجلس وزراء الداخلية العرب في 1997/01/05 أن قرار الاتفاقية العربية لمكافحة الإرهاب لم يتم إلا في اجتماعات الدورة الـــ 15 لمؤتمر وزراء الداخلية العرب في 5 يناير 1998، حيث تم وضع عدد من الآليات لتنفيذ هذه الإستراتيجية لمواجهة الإرهاب وقد تضمن مشروع الإستراتيجية العربية لمكافحة الإرهاب عددا من المنطلقات والأهداف والمقومات والآليات التي تحدد الأسس التي تقوم عليها سياسة مكافحة الإرهاب والسبل الكفيلة بتحقيق أقصى قدر من التعاون على الصعيد العربي والدولي لتطويق هذه الظاهرة والحد من الأخطار التي تشكلها على الدول المختلفة فاعتبرت أن الأعمال الإرهابية هي أعمال العنف منظم يسبب رعبا وفزعا، كما حدد هذه الإستراتيجية لكل دولة عدة إجراءات وتدابير للوقاية من الإرهاب يبرز في مقدمتها زيادة دعم الدولة للأسرة بما يكفل التربية السليمة للشيء والشباب، وتكثيف استخدام وسائل الإعلام المختلفة لتنمية الوعي الوطني القومي، مع حدث الدول اتخاذ تدابير فعالة وحازمة لمكافحة الإرهاب بمختلف صوره وأشكاله، بعد تحديث قوانينها وتشريعاتها الجنائية لتشديد العقوبات على مرتكبي الأعمال الإرهابية، وتجميد ومصادرة كافة الأموال الموجهة إلى هذه الأعمال وتشديد إجراءات المراقبة لمنع تسلل عناصر الإرهاب والتخريب أو تهريب الذخيرة والمتفجرات والسعي الحثيث للحيلولة دون اتخاذ أراض الدول العربية مسرحا لتخطيط وتنظيم أو تنفيذ أعمال إرهابية. كما تطرقت الإستراتيجية إلى موضوع تحديث وتطوير أجهزة الأمن من

[1]– سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، نفس المرجع، ص 31.

خلال دعمها بالمؤهلين وتوفير ما تحتاجه من معدات وتقنيات حديثة، وكذلك وضع خطط وقائية لمنع أي عمل إرهابي.[1]

وعلى صعيد التعاون العربي قد تضمنت الإستراتيجية عدة بنود أهمها تعزيز التعاون بين الدول الأعضاء لمنع ومكافحة الإرهاب وتقديم المساعدة المتبادلة في مجال إجراءات البحث الجنائي والتحري والقبض على الأشخاص الخارجين والمتهمين أو المحكوم عليهم في جرائم الإرهاب، كما أكدت الإستراتيجية على أهمية تبادل الخبراء والتقنيات الحديثة والمعلومات في مجال التعامل الأمني مع الجماعات الإرهابية ومواجهتها وتخص الأمانة العامة لمجلس وزراء الداخلية العرب بمتابعة مستجدات ظاهرة الإرهاب وسبل مكافحتها والتنسيق بين الدول العربية بهذا الشأن.

وفي المؤتمر العربي الثامن عشر مجلس وزراء الداخلية العرب بتونس 2015 أوصى المشاركون باتخاذ الوسائل اللازمة للحد من انتشار خطاب التطرف والطائفية، ودعا المؤتمر الدول الأعضاء إلى تبادل المعلومات بشأن المقاتلين الأجانب في بؤر التوتر في المنطقة العربية وتقاسم التجارب بشأن التعامل مع المقاتلين العائدين، ووافق المؤتمر على الخطة النموذجية لتعزيز الدور الإستخباري في الكشف عن المخططات الإرهابية.[2]

إن أبرز ما يمكن رصده من جهود على صعيد منظمة جامعة الدول العربية في مضمار التصدي لجرائم الإرهاب الإلكتروني وجرائم الحاسوب، اعتماد مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد كقانون نموذجي بموجب القرار رقم 229 لسنة 1996 الذي تضمن فصلا خاصا بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية مع النص بموجب المواد (461- 463) منه على وجوب حماية الحياة الخاصة وأسرار الأفراد في خطر المعالجة الآلية وكيفية جمع المعلومات أو عرقلة وإفساد نظام التشغيل أو تغيير المعلومات داخل النظام وتزوير وثائق المعالجة الآلية وسرقة المعومات من جانب آخر نجحت الجامعة العربية في إبرام الاتفاقية العربية لحماية حقوق المؤلف التي أوصى بها مؤتمر وزراء الثقافة المنعقد في بغداد عام 1981 التي

[1]- عماد علو، الجهود العربية المشتركة لمكافحة الإرهاب، صحيفة الزمان، لندن، العدد 5377، السبت 26 آذار، 2016، ص 32.

