جرائم الإرهاب عبر الوسائل الإلكترونية
« دراسة مقارنة »

د . ياسـر فيصل أميـن
عضو الجمعية المصرية للاقتصاد السياسي والتشريع

مقدمة

خير بداية على الدوام هي البدء بحمد الله على نعمته التي لا تحصى وفضله الذي لا يعد، والصلاة والسلام على أشرف المرسلين سيدنا ونبينا محمد بن عبدالله النبي الكريم وعلى آله و صحبه وسلم أجمعين فقد استعنت في بحثي هذا بالله عز وجل ليوفقني إلى خير العمل، ومن ثم فإنني أتناول في المقدمة العديد من المؤشرات البحثية المهمة التي تعرفنا بأوصاف البحث كمقدمة البحث وأهميته العلمية والهدف منه وإشكاليته ومنهجه ثم خطة البحث ، وبذلك أكون قد أعطيت فكرة موجزة عن موضوع البحث قبل الدخول والتعمق في موضوعاته الأساسية.

واكب ثورة تكنولوجيا المعلومات والاتصالات والتوسع في استخدام شبكة المعلومات الدولية (الإنترنت) تطوراً كبيراً في وسائل ارتكاب الجرائم . حيث ظهرت نوعية جديدة من الجرائم المستحدثة يتم ارتكابها من خلال استخدام التقنيات الحديثة والحاسبات الآلية عن طريق شبكة الإنترنت، أطلق عليها الجرائم المعلوماتية أو الجرائم الإلكترونية، ولقد أصبحت هذه الجرائم تهدد أمن وسلامة الأفراد والمؤسسات، فالمعلومات تتزايد يوماً بعد يوم، ولا تتناقص بالاستخدام أو تستهلك ، وتعتبر المعلومات مصدر قوة اقتصادية وسياسية وعسكرية واجتماعية، ومع تزايد المعلومات واستخدام الشبكة في تبادلها وكذا أعمال التجارة الإلكترونية وغيرها من الأنشطة، سوف تتزايد صور الاعتداءات والتهديدات وظهور العديد من أنماط القضايا المختلفة، وهو الأمر الذي تطلب ضرورة التصدي لهذه الطائفة من الجرائم بالشكل الذي يحقق فاعلية في مواجهتها[1].

1 http://www.child-trafficking.info/default.aspx Mokadema 3n elgraem elmosthdasa .pdf. Mokadema 3n elgraem elmosthdasa.pdf.

فإذا كان للوسائل الإلكترونية الحديثة العديد من الفوائد ، فإن الوجه الآخر المتمثل في الاستخدامات السيئة والضارة لهذه التقنيات الحديثة ومنها الإرهاب الإلكتروني أصبح خطراً يهدد العالم بأسره . إن خطر الإرهاب الإلكتروني يكمن في سهولة استخدام هذا السلاح مع شدة أثره وضرره ، فيقوم مستخدمه بعمله الإرهابي وهو في منزله، أو مكتبه، أو في مقهى أو حتى من غرفته في احدى الفنادق ، ولقد أصبح الإرهاب الإلكتروني هاجساً يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أى مكان في العالم[١] .

وبذلك فإن النشاط الإرهابي انتقل من المجال المادي الواقعي إلي الفضاء الإلكتروني ويعتمد الإرهاب الإلكتروني (cyber terrorism) على بعدين مهمين:

البعد الأول : في أن يصبح عاملاً مساعداً للعمل الإرهابي التقليدي المادي بتوافر المعلومات عن الأماكن المستهدفة أو كوسيلة في تنفيذ العملية الإرهابية.

أما البعد الثاني: فيمكن القول بأنه بُعد معنوي يرمي إلي التحريض على بث الكراهية الدينية وحرب الأفكار.

وتستهدف المنظمات والجماعات الإرهابية من وراء استخدام الإنترنت إلي تضخيم الصورة الذهنية لقوة وحجم تلك المنظمات أو الجماعات بما يخدم الجانب الإعلامي العسكري لهذه الجماعات، حيث أصبحت تلك الجماعات لا يهمها كم من الناس قد قتل بقدر ما يهمها كم من الناس شاهدو وتفاعلو مع الحادثة الإرهابية.

كما تسعى هذه المنظمات إلي الاستفادة من الإنترنت واستثماره في التنقيب عن المعلومات، والحصول على التمويل والتبرعات وعملية التجنيد والحشد لأتباعها، وكذلك تحقيق الترابط التنظيمي بين الجماعات وداخلها وتبادل المعلومات والأفكار والمقترحات والمعلومات الميدانية حول كيفية إصابة الهدف واختراقه وكيفية صنع المتفجرات والتخطيط والتنسيق للعمل الإرهابي[٢] ، وكذلك في تدمير مواقع الإنترنت المضادة أو اختراق مؤسسات حيوية أو تعطيل الخدمات الحكومية الإلكترونية أو محطات الطاقة.

١ د. على سالم محمد: جرائم الارهاب الالكتروني ، قسم القانون الجنائي ، الجامعة الخليجية. ٢٠١٠، الناشر الجامعة الخليجية قسم القانون ، ص ٢٨٦، ص ٣٢٠. بحث منشور على الانترنت.

www.platform.almanhal.com / article / article detail.

٢ د. ايسر محمد عطية القيس: بحث بعنوان ، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، الملتقي العلمي ، الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية. منشور بالانترنت. الاردن ـ ٢٠١٤ . www.assakina.com

أهمية البحث:

إن الإرهاب في الماضي كان يعتمد على قيام بعض الإرهابيين بقتل آمنين أو تفجير قنبلة في مكان ما، أو خطف طائرة، أو اغتيال شخصية تتناقض أفكاره مع أفكار الإرهابيين، وما إلى ذلك من صور الإجرام والاعتداء على الأنفس والأموال المعصومة التي تبنتها جماعات إرهابية ، كجماعة الجهاد الإسلامي وتنظيم القاعدة وجماعة التكفير والهجرة وداعش وشبهها.[١]

إلا أنه مع التقدم التقني الإلكتروني وعقب الطفرة الكبيرة التي حققتها تكنولوجيا المعلومات واستخدام الحواسب الآلية والإنترنت ظهر استخدام « الإرهاب الالكتروني » الذي يعد من أخطر أنواع الجرائم التي ترتكب عبر شبكة الإنترنت ، ويتضح هذا عن طريق النظر إلى فداحة الخسائر التي يمكن ان تسببها عملية إرهابية واحدة تندرج تحت مفهومه ، ويرجع ذلك إلى انتشار التقنية وتطبيقاتها المختلفة ورخص ثمنها وسهولة الحصول عليها والقدرة على تستر الإرهابيين عن طريق استخدامهم لهذه التقنية خلف أسماء وألقاب وهمية.[٢]

فالإرهاب الإلكتروني يعتمد على استخدام الإمكانات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الآمنين وإلحاق الضرر بهم ، أو تهديدهم بما يضرهم ومن أشهر وسائل الإرهاب الإلكتروني وسيلتان الأول ى: ممارسة الأعمال التخريبية لشبكات الحاسوب والإنترنت، والثانية : استخدام وسائل التواصل الاجتماعي الذي يوفرها الإنترنت التي أصبحت منبراً للجماعات والأفراد لنشر رسائل الإرهاب والعنف والغلو والاتصال ببعضهم البعض ومؤيديهم والمتعاطفين معهم.[٣]

إن الخطورة الإجرامية لجرائم الإرهاب الإلكتروني تتمثل في استخدام الأنظمة والشبكات المعلوماتية في تدمير البنية التحتية المعلوماتية التي تتمدد عليها الحكومات والمؤسسات العامة والشركات الاقتصادية الكبرى، كما حدث في كثير من دول العالم فالإرهاب الالكتروني يعد خطراً يهدد العالم بأسره ، ويكمن الخطر في

١ سامي على حامد عياد : استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، دار الفكر - الإسكندرية. ٢٠٠٨. ص ٧٣.

٢ د. عارف عيد: جرائم الإنترنت ، مجلة جامعة الشارقة للعلوم الشرعية والقانونية المجلد العدد ٣ أكتوبر ٢٠٠٨ ، ص٧٣.

٣ منير محمد الجهيني ، ممدوح محمد الجهيني: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها. دار الطباعة الجامعي. الإسكندرية. ٢٠٠٦ ص٧٥.

سهولة استخدام هذا السلاح الرقمي مع شدة أثره وضرره ، حيث يقوم مستخدمه بعيدا عن أنظار السلطة والمجتمع.[١]

لذلك فإن خطورة جرائم الإرهاب الالكتروني تزداد كلما ازداد استخدام الحواسب الآلية ، وكلما اتسع استخدام الشبكات المعلوماتية ، فبدلاً من استخدام المتفجرات تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية وتحقيق آثار تدميرية تفوق مثيلتها المستخدم فيها المتفجرات.

كما أن جرائم الإرهاب الالكتروني قد يكون لها مخاطر كبيرة على التنمية الاقتصادية ، وذلك حينما توجه هجمات الإرهاب الالكتروني إلى الأهداف الاقتصادية بالدولة.

حيث إنه أصبح يتم الاعتماد على شبكات الكمبيوتر بصفة مطلقة في عالم المال والأعمال ؛ مما يجعل هذه الشبكات نظراً لطبيعتها المترابطة وانفتاحها على العالم هدفاً مقرباً للعابثين وعصابات الجريمة المنظمة لسرقة البنوك والحسابات الشخصية وشبكات غسيل الأموال والفكرة ، ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل كبير بالانطباعات السائدة والتوقعات، والتشكيك في صحة المعلومات أو تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة وإضعاف الثقة في النظام الاقتصادي.[٢]

لذلك فإن الهجمات الالكترونية التي تتم ضد نظم المعلومات الاقتصادية يمكن أن يكون لها آثار سيئة للغاية مدمرة لكافة النواحي الاقتصادية ؛ مما يؤثر على الفرد والمجتمع من حيث عدم تحقيق التنمية الاقتصادية.

كما قد تتمثل جرائم الإرهاب الالكتروني في تدمير البنية التحتية المرتبطة والمدارة من خلال الحاسب الآلي وشبكة المعلومات كشبكات توزيع الكهرباء والمياه وأنظمة الخدمات المصرفية والسجلات الصحية وغيرها من البنية التحتية التي من شأن تدميرها أن يحدث أضراراً مباشرة وغير مباشرة بأفراد المجتمع.

كذلك فإن جرائم الإرهاب الالكتروني والتهديدات الموجهة لأجهزة الحاسب الآلي والشبكات الالكترونية والمعلوماتية الموجودة عليها قد يكون الهدف منها إجبار

١ رائد العدوان ، المعالجة الدولية لقضايا الإرهاب الالكتروني دورة تدريبية بعنوان توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب ٢٠١٢ صـ٢٥.

٢ سامي علي حامد عيد ، مرجع سابق ، ص ٢٥ .

الحكومات والمجتمعات على أفعال معينة لأغراض سياسية أو اجتماعية ؛ ذلك لأن الاستقرار السياسي والأمني يعد أحد أهم مقومات التنمية الاقتصادية.

وحيث إن هذه الجرائم لا يوجد لها نوع تقليدي ، بل تتطور بتطور تقنية المعلومات ، ونظراً للازدياد الملحوظ لهذه الجرائم وقلة التشريعات اللازمة لمواجهة الآثار السلبية الناجمة عن هذا التطور في ارتكاب الجرائم الالكترونية التي تؤثر على الدخل القومي والإنفاق العام وتنمية الفرد والمجتمع اقتصاديا.

فإن الأمر يتطلب ضرورة إيجاد حماية جنائية في التعاملات الالكترونية وتجريم أفعال الإرهاب الالكتروني التي تؤثر على الأفراد والمجتمع والتنمية الاقتصادية.

لذلك فإن موضوع هذه الدراسة له أهمية نظرية وعملية ؛ لكونه يمس كثيراً من مصالح المجتمع، كما تظهر أهميته في تحديد مصادر المخاطر التي تهدد النظام الالكتروني ونظم الشبكات وتحديد صور الاعتداء على المعلومات والأنماط المستجدة للجرائم الالكترونية.

أهداف البحث:

تسعى هذه الدراسة إلى محاو لة اكتشاف وتحديد معالم الظاهرة الإرهابية المستحدثة التي تعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصالات وشبكات المعلومات ، وذلك من حيث تحديد مفهوم هذه الجريمة الإرهابية المستحدثة ، وتحديد الأفعال المادية غير المشروعة لجرائم الإرهاب الالكتروني وهناك نوعان من الأفعال:

- النوع الأول : يستخدم أفعاله الإرهابية ضمن الشبكة الالكترونية عن طريق الكمبيوتر.
- النوع الثاني: كل الأفعال التي تخص الإرهاب الالكتروني مثل الإشاعات والتنظيم والتنسيق من خلال الفضاء الالكتروني.

كما تهدف هذه الدراسة إلى إلقاء الضوء على جريمة الإرهاب باستخدام الوسائل الإلكترونية وكيفية التعامل معها شكلاً وموضوعاً وتحديد المسؤولية الجنائية الناشئة عن الجرائم المرتكبة بالوسائل الالكترونية وكيفية إثباتها ، وضرورة إيجاد إجراءات جنائية عند التحقيق في هذه الجرائم تتفق مع طبيعتها.

منهج البحث:

تتنأو ل هذه الدراسة جرائم الإرهاب التي ترتكب عبر الوسائل الإلكترونية ، وذلك باستخدام المنهج الوصفي التحليلي والمنهج المقارن من خلال شرح وتحليل ووصف الجريمة ؛ بغرض الوصول إلي الضوابط الصحيحة للمسئولية الجنائية الناشئة عن جرائم الإرهاب باستخدام الوسائل الالكترونية ، بحيث لا تقوم هذه المسؤولية إلا بتوافر العلم والإرادة، وكذلك من خلال التشريعات المقارنة المتعلقة بالجرائم الإلكترونية .

إشكالية البحث:

خطورة هذه الظاهرة الإجرامية المستحدثة أنها تثير العديد من الأسئلة القانونية ؛إذ أن الجريمة يسهل ارتكابها على هذه الأجهزة أو بواسطتها، وأن تنفيذها لا يستغرق غالباً إلا دقائق معدودة ، بل وفي أحيان كثيرة تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالبا ما يلجأ إليه الجاني عقب ارتكابه للجريمة، فضلا عن أن مرتكبي هذه الجرائم، وبالذات في مجال الجريمة المنظمة يلجأو ن إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية في أنظمة الكترونية مع استخدام شفرات أو رموزسرية لإخفائها عن أعين أجهزة العدالة، مما يثير مشكلات كبيرة في جمع الأدلة الجنائية وإثبات هذه الجرائم قبلهم.

كما تثور إشكالية أخري تتعلق بمدي كفاية النصوص الواردة بالقواعد التقليدية في التشريع الجنائي لمواجهة المشكلات الناجمة عن جرائم الإرهاب الإلكتروني، حيث إن الجريمة المعلوماتية لها طبيعتها الخاصة التي تختلف عن الجرائم التقليدية في أنه يسهل ارتكابها على الأجهزة الإلكترونية أو بواسطتها، وهذه الطبيعة الخاصة ، تعني أن الإجراءات الجنائية التقليدية لا تتناسب بالقدر الكافي لمكافحة هذه الجرائم ، وتثير مشكلات كبيرة في مجال إجراءات تحقيق الدعوى الجنائية ، ومنها : صعوبة التحري والتفتيش والضبط وجمع الأدلة الجنائية وإثبات هذه الجرائم ، وهذا يتطلب صدور قوانين إجرائية خاصة بهذه الجرائم تعالج مشكلات التفتيش والتحقيق والاختصاص القضائي تتواكب مع طبيعة هذه الجرائم.

وفي ضوء ما تقدم فإن خطة الدراسة ستكون علي النحو الآتي :-

مبحث تمهيدي : ماهية الإرهاب باستخدام الوسائل الالكترونية .

الفصل الأول : المسؤولية الجنائية الناشئة عن جرائم الإرهاب الإلكتروني .

المبحث الأول :المسؤولية الجنائية عن الأفعال المادية في جرائم الإرهاب الإلكتروني.

المبحث الثاني: جوهر المسؤولية الجنائية العمدية الناشئة عن جرائم الإرهاب الإلكتروني.

الفصل الثاني: الإجراءات الجنائية لجريمة الإرهاب باستخدام الوسائل الالكترونية .

المبحث الأول :إجراءات التحقيق الابتدائي في جرائم الإرهاب عبر الوسائل الالكترونية.

المبحث الثاني : معوقات التحقيق في الجرائم الالكترونية .

الخاتمة .

مراجع البحث .

مبحث تمهيدي

ماهية الإرهاب باستخدام الوسائل الالكترونية

تمهيد وتقسيم:

تعتمد التنظيمات الإرهابية على إتباع وسائل لتحقيق أهدافها وغاياتها، وقد تستخدم هذه الجماعات الوسائل التقليدية كالاغتيال والضرب، أو تستخدم الوسائل العلمية والتقنية، وتقوم باستغلال وسائل الاتصالات وشبكة المعلومات.

لقد ساعد التطور العلمي التكنولوجي علي ازدياد العمليات الإرهابية، فالثورات العلمية والتكنولوجية هيأت المجال الخصب لإحداث تغيرات متنوعة على كافة المستويات وفي كافة المجالات ، كما ساعد في ارتكاب الجرائم الإرهابية الطبيعة الخاصة لجرائم التقنية الحديثة ، واختلافها عن الجرائم التقليدية في سهولة ارتكابها علي الأجهزة الإلكترونية أو بواسطتها ، كما يسهل ارتكابها عبر الحدود ، وإن تنفيذها لا يستغرق إلا دقائق معدودة وأحيانا تتم في ثوان، كذلك صعوبة الرقابة على الإنترنت أو المحاسبة على ما ينشر فيه ؛ مما جعل الإنترنت مقراً للإرهابيين ، ويهدف الإرهابيون للقيام بهذه العمليات إلى زعزعة الأمن والإخلال بالنظام العام، والاستيلاء على الأموال العامة والخاصة والحاق الضرر بالمرافق العامة والاتصال والمواصلات.[1]

لذلك فإن إدراك ماهية جرائم الإرهاب باستخدام الوسائل الإلكترونية ، وتحديد الطبيعة الخاصة لهذه الجريمة يتخذ أهمية بالغة لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية ، وهذا ما سأتناوله في هذا المبحث .

وبناء على ذلك فإننا سنقسم هذا المبحث إلى مطلبين على النحو التالي:

المطلب الأول : تعريف الإرهاب باستخدام الوسائل الالكترونية.

المطلب الثاني: الطبيعة القانونية لجرائم الإرهاب الإلكتروني .

---

١ عبد الله بن عبد العزيز فهد العجلان: الإرهاب الالكتروني في عصر المعلومات. بحث مقدم إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، المنعقد بالقاهرة، في المدة من ٢-٤ يونية ٢٠٠٨. بحث منشور بالإنترنت. صـ٢٥.
www.shaimaaatalla.com

المطلب الأول

تعريف الإرهاب باستخدام الوسائل الالكترونية

بات الإرهاب الإلكتروني يشكل هاجساً يقلق جميع الدول التي أصبحت عرضة للهجمات الإرهابية التخريبية ، عبر توظيف الإرهابيين للطبيعة المفتوحة للوسائل الإلكترونية ، كشبكة الإنترنت والهواتف المتنقلة والخدمات الإلكترونية الأخري لتنفيذ أنشطتهم الإجرامية ، مستفيدين من التقدم الهائل لتكنولوجيا المعلومات والحواسب الآلية وأنظمة الاتصالات .