[2]- عماد علو، نفس المرجع، ص 33.

دعت إلى وضع التشريعات اللازمة لحماية الملكية الأدبية والفنية والعلمية والتي قد تكون هدف للإرهاب الرقمي إذا ما وجدت طريقها للنشر على الشبكة الدولية للمعلومات لذا ألزمت المادة الثالثة والعشرون من هذه الاتفاقية الدول الأعضاء العمل على: "إنشاء مؤسسات وطنية لحماية حقوق المؤلف ويحدد التشريع الوطني بنية هذه المؤسسات واختصاصاتها" ولضمان تحقيق بنود هذه الاتفاقية والتزام الدول الأعضاء بها فقد أنشئت المادة الرابعة والعشرون منها:" لجنة دائمة لحماية حقوق المؤلف من ممثلي الدول الأعضاء لمتابعة تنفيذ هذه الاتفاقية وتبادل المعلومات بما يكفل حماية المصالح المعنوية والمادية للمؤلفين.

الفرع الثاني: دور الإتحاد الأوروبي في مكافحة الإرهاب الإلكتروني.

مارس الإتحاد الأوروبي دورا مهما في مجال التصدي لجرائم الإرهاب الإلكتروني عبر إقراره العديد من التوصيات الخاصة لحماية البيانات ذات الصبغة الشخصية من سوء الاستخدام وحماية تدفق المعلومات، ففي عام 1981 وقعت اتفاقية تحت مظلة المجلس الأوروبي تتعلق بحماية الأشخاص في مواجهة المعالجة الإلكترونية للبيانات ذات الصبغة الشخصية، كما صدر عن المجلس الأوروبي العديد من القواعد التوجيهية في مجال[1] جرائم الحاسب الآلي تضمنت وجوب تجريم العديد من السلوكيات التي تعد من الجرائم كالغش المعلوماتي وسرقة الأسرار المخزنة وتضمنت هذه القواعد عددا من الإجراءات الفنية التي يتوجب اتخاذها لحماية نظم المعلومات من كل أشكال الانتهاك في عام 1980 جرى توقيع معاهدة مجلس أوروبا الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات ذات الطابع الشخصي والتي سرى مفعولها في أكتوبر عام 1985 وانطوت على توجيهات بصدد وجوب توفير قواعد تكفل حماية البيانات الشخصية من مظاهر المعالجة الآلية فضلا عن ذلك فقد صدرا عن مجلس أوروبا العديد من التوصيات لحماية البيانات الحوسبية.

ولاسيما التوصية بالرقم (R 81/1) بشأن تنظيم البيانات الطبية المعالجة آليا في بنوك المعلومات وكذا البيانات الخاصة بحماية البحوث العلمية، ولا يمكن التغاضي كذلك

[1]– سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، المرجع السابق، ص 29.

عن جهود السوق الأوروبية المشتركة في مجال إصدار القرارات[1] المعنية بحماية الفرد في مواجهة التطور التقني للمعلوماتية كما حصل في الأعوام 1979 و1982 وإذا كانت الحماية الأوروبية للبيانات الشخصية لم تتوج حتى الآن، إلا أنه صدر إرشاد أوروبي في 11 آذار عام 1996 يتعلق بالحماية القانونية لقواعد البيانات واعتبار برامج الكمبيوتر ضمن مجال المؤلفات الفكرية.

المطلب الثالث: دور الأمم المتحدة في مكافحة الإرهاب.

يعود اهتمام المجتمع الدولي بمشكلة الإرهاب إلى عام 1934، حيث تقدمت فرنسا بطلب إلى سكرتير عصبة الأمم، ودعت فيه إلى اتفاق دولي وذلك للمعاقبة على الجرائم التي ترتكب بغرض الإرهاب السياسي اثر مقتل الملك ألكسندر الأول ملك يوغسلافيا، تم قراره في عام 1937 تضمن تجريم الإرهاب الذي يتخذ صيغة الأفعال الإجرامية الموجهة ضد الدولة عندما تكون هدفها إحداث رعب لدى أشخاص أو جماعات معينة أو لدى الجمهور، ومنذ ذلك الحين بدأت المنظمة الدولية رحلتها في مكافحة الإرهاب.

الفرع الأول: الإرهاب الإلكتروني في ضوء ميثاق الأمم المتحدة.

تشكل مكافحة الإرهاب جزءا لا يتجزأ من ولاية الأمم المتحدة التي يجعل ميثاقها من صوت السلم والأمن الدولتين مقصدا رئيسا، ويوجب اتخاذ تدابير جماعية لمنع التهديدات للسلام ولقمع العدوان وتعزيز حقوق الإنسان والتنمية الاقتصادية ليظهر الإرهاب ضمن هذا المنحى بوصفه انتهاكا وتهديدا لشروط ومقتضيات إشاعة الأمن والسلام الدولتين، فضلا عن انتهاكه الواضح لحقوق الإنسان، والتسوية السلمية للمنازعات التي حرص الميثاق الأممي على تكريسها وتأمينها. وعلى الرغم من كون ميثاق الأمم المتحدة لم ينص صراحة على تجريم استخدام المعلومات كأداة إرهابية ضمن إطار ما يعرف بـــ (الإرهاب الإلكتروني) إلا أن روح الميثاق تتفق مع تجريم[2] استخدامه بوصفه انتهاكا لما ورد في الميثاق بخصوص التهديد أو استخدام حرب المعلومات يقعان ضمن

[1]– طارق عزت رجا، المرجع السابق، ص 214.

[2]– الدليل التشريعي النظام القانوني العالمي لمكافحة الإرهاب، إعداد مكتب الأمم المتحدة المعني بالمخدرات والجريمة (فينا) 2008.

العدوان والذي يعني بحمل وإرغام دولة على الإثبات بعمل معين. فإنه تطبق هنا قوة القانون، لاسيما وأن ميثاق الأمم المتحدة في مادته الثانية فقرة (03) قد أورد ما نصه "يخص جميع أعضاء الهيئة منازعتهم الدولية بالوسائل السليمة على وجه لا يجعل السلم والأمن والعدل الدولي عرضة للخطر، من ثم فإن التجاء الدول إلى تسوية منازعاتها وصراعاتها عبر الفضاء الإلكتروني، يعرض الأمن والسلم الدوليين للخطر، كما أن الإرهاب الإلكتروني وما يتضمنه من خروقات للسيادة الوطنية لأية دولة وأساليب للتجسس على المعلومات التي تهدد الأمن الوطني للبلدان، وتجنيد العملاء تناقض ما ورد من توجه أممي ضمن مقتضيات الفقرة الرابعة من المادة نفسها لميثاق الأمم المتحدة التي تنص على أنه "يتمتع أعضاء الهيئة جميعا في علاقاتهم الدولية من التهديدات باستعمال القوة أو استخدامها ضد سلامة الأرض أو الاستقلال السياسي لأية دولة أو على وجه آخر لا يتفق ومقاصد الأمم المتحدة. وعلى الرغم من كون الفقرة (08) من المادة الثانية نفسها تقول "ليس في هذا الميثاق ما يسوغ للأمم المتحدة أن تتدخل في الشؤون التي تكون من صميم السلطات الداخلي لدولة ما، وليس فيه ما يقتضي الأعضاء أن يعترضوا مثل هذه المسائل لأن تحل بحكم هذا الميثاق. فإن هذا المبدأ لا يخل بتطبيق تدابير القمع الواردة في الفصل السابع الذي يقع ضمن طائلة المادة (39) في المادة 39 في الفصل السابع من ميثاق الأمم المتحدة التي تنص على "يقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملا من أعمال العدوان".

الفرع الثاني: جهود الأمم المتحدة في مجال مكافحة الإرهاب الإلكتروني.

تحركت الأمم المتحدة لمقاومة خطر الإرهاب الدولي بخط تصاعدي يؤشر بوضوح تطور الوعي الدولي بمخاطر الإرهاب وتداعياته على الأمن والسلم العالمي ويمكن التمييز في هذا التحرك الأممي بين مرحلتين رئيسيتين: تمثلت المرحلة الأولى في مواجهة الإرهاب التقليدي بصورته المادية والدموية على أرض الواقع، وكان أكبر رصيد من الإنجازات حققته منظومة الأمم المتحدة في هذا المضمار يتمثل بوضع نظام معاهدات واتفاقيات دولية يتألف من ست عشرة اتفاقية دولية لمكافحة الأنشطة الإرهابية وتجريم الدول والكيانات التي تلجأ لاستخدامها وفي هذا السياق لم تكتف الأمم المتحدة بدعوة الدول إلى الالتحاق بهذه الاتفاقيات ومتابعة مدى التزامها بتنفيذ بنودها من جانب الدول الأعضاء

فحسب بل ذهبت إلى أبعد من ذلك على طريق ترصين البناء لقانوني لمكافحة الإرهاب، عبر تقديم المساعدة القانونية للبلدان بشأن تحري أفضل سبيل تنفيذ أحكام المعاهدات في إطار تشريعاتها الوطنية، لاسيما بعد أن اتخذ المجلس الاقتصادي والاجتماعي[1] التابع للأمم المتحدة توصية بأن تأخذ المنظمة على عاقها دورا رئيسا في رسم سياسة من الجريمة وتحقيق العدالة الجنائية دوليا، وقد تحقق ذلك بموافقة الجمعية العامة للأمم المتحدة في العام 1950، وتم إنشاء اللجنة الاستشارية لخبراء منع الجريمة التي تقع على عاتقها مهمة مكافحة الجريمة وتقديم المنشور للأمن العام وإيجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية في مجال منع الجريمة ومعاملة المجرمين.