وفيما يلي نتناول في (الفرع الأول) : مفهوم الإرهاب الإلكتروني ، ثم في (الفرع الثاني): صور ووسائل الإرهاب الإلكتروني .

الفرع الأول : مفهوم الإرهاب باستخدام الوسائل الالكترونية .

أولا : تعريف الإرهاب في صورته التقليدية:

حاولت بعض الاتفاقيات الدولية أو الإقليمية تحديد المراد من هذا المصطلح ، كما قامت بعض القوانين الجنائية الوطنية بتعريف الإرهاب ، ويمكننا ذكر أهم التعاريف لهذا المصطلح فيما يلي:

عرف القانون المصري لمكافحة الإرهاب رقم ٩٤ لسنة ٢٠١٥ في المادة الثانية بأنه « كل استخدام للقوة أو العنف أو التهديد أو الترويع في الداخل أو الخارج ، بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع أو مصالحه أو أمنه للخطر، أو إيذاء الأفراد أو القاء الرعب بينهم ، أو تعريض حياتهم أو حرياتهم أو حقوقهم العامة أو الخاصة أو أمنهم للخطر ، أو غيرها من الحريات والحقوق التي كفلها الدستور والقانون ، أو الإضرار بالوحدة الوطنية أو السلام الاجتماعي أو الأمن القومي ، أو الحاق الضرر بالبيئة أو بالموارد الطبيعية أو بالآثار أو بالأموال أو بالمباني أو بالأموال أو بالأملاك العامة أو الخاصة ، أو احتلالها أو الاستيلاء عليها ، أو منع أو عرقلة السلطات العامة أو الجهات أو الهيئات القضائية ، أو مصالح الحكومة أو الوحدة المحلية ، أو دور العبادة أو المستشفيات أو المؤسسات ومعاهد العلم ، أو البعثات الدبلوماسية والقنصلية ، أو المنظمات والهيئات الإقليمية والدولية في مصر ، من القيام بعملها أو ممارستها لكل أو بعض أوجه نشاطها ، أو مقاومتها ، أو تعطيل تطبيق أي من أحكام الدستور أو القوانين أو اللوائح .

وكذلك كل سلوك يرتكب بقصد تحقيق أحد الأغراض المبينة بالفقرة الأولي من هذه المادة ، أو الإعداد لها أو التحريض عليها ، إذا كان من شأنه الإضرار بالاتصالات أو بالنظم المعلوماتيه أو بالنظم المالية أو البنكية ، أو بالاقتصاد الوطني أو بمخزون الطاقة أو بالمخزون الأمني من السلع والموارد الغذائية والمياه ، أو بسلامتها أو بالخدمات الطبية في الكوارث .»

يلجا إليه الجاني تنفيذاً لمشروع إجرامي فردي أو جماعي بهدف الإخلال بالنظام العام ، أو تعريض سلامة المجتمع وأمنه للخطر ، إذا كان من شأن ذلك إيذاء الأشخاص أو القاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو الحاق الضرر بالبيئة أو بالاتصالات أو المواصلات أو بالأموال أو المباني أو بالأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها أو تعطيل تطبيق الدستور أو القوانين واللوائح)

كما عرف الفقيه بولوك بأنه: « كل عنف يرتكب ضد أشخاص أو أفراد أو مؤسسات ذي طابع سياسي ، ويهدف للحصول على استقلال إقليم من الأقاليم ، أو قلب نظام الحكم أو التعبير عن اعتراض على بعض مظاهر سياسة الدولة.[١]

عرفه «سوتيل» أنه: الفعل المجرم المقترن بالرعب أو العنف أو الفزع بغرض تحقيق هدف معين.[٢]

ويعرف القانون الجنائي الإرهاب بأنه : « تلك الأفعال العنفية التي تهدف إلي خلق أجواء من الخوف وأهدافه مواجهة اتجاه أهداف سياسية أو اقتصادية أو دينية أو غيرها ، وهو الأفعال الإجرامية الموجهة ضد الدولة ، والتي يتمثل عرضها أو طبيعتها في إشاعة الرعب لدى شخصيات معينة أو جماعات من الأشخاص، أو من عامة الشعب ، وتتسم الأعمال الإرهابية بالتخويف المقترن بالعنف ، مثل : أعمال التفجير ، وتدمير المنشآت العامة ، وتحطيم السكك الحديدية والقناطر ، وتسميم مياه الشرب ، ونشر الأمراض المعدية ، والقتل الجماعي وغيرها[٣] ؛

1 Bernard bauloc: le terrorisme problèmes actuels de science criminelle, presses. Universitaires, Marseille, 1989,p. 65

2 Sotile : Le terrorisme international, recveil discours de l'académie de droit international, vol. 65, 1983, p. 96.

3 www.abouna.org. https:// ar.m.wikipedia.org terrorism history and it's types and it's kinds 16/05/2017

وبذلك فإن الإرهاب في أوسع معانيه هو : استخدام عشوائي عمداً للعنف كوسيلة لخلق الإرهاب أو الخوف من أجل تحقيق هدف سياسي أو ديني أو إيدلوجي[١].

ثانياً: تعريف الإرهاب الالكتروني :

الإرهاب الالكتروني هو استغلال أحدث ما توصل إليه العلم « التطور التكنولوجي » عبر الشبكة العنقودية للعدوان أو التخويف أو التهديد بصورتيه المادي ، أو المعنوي على الأفراد أو الجماعات أو الدول لإخافتهم وإخضاعهم ، ومهاجمة النظم المعلوماتية الخاصة بهم ؛ استنادا إلى دوافع سياسية أو عرفية أو دينية.[٢]

وهناك من يعرفه بأنه «الاستخدام الخاطئ للمعلومات المتاحة على الشبكة العنقودية الإنترنت.[٣]

وأهم ما يميز تلك النوعية الجديدة من الجرائم الإرهابية هو ارتباط الفعل بالمستوى التكنولوجي المتقدم على مستوى دول العالم، فالجرائم الإرهابية تعتبر واحدة ولكن طريقة إتيانها مختلفة. وعرفه البعض بأنه «هو استخدام الإنترنت للقيام بأعمال عنف تؤدي إلى خسائر في الأرواح أو ضرر جسدي كبير من أجل تحقيق مكاسب سياسية من خلال الترهيب.[٤]

وبذلك فإن الإرهاب الالكتروني (Cyber terrorism) قد يمثل تهديدا واضحاً للأمن القومي للدول ؛ حيث أصبحت البنية التحتية لأغلب المجتمعات تدار عن طريق أجهزة الحاسب الآلي والإنترنت ؛ مما يجعلها عرضة لهجمات متعددة من (الهاكرز) و (المحترفين) بشكل عام.[٥]

وفي ضوء ذلك فإن المجتمع الدولي قد تبنى سلسلة من الاتفاقات التي تحدد وتجرم أنواع مختلفة من الأنشطة الإرهابية باستخدام وصف سياسي في جرائم الإرهاب ، وقد أدانت الجمعية العامة للأمم المتحدة الأعمال الإرهابية حيث نصت على أن (الأعمال الإجرامية التي يقصد منها أو يراد بها إشاعة حالة من الرعب بين

1 http://www.sis.gov.eg/ar/templates/articles/tmprticles.aspx? Artid= 92145 vlodbl- 7f2m. www:// en.m.wikipedia.org.

٢ د. إبراهيم عيد نايل: السياسة الجنائية في مواجهة الإرهاب. دار النهضة العربية. القاهرة. ١٩٩٦. ص ٥٨.

٣ د. مدحت رمضان : جرائم الاعتداء على الأشخاص عبر الإنترنت . دار النهضة العربية. الطبعة الأولى. ٢٠٠٠. ص ٨٧.

4 However, uradnik, Kathleen: cyber terrorism. 2011. California, Greenwood Retrieved, 4 December, 2016 . p. 140-149.

5 Matusitz, Jonathan: cyber Terrorism crimes , April 2005. American foreign policy interests.

عامة الناس وهي مجموعة من الأشخاص أو أشخاص معينين لأغراض سياسية ، وفي أي ظرف من الظروف غير المبررة ، مهما كانت الاعتبارات الأخرى التي يمكن الاحتجاج بها لتبرير تلك الأعمال.[١]

وقد نصت المادة الخامسة عشر من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات وهي كالآتي :

نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.

تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات.

نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

نشر الثغرات والفتن والاعتداء على الأديان والمعتقدات.

من خلال التعريفات السابق ذكرها يتضح لنا أن الإرهاب سواء في صورته التقليدية أو باستخدام الوسائل الإلكترونية يستهدف نفس الغرض ، ألا وهو بث الرعب والخوف في نفوس الأفراد أو الجماعات ، ويختلف الإرهاب الالكتروني عن التقليدي في الأداة المستعملة المتمثلة في تقنيات تكنولوجيا الإعلام والاتصال.

لذا يطلق عليها اسم الأسلحة الناعمة « كونها تخلف أضراراً جسيمة دون الحاجة إلى إراقة الدماء».

علاقة التقنيات الحديثة بالإرهاب الالكتروني :

انطلق تعريف الإرهاب الالكتروني من تعريف الإرهاب ، والذي ينطوي على استخدام القوة أو العنف ضد الأفراد أو الممتلكات بقصد ترويج إكراه الحكومة أو المدنيين أو أي شريحة تابعة لها لتحقيق غايات سياسية أو اجتماعية.[٢]

لذلك فالإرهاب الالكتروني يعتمد على استخدام الإمكانيات أو مقدرات الحاسب الآلي في ترويع وإكراه الآخرين، فهو يتم عن بعد دون اللجوء للعنف المادي والجسدي.[٣]

وقد يمثل البريد الالكتروني إحدى الصور المستخدمة في التقنيات الحديثة،

1 Bruce Hoffman: the inside errorism edition 2006. Columbia university 2/ sbn o- p 231.

٢ د. فتوح أبو دهب هيكل، التدخل الدولي لمكافحة الارهاب وانعكاساته على السيادة الوطنية، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ط١، ٢٠١٤، صـ٦٧.

٣ القاضي كاظم عيد جاسم جبر، مكافحة الإرهاب في التشريع العراقي، موسوعة القوانين العراقية، بغداد، ط١، ٢٠١٠، صـ٨.

فبإمكان أي شخص أن يرسل عبر الشبكة العنكبوتية أو الإنترنت ملايين الرسائل بضغطة زر واحدة مهما كان محتوى الرسالة ، فإن المستلم يستقبلها دون حدود تذكر، خاصة إذا كانت هذه الرسالة لا تحتوي على أي ملف ضار بالجهاز لوجود برامج الحماية على جهاز حاسوب المستخدم ، فقد يرد عبر البريد الالكتروني رسائل تهديد أو نقل معلومات حساسة أو إشاعة استخدام الأكاذيب يهدف إشاعة الفوضى وإرباك الاستقرار الأمني للبلد المستهدف ؛ لذلك يعد الإرهاب الالكتروني أو الإرهاب المعلوماتي [١] إحدى صور الجرائم الإرهابية موازاة مع إرهاب الدولة وإرهاب المجموعات العقائدية والإرهاب الدولي [٢] والإرهاب الديني وغيرها من صور الإرهاب وهناك من الكتاب من يرى أنه بالكلام عن الإرهاب فإننا نتكلم أيضاً عن الجريمة المنظمة ، فهما وجهان لعملة واحدة، فالكثير من الصفات والسمات تتشابه بينهما، فالاثنان يتشابهان في أسلوب العمل والتنظيم ، وكلاهما يسعى إلى إفشاء الرعب والخوف. [٣]

وقد يكون أعضاء المنظمات الإرهابية هم أساسا من محترفي الجرائم المنظمة، حيث يمكن الاستفادة من خبراتهم الإجرامية في التخطيط والتنفيذ ، ولكن تبقى الجريمة المنظمة لها سماتها التي تمتاز بها عن الجريمة الإرهابية. [٤]

والحقيقة أن مصطلح الإرهاب الالكتروني جاء ليدل على الوسيلة المستخدمة في تحقيقه مع الحفاظ على الصفات العامة للإرهاب بمفهومه العام ؛ إذ أن الاختلاف بين الإرهاب بصورته التقليدية والإرهاب الالكتروني يكمن في الوسيلة المستخدمة لتحققه ؛ لذلك يعرف البعض الجريمة المعلوماتية بأنها فعل تستخدم فيه التقنية الالكترونية لتحقيق هدف إجرامي فيه اعتداء على النفس أو المال أو المصلحة العامة. [٥]

ولهذا تندرج جرائم الإرهاب الإلكتروني ضمن الجرائم الإلكترونية التي تستهدف السيطرة علي نظم المعلومات ، بغية التخويف ونزع الثقة بنظم التقنية ، وذلك باستخدام نظم الكمبيوتر والشبكات الإلكترونية بوصفها وسيلة لارتكاب جرائمها إضافة الي استخدامها التكنولوجيا بهدف سرقة المعلومات أو نشرها أو من أجل تمويل العمليات الإرهابية ، أو تجنيد الإرهابيين . [٦]

---

١ القاضي كاظم عبد جاسم جبر، مرجع سابق، ص١٠١.

٢ طاهر سليمان خليل ، مكافحة الإرهاب وتأثيره على حقوق الإنسان المدنية (دراسة مقارنة) مكتبة الصباح، بغداد، ٢٠١٤ ، ص ٢٠.

٣ د. عبد الرحمن جلهم حمزة، جرائم الإنترنت من منظور شرعي وقانوني، دراسة مقارنة، بدون تاريخ نشر. صـ٨٤.

٤ د. أحمد محمد يوسف حريه، الإرهاب والأمن الجنائي (الظواهر الإجرامية، جامعة نايف للعلوم الأمنية، الرياض، ٢٠٠٧. ص ١٠.

٥ نسرين عبد الحميد نبيه ، الجريمة المعلوماتية والمجرم المعلوماتي ، منشأة المعارف، الإسكندرية، ٢٠٠٥ ، ص ٢١٢.

٦ د. عادل عبد الصادق ، الإرهاب الإلكتروني - القوة في العلاقات الدولية ، نمط جديد وتحديات مختلفة ، المركز العربي لأبحاث الفضاء الإلكتروني ، الطبعة الثانية ، ص١٦٧ .

وبناء على تطور أساليب التكنولوجية الحديثة فقد شكل الرئيس الأمريكي بيل كلينتون لجنة خاصة مهمتها حماية البنية التحتية الحساسة في أمريكا، قامت هذه الهيئة بتحديد الأهداف التي يمكن أن يسعى إليها الإرهابيون للإضرار بها وهي مصادر الطاقة الكهربائية والاتصالات وأيضا شبكات الحاسب الآلي تلاها إنشاء مراكز متخصصة في كل ولاية لإمكانية التعامل مع احتمال حدوث هجمات إرهابية.(١)

كما قامت وكالة الاستخبارات المركزية CIA بإنشاء مركز حروب المعلوماتية عمل به ألف من خبراء أمن المعلومات ولم يقتصر الأمر على الوكالة وإنما تعداها ليشمل الأجهزة الحكومية الأخرى كالمباحث الفيدرالية والقوات الجوية.

علاقة الإرهاب الالكتروني بالجريمة المنظمة: لا يشترط في السلوك الإجرامي للإرهاب أن تتوافر فيه خصائص الجريمة المنظمة، إلا أن هذه الخصائص قد تتوافر في هذا السلوك عندما يصدر من خلال جمعية أو هيئة أو منظمة أو عصابة تستخدم الإرهاب لتحقيق أهدافها.(٢)

فبعض الجماعات المنظمة وعصابات المافيا قد سارعت إلى الأخذ بوسائل التقنية الحديثة سواء في تنظيم أو تنفيذ أعمالها ومن ذلك إنشاء مواقع خاصة على شبكة الإنترنت واستغلت الإمكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بسهولة ويسر.(٣)

فالإرهابيون يعملون مع جماعات الجريمة المنظمة جنباً إلى جنب وبشكل يومي، ولا سيما في مجالات التزييف وتهريب الأسلحة، وكذلك وبشكل متزايد في الجرائم المالية التي تتم عبر الفضاء الالكتروني، فهم في بعض الأحيان يتبادلون التقنيات ولكن بشكل متزايد يستخدمون نفس الأشخاص والمهارات والنشاطات التي تدر عليهم الأموال.(٤)

فكافة الأعمال الإرهابية التي تتم عن طريق شبكة الإنترنت ويتحقق ما يتبعها من تهديد وترويع وتخويف لإجبار الدول أو الجماعات أو الأفراد على إتيان فعل معين أو الامتناع عن فعل معين، أيا كان مرتكب ذلك العمل الإرهابي عبر الإنترنت « دولة أو افراد أو منظمة.

١ د. عبد الرحمن جلهم حمزة: مرجع سابق، ص ١٠٢.

٢ د. محمد سامي الشوا: الجريمة المنظمة وصداها على الأنظمة العقابية، دار النهضة العربية، القاهر، بدون تاريخ نشر، الطبعة الأولى، ص ١٧٠.

٣ عبد الحميد إبراهيم محمد العريان: مكافحة الجرائم الإرهابية المعلوماتية بحث منشور بالإنترنت، ٢٠٠٦، المغرب، ص ١١٥.

٤ د. محمد سامي الشوا: مرجع سابق ص ١٧٣.

كما أن كل من أفعال التخابر والسعي والتحضير والدعوة والحث والانضمام لجمعية أو منظمة أو عصابة لنشر أفكار ما أو للترويج لها سواء كانت ذات طابع سياسي أو ديني تحدث عبر الإنترنت بمجرد ضغطه على الزر.[١]

الفرع الثاني

آليات الإرهاب باستخدام الوسائل الالكترونية.

يتخذ الإرهاب الالكتروني صورا وأشكالا عدة ، وان كان الغرض واحدا، ومن بين صور الإرهاب الرقمي ما يلي :

تدمير واختراق المواقع الالكترونية والنظم المعلوماتية:

يقصد بالاختراق : الهجوم على شبكة الإنترنت واختراق المواقع الرسمية والشخصية للأفراد ،كاختراق البريد أو الاستيلاء عليه أو إغراقه بالرسائل وقرصنة اشتراكات الآخرين من خلال الاستيلاء على أرقامهم السرية.

٢-التجسس الالكتروني:

في عصر الانفجار الرقمي أصبحت الحدود الجغرافية مستباحة بأقمار التجسس والبث الفضائي ، الأمر الذي أصبح يهدد سيادة الدول من خلال عمليات التجسس التي تقوم بها أجهزة الاستخبارات للحصول على الأسرار والمعلومات الحساسة للدولة وإفشائها لدولة معادية لها، أو استغلالها ضد المصلحة الوطنية لتلك الدولة المستهدفة[٢] ، وقد تم رصد بعض حالات التجسس الدولي من طرف وكالة الأمن القومي الأمريكي «NSA» ، والكشف عن شبكة دولية ضخمة للتجسس بإدارة كندا وبريطانيا واستراليا ونيوزيلندا لرصد المكالمات الهاتفية والرسائل بمختلف أنواعها وتدعى هذه الشبكة باسم (ECHELOW).[٣]

٣-إنشاء المواقع الإرهابية الرقمية: أصبحت الجماعات الإرهابية تعتمد على التقنية الالكترونية لتعليم صناعة المتفجرات وتقديم النصائح والإرشاد لأعضائها حول كيفية اختراق وتدمير المواقع المحجوبة ونشر الفيروسات ونشر الفكر الضال.[٤]

١ د. أحمد رشاد سلام، جريمة الإرهاب الدولي والتعويض عنها والقانون الواجب التطبيق عليها، دار النهضة العربية، القاهرة ٢٠١٧، ص٩٥.

٢ خالد المهيري، جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية ، معهد القانون الدولي ، دبي ، ٢٠٠٤ ، ص١٨٥ .