ومن واقع قناعتها بأهمية التكامل بين البنى والأدوات القانونية من جهة الاستراتيجيات المطبقة على أرض الواقع لمواجهة خطر الإرهاب الدولي من جهة أخرى أصدرت الأمم المتحدة عبر جمعيتها العامة ومجلس الأمن فيها مجموعة من القرارات الدولية التي اعتمدت بموجب الصلاحيات الواردة في الفصل السابع من ميثاق الأمم المتحدة، والتي تضمنت التحذير من تزايد الأنشطة الإرهابية وتنوع صورها وفداحة نتائجها على الأمن الدوليين، وإدانة الأعمال الإرهابية بأقوى العبارات أيا كان دوافعها أو مرتكبوها بوصفها أعمالا إجرامية تهدد السلام والأمن الدوليين وتتنافى مع مقاصد ومبادئ ميثاق الأمم المتحدة مع التأكيد بأن الإرهاب لا يمكن دحره إلا بإتباع نهج شامل ينطوي على مشاركة وتعاون فعليين من جانب كافة الدول والمنظمات الدولية، ومضاعفة الجهود على الصعيدين الوطني والعالمي لنزع أسباب التطرف والإرهاب وتصفية العوامل والأجواء المساعدة عليه بالمقام الأول عبر الدعوى إلى تعزيز الحوار والتفاهم بين الحضارات لمنع استهداف العشوائي للأديان والثقافات أو ربطها بالإرهاب، ومعالجة الصراعات الإقليمية المتبقية دون حل والقضايا العالمية لإسهامها في تعزيز جهود المكافحة، مع التشديد على أهمية ور وسائط الإعلام والمجتمع المدني والديني والمؤسسات التعليمية في تعزيز الحوار وتوسيع آفاق التفاهم وتشجيع التسامح وتهيئة بيئة لا تقضي إلى

[1]- محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، دون طبعة، دار الثقافة للنشر والتوزيع، 2005، ص 253.

التحريض على الإرهاب، وبيان فاعلية تدابير احترام حقوق الإنسان والحريات الأساسية وسيادة القانون بوصفها عناصر أساسية في الوقاية من آفة الإرهاب والتطرف.[1]

وفي ضوء ما تقدم وجه مجلس الأمن دعوى إلى دول العالم لاتخاذ التدابير للتصدي للتحريض على ارتكاب أعمال إرهابية بدافع التطرف واستنكار المحاولات الرامية إلى تبرير أو تجميل الأعمال الإرهابية التي قد تحرض على ارتكاب المزيد من تلك الأعمال واستعمال جميع الوسائل القانونية لهذا المسعى وحرمان من يخططون لأعمال الإرهاب أو يمولونها أو يرتكبونها مع التأكيد على أهمية التعاون الدولي في مكافحة الإرهاب عبر الدعوة إلى الالتحاق وتنفيذ الاتفاقيات الدولية ذات الصلة للتنسيق فيما بين الدول لمنع وقمع أعمال الإرهاب.

الفرع الثالث: إجراءات وتدابير الأمم المتحدة لمكافحة الأعمال الإرهابية.

وتتمثل في الدعوة لأهمية الدول العالم واتخاذ الإجراءات والتدابير العملية الفعالة لمكافحة الأعمال الإرهابية وملاحقة ومحاسبة مقترفيها عبر إلزامها بالآتي:

1- الامتناع عن تقديم أي شكل من أشكال الدعم الصريح والضمني للكيانات الإرهابية تم وضع حد لعملية تجنيد أعضاء الجماعات الإرهابية ومنع تزويد الإرهابيين بالسلاح.

2- عدم توفير الملاذ لمن يمولون الأعمال الإرهابية أو يديرونها أو يرتكبونها، منع استخدام أراضي الدول في تنفيذ تلك المآرب، نص ضوابط مشددة على الحدود وعلى إصدار الأوراق الثبوتية ووثائق السفر.

3- تعزيز التدابير الرامية إلى كشف ووقف تدفق التمويل والأموال للأغراض الإرهابية.[2]

وضع الإرهابيين من استغلال الأنشطة الإجرامية الأخرى كـ (الاختطاف، والاتجار بالبشر والمخدرات والأسلحة) لتمويل أنشطتهم الإرهابية، وتجريم ومحاسبة كل من يمول الأعمال الإرهابية أو يدريها أو يدعمها أو يرتكبها أو يورد السلاح إليهم.

[1]- محمد أمين الشوابكة، جرائم الحاسوب والانترنت المعلوماتية، دون طبعة، دار الثقافة للنشر والتوزيع، عمان، 2009.
[2]- محمود أحمد عباينة، المرجع السابق، ص 156 ص 157.

4- تشجيع الدول على تبادل المعلومات على وجه السرعة مع الدول الأعضاء وتقديم تقارير إلى لجنة مكافحة الإرهاب حسب جدول زمني تحدده اللجنة بعد الإجابة عن كل أسئلتها واستفساراتها، وتزويد اللجنة بأسماء من يشاركوا من أفراد تلك الكيانات الإرهابية في تمويل أو دعم أعمال أو أنشطة القاعدة والتنظيمات الإرهابية بغية المساعدة في مواجهة الأنشطة الإرهابية وانتقال الإرهابيين إلزام الدول.

5- دعوة المنظمات الدولية لتعزيز التعاون مع الأمم المتحدة في نطاق ولايتها بهدف تطوير قدراتها على معاونة الدول الأعضاء في جهودها على التصدي لتهديدات الإرهابية. وأن تعمل مع لجنة مكافحة الإرهاب والمنظمات الدولية الأخرى من أجل تسهيل تبادل أفضل الممارسات في مجال مكافحة الإرهاب، مع عزم المجلس على عقد اجتماعات منظمة مع رؤساء هذه المنظمات لتحقيق هذه الغايات.[1]

ومع تزايد خطر الإرهاب الدولي وبروز وانتشار نوع جديد من الجريمة المرتبطة بالحاسوب الآلي بفعل تسارع وتيرة التطور التقني في أنظمة المعلومات والاتصالات وما أفرزه ذلك التهديد من أضرار ومخاطر على أمن البلدان والأفراد لاسيما بعد دخول الشبكة الدولية للمعلومات بوسائلها المتنوعة والمطورة على خط الإرهاب الدولي ومواجهة تزايدات الحاجة إلى تضافر الجهود الدولية وتعاضدها تحت مضلة المنظمات الدولية والإقليمية لمواجهة هذا التهديد، وكانت الأمم المتحدة المحفل العالمي الأهم لترجمة الجهود واستثمارها الأمثل في هذه المواجهة لما تتمتع به هذه الأخيرة من مصداقية في مجال تعزيز التعاون الدولي لتحقيق مقاصدها في ضمان الأمن والسلام الدوليين في مواجهة مختلف التهديدات العالمية بضمنها خطر الإرهاب الدولي فتزايد تبعا لذلك اهتمام الأمم المتحدة بهذا الخطر المتصاعد المتجدد بوسائله وشهدت مواجهة الإرهاب نقلة نوعية الحاسب الآلي والفضاء الرقمي.

[1]- عادل عبد الصادق، الأمم المتحدة ودعم الإستخدام السلمي للفضاء الإلكتروني، دوريات – قضايا إستراتيجية، 16 أوغسطس 2015 على الرابط: www.accroulin.com/printarticle.aspx!id=22762
-http://www.inorg/ar/terrorism.

الخاتمة

الخاتمة:

من خلال المتابعة المتأنية لهذا الموضوع والدراسة الدقيقة توصلنا لجملة من النتائج والتوصيات نجملها في النقاط التالية:

أولا: النتائج

✓يعد الحاسوب في ظل الإرهاب الإلكتروني الأداة والساحة الرئيسية لتحقيق النوايا الإجرامية للإرهابي على أرض الواقع، فيكون الإرهاب الإلكتروني تبعا لذلك صلة الوصل بين العالم الافتراضي والعالم المادي الذي يتحقق به التأثير المادي للمعلومات... الإرهاب الإلكتروني هو نتاج الثغرات القيمة ذاتها، مضافا إليها الثغرات في نظم المعلومات وبرامجها في طور ما بعد الحياة.

✓تصميم وإنشاء المواقع ذات الصبغة الإرهابية ينتشر انتشارا مذهلا، فقد أنشئت مواقع لتعليم صناعة المتفجرات وكيفية اختراق وتدمير المواقع وطرق اختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، وطريقة نشر الفيروسات وغير ذلك.

✓حجب المواقع الضارة والتي تدعو إلى الفساد والشر، ومنها المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق من الأساليب المجدية والنافعة لمكافحة الإرهاب الإلكتروني.