٣ د. عبد الحميد إبراهيم محمد العريان، العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة. بحث منشور بالإنترنت.
http:www.nauss.edu.sa

٤ د. عبد الرحمن بن عبد الله السند، وسائل الإرهاب الالكتروني حكمها في الإسلام وطرق مكافحتها. مقال منشور على موقع السكينة الالكتروني، ص٩.

ولم يقف الأمر عند هذا الحد بل تجاوز ذلك بإنشاء قسم خاص بالمعلومات وشركات إعلامية نشطة ، فأصبحت الجماعات الإرهابية تدير عدة شركات إعلامية عالمية ومواقع الكترونية جهادية.[١]

٤- تبادل المعلومات الإرهابية:

تتواصل الجماعات الإرهابية مع أعضائها عن طريق شبكة الإنترنت ؛ من أجل التنسيق لتنفيذ الأعمال الإرهابية دون الخضوع للمراقبة الأمنية ودون التقيد بالحدود الجغرافية.[٢]

العناصر الأساسية لاستخدامات الإنترنت في أغراض إرهابية هي :

يستخدم الإرهابيون شبكة الإنترنت في أغراضهم الخبيثة كل يوم ، علي النحو الآتي :

أ-الاتصال والتخفي: يتم ذلك عن طريق وضع رسائل مشفرة تمكنه من التواصل دون كشف هويته أو ترك أي أثر.

ب-جمع المعلومات الإرهابية: تعتمد الجماعات الإرهابية على شبكة الإنترنت من أجل الحصول على المعلومات الاستراتيجية والحساسة للدول، كمواقع المنشآت النووية، مصادر توليد الطاقة، مواعيد الرحلات الجوية، والاطلاع على الإجراءات المقررة لمكافحة الإرهاب لتجنبها.

ج-التخطيط والتنسيق للعمليات الإرهابية: تعتبر شبكة الإنترنت وسيلة للاتصال بالغة الأهمية بالنسبة للمنظمات الإرهابية ، حيث تتيح لهم حرية التنسيق الدقيق تنفيذ هجمات إرهابية محددة، كذلك يضمن لهم الإنترنت السرية وسرعة التنسيق لتنفيذ الهجمات الإرهابية.[٣]

د-الحصول على التمويل: يستعين الإرهابيون ببيانات إحصائية سكانية منتقاه من المعلومات الشخصية التي يُدخلها المستخدمون علي الشبكة من خلال الاستفسارات والاستطلاعات الموجودة علي المواقع الإلكترونية ، من خلال ذلك يتم استغلال تلك المعلومات للتعرف علي الأشخاص ذوي القلوب الرحيمة ، ثم يتم استجداؤهم لدفع تبرعات مالية لأشخاص اعتباريين يمثلون واجهة لهؤلاء الإرهابيين ، ويتم ذلك

١ صالح مختاري ، كيف تستخدم الجماعات الإرهابية الإنترنت لهندسة جرائمها المنظمة، مقال منشور بالإنترنت، ص ٣٥.
٢ معتز محيي الدين، الإرهاب وتكنولوجيا المعلومات، مقال متاح على الإنترنت.
٣ د. عبد الله بن عبد العزيز بن فهد العجلان، مرجع سابق ٢٠٠٨، ص٥٢ .

بواسطة البريد الإلكتروني بطريقة ماكرة لا يشك فيها المتبرع بأنه يساعد إحدي المنظمات الإرهابية.[١]

هـ-التدريب الإرهابي الإلكتروني: تحتاج العمليات الإرهابية إلى تدريب خاص ، ويعد التدريب من أهم هواجس التنظيمات الإرهابية ، وقد أنشئت معسكرات تدريبية سرية – كما ظهر بعضها في وسائل الإعلام – لكن مشكلة معسكرات التدريب الإرهابية أنها دائماً معرضة للخطر ، ويمكن اكتشافها ومداهمتها في أي وقت ، لذا فإن الشبكة المعلوماتية بما تحتويه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب الإرهابي، كما قامت بعض الجماعات الإرهابية بإنتاج ونشر أدلة إرشادية الكترونية تتضمن وسائل التدريب والتخطيط والتنفيذ على شبكة الإنترنت لتصبح في متناول الإرهابيين على المستوى العالمي.[٢]

و-إصدار البيانات الالكترونية : تقوم المنظمات الإرهابية باستخدام الشبكات المعلوماتيه في نشر بياناتها الإرهابية عن طريق المواقع الالكترونية المختلفة أو بواسطة البريد الالكتروني أو من خلال المنتديات والقنوات الفضائية، وذلك من أجل بث مختلف الأنشطة التي تقوم بها الجماعات الإرهابية سواء بغرض التصريح بتبنيها عمليات فدائية معينة، أو لبث تهديدات بتنفيذ هجمات إرهابية أو تصريحات ترتبط بالمشروع الإرهابي.

ز- التهديد والترويع الالكتروني: تستغل الجماعات الإرهابية شبكة الإنترنت العالمية من أجل بث الرعب والخوف في نفوس الأفراد والدول، من خلال التهديد باغتيال شخصيات سياسية مهمة في الدولة، أو التهديد بتدمير البنية التحتية المعلوماتية عن طريق نشر الفيروسات لتدمير الشبكات المعلوماتية والأنظمة الالكترونية.[٣]

ر- تعبئة وتجنيد الإرهابيين: يعد من أخطر أساليب وصور الإرهاب الإلكتروني نظراً للتأثير الفعال للوسائل التقنية المعتمد عليها في عملية التجنيد وسرعة فعاليتها على الأفراد في تكوين قناعات فكرية متطرفة ،التي لا تتطلب سوى جهاز حاسوب وشبكة إنترنت واحترافية تقنية وسوسيولوجية نفسية لدى القائم بالتجنيد ؛ لتكون في ظرف وجيز جداً جيوشا افتراضية في مختلف بقاع العالم.

---

١ يونس محمد عرب ، استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابين. ط١. جامعة نايف العربية للعلوم الأمنية. الرياض، ٢٠١٢، صـ١٦٦-١٦٧.

٢ د. مايا حسن ملا خاطر ، الإطار القانوني لجريمة الإرهاب الإلكتروني . السعودية ،٢٠١٥ ، ص ١٢٢

٣ د. عبد الله بن عبد العزيز بن فهد العجلان، مرجع سابق ص ٢٥.

المطلب الثاني

الطبيعة القانونية لجرائم الإرهاب باستخدام الوسائل الإلكترونية .

تمهيد وتقسيم :

تعد جرائم الإرهاب الإلكتروني جريمة ذات طبيعة خاصة ؛ نظراً للخطورة الإجرامية التي تشكلها علي المستوي الدولي، والخسائر التي تتسبب بها، وتتميز جرائم الإرهاب الإلكتروني بصعوبة اكتشافها ، فالمجرم يمكنه ارتكاب هذه الجريمة في دول وقارات مختلفة فهذه الجريمة عابرة للدول، وكذلك فإن قدرة الجاني علي تدمير دليل الإدانة في أقل من الثانية الواحدة يشكل عاملاً إضافياً في صعوبة اكتشاف هذا النوع من الجرائم . وإذا تم اكتشاف هذه الجريمة فمن الصعب إثبات هذا النوع من الجرائم فجرائم الإرهاب الإلكتروني تتم في محيط غير تقليدي ؛ حيث تقع خارج إطار الواقع المادي الملموس ، لتقوم أركانها في بيئة الحاسوب مما يجعل الأمور تزداد صعوبة وتعقيداً لدي سلطات الأمن وأجهزة التحري والتحقيق والملاحقه [١].

كما تتمثل الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات علي نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد ؛ للاعتداء علي الخصوصية ، ويسهل ذلك توسع بنوك المعلومات بأنواعها علاوة علي توسع الأفراد وسعيهم إلي ربط حواسيبهم بالشبكة المذكورة ..[٢]

وبناءً علي ذلك فإن جرائم الإرهاب الإلكتروني تستمد طبيعتها الخاصة من الصفات الخاصة التي يتميز بها المجرم الإلكتروني ، فهو مجرم ذات مواصفات خاصة بالإضافة إلي الخصائص المميزة التي يتصف بها المجرم الإلكتروني.

لذلك فإننا سنقسم هذا المطلب الي فرعين علي النحو الآتي :-

الفرع الأول : مواصفات المجرم الإلكتروني .

الفرع الثاني : خصائص المجرم الإلكتروني:

---

١ د. محمد السعيد رشدي، الإنترنت والجوانب القانونية لنظم المعلومات بحث مقدم إلي مؤتمر الإعلام والقانون، كلية الحقوق جامعة حلوان، من ٩-١٠ مارس ١٩٩٩.

٢ د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجية الحديثة للجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية القاهرة، ١٩٩٢، ص١١.

الفرع الأول

مواصفات المجرم الإلكتروني

يمكن أن نستخلص مجموعة من السمات والمواصفات التي يتميز بها المجرم الإلكتروني، والتي يساعد علي التعرف عليها في مواجهة هذا النمط من المجرمين ، وحيث إن المجرم الإلكتروني وان كان يتميز ببعض السمات الخاصة : إلا أنه في النهاية لا يخرج عن كونه مرتكباً لفعل إجرامي يتطلب توقيع العقاب عليه.

وفيما يلي عرض لبعض الصفات العديدة للمجرم الإلكتروني والتي في الغالب تميزه عن غيره من المجرمين العاديين:

المجرم الإلكتروني، مجرم متخصص:

تبين في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر ، أي أنهم يتخصصون في هذا النوع من الجرائم دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يعكس أن المجرم الذي يرتكب الجرائم الإلكترونية هو مجرم في الغالب متخصص في هذا النوع من الإجرام[١].

المجرم الإلكتروني، مجرم عائد إلي الإجرام:

يعود كثير من مجرمي المعلومات إلي ارتكاب جرائم أخري في مجال الكمبيوتر انطلاقاً من الرغبة في سد الثغرات التي أدت إلي التعرف عليهم ، وأدت إلي تقديمهم إلي المحاكم في المرة السابقة ، ويؤدي ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلي تقديمهم إلى المحاكم[٢].

المجرم الإلكتروني مجرم محترف:

يتمتع المجرم الإلكتروني بإحترافية كبيرة في تنفيذ جرائم، حيث إنه يرتكب هذه الجرائم عن طريقة الكمبيوتر الأمر الذي يقتضي الكثير من الدقة والتخصص والاحترافية في هذا المجال للتواصل إلي التغلب علي العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية[٣].

١ د. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي. دار الجامعة الجديدة للنشر، الإسكندرية. ٢٠٠١ ص٧٥.
٢ د. نهلا عبد القادر المؤمن، الجرائم المعلوماتيين. دار الثقافة للنشر والتوزيع، الطبعة الأولي، عمان. ٢٠٠٨. ص٥١.
٣ د. يوسف الصغير، الجريمة المرتكبة عبر الإنترنت . مذكرة لنيل درجة الماجستير في القانونية كلية الحقوق والعلوم السياسية جامعة مولود المعمري- الجزائر. ٢٠١٢. بحث منشور بالإنترنت. ص١٢ .

المجرم الإلكتروني مجرم غير عنيف:

المجرم الإلكتروني من المجرمين الذين لا يلجأون إلي العنف في تنفيذ جرائمهم، وذلك لأنه ينتمي إلي إجرام ـــ الحيلة ـــ فهو لا يلجأ إلي العنف في ارتكاب جرائمه، وهذا النوع من الجرائم لا يستلزم أي قدر من العناء للقيام به، فضلاً عما تقدم، فالمجرم الإلكتروني مجرم ذكي، ويتمتع بالتكييف الاجتماعي، أي لا يناصب أحدًا العداء، وأيضًا يتمتع بالمهارة والمعرفة، وأحيانًا كثيرة علي درجة عالية من الثقافة.

الفرع الثاني

خصائص المجرم الإلكتروني

يتميز المجرم الإلكتروني كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين وهي:

المهارة: يتطلب تنفيذ الجريمة الإلكترونية قدراً من المهارة يتمتع بها الفاعل والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال التكنولوجيا، أو بمجرد التفاعل الإجتماعي مع الآخرين، وهذه ليست قاعدة في أن يكون المجرم الإلكتروني علي هذا القدر من العلم، وهذا ما أثبته الواقع العملي أن جانبًا من أنجح مجرمي المعلوماتيين لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الإجرام.

المعرفة: يتميز مجرمو المعلوماتية بالمعرفة، حيث يستطيع المجرم الإلكتروني أن يكون تصوراً كاملاً لجريمته، ويرجع ذلك إلي أن المسرح الذي تمارس فيه الجريمة الإلكترونية هو نظام الحاسب الآلي فالفاعل يستطيع أن يطبق جريمته علي أنظمة مماثلة وذلك قبل تنفيذ الجريمة.[1]

الوسيلة: ويراد بها الإمكانيات التي يحتاجها المجرم الإلكتروني لإتمام جريمته. وهذه الوسائل قد تكون في غالب الأحيان وسائل بسيطة وسهلة الحصول عليها خصوصاً إذا كان النظام الذي يعمل به الكمبيوتر من الأنظمة غير المألوفة، فتكون هذه الوسائل معقدة وعلي قدر من الصعوبة.[2]

---

١ د. عمر عبد العزيز موسي، آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية. بحث مقدم لمؤتمر مركز جيل البحث العلمي ١٤ الجرائم الإلكترونية منشور بالإنترنت. www.jil.ac/Cemter/Ham.jil

2 Http: //www.nipc. Gov/cabernet/cybernetic. Htm.

السلطة: يقصد بالسلطة الحقوق والمزايا التي يتمتع بها المجرم الإلكتروني والتي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتييه لديهم سلطة مباشرة ، أو غير مباشرة في مواجهة المعلومات محل الجريمة.(١)

وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلي النظام الذي يحتوي علي المعلومات ، وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلي الحاسب الآلي وإجراء المعاملات. كما أن السلطة قد تكون شرعية . ومن الممكن أن تكون غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص آخر.

ونتيجة لهذه الطبيعة الخاصة التي تتصف بها جرائم الإرهاب الإلكتروني ، ونظرا للخطورة التي تشكلها علي المستوى الدولى، والخسائر التي قد تتسبب بها فيجب التعاون الدولي المكثف من أجل التصدي لهذه الجرائم.

وبالتالي من أجل التصدي لجرائم الإرهاب الإلكتروني لابد أن تعمل الدولة في اتجاهين.

الأول : داخلي حيث تقوم الدول المختلفة بسن القوانين الملائمة لمكافحة هذه الجرائم. الثاني: دولي عن طريق عقد اتفاقيات دولية، حتى لا يستفيد مجرموا المعلوماتية من عجز التشريعات الداخلية من ناحية وغياب الاتفاقيات الدولية التي تتصدى لحماية المجتمع الدولي من نتائج وآثار هذه الجرائم.

الفصل الأول

المسؤولية الجنائية الناشئة عن جرائم الإرهاب الالكتروني

تمهيد وتقسيم:

المسؤولية الجنائية : هي الرابطه التي تنشأ بين الدولة والفرد، الذي يثبت من خلال الإجراءات القضائية التي رسمها القانون صحة إسناد فعل مكون لجريمة إليه متي شمل هذا الإسناد كافة العناصر القانونية التي أوجب المشرع توافرها حتي يوصف الفعل أنه جريمة .(٢)

وإذا كانت الدولة هي وحدها التي تحتكر السلطة العامة بما تصنعه من قواعد قانونية لتنظيم حركة المجتمع ، فإن الجزاء الذي تتضمنه هذه القواعد هو الذي

---

1 \Www. Pkiforwm. Org.

٢ د. يسر أنور علي، شرح قانون العقوبات. النظرية العامة، دار الثقافة الجامعية. ١٩٩١، ص٧٨٢.

يضمن احترامها من قبل المخاطبين بها، أي أن الجزاء هو الذي يحقق الحماية الفعالة للقاعدة الجنائية.[١]

وأي قاعدة قانونية لابد أن يكون لها شقان (الأول) هو الذي يحدد الأوامر والنواهي بالنسبة لسلوك معين، (الثاني) الجزاء الذي رتبة القانون علي مخالفه تلك الأوامر والنواهي.[٢]

وقد استقر الفقه علي أن انعقاد المسؤولية الجنائية لا يكفي لكي يكون ثمن سلوك إجرامي قد أتاه الجاني ، أو تكون ثمة نتيجة قد تحققت ، وإنما ينبغي أن تكون هناك علاقة سببية أو رابطة سببية معينة ذات طبيعة مادية.[٣]

فيجب أن تتوافر علاقة السببية بين فعل الجاني وبين الضرر، فإذا ثبت أن الضرر يرجع لسبب أجنبي لا دخل لإرادته فيه انقطعت صلة السببية ، ولا يلزم فقط أن تتوافر علاقة السببية المادية بين السلوك والنتيجة لوجود الجريمة والمسؤولية عنها ، وإنما يلزم بالإضافة إلي ذلك أن تتوافر إرادة تقبل الخضوع إلي تقييم قانوني معين يسمح بتكييفها بأنها جديرة بالتأثيم.[٤]

لذلك تفترض فكرة الإثم التي تنهض عليها المسؤولية الجنائية وفقاً للمبادئ المستقرة تقليدياً في قانون العقوبات ، ليس فقط أن يسهم الشخص بسلوكه في تحقيق الوقائع المادية المعاقب عليها ، وإنما أيضاً أن تتوافر علاقة ذات طابع ذهني أو نفسي بين هذا الشخص والوقائع المادية التي أسهم فيها، وهذه العلاقة تتحقق في أخطر صورها حينما يعلم الفاعل بسلوكه لحظة إتيانه ، وكذلك بالآثار الضارة المرتبطة به ، وتتجه إرادته إلي إتيان هذا السلوك والى إحداث هذه الآثار ويطلق علي هذه العلاقة النفسية القصد الجنائي.[٥]

وحيث إن الجريمة بمعناها التقليدي تعني الخروج عن السلوك أو المعايير الاجتماعية والثقافة والاقتصادية التي يحكمها القانون الوضعي لأي مجتمع ، وبالتالي فإن التعدي علي الفرد وحقوقه وكذلك المجتمع يعرض دائماً مرتكبي هذا السلوك للمساءلة القانونية والجنائية، فالجريمة التقليدية تعني كل عمل إنساني يخالف القانون ويقوم به المجرم لتحقيق أهداف إجرامية محددة.

١ د. عبد الفتاح مصطفي الصيفي، القواعد الجنائية. الإسكندرية. ١٩٦٧. ص٣٥.
٢ د. حسنين إبراهيم صالح عبيد، دروس في قانون العقوبات. القسم العام دار النهضة العربية. ١٩٩٩. ص٢١٨.
٣ د. مأمون محمد سلامة، قانون العقوبات. دار الفكر العربي. ١٩٩٦. ص٣٢١.
٤ د. محمد عبد اللطيف عبد العال، الجرائم المادية وطبيعة المسؤولية الناشئة عنها. دار النهضة العربية. القاهرة ١٩٩٧. ص٣.
٥ د. محمود نجيب حسني، شرح قانون العقوبات. القسم الخاص. دار النهضة العربية. ١٩٨٨. فيه ١٨٥. ص٢٧٥.