✓اعتماد الدول على وسائل الاتصالات وشبكات المعلومات في إدارة مؤسساتها وتقديم خدماتها المختلفة، قد ضخم الإرهاب الإلكتروني، وزاد على ذلك التطور المستمر والتنوع في وسائله وصعوبة تعقب القائم، أو حتى تحديد حجم الضرر الذي يخلفه.

✓تنوع وسائل الإرهاب الإلكتروني بدرجة كبيرة تبعا لقدرة ومهارة الإرهابيين، والهدف المنشود من الفعل الإرهابي، والجهة المستهدفة مثلما تتباين أهداف الإرهاب الإلكتروني بين مساحات مكانية وزمنية ونوعية مختلفة الحدود والأبعاد.

✓لا تزال الجهود المبذولة لدراسة وتنظيم ومتابعة الالتزام بتلك الأحكام في مراحلها الأولية، وما تم في هذا الشأن لا يتجاوز مجموعة من القرارات المنفصلة واللوائح الجزئية

التي لا تستوعب القضايا المستجدة في أعمال تقنية المعلومات كما لا توجد بصورة منظمة ومعلنة أقسام أمنية، وحاكم مختصة، ومنتجات إعلامية لشرائح المجتمع المختلفة.

✓مع تنامي خطر الإرهاب الإلكتروني وتجاوزه حدود الدول وقدرته المتنامية على تعويض سيادتها وتهديد أمنها، تزايدت الحاجة لتضافر الجهود الدولية في إطار المنظمات الدولية لمواجهة هذا التحدي واستئصاله.

✓يمكن تأشير التطور التدريجي في مستوى إدراك المنظمات الدولية لخطر الإرهاب وقدرتها على مواجهته مع تطور حجم التهديد الذي يفرضه هذا الأخير على الأمن والسلم الدوليين لاسيما بعد إفادته من معطيات الشبكة الدولية للمعلومات ومميزاتها لتنفيذ الأعمال الإرهابية، دون أن نرصد توجيها مستقلا من جانب تلك المنظمات لمواجهة الإرهاب الإلكتروني على سبيل الحصر والتخصص.

✓انتقلت جهود المنظمات الدولية التي تقدمتها منظمة الأمم المتحدة في مجال الإرهاب والتحذير غير المنتظم بنسق وإطار محدد إلى مرحلة التأطير القانوني ووضع إستراتيجيات لمواجهة هذا التهديد.

✓مما يزيد من تعقيد المشكلة غياب اتفاقية واضحة ومتخصصة على المستوى الدولي للتعامل مع ها التحدي الجديد أو حتى تنظيم استخدام الفضاء الإلكتروني.

ثانيا: التوصيات

- **على المستوى الدولي:**

✓أهمية تعزيز الجهود الدولية الرامية إلى مكافحة الإرهاب الإلكتروني وإساءة استعمال التكنولوجيا لأغراض إجرامية.

✓الاستفادة من الخبرة الدولية التي تتمتع بها الدول المتقدمة في مجال مكافحة الإرهاب الإلكتروني وإنشاء وحدات مشابهة ومراكز متخصصة.

✓تشجيع وتوفير المساعدة التقنية من خلاف الخبرة الفنية وتطوير مبادرات التعاون التقني من خلال تنظيم دورات تدريبية محلية إقليمية وعالمية.

✓الإسراع إلى إيجاد تعريف موحد لإرهاب بكافة تصنيفاته لتوحيد القوانين والتشريعات الدولية.

- **أما على المستوى العربي:**

✓ضرورة انضمام الدول العربية إلى الاتفاقيات العالمية الخاصة بالجرائم الإلكترونية وإنشاء وجدات مختصة لدى الدول العربية بالجرائم الإلكترونية.

✓ضرورة إنشاء وحدات إنذار مبكر للإبلاغ عن أي عملية اختراق تتعرض لها أي منظومة من المنظومات العربية الإلكترونية وزيادة الوعي والتدريب للقائمين على المنظومات الإلكترونية العربية.

✓السعي إلى إنشاء منظمة عربية لتنسيق أعمال مكافحة الإرهاب عبر الانترنت وتشجيع قيام اتحادات عربية تسعى للتصدي لجرائم الإرهاب عبر الانترنت.

✓تحديث القوانين العربية والمحلية الخاصة بالجرائم الإلكترونية والتشريعية الخاصة بالبيئة الإلكترونية.

قائمة المراجع والمصادر

قائمة المصادر:

القرآن الكريم

السنة النبوية الشريفة.

الدستور:

المادة 111 من الدستور الإماراتي

الاتفاقيات:

- ✓ اتفاقية جنيف لقمع الإرهاب لعام1937م.
- ✓ الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة لعام 1998م.
- ✓ اتفاقية بودابيست لعام 2001.
- ✓ المادة 2 من الاتفاقية الدولية للإجرام.