أما الإرهاب فهو ذلك السلوك الإجرامي الذي يسبب قدراً كبير من الدمار والخسائر البشرية وتنفذه جماعات متخصصة من ذوي الخبرات العالية التي تملك معرفة تكنولوجية في مجالات متعددة ولها قدرة عالية في التخطيط.[١]

في حين أن مفهوم الجريمة الإرهابية التقنية يمكن تحديدها بأنها « أي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإرهابي المقصود".[٢]

ويري آخرون أن الإرهاب الإلكتروني : هو سلوك غير مشروع ـــ يعاقب عليه القانون ـــ صادر من إرادة إجرامية ومحلة معطيات الحاسب الآلي ، ولذلك فهي جريمة مستترة تتسم بالسرعة والتطور في أساليب ارتكابها أقل عنفاً في التنفيذ وعابرة للحدود ويصعب إثباتها ويسهل إتلاف الأدلة الخاصة بها .[٣]

وحيث إن المسؤولية الجنائية تثبت عند ارتكاب الجاني فعلاً يحدث أثره في العالم الخارجي أو هو مادياتها التي تلمسها الحواس وتدخل في كيانها، وهو يتشكل من ثلاثة عناصر « الفعل الإجرامي » الذي يشكل السلوك الإيجابي المتمثل في الإقدام علي فعل ينهي القانون عن ارتكابه لخطورته علي المجتمع ، أو « السلوك السلبي » الذي يصدر عن الجاني بامتناعه عن إثبات عمل بأمر القانون بالإقدام عليه للصالح العام بالإضافة إلي « النتيجة لإجرامية» وهي الأثر المترتب علي الفعل الإجرامي وأخيراً « علاقة السببية» وهي الصلة بين الفعل الإجرامي بالنتيجة المتحققة ويجب أن تتوافر الإرادة كرابطه نفسية بين الجاني وبين ما تحقق من سلوك ونتيجة.[٤]

ولكي يمكن القول بوجود جريمة ما فإن المشرع يتطلب بجانب الركن المادي وجود الركن المعنوي ، وبغير هذين الركنين لا يمكن القول بوجود جريمة فالركن المادي هو النشاط أو السلوك الذي تتم به الجريمة ، أما الركن المعنوي فيأخذ شكل القصد الجنائي.

لذلك فإننا سنقسم هذا الفصل إلي مبحثين علي النحو الآتي :

---

١ د. هاشم الزهراني: الإرهاب المعلوماتي. كلية الملك فهد الأمنية. مركز البحوث. ندوه المجتمع والأمن والجرائم الإلكترونية. الرياض٢٠٠٧. ص٣٣٩.

٢ د. عبد الفتاح بيومي: عالم الجريمة والمجرم المعلوماتي، منشأة المعارف الإسكندرية. ٢٠٠٩. ص١٧.

٣ د. عبد الفتاح بيومي: الأحداث والإنترنت. أثر الإنترنت في انحراف الأحداث. دار الفكر العربي. الإسكندرية. ٢٠٠٧. ص١٩.

٤ د. مأمون محمد سلامة: قانون العقوبات. القسم العام، مطبعة جامعة القاهرة. ١٩٩١/٩٠. ص١٠٨.

المبحث الأول : المسؤولية الجنائية عن الأفعال المادية في جرائم الإرهاب الإلكتروني.

المبحث الثاني: جوهر المسؤولية الجنائية العمدية الناشئة عن جرائم الإرهاب الإلكتروني.

المبحث الأول

المسؤولية الجنائية عن الأفعال المادية في جرائم الإرهاب الإلكتروني.

تمهيد وتقسيم:

المسؤولية الجنائية هي التزام قانوني من النوع الجزائي لابد وأن يكون لها مصدر، مثلها في ذلك مثل أي التزام قانوني آخر، كما يتعين أيضاً أن يكون هناك شخص يقوم بها أو يحملها، كما يجب أخيراً أن يكون لها أركان تقوم عليها واليها ترتكز، فيلزم لقيام المسؤولية الجنائية قيام العلاقة المادية بين المتهم وبين الجريمة أو أن يثبت إسناد الجريمة للمتهم، بمعني أن تكون الجريمة ناشئة عن تصرفه سواء باعتباره فاعلاً أصلياً أو شريكه في ارتكابها.[١]

فلا يسأل الشخص إلا عن فعله أو امتناعه فالشرط الأول للمسؤولية : يتمثل في وجود علاقة مادية بين الجريمة والسلوك الشخصي للمسؤول عنها، ويفترض هذا الإسناد المادي توافر عنصرين:الأول : مساهمة الشخص بفعله الشخصي في الجريمة ، الثاني: توافر علاقة السببية بين فعل المساهمة والنتيجة الإجرامية التي يعتد بها المشرع في التجريم والعقاب.[٢]

ودور علاقة السببية علي هذا النحو هو بيان ما إذا كان للفعل من نصيب في إحداث النتيجة ، أو بتعبير آخر إثبات أن الفعل كان (سبب) حدوث النتيجة.[٣]

لذلك فإننا سنقسم هذا المبحث إلي ثلاثة مطالب علي النحو الآتي :

المطلب الأول : الأفعال المادية في جرائم الإرهاب الإلكتروني .

المطلب الثاني : النتيجة في جرائم الإرهاب الإلكتروني .

المطلب الثالث : علاقة السببية في جرائم الإرهاب الإلكتروني .

---

١ د. محمد مصطفي القللي، شرح قانون العقوبات في جرائم الأموال، دار الياس للطباعة، الطبعة الأولي، ١٩٤٧، ص٣٦.

٢ د. أحمد فتحي سرور، القانون الجنائي الدستوري، دار الشروق، الطبعة الثانية، ٢٠٠٢، نبذ ٨، ص١٩٨.

3 Andria decoc: Droit penal general- Dalloz. Paris 2.5 eme. 1971. P185.

المطلب الأول

الأفعال المادية في جرائم الإرهاب الإلكتروني

تتكون جرائم الإرهاب الإلكتروني أو الافتراضية «cyber crime» من مقطعين Terrorism (الإرهاب) و(Cyber) الكتروني ويستخدم مصطلح الإلكتروني لوصف جزء من الحاسب الآلي أما جريمة الإرهاب ، فهي السلوكيات والأفعال التي تؤدي إلي نشر جرائم العنف والتي ترتكب ضد الأفراد أو المجموعات والتي قد تؤدي إلي ارتكاب جرائم فردية.(١)

الفعل هو ذلك السلوك الإرادي الذي يصدر عن الفاعل ويسبب نتيجة معينة تنال من حق محل حماية تشريعية ، ويتسع ليشمل السلوك الإيجابي المفترض حركة عضوية من الجاني فضلا عن الفعل السلبي والمتمثل في الامتناع عن سلوك معين يتطلبه المشرع في ظروف معينة ، وهو بصورتيه عنصر في الركن المادي للجريمة سواء كانت عمدية أو غير عمدية.(٢)

الركن المادي في جرائم الإرهاب الإلكتروني :-

أولا : بداية النشاط :

لا شك في أن الجريمة تمر بعدة مراحل حتى تتحقق نتيجتها الإجرامية ، فتبدأ بتفكير الجاني في ارتكابها ، ثم بعقد العزم على هذا التنفيذ ، ثم ينتقل الجاني من مرحلة العزم على ارتكاب الجريمة إلى مرحلة الأعمال التحضيرية لكيفية تنفيذها بما يتفق مع طبيعة ونوع هذه الجريمة ، والمشرع لا يعاقب على هذه المرحلة ؛ لأنها لا تنطوي على خطر يهدد حقا أو مصلحة ، وهي ما زالت قابلة لرجوع الجاني عن تنفيذ الجريمة.(٣)

إلا أن الأفعال المادية غير المشروعة التي ترتكب بواسطة الأجهزة الالكترونية ليست مثل أي جريمة تستلزم وجود أعمال تحضيرية ؛ إذ يصعب الفصل بين العمل التحضيري والبدء في التنفيذي أو النشاط الإجرامي في جرائم الكمبيوتر والإنترنت، أما في مجال تكنولوجيا المعلومات فإن الأمر يختلف بعض الشيء ، فشراء برامج

---

1 www. Democratic. com = 35426.

٢ أ.د. أحمد عوض بلال، مبادئ قانون العقوبات المصري، القسم العام، دار النهضة العربية، طبعة ٢٠٠٥، ٢٠٠٦، ص٢٥٩.

٣ د. إبراهيم حامد طنطاوي، شرح الأحكام العامة لقانون العقوبات، الجزء الأول، النظرية العامة للجريمة، دار النهضة العربية، ٢٠١٧ ص ٥٥.

اختراق ومعدات لفك الشفرات وكلمات المرور أو حتى بعض الفيروسات التي لم يتم إطلاقها على الشبكة الالكترونية كل هذه الأعمال التحضيرية تمثل جريمة في حد ذاتها.[١]

وقد يرتبط السلوك الإجرامي في الجريمة الالكترونية بالمعلومة المخزنة على الحاسب الآلي ، أو تلك التي يتم إدخالها للحاسب الآلي ، وصعوبة المشكلة أن السلوك الإجرامي قد يتحقق بمجرد ضغط الزر في الحاسب ، فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك أو إساءة استعمال بطاقة الائتمان.[٢]

لذلك يجب على المشرع عند التجريم أن يأخذ في الاعتبار السلوك المادي الإيجابي المتمثل في المنطق التقني ، وذلك لأن الجريمة عبر الإنترنت ذات طابع موحد ، فهي تباشر من حيث السلوك أو النشاط المادي فيها، كأحد عناصر الركن المادي.[٣]

وحيث إن الإرهاب الإلكتروني يعد جريمة معلوماتية تمس بأنظمة المعالجة الآلية للمعطيات، وتشكل المساس بالملايين من الأنظمة المعلوماتية، وغالباً ما يتحقق ذلك في آن واحد بحيث يمثل ذلك هجومًا معلوماتيًا [٤] ، وتشكل الجريمة المعلوماتية كل فعل أو امتناع عن فعل يصدر من الإنسان عن قصد الهدف منه الوصول الي أجهزة تقنية بغرض إلحاق ضرر بشخص آخر، [٥] وقد نص المشرع الفرنسي علي الأفعال غير المشروعة في الجرائم المعلوماتية ، ومن بين هذه الأفعال فعل الدخول أو البقاء في نظام المعالجة الآلية للمعطيات ، فعل إعاقة أو تقليد عمل نظام المعالجة الآلية للمعطيات ، فعل إزالة أو تغيير المعطيات التي يحتوي عليها نظام المعالجة .[٦]

ويمكن حصر الأفعال التي تشكل المساس بأنظمة المعالجة الآلية للمعطيات والتي يجب تجريمها علي النحو الآتي :-

الدخول الاحتيالي إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات أو البقاء فيه.

١ د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، ٢٠٠٩، دار الفكر، الإسكندرية، ط١، ص٨٥.
٢ سميرة المعاشي، ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، الجزائر، ٢٠١١، ص ٢٨٠.
٣ خالد ممدوح إبراهيم ، مرجع سابق، ص ٨٧.
٤ أمينة نشناش،، الركن المفترض في الجريمة المعلوماتيية بين الوقاية والمكافحة، محاضرة القيت بتاريخ ٢٠١٥/١١/١٦ ، حقوق جامعة محمد خيصرة ، بسكرة ، الجزائر ، ص١٥٦.
٥ محمد صالح كريدي، الأفعال غير المشروعة في الجرائم المعلوماتيية ، كلية الحقوق جامعة عنابة ، ٢٠٠٠ ، ص٢٠.
6 Suzan w. BRENNER: "At Light Speed" Attribution and Response to Cybercrime, terrorism / Warf are. 2007. Journal of criminal law criminology, P390.

حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو التسبب في تخريبه .

العرقلة العمدية لسير نظام المعالجة الآلية للمعطيات أو إحداث خلل .

إدخال معطيات في نظام للمعالجة الآلية للمعطيات أو إتلافها أو حذفها منه أو تغيير المعطيات المدرجة فيه أو تغيير طريقة معالجته أو طريقة إرسالها بشكل احتيالي.

التزوير أو التزييف لوثائق المعلومات أياً كان شكلها إذا كان من شأن التزوير أو التزييف الحاق ضرر بالغير .

استعمال وثائق مزورة أو مزيفة .

صنع تجهيزات أو أدوات أو إعداد برامج للمعلومات أو أية معطيات أعدت أو اعتمدت خصيصاً لأجل ارتكاب هذه الجرائم أو تملكها أو حيازتها أو التخلي عنها للغير .

المشاركة في عصابة أو إتفاق لأجل إعداد واحدة أو أكثر من هذه الجرائم .

ثانياً - السلوك الإجرامي للإرهاب الإلكتروني :

يعتبر العنف هو أهم ما يميز جريمة الإرهاب بصورته التقليدية وهذه الخاصية تشير إلى استخدام القوة أو التهديد بها، ويتسع هذا المعنى إلى الصور الجديدة التي جاءت بها التكنولوجيا الحديثة فلا يقف عند المعنى العادي للعنف، فيعتبر من قبيل العنف المكون للإرهاب استخدام نظم المعلومات لأغراض إرهابية ، مثال ذلك : تدمير المعلومات الالكترونية أو العبث بنظم التوجيه والمراقبة في مجال الطيران وفي مجال الاتصالات أو في مجال إطلاق الصواريخ[1] ، ومن الأفعال الإجرامية التي يجب أن تدخل في نطاق الإرهاب الإلكتروني جريمة التنصت علي المراسلات الإلكترونية أو التقاطها أو اعتراضها ، والدخول غير المشروع لتهديد شخص وابتزازه ، وجريمة الدخول غير المشروع إلي المواقع الإلكترونية والقيام بتغييرها وتصاميمها أو إتلافها أو تعديلها، وجريمة التشهير بالآخرين والحاق الضرر بهم عبر وسائل تقنيات المعلومات .

١ د. أحمد فتحي سرور، المواجهة القانونية للإرهاب، الطبعة الثانية، دار النهضة العربية، ٢٠٠٨، ص٢٣٦.

هذه الأفعال غير المشروعة أدت إلى ظهور صورة جديدة من صور الإرهاب تسمى بجرائم الإرهاب الالكتروني ، والنشاط أو السلوك المادي في هذه الجرائم يتطلب وجود بيئة رقمية واتصال بالإنترنت ، وتتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته ، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث النتيجة الإجرامية فيقوم بتحميل الحاسب ببرامج اختراق أو أن يقوم بإعداد هذه البرامج بنفسه، كما قد يقوم بإعداد برامج تحمل فيروسات.[١]

ومما يزيد من صعوبة السلوك أو الفعل المادي في جرائم الإرهاب الالكتروني أن السوك الإجرامي يتم ارتكابه عن طريق معلومات تتدفق عبر نظم الحاسب الآلي لا يمكن الإمساك به مادياً، تماماً مثل التيار الكهربائي الذي يسري في توصيله دون أن نراه ، وذلك بعكس السلوك الإجرامي في الجريمة التقليدية الذي يتم رؤيته بالعين والتأكد منه كفعل القتل والسرقة أو التزوير [٢]

وهذه الأفعال غير المشروعة يكون الدليل فيها غير مرئي ؛ لأن هؤلاء المجرمين يستخدمون أساليب وتقنيات عالية ، فقد تحولت أساليب النقل المعلوماتي من التمثيلي إلى الرقمي وأصبحت المعلومة عبارة عن نبضات الكترونية غير مرئية تجوب شبكات مشفرة.[٣]

لذلك فإن طبيعة الركن المادي في الجريمة الالكترونية تعد من المشكلات العملية التي تثيرها تلك الجريمة، ذلك لأن مفهوم أو مناط التجريم ينصب على نظام الكتروني يساء استعماله أو اقتحامه على نحو غير مشروع ، دون أن يكون لذلك الاستعمال أو الاقتحام من أثر مادي ملموس يظهر في صورة تدمير للمعلومات، وهو ما يثير إمكانية الإتلاف العمدي للمنقولات أو السرقة ،أو يثير شبهة التزوير عن طريق التلاعب في بيانات الحاسب الآلي .[٤]

وقد يتمثل السلوك المادي أو النشاط الإجرامي في إطلاق المواقع التي تحث إما على الانضمام إلى الجماعات الإرهابية أو تورد كيفية صنع القنابل اليدوية وكذلك تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية ، فقد أنشأت مواقع

١ د. حسن تركي عمير، الإرهاب الالكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، بحث منشور على الإنترنت، ص٢٧٥.

٢ د. حجازي عبد الفتاح بيومي، التزوير في جرائم الكمبيوتر والإنترنت دار الكتب القانونية، القاهرة، ٢٠٠٨ ، ص ١١٤.

3 www.droitmaantada.com.

٤ عبد الله دغمش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، ٢٠١٤م، ص ٤٥.

التعليم صنع المتفجرات وكيفية اختراق وتدمير المواقع، وطرق البريد الالكتروني وكيفية الدخول إلى المواقع المحجوبة وطريقة نشر الفيروسات.[١]

وبذلك فإن الأفعال المادية غير المشروعة عبر الإنترنت « للإرهاب الالكتروني» تعد جريمة سلوك دون النظر لتحقيق النتيجة لكون السلوك هو مجرد النشاط المادي دون النظر لما يرتبه من نتائج لتلك الأفعال المادية.[٢]

ثالثاً- صور السلوك الإجرامي للإرهاب الإلكتروني:

الأصل في التجريم عدم الاهتمام بالوسائل المستعملة في النشاط الإجرامي. فمثلا في جريمة القتل يستوي أن يتم السلوك الإجرامي بالطعن بآلة حادة أو بإطلاق الرصاص أو الخنق إلى غير ذلك من الوسائل.

وقد يشترط القانون وسيلة معينة يتم بها السلوك الإجرامي مثل القتل بالسم إذ يشترط استخدام وسيلة معينة هي المواد السامة (المادة ٢٣٣ عقوبات مصري).[٣]

إلا أن التجريم في أفعال الإرهاب الالكتروني - التي تستخدم عبر الإنترنت -يجب أن تنصب على الوسائل المستخدمة في جرائم الإرهاب الالكتروني التي يستخدمها الإرهابيون لتنفيذ مآربهم. وتتمثل الوسائل المستخدمة في جرائم الإرهاب الالكتروني في الآتي :

التجنيد الإلكتروني للإرهاب : إن جريمة التجنيد الإلكتروني للإرهاب تعد جريمة رقمية ظاهريا ذات وصف إرهابي ، فلا يمكن أن تنفذ إلا بواسطة وسائل تكنولوجيات الإعلام والاتصال بصفة عامة وعن طريق مواقع التواصل الاجتماعي بصفة خاصة، وبالتالي تنتقل جريمة التجنيد من البيئة المادية الواقعية إلى البيئة الإفتراضية الرقمية.[٤]

ويمكن تحديد عناصر السلوك الإجرامي للركن المادي لجريمة التجنيد كما يلي: -

---

١ ففي عام ٢٠٠٥ استطاع أحد الطلبة بكلية الهندسة بمصر من استخدام المعلومات المتاحة على شبكة الانترنت وقام بتصنيع قنبلة بدائية يدوية استخدمها في العملية الإرهابية الشهيرة بالأزهر. راجع د/ مدحت رمضان: جرائم الاعتداء على الأشخاص عبر الإنترنت. الطبعة الأولى. دار النهضة العربية. ٢٠٠٠. ص ٨٧.

٢ د. محمود أبو اليزيد: الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية-رسالة دكتوراه. حقوق القاهرة ٢٠١٦. صـ٤٤٤.

٣ د. أحمد فتحي سرور: الوسيط في قانون العقوبات. القسم العام، طبعة ١٩٨٥، ص ٢١٢.

٤ د. عبد الله سليمان: شرح قانون العقوبات الجزائري. القسم العام. الجزء الأول (الجريمة). ديوان المطبوعات. الجامعية. الطبعة السابعة، الجزائر، ٢٠٠٩، ص٢٩.

فعل التجنيد: يقصد به تصيد واستقطاب الشباب وجمعهم للانخراط في الجماعات الإرهابية محلية كانت أو دولية، عن طريق إعدادهم ماديا ومعنويا للعمل في خدمة هذه الجماعات وتنفيذ مخططاتها الإرهابية[١]

ويتم ذلك عن طريق إنشاء مواقع إلكترونية تسمى» خلايا التجنيد » تستخدمها كبيئة افتراضية لجمع الأشخاص المغرر بهم أو المتعاطفين والمؤيدين للفكر الإرهابي.

والتجنيد قد يكون مباشرا كأن تخترق الجماعات الإرهابية حسابات البريد الإلكتروني لأشخاص وترسل لهم رسائل تجبرهم على الإنضمام إلى التنظيم الإرهابي، أو عن طريق اختطاف واحتجاز الرهائن لتجنيدهم فيما بعد، أو عن طريق الإعلان الصريح والانضمام الطوعي للجماعات الإرهابية، كما قد يكون التجنيد غير مباشر ويتم ذلك عن طريق أساليب الاستقطاب والاستدراج المختلفة كغسيل الدماغ الكترونيا وزرع الإفكار المتطرفة

وقد يقع التجنيد سواء على أشخاص معينين كالشباب ذوي الكفاءات العلمية العليا، كأن يكون خبير في تقنيات وسائل التكنولوجيا والإعلام، أو شخصية مشهورة لاستخدامه كقدوة، كما قد يقع التجنيد على أشخاص غير معنيين بذاتهم ويتم ذلك سواء عن طريق اصطياد الفتيات باسم الزواج في إطار ما يعرف ب «زواج النكاح»، أو عن طريق الدعاية المغرضة وأساليب الاستدراج والتجنيد الإلكتروني المختلفة التي سبق بيانها والتي تستهدف أي شاب مهما كانت صفته أو مستواه الثقافي والاجتماعي[٢]

وقد يكون القائم بالتجنيد شخص طبيعي كأن يقوم به إرهابي مكلف بتجنيد الشباب، كما قد يكون شخص معنوي كأن تكون شركة إعلامية أو دعائية أو جمعية خيرية أو دينية.

وبناء علي ذلك يجب تجريم كل من يستخدم وسائل التقنية الحديثة لتجنيد الأشخاص لصالح إرهابي أو جمعية أو جماعة أو منظمة يكون هدفها تدعيم أنشطتها ونشر أفكارها بصورة مباشرة أو غير مباشرة" .

البريد الإلكتروني : ويعد من أهم الوسائل المستخدمة في الإرهاب الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل في كثير من العمليات التي

١ نورا بنداري عبدالحميد فايد، دور وسائل التواصل الإجتماعي في تجنيد ، أعضاء التنظيمات الإرهابية ، دراسة حالة داعش، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسة والإقتصادية. ٢٠١٧ . ص٤٥.

٢ فتحية رصاع، الحماية الجنائية للمعلومات علي شبكة الإنترنت . رسالة ماجستير ، كلية الحقوق والعلوم الانسانية . جامعة تلمسان ،٢٠١٢ ، ص٥٦ .

حدثت كان البريد الإلكتروني فيها وسيلة من وسائل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها ، ويستغل الإرهابيون البريد الالكتروني أسوء الاستغلال أيضا من خلال قيامهم بنشر أفكارهم والترويج لها والسعي لتكثير الاتباع والمتعاطفين.(١)

إنشاء مواقع على الإنترنت: يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم ، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية.(٢)

التهديد والترويع الإلكتروني :

قد تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات ، ومن خلال الشبكة العالمية للمعلومات internet وتتعدد أساليب التهديد وتتنوع طرق وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية ومن أجل الحصول على التمويل المالي ولإبراز قوة التنظيم الإرهابي من ناحية أخرى.(٣)

رابعاً- تجريم وسائل الإرهاب الالكتروني في الشريعة الإسلامية:

إن الشريعة الإسلامية جاءت شاملة، صالحة لكل زمان ومكان محققة لسعادة البشرية في الآجل والعاجل فقد جاءت من عند الله سبحانه وتعالى- خالق الناس، والعالم بما يصلحهم في دنياهم وأخراهم، قال الله تعالى (مَا فَرَّطْنَا فِي الْكِتَابِ مِنْ شَيْءٍ) سورة الأنعام، آية ٣٨.

وقال الله تعالى : (الْيَوْمَ أَكْمَلْتُ لَكُمْ دِينَكُمْ وَأَتْمَمْتُ عَلَيْكُمْ نِعْمَتِي وَرَضِيتُ لَكُمُ الإِسْلامَ دِيناً) سورة المائدة، آية ٣.

لقد خلق الله الإنسان فأكرمه قال الله سبحانه وتعالى (وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ وَحَمَلْنَاهُمْ فِي الْبَرِّ وَالْبَحْرِ وَرَزَقْنَاهُمْ مِنَ الطَّيِّبَاتِ وَفَضَّلْنَاهُمْ عَلَى كَثِيرٍ مِمَّنْ خَلَقْنَا تَفْضِيلاً) سورة الإسراء، الآية ٧٠.

---

١ د. عبد الرحمن بن عبد الله السند: وسائل الإرهاب الالكتروني وحكمها في الإسلام وطرق مكافحتها. بحث منشور بالإنترنت، ٢٠١٠. ص ٣٥.

٢ د. سامي علي حامد عياد: استخدام تكنولوجيا المعلومات في مكافحة الإرهاب. مرجع سابق. ص٧١.

٣ د. عبد الله بن عبد العزيز بن فهد العجلان: مرجع سابق . ص ٢٥.

ولقد ميز الله الإنسان بالعقل والفهم ليعمل على إسعاد نفسه وبيئته ، ويسعى في عمارة الكون بما يصلح الخلق والأرض، واذا انحرف الإنسان عن هذه المهمة ونزع إلى الشر والفساد فهو مصادم للفطرة السليمة التي فطر الله الإنسان عليها.

إن من أبرز مظاهر الإنحراف عن الفطرة السليمة في هذا العصر الإرهاب ولا سيما استغلال الوسائل الحديثة في ذلك ، ولعل من الصور الحديثة للإرهاب استخدام الوسائل الالكترونية فيه.

البريد الالكتروني:

ويعد البريد الالكتروني من أعظم الوسائل المستخدمة في الإرهاب الالكتروني، من خلال استخدام البريد الالكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم ونشر أفكارهم والترويج لها ، ومما يقوم به الإرهابيون أيضا اختراق البريد الالكتروني للآخرين وهتك اسرارهم والاطلاع على معلوماتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية.[١]

لقد نهى الله جل جلاله – عن التجسس ، فقال سبحانه ، (ولا تجسسوا)[٢]

ونهت الشريعة الإسلامية عن الاطلاع على أسرار الناس وهتك حرماتهم ففي الحديث أن النبي صلى الله عليه وسلم قال (إنك إن اتبعت عورات المسلمين أفسدتهم أو كدت أن تفسدهم) (أبو داود الأدب ٤٨٨٨).

واختراق البريد الالكتروني هو خرق لخصوصية الآخرين وهتك لحرماتهم وتجسس على معلوماتهم وبياناتهم التي لا يرغبون أن يطلع عليها غيرهم والنبي صلى الله عليه وسلم يقول (لا تحسسوا ولا تجسوا) رواه البخاري في كتاب الأدب، باب ما ينتهي عن التحاسد والتدابير، ورواه مسلم في كتاب البر والصلة والأدب، باب تحريم الظن التجسس والتنافس.

وبذلك فإن الشريعة الإسلامية قد كفلت حفظ الحقوق 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 الحكم

١ د. محمود صالح العدلي: الفراغ التشريعي في مجال مكافحة الجريمة الالكترونية، ٢٠٠٩، جامعة طنطا، بحث منشور على الإنترنت، ص ٣٥.
٢ سورة الحجرات، الآية ١١٢.

بين الناس وتوعية المتعاملين بشبكة المعلومات العالمية (الإنترنت) بخطورة انتهاك خصوصية الآخرين وحكم ذلك في الشريعة الإسلامية.[١]

وأن هذا الامر مما استقرت الشريعة على تحريمه والنهي عنه، وقد تضافرت نصوص الكتاب والسنة على حفظ حقوق الآخرين وعدم انتهاكها ، بل قد تنادت الدول إلى تجريم مخترقي البريد الالكتروني لما فيه من ضياع للحقوق واعتداء على خصوصيات الآخرين وأسرارهم ولا سيما إذا كان ذلك لاستغلالها في الجرائم الإرهابية والعدوان على الآخرين.

إنشاء المواقع الالكترونية:

كان يقوم الإرهابيون بإنشاء مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم بل وتعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية.

ولا شك أن إنشاء المواقع للعدوان على الآخرين وتضليلهم ونشر الأفكار الهدامة محرم ولا يجوز ويقول الله سبحانه وتعالى : (وَلْتَكُنْ مِنْكُمْ أُمَّةٌ يَدْعُونَ إِلَى الْخَيْرِ وَيَأْمُرُونَ بِالْمَعْرُوفِ وَيَنْهَوْنَ عَنِ الْمُنْكَرِ) سورة آل عمران ، الآية ١٠٤.

ويقول رسول الله صلى الله عليه وسلم كما في الحديث الذي رواه أبو سعيد الخدري رضي الله عنه (من رأى منكم منكراً فليغيره بيده ، فإن لم يستطع فبلسانه ، فإن لم يستطع فبقلبه ، وذلك أضعف الإيمان)[٢].

تدمير المواقع الالكترونية:

لقد جاءت الشريعة الإسلامية بحفظ حقوق الآخرين وصيانتها قال الله جل وعلا في النهي عن الاعتداء: (وَلا تَعْتَدُوا إِنَّ اللَّهَ لا يُحِبُّ الْمُعْتَدِينَ) سورة البقرة آية ١٩٠.

فنهى الله سبحانه وتعالى عن الاعتداء، وان المواقع على شبكة المعلومات العالمية حق للآخرين لا يجوز الاعتداء عليه بأي وجه من الاعتداء ، وتدمير الموقع نوع من الاعتداء المحرم فهو لايجوز وقد صدر قرار مجمع الفقه الإسلامي في دورته الخامسة سنة ١٤٠٩ هـ بأن حقوق التأليف والاختراع أو الابتكار مصونة شرعاً ولأصحابها حق التصرف فيها ولا يجوز الاعتداء عليها.[٣]

---

١ د. عبد الرحمن بن عبد الله السند، وسائل الإرهاب الالكتروني، بحث منشور بالإنترنت، ص ٨.

٢ أخرجه الإمام مسلم في باب، بيان كون النهي عن المنكر من الإيمان، من كتاب الغيمان، صـ٦٩.

٣ مجلة مجمع الفقه الإسلامي، العدد الخامس، المجلد الثالث. صـ٢٢٦٧. مشار إليه لدى الدكتور/ عبد الله بن عبد الرحمن السند. مرجع سابق، ص ١٣.

فالاعتداء على مواقع الإنترنت ممنوع شرعاً من باب أولى، فإذا كان حق الاختراع والابتكار مصوناً شرعاً فكذلك المواقع على شبكة الإنترنت مصون.[١]

خامساً - تجريم أفعال الإرهاب الإلكتروني في تشريعات بعض الدول :

عندما نتحدث عن جرائم الإرهاب الإلكتروني فإننا نتحدث عن إحدى المفاهيم التي ظهرت حديثاً و التي لم تكن موجودة في الماضي، ففي الماضي لم يكن هناك تصور لدى فقهاء القانون الجنائي أن يكون هناك شئ يسمى « الجريمة الالكترونية» التي ترتكب في عالم افتراضي ليس له أي كيان مادي وأن الفضاء الإلكتروني سيكون مسرحاً لارتكاب جرائم على درجة عالية من الخطورة[٢].

وفيما يتعلق بالأساليب التشريعية في مواجهة خطر الجرائم الإلكترونية نجد أن هناك عدة مناهج أتبعت لمواجهة الإجرام الإلكتروني [٣].

فبعض التشريعات ركنت على النصوص العقابية التقليدية في مواجهة هذا النوع من الإجرام، ولم تقم بتعديل تشريعها لتتناسب مع هذا النوع الجديد من الجرائم[٤].

أما البعض الآخر من التشريعات فقد تنبه للطبيعة الخاصة لهذا النوع من الجرائم وأوجد نصوصًا عقابية خاصة تراعي الطبيعة الخاصة لهذا النوع من الجرائم، وتبني هذا الاتجاه أسلوبين: الأول : إدارج نصوص ضمن التشريعات العقابية التقليدية «أسلوب الإدراج» وبعضها أوجد قوانين خاصة بالإجرام الإلكتروني وعزلها عن التشريعات التقليدية وهو ما يسمى بأسلوب التشريع الخاص[٥].

القانون السعودي والإماراتي :

النظام السعودي قد بين في نظام مكافحة الجرائم المعلوماتية الأفعال التي جرمها بعقوبات محددة ومنظمة وهي كل الأفعال التي ترتكب بواسطة الوسائل الالكترونية.

إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها

---

١ د. عطا عبد العاطي محمد السنباطي، موقف الشريعة الإسلامية من جرائم الحاسب الآلي والإنترنت، دراسة مقارنة، دار النهضة العربية ١٤٢٢هـ- ط١ ، ٢٠٠٢، ص ٣٥.

2 http://www.shaimaaatalla.com/ Vb/ new thread.php? Do= new thread= 77#-ftn1.

٣ د. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن. دار النهضة العربية. القاهرة. ١٩٩٢. ص ٢٠.

٤ د. عبدالله محمد النويسه، جرائم تكنولوجيا المعلومات ، دارسة تحليلية مقارنة.، دار وائل للطباعة والنشر والتوزيع. ص ٩.

٥ د. على عدنان الفيل. الإجرام الإلكتروني. دراسة مقارنة. لبنان ، الطبعة الأولى. ٢٠١٠. ص ٧٤.

أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أدوات تستخدم في الأعمال الإرهابية .

كما جرم الدخول غير المشروع إلى موقع الكتروني أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي، أو الخارجي للدولة أو اقتصادها الوطني.

كما نص قانون مكافحة جرائم تقنية المعلومات الإماراتي على الجرائم الإرهابية التي ترتكب بواسطة الوسائل الالكترونية.

تنص المادة(٩) من القانون الإماراتي علي أن « كل من استعمل الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها في تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عن فعل ، ولو كان هذا الفعل أو الامتناع مشروعاً ، يعاقب بالحبس .... والغرامة .....أو بإحدى هاتين العقوبتين »

فنص في المادة (٢١) على « كل من أنشأ أو نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالسجن).

كما نصت المادة (٢٠) «كل من أنشأ أو نشر موقعا على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لأي مجموعة تدعو لتسهيل وترويج أفكار وبرامج مخالفة للنظام العام يعاقب بالحبس والغرامة...).

المادة (٢٢) كل من دخل عمدا وبغير وجه حق موقعاً أو نظاماً مباشراً أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني يعاقب بالسجن.

بالنسبة للمشرع الأردني ، ففي ظل قانون العقوبات رقم ١٦ لسنة ١٩٦٠ وقانون منع الإرهاب رقم ٥٥ لسنة ٢٠٠٦ (قبل التعديل الأخير) لم ينص المشرع بنص خاص على تجريم الإرهاب الإلكتروني ،وانما ركن إلي النصوص التقليدية في تجريم الإرهاب

بصورته التقليدية ؛ حيث إن النصوص التقليدية تسمح بإدراج كافة صور الإرهاب الإلكتروني ، إضافة إلي أن النصوص الناطقة لجرائم أمن الدولة تتسم بالمرونة بشكل يستوعب الإرهاب الإلكتروني، ولكن أجرى المشرع تعديلاً على قانون منع الإرهاب وعدل القانون القديم بالقانون رقم ١٨ لسنة ٢٠١٤ وأضاف إليه نصاً صريحاً اعتبر فيه الإرهاب الإلكتروني في حكم الأعمال الإرهابية المحظورة حيث أورد في نص المادة ٣ فقرة (٥) (استخدام نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو إعلام أو إنشاء موقع إلكتروني لتسهيل القيام بأعمال إرهابية أو الترويج لأفكارها أو تمويلها أو القيام بأي عمل من شأنه تعريض الأردنيين أو ممتلكاتهم لخطر أعمال عدائية أو انتقامية تقع عليهم).

في الولايات المتحدة الأمريكية : تعتبر الولايات المتحدة الأمريكية من الدول السباقة إلي إعداد وإصدار قوانين تخص محاربة الإرهاب الإلكتروني ، فمباشرة بعد أحداث ١١ سبتمبر ٢٠٠١ ظهرت أول اتفاقية أمريكية لمكافحة الإرهاب الإلكتروني ، والتي بمقتضاها يتم تعزيز سلطات البحث والتحقيق وتوسيع صلاحيات المراقبة الإلكترونية ، ومن بين البنود العملية التي ينص عليها القانون الأمريكي لمكافحة الإرهاب الإلكتروني تلك التي تنص علي الصلاحية المخولة لقاضي النيابة ولمكتب التحقيقات الفيدرالي بالتقاط الرسائل الإلكترونية المشتبه فيها بدون إذن القاضي ، شريطة إثباتهم بأن الأمر يتعلق بقضية مكافحة إرهاب ، ومن المقتضيات التي ينص عليها القانون تلك التي تسمح للنائب الفيدرالي أو العام وبدون اشتراط الحصول علي إذن القاضي بمراقبة أنشطة المشتبه فيهم علي شبكة الإنترنت بواسطة نظام Dcs ١٠٠٠ المتطور، كما يجبر القانون الأمريكي ـ الخاص بالمراقبة الإلكترونية ـ كل المزودين بحق الولوج الي الإنترنت وشركات استغلال خطوط الهاتف بتقديم جميع المعلومات المطلوبة عن عملائهم المشتبه فيهم من قبل الشرطة الفيدرالية ، وذلك في حالة ما إذا كانت التسجيلات المطلوبة لها علاقة بأبحاث وتحقيقات مسموح بها في إطار الوقاية من الإرهاب الدولي ، كما وسع القانون الأمريكي الجديد من مفهوم الإرهاب ؛ حيث أصبح في عداد الإرهاب الإلكتروني كل فعل أو قرصنة ينتج عنه ضرر يقدر بـ ٥٠٠٠ دولار في السنة ، ولتفعيل المقتضيات الجديدة ينص قانون مكافحة الإرهاب علي إنشاء مركز للخبرة وللتكوين المعلوماتي يوضع رهن إشارة السلطات الفيدرالية .[١]

١ عبد الحق باسو ، الإرهاب المعلوماتي في القانون المغربي والدولي . المؤتمر العام لمكافحة الجرائم الإرهابية المعلوماتية بالمغرب خلال الفترة من ١١ـ ١٥ /٢/ ٢٠٠٦ م صـ ٢١ .

في مصر لم يفرد المشرع نصاً خاصاً لتجريم الإرهاب الإلكتروني وانما ركن إلي النصوص التقليدية في تجريم الإرهاب بصورته التقليدية ، ونص في قانون مكافحة الإرهاب رقم ٩٤لسنة ٢٠١٥ في المادة «٢٩» علي أن (يعاقب بالسجن المشدد مدة لا تقل عن خمس سنين : كل من أنشأ أو استخدم موقعاً علي شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها ؛ بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية ، أو لبث ما يهدف إلى تضليل السلطات الأمنية ، أو التأثير علي سير العدالة في شأن أي جريمة إرهابية ، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها في الداخل ، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج .

ويعاقب بالسجن المشدد مدة لا تقل عن عشر سنين، كل من دخل بغير حق أو بطريقة غير مشروعة موقعاً الكترونياً تابعاً لأية جهة حكومية ، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الأطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها . وذلك كله بغرض ارتكاب جريمة من الجرائم المشار اليها بالفقرة الأولى من هذه المادة أو الإعداد لها .)