القانون

- ✓ المادة الأولى من الأمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم.
- ✓ الأمر رقم 11/95 المتضمن الجرائم الموصوفة بأفعال إرهابية، المؤرخ في 25 فبراير 1995 المتضمن قانون العقوبات المعدل والمتمم.
- ✓ القانون 15/04 المؤرخ في 2004/11/10 المتضمن قانون العقوبات المعدل والمتمم.
- ✓ المادة 394 مكرر 3 من قانون العقوبات.
- ✓ المادة 394 مكرر 2/2 من قانون العقوبات.

✓ القانون 04/09 المؤرخ في 5 غشت 2009 المتضمن قانون العقوبات المعدل والمتمم.

✓ القانون رقم 16/02 المؤرخ في 22 يونيو 2016 المتضمن تعديل قانون العقوبات، الجريدة الرسمية، العدد 37، 2016.

✓ المادة 87 مكرر 11 من قانون العقوبات.

✓ المادة 87 مكرر 11 ومكرر 12 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية.

✓ المادة 65 مكرر 11 القانون رقم 14/04 المؤرخ في 10 نوفمبر سنة 2004 المتضمن قانون الإجراءات الجدزائية.

✓ المادة 20 من القانون الإتحادي الإماراتي لمكافحة جرائم تقنية المعلومات رقم 2 لسنة 2006.

✓ المادة 147 من قانون العقوبات السويسري، المتضمن الإحتيال المعلوماتي.

المراسيم التشريعية:

✓ المرسوم التشريعي 92-03 المؤرخ في 1992/09/30.

✓ المرسوم التشريعي 05 لسنة 2012، بشأن جرائم تقنية المعلومات.

✓ الدليل التشريعي النظام القانوني العالمي لمكافحة الإرهاب، إعداد مكتب الأمم المتحدة المعني بالمخدرات والجريمة (فينا) 2008.

قائمة المراجع:

المؤلفات بالغة العربية:

- ✓ أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية، والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2011.
- ✓ أمير فرج يوسف، مكافحة الإرهاب الإلكتروني في ظل ثقافة دول مجلس التعاون لمكافحة الإرهاب،د ط، دار الكتب والدراسات العربية الإسكندرية– مصر، 2011.
- ✓ أنظر عبد الرحيم صدق، الإرهاب السياسي والقانون الجنائي، دار النهضة العربية،القاهرة،1985م.
- ✓ حارث سليمان الفاروقي، المعجم القانوني، ط5، بيروت، مكتبة لبنان، 2003.
- ✓ خليل حسين، التنظيم الدولي، النظرية العامة والمنظمات العالمية، دون طبعة، دار المنهل اللبناني، 2010، بيروت.
- ✓ ذياب موسى البدانية، الانترنت والإرهاب، الإرهاب المعلوماتي، دون طبعة، القاهرة، 2008.
- ✓ رائد العدوان، توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، المعالجة الدولية لقضايا الإرهاب الإلكتروني، دون طبعة، الرياض، 2013.
- ✓ ريتشارد كلارك وروبرت نيك، حرب القضاء الالكتروني/التهديد الآلي للأمن القومي وكيفية التعامل معه، مركز الإمارات للدراسات الإستراتيجية، الإمارات العربية المتحدة، 2012.
- ✓ سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، دور المنظمات في مكافحة الإرهاب الإلكتروني، د ط، د د ن، د ب، د س.
- ✓ سايمون لوكن، التجارة عبر الانترنت، ترجمة يحي ديت الأفكار الدولية، نيويورك، 1999م.
- ✓ طارق عزت رخا، المنظمات الدولية المعاصرة، دون طبعة، دار النهضة العربية، القاهرة، 2006.

- ✓ عادل عبد الصادق، هل يمثل الإرهاب شكل جديد من أشكال الصراع الدولي، ملف الأهرام الإستراتيجي، مركز الأهرام للدراسات السياسية الإستراتيجية، أكتوبر، 2010.
- ✓ عفيفي كامل عفيفي، جرائم الكمبيوتر وتعرف المؤلف والمصنفات ودور الشرطة والقانون: دراسة مقارنة. دون طبعة، منشاة المعارف، الإسكندرية، دون سنة.
- ✓ عمر يونس، الجرائم الناشئة عن استخدام الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004.
- ✓ قورة نائلة، جرائم الحاسب الاقتصادية، دون طبعة، القاهرة: دار النهضة العربية،2004 .
- ✓ محسن الحيدري، الإرهاب والعنف في ضوء القران والسنة والتاريخ والفقه المقارن.دون طبعة، دار الولاء، بيروت، 2010م.
- ✓ محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دون طبعة، دار المطبوعات الجامعية،2003، الإسكندرية–مصر.
- ✓ محمد أمين الشوابكة، جرائم الحاسوب والانترنت المعلوماتية، دون طبعة، دار الثقافة للنشر والتوزيع، عمان، 2009.
- ✓ محمد طارق عبد الرءوف الخن، جريمة الاحتيال عبر الانترنت، الأحكام الموضوعية والأحكام الإجرائية، الطبعة الأولى. منشورات الحلبي الحقوقية، بيروت–لبنان،2011.
- ✓ محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، دون طبعة، دار الثقافة للنشر والتوزيع، 2005
- ✓ مصطفى محمد موسى، الإرهاب الالكتروني: cyber terrorism دراسة قانونية أمنية –نفسية –اجتماعية. الطبعة الأولى، مصر: دار الكتب، الوثائق القومية المصرية، 2009.
- ✓ ممدوح الشيخ، التجسس التكنولوجي سرقة الأسرار الاقتصادية والتقنية، دون طبعة، مكتبة بيروت، سلطنة عمان، 2008.
- ✓ نهلا عبد القادر المومني، الجرائم المعلوماتية، دون طبعة، ددن، عمان،2008 .
- ✓ نوفل علي عبد الله الصفو، جريمة إنشاء معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات دراسة مقارنة، دون طبعة، جامعة الموصل كلية الحقوق، العراق، دون سنة.

المؤلفات باللغة الأجنبية:

✓ tanje grunnon, cyberterrorisme hovedoppgrave istatsvitenskop, universitete ioslo intitut for statsvi tenskap, varen, 2007.

المداخلات:

✓ حملاوي عبد الرحمن، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجريمة الإلكترونية، جامعة محمد خيضر بسكرة، كلية الحقوق، 2016.

✓ سالم عبد الرزاق، ملتقى المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية بمحكمة سيدي محمد.

✓ 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 من 2الى 4يونيو2008م.

✓ هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة، المعهد للأدلة الجنائية وعلم الإجرام، جامعة بسكرة كلية الحقوق، 2016.

الأطروحات والمذكرات الجامعية:

✓ بعزة سعيدة، الجريمة الإلكترونية في التشريع الجزائري دراسة مقارنة، مذكرة مكملة نيل شهادة الماستر حقوق، 2015- 2016.

✓ حمزة بن عقون، السلوك الإجرامي للهجوم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، باتنة: جامعة الحاج لاخضر، 2011-2012.

✓ سراب تامر احمد، الهجمات على شبكات لحاسوب في القانون الدولي الإنساني، أطروحة الدكتوراه، جامعة النهرين، 2014.

التقارير:

✓ تقرير اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة الحادي والثلاثين، 2011.

الانترنت:

✓بن يحي، الطاهر ناعوس، مكافحة الإرهاب الالكتروني ضرورة بشرية وفريضة شرعية http://aloukah.met

✓ عادل عبد الصادق، الأمم المتحدة ودعم الإستخدام السلمي للفضاء الإلكتروني، دوريات – قضايا إستراتيجية، 16 أوغسطس 2015 على الرابط:
www.accroulin.com/printarticle.aspx!id=22762

✓علي مطر، الإرهاب الالكتروني في القانون الدولي، مقال منشور على موقع الشبكة الالكترونية بتاريخ 4 نوفمبر 2013 على الرابط:
hhp://www.assakim.com/about.php

✓ معتز محي الدين، الإرهاب وتكنولوجيا المعلومات، مقال منشور على مواقع مدارك الالكتروني، على الرابط.21: d/! www.net neus delacls.help .

✓ http//www.ituarabic.org/2008/c :p1doho.doha.déclaration

✓ http://www.inorg/ar/terrorism.

المقالات العلمية:

✓ الإرهاب والجرائم المعلوماتية، مجلة معلومات، المركز العربي للمعلومات، بيروت، تموز، 2010، العدد 80.

✓ هوزة المزوعي، الاختراقات الالكترونية خطر كيف نواجهه، مجلة أفاق اقتصاد دولة الإمارات العربية المتحدة، العدد التاسع، سبتمبر 2000م.

✓ كاظم مهدي النجار، الاتفاقيات الدولية ومكافحة الإرهاب، صحيفة النهار، بغداد، العدد 854، التاريخ: 24 آذار 2016.

✓ عماد علو، الجهود العربية المشتركة لمكافحة الإرهاب، صحيفة الزمان، لندن، العدد 5377، السبت 26 آذار، 2016.

الفهرس

الفهرس