المطلب الثاني

النتيجة في جرائم الإرهاب الالكتروني

١-النتيجة في مدلولها القانوني: هي العدوان الذي ينال مصلحة أو حقاً قدر الشارع جدارته بالحماية الجنائية.[١] فالنتيجة القانونية للسلوك الإرهابي تنصرف إلى العدوان على حق أو مصلحة من خلال المساس بها مساساً من شأنه الإضرار بها أو تعطيلها كلياً أو جزئياً أو الانتقاص منها أو مجرد تعريضها للخطر.

وهذا يعني أن النتيجة القانونية في الجرائم الإرهابية تتحقق بمجرد المساس بالمصلحة المحمية من خلال السلوك الاجرامي الإرهابي مساسا من شأنه الإضرار بها أو مجرد تعريضها للخطر.[٢] والذي تستهدفه الجريمة في هذه الحالة هو خطر عام موجه ضد أسس النظام الاقتصادي والاجتماعي في الدولة.[٣]

---

١ د. محمود نجيب حسني، علاقة السببية في قانون العقوبات، نادي القضاة، ١٩٨٤، ص٤٥.

٢ د. عثمان حسن، الإرهاب الدولي ومظاهره القانونية والسياسية، دار الكتب القانونية، الطبعة الأولى، ٢٠١١، ص١١١-١١٢.

٣ د. أمال عثمان، فكرة الخطر في الجرائم الاقتصادية بصفة عامة، دار النهضة العربية، بند ١٧، ص٤٥.

مثال ذلك جريمة التجنيد الإلكتروني وهي جريمة شكلية لا تتطلب تحقق النتيجة الإجرامية لقيام ركنها المادي ، وإنما تتحقق بمجرد الشروع في الأعمال التحضيرية مثل(إنشاء وتصميم مواقع وحسابات الكترونية إرهابية) وبالتالي فهي تشكل جريمة قائمة بذاتها ولو لم يتحقق فعل التجنيد فعليا كونها جريمة خطر وليس ضرر، وذلك بالنظر للوسيلة المعتمد عليها في تنفيذ الجريمة .

والخطر هنا : هو النتيجة التي يجب أن يعاقب عليها القانون ليتفادى حدوث الضرر.[١]

وقد تستهدف الأفعال غير المشروعة لجرائم الإرهاب الالكتروني أسس التعامل الاقتصادي ، مثل : الإضرار بالبورصة والتلاعب بالأسهم من خلال الشبكات الالكترونية ؛ مما يؤدي إلى الإخلال بالثقة في التعامل بين الشركات التي تعمل في مجال سوق المال وبين الأفراد المتعاملين معها. ويعد من أبرز الجرائم التي تهدد الاقتصاد هي التلاعب بالتجارة الالكترونية ،وذلك من خلال عرض أسهم واستثمارات مزورة وبيعها.

وكذلك اختراق البنوك وسرقة معلومات العملاء وكذلك سرق الأرصدة وتحويلها لبنوك أخرى.[٢]

وحيث إن جوهر القصد في هذه الجريمة إنما يكمن في ارتكاب السلوك المادي لأجل تحقق النتيجة التي تتمثل في إهدار مصلحة يحميها القانون.[٣]

فهنا ينال التجريم سلوكا صدر من الجاني وانطوى على خطر إحداث النتيجة دون أن تكون هذه النتيجة عنصرا في الركن المادي للجريمة ، فنشاط الجاني وقف عند تهديده للمصلحة المحمية بالخطر دون أن يترتب عليها ضرر حقيقي.[٤]

وبذلك فإن النتيجة الإجرامية اللازمة لوقوع جريمة الإرهاب الالكتروني تتوافر بمجرد المساس بالحقوق والمصالح المحمية التي يقع عليها العنف الإرهابي ، سواء بوقوع الضرر أو بمجرد التعريض للخطر.[٥]

---

١ د. محمود محمد مصطفى، شرح قانون العقوبات، القسم العام الطبعة العاشرة، ١٩٨٣، مطبعة جامعة القاهرة، ص٢٨٠.

٢ د. سيد شوربجي عبد المولى، تأثير الجريمة على خطط التنمية الاجتماعية والاقتصادية في الوطن العربي. بحث منشور بالإنترنت، ص١٦٦-١٦٧.

3 0 Alice yatopaulous-Marangop oulos: les mobiles du delet decriminalogyet de droit penal- Bibliotheque de sciences criminelles. Tome xvll. 2004.p. 103.

٤ د. أمال عثمان، شرح قانون العقوبات الاقتصادي في جرائم التموين، ١٩٨٣. دار النهضة العربية. بند ١٥، ص٤٣.

٥ د. أحمد فتحي سرور، المواجهة القانونية للإرهاب، مرجع سابق ص٢٤٧.

ولذلك فإن القانون القطري رقم ٣ لسنة ٢٠٠٤ بشأن مكافحة الإرهاب قد ربط بين السلوك الإجرامي وبين المساس بالحقوق أو المصالح التي يكون من شأن هذا السلوك تحقيقه.[١]

كما أن القانون البريطاني للإرهاب الصادر سنة ٢٠٠٠ المعدل سنة ٢٠٠٣ وسنة ٢٠٠٦ نجد أنه من حيث السلوك الإجرامي قد نص على أن العمل الإرهابي يقصد به استخدام فعل أو التهديد به (أ) إذا كان يتضمن أو يقضي حتما (involves) إحداث أذى جسيم ضد شخص (ب) أو إحداث ضرر جسيم ضد الملكية ، (ج) أو تعريض حياة شخص للخطر- غير الشخص الذي ارتكب الفعل، (د) أو أن يكون قد رتب خطراً جسيماً على الصحة أو سلامة العامة أو بعضهم، (هـ) أو إذا كان الفعل موجباً على نحو جسيم للتدخل أو التعطيل الجسيم لنظام الكتروني.[٢]

وعلى المنهج نفسه في تحديد النتيجة القانونية سار قانون العقوبات الفرنسي (٤٢١-١) إذ اعتبر أعمال الإرهاب متوفرة إذا كانت مرتبطة بمشرع فردي أو جماعي يهدف إلى إحداث اضطراب جسيم بالنظام العام من خلال الترويع أو التخويف.

وذلك من خلال قائمة من الجرائم منها على سبيل المثال الجرائم الماسة بالحياة وسلامة الشخص ، وحريته وسلامة الطيران ، وغير ذلك من وسائل النقل والماسة بحق الملكية المعلوماتية[٣].

ويتضح من ذلك أن قانون العقوبات الفرنسي يشترط نتيجتين قانونيتين الأولى: هي المساس بالنظام العام بإحداث الترويع أو التخويف . والثانية : هي المساس بنوع من الحقوق والمصالح التي يحميها قانون العقوبات يصل إلى حد وقوع الجرائم التي نص عليها قانون العقوبات عند المساس بهذه الحقوق.

٢-أما النتيجة في مدلولها المادي فتتمثل : في أثر السلوك الإجرامي كنتيجة مادية يتمثل بالتغير الذي يستهدف الأشخاص أو الأشياء كالوفاة في جرائم القتل والأذى في جرائم الإيذاء والتخريب والتدمير والهدم في جرائم الإتلاف.[٤]

---

١ وهو على حد تعبير القانون القطري (إيذاء الناس أو تسبيب الرعب لهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو الصحة العامة أو الاقتصاد الوطني ، أو المرافق أو المنشآت أو الممتلكات العامة أو الخاصة أو الاستيلاء عليها أو عرقلة أدائها لأعمالها أو منع أو عرقلة السلطات العامة عن ممارسة أعمالها (المادة ١)

٢ د. سعيد على النقبي، المواجهة القانونية للإرهاب ، دار النهضة العربية . القاهرة. الطبعة الأولى، ٢٠١١. صـ١٦٩-١٧٠.

٣ د. أحمد فتحي سرور، المواجهة القانونية للإرهاب . مرجع سابق. ص ٢٥٠.

٤ د. حسن عثمان، الإرهاب الدولي مظاهره القانونية، مرجع سابق، ص١١٢.

ولا يشترط لتوافر النموذج القانوني للإرهاب وقوع نتيجة مادية معينة ؛ إذ يكفي لانطباق وصف جرائم الإرهاب مجرد المساس بالحقوق أو المصالح المحمية ، سواء تم هذا المساس في صورة ضرر أو في شكل التعريض للخطر، وهو ما عني أن هذه الجريمة يكفي لوقوعها قانونا توافر مجرد الخطر. كما يلاحظ أن مسألة النتيجة الاجرامية في جرائم الإنترنت تثير مشاكل عديدة ، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية ، فإذا قام أحد المجرمين في بلد ما باختراق جهاز خادم server لأحد الشركات في أوربا ، وهو في بلد موجود في كندا فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت الجهاز الخادم ، والقانون الواجب التطبيق في هذا الشأن.[١]

أيضا ارتكاب الجرائم بواسطة التقنية الحديثة تثير مشكلة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بواسطة شبكة الاتصال عن بُعد ، والقواعد التقليدية في الإثبات لا يكفي لضبط مثل هذه المعلومات بحثا عن الأدلة وتحقيقها، فمن الصعب إجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية ، حيث إن هذا الإجراء يتعارض مع سيادة هذه الدولة الأخيرة.[٢]

من ناحية أخرى فإن أدلة الإثبات المتحصلة من التفتيش على نظم الحاسوب والإنترنت تحتاج إلى خبرة فنية ودراية فائقة في هذا المجال ؛ ذلك لأن نقص الخبرة في جمع الأدلة قد يؤدي إلى ضياع الدليل بل تدميره أحيانا.[٣]

إن الغاية المادية البحتة التي يسعى إلى تحقيقها المجرم الالكتروني من سطو على الأموال ، واعتداء على البيانات السرية وتدمير البرامج المعلوماتية لأية دولة لتهديد أمنها القومي وسلامة أراضيها. ولعل أبرز مثال على ذلك اقتحام موقع وزارة الدفاع الأمريكي ، وهو الصورة الحديثة للإرهاب الذي يعرف بإرهاب المستقبل.[٤]

الذي أصبح هاجسا حقيقيا يهدد سلامة وأمن المجتمع الدولي عن طريق التهديد بتدمير أساليب واستراتيجية الدفاعات الأمنية والاقتصادية للدول وعوائدها المالية باستخدام الخطط التخريبية والفيروسات لتدمير مختلف المعلوماتية ، وإتلاف مختلف البيانات الخاصة بالتقنية الرقمية في حفظ وتخزين البرامج المعلوماتية لأية دولة مهما كانت درجة سريتها.

---

١ صغير يوسف، الجريمة المرتكبة عبر الإنترنت ، رسالة ماجستير منشورة بالإنترنت ، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١٣، ص ٦٥.

٢ د. أمال عبد الرحيم عثمان، مرجع سابق ، ص ٢٤

٣ د. جلال محمد الزعبي، جرائم الحاسوب الآلي والإنترنت. دراسة تحليلية مقارنة، ط١، دار وائل، عمان، ٢٠٠١م، ص٢٨٩-٢٩٧.

٤ د. علي سعيد عبد اللطيف، الجرائم الناشئة عن استخدام الحاسب الآلي، كلية الشريعة والقانون، القاهرة، بحث منشور بالإنترنت، ص٩٣.

المطلب الثالث

علاقة السببية في جرائم الإرهاب الالكتروني

السببية المادية : هي علاقة بين سلوك الجاني وما تحقق من نتائج بحيث يسمح بنسبتها ماديا إلى الجاني، فلا يكفي لقيام الركن المادي للجريمة أن يقع سلوك إجرامي من الفاعل ، وأن تحصل نتيجة بل يلزم فضلا عن ذلك أن تنسب هذه النتيجة إلى ذلك السلوك.(١)

فعلاقة السببية تسند النتيجة الإجرامية إلى فعل ومعنى ذلك أنها تقرر توافر الركن المادي للجريمة ، إذ باتصال النتيجة بالفعل تقوم وحدة الركن المادي للجريمة.

وهذا الركن يعد عنصرًا أساسيًا للمسؤولية فيكون مؤدى ذلك أن عناصر هذا الركن ومنها علاقة السببية هي كذلك من عناصر المسؤولية .(٢)

ولا تثير علاقة السببية صعوبة في مدى توافرها وإثباتها في جرائم الإرهاب بصورتها التقليدية فجرائم الإرهاب بصورتها التقليدية تأخذ صورة الجرائم المادية التي تستلزم تحقق نتيجة إجرامية ترتبط بالسلوك ويكون من السهل إثباتها.

ولكن المشكلة تثور في جرائم الإرهاب الالكتروني حيث إنه يكون من الصعب إثبات علاقة السببية في الجرائم المرتكبة عبر الإنترنت ، فهنا الفرق بين الجريمة الالكترونية والجريمة العادية يظهر في علاقة السببية ودليل الإثبات الجنائي.

فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات أو مقدرات الحاسب الآلي في ترويع وإكراه الآخرين، فهو يتم عن بعد دون اللجوء للعنف المادي والجسدي.(٣)

وقد يمثل البريد الالكتروني إحدى الصور المستخدمة في التقنيات الحديثة ، فإذا قام شخص بالاحتيال على شخص آخر من خلال إرسال رسائل له عن طريق البريد الالكتروني، فهنا لا يكتمل الركن المادي لجريمة الاحتيال إلا من خلال إثبات السلوك الذي قام به الجاني من خلال البريد الالكتروني وعلاقة السببية بين الفعل الذي استخدمه الجاني للنصب على المجني عليه وبين النتيجة المتمثلة في تسلم المال محل الجريمة ، أي أن تسلم المال كان نتيجة منطقية ثابتة للخدعة التي وقع بها المجني عليه.

١ د. محمود محمود مصطفى: مرجع سابق، ص ٢٨٦.
٢ د. محمود نجيب حسني: علاقة السببية في قانون العقوبات، مرجع سابق، ص ٤٩
٣ د. حيدر علي نوري: الجريمة الإرهابية، دراسة في ضوء قانون مكافحة الإرهاب، منشورات زين الحقوقية، لبنان، ط١، ٢٠١٣، ص ١٩٩.

وبالرجوع إلى القواعد العامة في الجريمة نجد أن مثلث الركن المادي للجريمة لا يكتمل عدد أضلاعه إلا بوجود رابطة بين السبب المتمثل بالسلوك المادي للجاني والنتيجة المتحققة بسبب هذا السلوك ، فإن لم تكن النتيجة بسبب ذلك السلوك انعدمت الرابطة السببية بينهما.[١]

فعلاقة السببية في جريمة الاحتيال تفيد أن ما قام به الجاني من أفعال وسلوكيات كانت هي السبب الذي حمل المجني عليه على تسليم المال أو نقل حيازته .

ومن ثم إذا انعدمت طريقة الاحتيال ومع ذلك انخدع الشخص الآخر ، فإن الواقعة لا تعد احتيالاً، عندئذ تنتفي علاقة السببية متى ثبت أن تسليم المال لم يكن نتيجة للغش والخداع ، بل كان بسبب آخر كالخوف والرهبة من الجاني.[٢]

فالإثبات الجنائي في جرائم الإرهاب الالكتروني يهدف إلى الوصول إلى اليقين القضائي طبقا لمعيار الحقيقة وذلك بشأن الاتهام أو أي تأكيد أو نفي آخر يتوقف عليه إجراء قضائي بمعنى آخر هو إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعلها.[٣]

وتثير مسألة الإثبات في نظم الحاسوب والإنترنت صعوبات كبيرة أمام القائمين على التحقيق.[٤]

مثال ذلك التخزين الالكتروني للمعطيات الذي يجعلها غير مرئية وغير مفهومة بالعين المجردة ويشكل انعدام الدليل المرئي عقبة كبيرة أمام كشف الجرائم، وقد يشكل تشفير البيانات المخزنة الكترونيا أو المنقولة عبر الاتصال عن بُعد عقبة كبيرة أمام إثبات الجريمة المعلوماتية والبحث عن الأدلة، كما أن سهولة محو الدليل في زمن قصير تعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسوب والإنترنت.[٥]

---

١ د. خالد حامد مصطفى، المسؤولية الجنائية المباشرة، الخدمات التقنية ومقدميها بحث منشور بالإنترنت، ٢٠١٦، ص ٩٥.

٢ د. سامر سعدون عبود، التحريض على ارتكاب الجرائم الإرهابية باستخدام وسائل التقنية الحديثة، كلية القانون جامعة بغداد. بحث منشور بالإنترنت، ٢٠١٦، ص ٥٣٩.

٣ د. آمال عبد الرحيم عثمان، الإثبات الجنائي ووسائل التحقيق العلمية دار النهضة العربية، القاهرة، ١٩٧٥م. ص٤.

٤ د. سعيد عبد اللطيف حسن، الإثبات في جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية. القاهرة. ١٩٩٩. ص٩٥ وما بعدها.

د. عبد الفتاح بيومي حجازي : الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٢م ص ٤٦.

لذلك لا يكفي لقيام جرائم الإرهاب المستخدمة بوسائل التقنية الحديثة أن يرتكب الجاني السلوك غير المشروع وإنما يجب أن تكون هناك علاقة سببية قائمة بين الأفعال التي يرتكبها الجاني وبين النتيجة الإجرامية.

فعلاقة السببية في المواد الجنائية علاقة مادية تبدأ بالفعل المتسبب وترتبط به من الناحية المعنوية بما يجب عليه أن يتوقعه من النتائج المألوفة لفعله إذا أتاه عمدا، أو خروجه فيما يرتكبه بخطئه عن دائرة التبصر بالعواقب العادية لسلوكه والتصون من أن يلحق عمله ضررا بالغير.(١)

من ناحية أخرى فإن جرائم الإرهاب المستخدم بوسائل التقنية الحديثة البعض منها يأخذ صور الجرائم المادية التي تستلزم تحقق نتيجة إجرامية ترتبط بالسلوك، والبعض الآخر يأخذ صور الجرائم الشكلية التي يكفي فيها توافر السلوك دون وقوع النتيجة، فهذه الجرائم الأخيرة تعد من جرائم الخطر، الفرض فيها أن هناك حالة خطر ناشئة عن السلوك ، وهنا تقدير الفاعلية السببية يكون بناءً على تقدير احتمالي سابق على تحقيق النتيجة.

فإذا كان تقييم السلوك يؤدي إلى القول بإحداث النتيجة الضارة اكتمل الركن المادي للجريمة، لأنه بذلك يحقق الخطر المعاقب عليه والمتمثل في مكنه تحقيق النتيجة الضارة.(٢)

والجرائم الشكلية تمثل طائفة من الصور التي تجرم بعض صور الإرهاب مثل جريمة تعريض حياة الناس وحرياتهم وأمنهم للخطر وجريمة الاعتداء بالأسلحة النارية على دوائر أجهزة الجيش والشرطة وجريمة استخدام أجهزة متفجرات أو الحارقة وهذه الجرائم يكتفي فيها الشرع بذكر السلوك دون النتيجة.(٣)

وبذلك فإن علاقة السببية تكتسب أهمية بالغة في تحديد المسؤولية الجنائية للفاعل في الجرائم الإرهابية التي تتم بواسطة وسائل التقنية الحديثة.

---

١ نقض ١٩٨٠/٢/٧ مجموعة أحكام محكمة النقض – الدائرة الجنائية – س ٤٩ ق – رقم ٨٧٧ – ص ٢٠٠.

٢ د. مأمون محمد سلامة، قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العامة، دار الفكر العربي، ١٩٩٦، ص ١٦٨.

٣ د. سعد صالح الجبوري، الجرائم الإرهابية في القانون الجنائي، دراسة مقارنة في الأحكام الموضوعية، المؤسسة الحديثة للكتاب، ط١، ٢٠١١، ص ٦٦.

المبحث الثاني

جوهر المسؤولية الجنائية العمدية الناشئة عن جرائم الإرهاب الالكتروني

الركن المعنوي في جرائم الإرهاب الالكتروني :

يؤدي الركن المعنوي دوراً مهما في إضفاء الوصف القانوني لجريمة الإرهاب لتمييزها عن غيرها من الجرائم، فيتمثل في رابطة نفسية تربط الواقعة المجرمة بإرادة الإرهاب والتي تأخذ شكل العمد وهي تعبر عن موقف الإرادة المؤثمة قانونا حيال الواقعة المرتكبة.[١]

فلا يشترط لقيام الجريمة الإرهابية مجرد قيام مشروع فردي أو جماعي يستهدف المساس الخطير بالنظام العام بواسطة التخويف أو التهديد أو العنف ولو تحققت الصورة الإجرامية المنصوص عليها في هذا الشق ، بل يتعين وجوب توافر عنصر العمد لدى الفاعل الإجرامي وهو ما يصطلح على تسميته بالركن المعنوي في الجريمة الإرهابية.[٢] والركن المعنوي هو الذي يعبر عن الناحية المعنوية للجريمة وبه تنسب الجريمة لشخص ما ويتحمل مسؤوليتها أو لا تنسب إليه وهو إما خطأ غير عمدي أو جريمة عمدية تعبر عن روح العدوان لدى صاحبه وهو ما يعرف بالقصد الجنائي.[٣]

وتعد جريمة العمل الإرهابي باستخدام وسائل التقنية الحديثة من الجرائم القصدية التي يتمثل فيها الركن المعنوي في صورة القصد الجنائي ، فهي لا تقع بطريقة الخطأ إلا أن القصد الجنائي العام لا يكفي لقيام هذه الجريمة ، بل لابد من توافر القصد الجنائي الخاص المتمثل في إيجاد حالة من الذعر بين الناس أو الإخلال بالأمن العام أو الأضرار بالبنية التحتية أو الأساسية للدولة ، وهذا القصد الخاص هو الذي يميز جريمة العمل الإرهابي عن غيرها من الجرائم التي قد ترتكب بالأفعال والوسائل نفسها.

وفي الجرائم الإرهابية لا يتصور عدم اتجاه إرادة الفاعل إلى إحداث النتيجة الإجرامية.[٤]

---

١ د. سعيد الجبوري، مرجع سابق، ص ٦٦.

٢ د. حسن عثمان، مرجع سابق، ص ١١٥.

٣ د. سعد صالح الجبوري، مرجع سابق ص ٦٧.

٤ د. محمود داوود يعقوب، المفهوم القانوني للإرهاب ، دراسة تحليلية تأصيلية مقارنة ، منشورات أين الحقوقية، الطبعة الثانية، ٢٠١٣، تونس، ص ٧٠.

وبذلك فإن جرائم الإرهاب تتطلب توافر القصد الجنائي العام بوصفها جريمة عمدية ، وقصد جنائي خاص يعبر عنه بالنية الإرهابية.

وعلى هدي ما سبق سنقسم هذا المبحث إلى ثلاثة مطالب على النحو الآتي :

المطلب الأول : القصد الجنائي العام في جرائم الإرهاب الالكتروني.

المطلب الثاني: القصد الجنائي الخاص في جرائم الإرهاب الالكتروني.

المطلب الثالث : القصد الجنائي في جرائم الإرهاب باستخدام الوسائل الالكترونية في القانون السعودي والإماراتي.

المطلب الأول

القصد الجنائي العام في جرائم الإرهاب الالكتروني

يتحقق القصد الجنائي العام بانصراف إرادة الجاني إلى إتيان السلوك الإجرامي وهو عالم لصفته مدرك لنتيجته ، بمعنى أن إرادة الفاعل يجب أن تنصب على ماديات الجريمة أي ركنها المادي بحيث تسيطر على السلوك وتوجهه إلى النتيجة التي تهدف إليها ، كما يتوجب أن تحيط علم الجاني بالواقعة المجرمة بحيث يشمل ماديات الجريمة جميعها من سلوك ونتيجة وعلاقة سببية ، وكل واقعة يستند فيها السلوك الإجرامي لدلالته الإجرامية عن ضرورة انصراف علم الجاني إلى الركن الخاص في الجريمة الإرهابية ، وهو المشروع الإجرامي الإرهابي والقصد الإجرامي هو علم الجاني بحقيقة فعله الإرهابي ووسيلته وانصراف إرادته إلى ارتكابه.[١]

ففي جرائم الإرهاب بصورتها التقليدية يشترط اتجاه إرادة الجاني إلى استخدام القوة أو العنف أو التهديد أو الترويع مع علمه أن هذا السلوك من شأنه ، أي من طبيعته أن يؤدي إلى المساس بالحقوق والمصالح التي حددتها هذه المادة والذي يتمثل في الاعتداء على الحق في الحياة أو الحق في الأمن أو الحق في البيئة أو غير ذلك من الحقوق والمصالح العامة.[٢]

أما في جرائم الإرهاب الالكتروني يجب أن يكون الجاني على علم بتدخله في خصوصية الغير على وجه غير مشروع واتجاه وإرادته إلى إتيان فعل الاستعمال.[٣]

---

١ د. علي حامد عيد ، تمويل الإرهاب ، دار الفكر العربي، الإسكندرية، ط١، ٢٠٠٧، ص ١١٥.

٢ د. كاظم عيد جاسم جبر، مكافحة جرائم الإرهاب في التشريع العراقي، دار الكتب والوثائق، بغداد، ٢٠١٠، ط١، بحث منشور بالإنترنت، ص ٣٤.

٣ د. أحمد محمد مصطفى، الإرهاب ومواجهته جنائيا دار الفتح للطباعة والنشر ، القاهرة، ط١، ٢٠٠٦، ص ١٥٦.

وحيث إن المجرم الالكتروني يتسم بصفات خاصة أهمها : أنه يتمتع باحترافية كبيرة في تنفيذ جرائمه حيث إنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر الذي يقتضي الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.[١]

فهنا عندما يقوم الإرهابيون باستخدام وسائل التقنية الحديثة مثل البريد الالكتروني في إرسال رسائل تهديد وقد تتنوع أساليب التهديد وطرقها من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب، أيضا إذا قام المجرم الالكتروني بإرسال رسائل تدمير البيانات المخزنة في الغالب في نظم المعلومات.[٢]

فهذا المجرم يتوافر لديه القصد الجنائي العام باتجاه إرادة الجاني إلى السلوك الإجرامي الذي باشره والى النتيجة المترتبة عليها.

إن المجرم الالكتروني يتجه من أجل ارتكاب فعل غير مشروع أو غير مسموح مع علم هذا المجرم بارتكاب الجريمة ، وبالرغم من ذلك فإن بعض المخترقين يبررون أفعالهم بأنهم مجرد فضوليين ، وأنهم قد تسللوا صدفة ، فهنا لا ينتفي العلم كركن في القصد الجنائي.

وكان يجب عليهم أن يتراجعوا لمجرد دخولهم ، ولا يستمر في الاطلاع على أسرار الأفراد والمؤسسات ؛ لأن جميع المجرمين والأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية ومعرفية كبيرة تصل في كثير من الأحيان إلى حد العبقرية ، فالقصد الجنائي متوافر في جميع الجرائم الإلكترونية دون استثناء ، ولكن هذا لا يمنع أن هناك بعض الجرائم الالكترونية تتطلب أن يتوافر فيها القصد الجنائي الخاص ، مثل : جريمة تشويه السمعة عبر الإنترنت ، أما جرائم نشر الفيروسات عبر الشبكة فهي تتوافر في القصد الجنائي الخاص.[٣]

تحديد القصد الجنائي العام:

القصد الجنائي العام يعد من أخطر صور الركن المعنوي للجريمة ، ففيه تنصرف إرادة الجاني إلى الفعل الذي يأتيه ، والى النتيجة المقصودة بالعقاب ، فتبدو المعصية لأوامر الشارع ونواهيه في أخطر صورها.[٤]

١ د. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠١، ص ٧٥.
٢ د. عبد الله بن عبد العزيز بن فهد العجلان، مرجع سابق ، ص ٢٥.
٣ د. سعيد علي النقبي ، مرجع سابق ، ص ١٧١.
٤ د. علي محمود علي حمودة ، شرح قانون العقوبات القسم العام، الجزء الأول، دار الهاني للنشر، ٢٠٠٣، صـ٤٥.

فتوافر الركن المعنوي في الجرائم الإلكترونية يعد من الأمور المهمة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلزم تطبيقها إذ بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع.

فمثلا التمييز بين جريمة الدخول غير المشروع على نظام المعالجة الآلية للبيات وبين جريمة تجاوز الصلاحيات في الدخول على مثل هذا النظام يعد تمييزا دقيقا.

ففي جريمة تجاوز صلاحية الدخول، فإنه يلزم لتوافرها أن يكون هناك صلاحية للدخول على نظام ما، على أن تتوافر في داخل هذا النظام أنظمة معينة ليس من حق هذا الشخص الدخول عليها، فيقوم المذكور بالدخول عليها ففي هذه الحالة لا تتوافر سوى جريمة واحدة حيث إن المذكور يملك صلاحية الدخول على النظام الأساسي ولا يملك الدخول على أنظمة خالية فيها، إلا أن تكوين النشاط المادي هنا يلزم أن يكون السلوك الإجرامي مرتكبا في إطار نشاط ثان وليس النشاط الأول ، مثل هذا الأمر يجعل جريمة تجاوز صلاحيات الدخول معتبراً من الجرائم التي يتطلب فيها توافر القصد الجنائي العام.(١)

ترتيباً على ذلك فإن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام وسائل التقنيات الحديثة من حيث مدى تحديد ما إذا كانت تتطلب قصدا عاما أم خاصا، فذلك لا يمانع في تطلب قصد جنائي خاص في جريمة التهديد الالكتروني، إلا أنه يقر من جديد أنه يكتفي بالقصد العام عن ذات الجريمة ، كما هو الشأن في جريمة التهديد بالبريد الالكتروني.(٢)

أما القضاء الفرنسي فإن منطق سوء النية يكتسح النصوص التي تطبق بشأن الإنترنت، حتى أن هذه الجرائم لا يمكن أن تدخل حيز التطبيق ما لم يتوافر سوء النية في منطقة القصد الخاص وإرادة الإضرار، ومن ذلك ما هو مقرر في المادة(١٥-٢٢٦) عقوبات فرنسي جديد، التي تشترط سوء النية حين وجود عدوان على البريد الالكتروني، وبما يجعل ذلك بالضرر متطابقا مع ما هو مقرر في المادة(L32-1 II-5) من تقنين البريد والاتصالات الصادر بالقانون المؤرخ في١٩٩٦/٧/٢٦ والتي تلزم وزير الاتصالات الفرنسي بالسهر على مبدأ احترام سرية الاتصالات.(٣)

١ عبد الله دغش العجمي ، المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة . رسالة ماجستير. جامعة الشرق الأوسط، ٢٠١٤، ص ٢٧.

٢ د. خالد ممدوح إبراهيم، مرجع سابق، ص ١٠٩

٣ د. مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت ، دار الكتب القانونية، القاهرة، ٢٠١٠، ص ١٤٣.

أما المشرع البريطاني فقط تطلب توافر القصد الجنائي العام في الجريمة الالكترونية لذا يجب أن تنصرف إرادة الجاني نحو الدخول إلى البيانات أو المعطيات المخزنة في أي حاسوب، إذ جرم المشرع البريطاني الدخول غير المصرح به للنظام الالكتروني بموجب المادة الأولى من قانون إساءة استخدام الحاسوب لعام ١٩٩٠، وكذلك جرم الدخول غير المصرح به إلى النظام الالكتروني بهدف ارتكاب جريمة أخرى بموجب المادة الثانية من ذات القانون.[١]

وفي القانون الإماراتي الخاص بجرائم تقنية المعلومات رقم (٢) لسنة ٢٠٠٦ أوضح أن جرائم تقنية المعلومات هي (كل فعل عمدي) وهذا يعني وجوب توافر القصد الجنائي لكل عمل تقوم به المسؤولية الجنائية.

فمن يدخل إلى موقع أو نظام أو يلغي أو يحذف بيانات أو معلومات أو يفشي أسرارها يجب أن يكون عالما ومريدًا لسلوكه ؛ ذلك لأن النتائج التي تترتب على هذا السلوك مما يجعله خاضعا للمسئولية الجنائية ، أما إذا كان فعله نتيجة خطأ فلا تقوم عليه المسؤولية ما لم ينص القانون على خلاف ذلك.[٢]

المطلب الثاني

القصد الجنائي الخاص في جرائم الإرهاب الالكتروني

القصد الخاص هو الذي يعتد فيه المشرع بغاية معينة بتطلبها لاكتمال الركن المعنوي للجريمة.[٣]

أي أن القصد الخاص : هو عبارة عن نية خاصة تتجسد بغاية معينة يسعى الجاني إلى تحقيقها أو باعث يحمله على ارتكابها، وإذا كان القصد الإجرامي العام المكون من الإرادة يجب توافره في جميع الجرائم العمدية دون استثناء فإن القصد الجنائي الخاص ليس كذلك إذ يلزم توافره في بعض الجرائم العمدية التي تتطلب قصدا خاصا أو شرط تجريم فلا يكتفي بالعلم والإرادة.[٤]

ويتمثل القصد الخاص في جريمة الإرهاب في النية الإرهابية وقد نصت غالبية الاتفاقيات الدولية الخاصة بالإرهاب على ضرورة توافر النية الخاصة بالإرهاب،

١ أحمد سامي الرواشدة ، مكافحة الجريمة المعلوماتية بالتجريم والعقاب. المجلة الأردنية في القانون والعلوم السياسية . جامعة مؤتة. الأردن، المجلد (١) العدد ٣ . ٢٠٠٩، ص ١٢٨.

٢ د. عبد الجبار رضاحي عواد ؛ جرائم تقنية المعلومات وإثباتها جامعة النهرين، بغداد. مرجع منشور بالإنترنت، ص ١٧.

٣ د. مأمون سلامة، مرجع سابق . ص ٣٣٧.

٤ د. كاظم عيد جاسم، مكافحة الإرهاب في التشريع العراقي دار الكتب والوثائق. بغداد، ٢٠١١، ط٢، بحث منشور بالإنترنت، ص ٤٠.

وقد استهدفت هذه الاتفاقيات حماية كل من الدولة والأشخاص والأموال والبيئة وذلك باشتراط أن يكون الهدف من وراء العمل الإرهابي هو ترويع السكان أو قهر حكومة أو منظمة دولية وقد نصت الاتفاقيات الإقليمية والدولية على صور القصد الخاص على النحو الآتي .[١]

الصورة الأولى: اتجاه نية الجاني إلى نشر الخوف العام أو الترويع والتهديد:

تعتبر هذه النية هي جوهر القصد في جرائم الإرهاب فالقانون يتطلب في بعض الجرائم أن يتوافر لدى الجاني قصداً جنائياً خاصاً هو إرادة تحقيق غاية معينة من وراء الجريمة فلا يكتفي بتحقيق غرض الجاني المباشر ، كما في القصد الجنائي العام ، بل يذهب إلى أبعد من ذلك إلى الباعث من وراء ارتكاب الجريمة ، وهو الدافع النفسي لتحقيق سلوك معين بالنظر لغاية معينة، أو النتيجة القصوى التي يرمي إليها الجاني، التي يتم الكشف عنها بسؤال الجاني لماذا ارتكبت الفعل، والهدف من ذلك هي تمييز الجريمة محل المتابعة عن الجرائم المشابهة لها في العناصر.[٢]

وبذلك فإن لكل سلوك إرهابي غاية تدفع أو تحمل الفاعل على ارتكابه سعياً وراء حاجة معينة يرمي إليها ، بمعنى الهدف العملي من اقتراف الفعل الإرهابي أو النتيجة الشخصية التي يتوخاها الفاعل ويرتجيها ويرمي إلى إحداثها ويسعى للحصول عليها عبر العمل الذي قام به من أجلها، وتختلف هذه الأعمال باختلاف الأشخاص والبيئة والمحيط ، فغالبا ما تكون هي المحرك لإرادة الإرهابي الذي جعله يرتكب فعله ، وهي بذلك النتيجة القصوى التي يتوخاها.[٣]

ويستهدف الإرهاب الالكتروني التقنية الحديثة الذي تؤثر على قوة الإنتاجية والثقة بالمجتمعات ما بعد الصناعية ويسعى إرهابيو الإرهاب الالكتروني من خلال استغلال موارد العالم المادي الافتراضي ، ومن خلال الوصول إلى المداخل العامة والخاصة بين العاملين، والانتقال والتجمع والاسترداد إلى تدمير نقاط الالتقاء الإيجابية، والتي تمثل حالة للرفاهية المجتمعية والمعرفة بالإضافة إلى عمل تغيرات أساسية في الأنظمة العاملة ، كما تسعى المنظمات الإرهابية إلى تدمير البنية المعلوماتية التحتية للخصوم والأعداء ، وخاصة فيما يتعلق بالقوات المسلحة من حيث تدمير أنظمة الاتصال الجوية والبرية والبحرية.[٤]

١ د. أحمد فتحي سرور: مرجع سابق، ص ٢٥٥.

٢ رحماني منصور: الوجيز في القانون الجنائي العام، دار العلوم للنشر والتوزيع، عنابة الجزائر، ٢٠٠٦، ص ١٠٨-١١٠.

٣ محمود داوود يعقوب: المفهوم القانوني للجرائم الإرهابية . دراسة تحليلية تأصيلي، مقارنة، منشورات زين الحقوقية، الطبعة الثانية، ٢٠١٢، تونسن بحث منشور ص٢٧١.

٤ د. علي عدنان الفيل: مرجع سابق ، ص٧٥ .

فالإرهاب الالكتروني يهدف إلى تدمير البنية التحتية المعلوماتية وتعريض المجتمعات العالمية إلى مخاطر غير محتملة وغير متوقعة ، ويكون الهدف النهائي لجرائم الإرهاب الالكتروني: هو الإخلال بالنظام عن طريق بث الذعر وإثارة الخوف والاضطراب بالمجتمع.[١]

وبذلك فإن جريمة الإرهاب باستخدام الوسائل الالكترونية تعد من الجرائم القصدية التي يشترط لقيامها توافر القصد الإجرامي الخاص.

الصورة الثانية: استهداف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر:

النظام العام بالدولة هو المعبر الحقيقي عن الحاجات الأساسية لضمان التعايش الاجتماعي وحماية واستقرار المجتمع فاستهداف المقومات الأساسية للمجتمع وأمنه إستهداف للأمن العام ، ولقد أورد المشرع سلامة المجتمع وأمنه إلى جانب الأمن العام من باب الاحتياط[٢].

ويتعرض سلامة المجتمع للخطر إذا كان من شأن استخدام العنف أو التهديد باستخدامه تعطيل مظاهر الحياة في الدولة كما يتعرض أمن المجتمع للخطر إذا كانت الأفعال التي يؤديها الإرهابيون تؤدي إلى زعزعة السكينة عند الأفراد في المجتمع.

الصورة الثالثة: الحاق الضرر بالاتصالات والمواصلات:

فالأعمال الإرهابية تؤدي إلى إلحاق الضرر بالمواصلات فيشمل الأعمال التي تؤدي من شأنها إلى إيقاف حركة المواصلات أو تعطيلها سواء كانت برية أو بحرية أو جوية مثل التسبب في خروج أحد القطارات عن القضبان أو تفجير الطائرات أو قصفها بالإضافة إلى أعمال القرصنة البحرية.[٣]

كما تؤدي الأعمال الإرهابية إلى تعطيل سبل الاتصالات وأنظمة الحاسوب أو اختلاط الشبكات ، ولن يتأتى الإرهاب الالكتروني إلا من خلال هذا الفعل الذي ينجم عنه إما تعطيل اختراق أو تشويش على أنظمة الحاسوب.

---

١ مصطفى سعد حمد خلف ، جريمة الإرهاب الالكتروني، دراسة مقارنة بين التشريعين الأردني والعراقي، كلية الحقوق جامعة الشرق الأوسط، ٢٠١٧، رسالة ماجستير، ص٢٨٢.

٢ سعد الجبوري، مرجع سابق ، ص ٦٥.

٣ د. محمد العفيف، جرائم الإرهاب في التشريع المقارن ، المكتبة الوطنية، عمان، ٢٠٠٧، ص ١٢٥.

المطلب الثالث

القصد الجنائي في جرائم الإرهاب باستخدام الوسائل الالكترونية في القانون السعودي والإماراتي

يرتكز القصد الجنائي العام على عنصري العلم والإرادة أي علم الجاني بالفعل والنتيجة المتوقعة ، ولذلك يعاقب الجاني على العلم بالفعل والنتيجة.[١]

ويتحقق القصد الجنائي العام بانصراف إرادة الفاعل إلى إتيان السلوك الإرهابي، وهو عالم لصفته مدرك لنتيجته ، بمعنى أن إرادة الفاعل يجب أن تنصب على ماديات الجريمة أي ركنها المادي ، بحيث تسيطر على السلوك وتوجيهه إلى النتيجة التي تهدف إليها ، كما يتوجب أن تحيط علم الجاني بالواقعة المجرمة ، بحيث تشمل ماديات الجريمة جميعها من سلوك ونتيجة وعلاقة سببية وكل واقعة يستند فيها السلوك الإجرامي لدلالاته الإجرامية فضلا عن ضرورة انصراف علم الجاني إلى الركن الخاص في الجريمة الإرهابية ، وهو المشروع الإجرامي الإرهابي والقصد الإجرامي ، وهو علم الجاني بحقيقة فعله الإرهابي وسيلته وانصراف إرادته إلى ارتكابه.[٢]

وعلى ذلك فإننا سوف نتحدث عن العلم والإرادة في قانون الجريمة الالكترونية السعودي والإماراتي.

أولا : العلم في الجريمة المعلوماتية في نظام مكافحة الجرائم المعلوماتية السعودي:

عرف نظام مكافحة الجرائم المعلوماتية السعودي الجريمة المعلوماتية بأنها : أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام. وسوف نبدأ بكل جريمة على حده وشرح عنصر العلم في هذه الجريمة.

التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه.

وفي هذه الجريمة يلزم أن يتوافر العلم لدى الجاني بأن ما يقوم به من سلوك يتمثل في التنصت عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي ، وأن هذه الشبكة المعلوماتية أو أجهزة الحاسب الآلي تخص الغير، وأن ما يقوم به من سلوك يخالف نص قانون نظام مكافحة الجرائم المعلوماتية .

١ نقض جنائي ١٩٩٩/٧/٤ مجموعة القواعد القانونية لأحكام محكمة النقض – ١٤٢٩-س٦٧ ق .
٢ د. علي حامد عيد ، تمويل الإرهاب ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى، ٢٠٠٧، ص ١١٥.

فيجب أن يكون الجاني عالما بأن السلوك الذي يقترفه يمثل اختراقاً وانتهاكاً لحرمة وسرية مواد مرسلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي ، فإن كان يعتقد أن هذه المادة منشورة بصورة علنية ، ومن حق الجميع الاطلاع عليها وسماعها تنتفي الجريمة ، ويجب أن يكون عالما أنه ليس بيده مسوغا قانونيا يبيح له هذا التنصت ، فإن كان يعتقد أنه يمتلك هذا المسوغ انتفت الجريمة[١]

الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا.[٢]

ويقصد بالدخول غير المشروع حسب ما عرفها نظام مكافحة الجرائم المعلوماتية السعودي: دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع الكتروني أو نظام معلوماتي أو شبكة حاسبات آلية ويكون غير مصرح لذلك الشخص بالدخول إليها.[٣]

وعنصر العلم هنا المقصود به أن النظام اشترط العلم بالأوصاف القانونية للفاعل والتي تكون من خلال استخدام الدخول غير النظامي من قبل شخص غير مصرح له ، ولكن في حالة ما إذا كان لهذا الجاني تصريح دخول في القيام بالأفعال ، فهنا ينطوي العلم على العلم بالظروف المشددة للجريمة ، والتي تتمثل في استغلال الوظيفة أو العمل ، وبالتالي ينبغي أن يتوافر العلم لدى الفاعل وقت ارتكاب الجريمة على جميع عناصر الجريمة المادية حسب نموذجها الإجرامي ينصب ذلك على علم الفاعل أولا على صفته الخاصة ، وهي كونه مصرحا له بالدخول، وإذا أثبت الفاعل أنه كان يجهل حقيقة صفته عند ارتكاب القصد الجنائي لديه ولا تقوم الجريمة والقصد الخاص يكون في التهديد أو الابتزاز والإرادة هنا تتمثل في تحقيق النتيجة الإجرامية كالتهديد والابتزاز.[٤]

الدخول غير المشروع إلى موقع الكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.[٥]

وهنا يجب على الجاني أن يعلم بأن ما قام به من سلوك يتمثل في دخول غير مشروع ولا مصرح له بذلك ، وأن الموقع الذي قام بالدخول عليه مملوك للغير ولا يحق له إتلافه أو تعديله أو شغل عنوانه.

---

١ أحمد خليفة الملط ، الجرائم المعلوماتيه . دار الفكر الجامعي ، الإسكندرية ، الطبعة الثانية ، ٢٠٠٦ ، ص١٨٧.
٢ المادة الثالثة فقرة ٢ من قانون الجرائم المعلوماتيه السعودي.
٣ نص المادة الأولي من نظام مكافحة الجرائم المعلوماتي السعودي.
٤ د . نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، ص٣٦٤ .
٥) المادة الثالثة فقرة ٣ من قانون مكافحة الجريمة المعلوماتية السعودي.

أما إذا كان الجاني مصرحا له بالدخول على هذا الموقع ، ولكنه قام بالسلوك الإجرامي المتمثل في التغيير أو الإتلاف أو التعديل أو شغل العنوان فهذه من الظروف المشددة للجريمة إذا أثبت الجاني عكس ذلك بأن السلوك الإجرامي كان عند طرق استعمال الحق أو عن طريق الخطأ وبالتالي ينتفي العلم هنا.[١]

إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات أو أداة تستخدم في الأعمال الإرهابية.[٢]

وينبغي لتوافر العلم هنا أن يعلم الجاني أن ما يقوم به من سلوك يتمثل في إنشاء الموقع للمنظمة الإرهابية بهدف النشر أو تسهيل الاتصال أو ترويج الأفكار أو التمويل أو كيفية صناعة الأجهزة الحارقة أو المتفجرة أو أي أداة تستخدم في الأعمال الإرهابية فعل مجرم بنص القانون وقت ارتكاب الجريمة.

الدخول غير المشروع إلى موقع الكتروني، أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.[٣]

ويتمثل هنا العلم بأن يعلم الجاني بأن دخوله إلى الموقع الالكتروني أو النظام المعلوماتي غير مصرح له ومخالف للقانون وليس لديه إذن بالدخول وقت ارتكاب الفعل وإن كان لديه تصريح دخول وقت ارتكاب الفعل فيجب عليه العلم بأن ما يقوم به من الحصول على بيانات تمس الأمن الداخلي أو الخارجي أو الاقتصاد الوطني تشكل جريمة معاقبا عليها ويعتبر من الظروف المشددة للجريمة.

ثانياً: العلم في الجريمة المعلوماتية في قانون مكافحة جرائم تقنية المعلومات الإماراتي:

لم يتطرق نظام مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة إلى تعريف الجريمة المعلوماتية كما عرفها النظام السعودي أو الأنظمة العربية

---

١ ممدوح محمد الجنبيهي ، منير محمد الجنبيهي: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي ، ٢٠٠٥ ، ص٥٢.

٢ المادة السابعة الفقرة الأولى من قانون الجرائم المعلوماتي السعودي .

٣ المادة السابعة فقرة (الثانية) م من قانون الجرائم المعلوماتي السعودي .

الأخرى ، ولكنه يبين النظام الجرائم المعلوماتية التي جرمها بعقوبات محددة ومنظمة في مواد النظام.

وسيتم شرح عنصر العلم في كل جريمة على النحو الآتي :

جرائم اختراق المواقع أو النظام المعلوماتي:-

نصت المادة الثانية من قانون الاتحادي الإماراتي على أن « كل فعل عمدي يتوصل فيه بغير حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين.

فإذا كانت البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرة آلاف درهم أو بإحدى هاتين العقوبتين.

وفي هذه المادة ثلاث صور للجريمة وهي:

جريمة التوصل عمدا بغير وجه حق إلى موقع أو نظام معلومات في صورتها البسيطة.

ويجب هنا أن يتجه علم الجاني إلى كل واقعة تدخل في تكوين جريمة الدخول إلى الموقع أو النظام المعلوماتي ، وأن يقوم بذلك بدون وجه حق وعلى غير رضاء صاحب النظام أو المسؤول عنه وينبغي أن يعلم الجاني بخطورة فعله على محل الجريمة.[1]

ب- التوصل إلى الموقع أو النظام المعلوماتي في صورتها المشددة.

وهنا يلزم أن يعلم الجاني بأنه يقوم بفعل التوصل إلى الموقع أو النظام المعلوماتي وأن من شأن هذا الفعل تحقيق إحدى صور الضرر التي تضمنها نص المادة الثانية من القانون الإماراتي.

ج-جريمة التوصل إلى موقع أو نظام معلوماتي يتضمن بيانات أو معلومات شخصية.

١ د عبد الفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى ، ٢٠٠٦ ، ص٣٦٦.

ويلزم هنا أن يعلم الجاني أنه يقوم بهذا الفعل الذي أو صله للموقع أو النظام المعلوماتي وأن هذا الموقع أو النظام يتضمن بيانات أو معلومات تخص الغير ولا يحق له الدخول أو الاطلاع عليها.

ويجب أن يعلم الجاني أن ما يقوم به من سلوك ينصب على حق يحميه القانون ولا يملك التصريح اللازم له بعمل هذا السلوك.

جريمة تزوير المستندات المعترف بها قانونا في نظام معلوماتي.

وقد ذكر النظام أنواع المستندات التي تخضع للنظام وهي من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفا به قانوناً في نظام معلوماتي.

وهنا يلزم أن يعلم الجاني بأنه يغير الحقيقة في مستند وأن من شأن هذا السلوك الذي قام به أن يرتب عليه ضرر سواء كان حالاً أو محتملاً.[1]

جريمة إعاقة أو تعطيل وصول الخدمة إلى مصادر المعلومات عن طريق أحد وسائل تقنية المعلومات.

وينبغي أن يعلم الجاني أنه يقوم بأحد الأفعال التي أوردها النص القانوني والتي من شأنها إعاقة الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات والمعلومات وأنه غير مخول له ذلك وقت ارتكاب الجريمة.

جريمة إيقاف الشبكة المعلوماتية أو وسائل تقنية المعلومات عن العمل أو تعطيلها أو تدمير البرامج أو البيانات أو المعلومات فيها.

يلزم أن يتوافر لدى الجاني بأنه يقوم بالسلوك المتمثل في الإيقاف أو التعطيل أو التدمير ويعلم بأن ما يقوم به ينصب على الشبكة المعلوماتية أو إحدى وسائل التقنية ، وأن من شاء هذا السلوك أن يقوم بإيقاف الشبكة أو الوسيلة المعلوماتية وتعطيلها عن العمل أو تدمير البرامج أو البيات أو المعلومات فيها وأن يعلم الجاني بأن هذه الشبكة أو الوسيلة تخص الغير.

تنص المادة ٢١ من قانون الاتحاد الإماراتي علي أن « كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية

١ أحمد خليفة الملط ، مرجع سابق ، ص ٤٤٧ .

تحت مسميات تمويهية لتسهيل الاتصالات بقيادتها أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالحبس مدة لا تزيد على خمس سنوات.

والعلم هنا يلزم أن يتوافر لدى الجاني العلم بأنه ينشئ موقعا أو نشر معلومات لجماعة إرهابية يستوي أن يكون منتميا إليها أم غير منتم لها، فإذا جهل أن هذا الموقع لجماعة إرهابية أو لنشر معلومات عنها فإنه ينتفي معه القصد الجنائي ، ويحدث ذلك عندما ينشئ المتهم موقعا ما على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لغرض برئ فيدخل عليه أعضاء الجماعات الإرهابية ويخصصون هذا الموقع للجماعات الإرهابية أو لنشر معلومات تتعلق بأفكار هذه الجماعة.

جريمة الدخول بغير وجه حق موقعا أو نظاما مباشر أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي بقصد الحصول على بيانات أو معلومات حكومية سرية أو خاصة بالمنشآت المالية .

نص المادة الثانية والعشرون من القانون الإماراتي علي أن : (يعاقب بالسجن كل من دخل وبغير وجه حق موقعا أو نظاما مباشرا أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني.....الخ) .

والعلم الواجب توافره هنا هو أن يعلم الجاني وقت تنفيذه للجريمة بأن دخوله للموقع أو النظام علي الشبكة المعلوماتية أو إحدى وسائل التقنية الحديثة كان بدون وجه حق وغير مصرح له به ، وأن يتوافر العلم لدي الجاني بأن المعلومات أو البيانات الحكومية سرية ولا يجوز نشرها .

ثالثا: الإرادة في الجرائم المعلوماتية في نظام مكافحة الجرائم المعلوماتي السعودي:

التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح، أو التقاطه أو اعتراضه.

والإرادة هنا تقتضي أن تتجه إرادة الجاني وقت ارتكابه الجريمة إلى التنصت على ما هو مرسل أو التقاطه أو اعتراضه دون مسوغ نظامي وان يقصد من ذلك التنصت على الآخرين وسماع ما يتحدثون به وما يتناقلونه بدون وجه حق ولا مشروعية.[1]

١ أحمد خليفة الملط، مرجع سابق، ص١٨٧ .

الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.

وهنا جريمتان وليس جريمة ، فالجريمة الأولى : تتمثل في الدخول غير المشروع وأن تتجه إرادة الجاني إلي الدخول وهو غير مصرح له . والجريمة الأخرى : تتمثل في أن يقصد الجاني من هذا الدخول التهديد أو الابتزاز، وإذا انتفت الجريمة الأولى لا يلغي ذلك الجريمة الثانية ؛ لأن الغاية الاجرامية المتمثلة في التهديد والابتزاز قد توافرت هنا.[1]

الدخول غير المشروع إلى موقع الكتروني أو الدخول إلى موقع الكتروني لتغير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه .

وينطبق الحال هنا كما في الفقرة السابقة حيث إن الدخول غير المشروع بحد ذاته جريمة تتمثل في أن الجاني قصد الدخول غير المشروع إلى الموقع الالكتروني، وأن تتجه إرادة الجاني حين دخول الموقع إلى تغيير تصميمه أو إتلافه أو تعديله أو شغل عنوانه.

إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات أو أداة تستخدم في الأعمال الإرهابية.

والإرادة هنا تتمثل في تحقيق النتيجة الإجرامية ، وهي في هذه الجريمة العمل الإرهابي وتسهيل الاتصال بالقيادات الإرهابية أو ترويج الفكر الإرهابي والتمويل له أو في كيفية تصنيع الأجهزة الحارقة أو المتفجرات وجميع ما يستخدم في العمليات الإرهابية[2]

الدخول غير المشروع إلى موقع الكتروني أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني.

وهذه الجريمة تتمثل في الدخول غير المشروع وهي جريمة أولى تتمثل في اتجاه إرادة الجاني إلى الدخول إلى الموقع مع العلم بأنه يعلم أنه غير مصرح له بالدخول

١ د. نائلة عادل محمد قورة، مرجع سابق . ص٣٧٠ .
٢ منير محمد ، ممدوح محمد الجنبيهي ، مرجع سابق ، ص٩٦ .

، ثم تتكون جريمة أخرى وهي امتداد للسلوك الإجرامي في الجرائم السابقة مع اختلاف الهدف واتجاه الإرادة فيها إلى الحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني ، أما إذا كان مخولاً له الدخول ، فإن القصد الخاص يتمثل في الحصول على بيانات تمس الأمن والاقتصاد ، ويمثل ذلك ظرفا مشددًا على الجاني.[1]

رابعاً: الإرادة في الجريمة المعلوماتية في النظام الإماراتي:

ويتمثل عنصر الإرادة في كل جريمة على النحو الآتي :

١- جرائم اختراق المواقع أو النظام المعلوماتي.

نصت المادة الثانية من قانون الاتحادي الإماراتي على أن : « كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل غير مصرح به ، يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين .

وهنا تتجه إرادة الجاني إلى إرتكاب الفعل وإلى تحقيق النتيجة الإجرامية في التوصل إلى موقع أو نظام معلوماتي .

٢ - جريمة إيقاف الشبكة المعلوماتية أو وسائل تقنية المعلومات عن العمل أو تعطيلها أو تدمير البرامج أو البيانات أو المعلومات فيها .

وهنا يجب أن تتجه إرادة الجاني إلي إرتكاب فعل الإدخال عن طريق الشبكة المعلوماتية أو الحاسب الآلي ، وأن تتجه إرادته إلي إحداث النتيجة الإجرامية وهي إيقاف الشبكة عن العمل أو تعطيلها أو إحداث تدمير أو إتلاف البرنامج أو البيانات أو المعلومات فيها .

٣ - جريمة استعمال شبكة المعلومات في تهديد أو ابتزاز الأشخاص .

وتتحقق الإرادة هنا بأن تتجه إرادة الجاني إلى ارتكاب هذه الجريمة التي تقوم بفعل التهديد أو الابتزاز ، وأن يحدث الرهب في نفس المجني عليه لحمله علي القيام بما يريد أو الامتناع عنه .

٤ - المادة (٢١) : كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات

١ عبد الفتاح بيومي حجازي ، مرجع سابق ص٣٦٧ .

بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالحبس مدة لا تزيد على خمس سنوات.

الإرادة هنا يجب أن تتجه إلى تسهيل الاتصالات بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية.

٥ - وتنص المادة الثانية والعشرون من قانون مكافحة جرائم تقنية المعلومات على أن: يعاقب بالسجن كل من دخل وبغير وجه حق موقعا أو نظاما مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية ، إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك.

فإذا ترتب على الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها، تكون العقوبة السجن مدة لا تقل عن خمس سنوات ، ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى والتجارية والاقتصادية.

وهنا ينبغي أن تتجه إرادة الجاني وقت ارتكاب الجريمة إلى تحقيق النتيجة ، وهي أن دخوله للموقع أوالنظام على الشبكة المعلوماتية أواحدى وسائل التقنية كان بدون وجه حق وغير مصرح له بذلك، وأن تتجه إرادة الجاني إلى الحصول علي معلومات أو البيانات الحكومية السرية أو منشآت مالية أو تجارية أو اقتصادية بقصد نشرها أو إعادة نشرها أو بإلغاء البيانات أو المعلومات أو إتلافها أو تدميرها .

الفصل الثاني

الإجراءات الجنائية لجريمة الإرهاب باستخدام الوسائل الالكترونية

تمهيد وتقسيم:

يترتب على قيام مسئولية الجاني مجموعة من العقوبات تطبق بحقه ، وهي عقوبات أصلية وتبعية تمثل الجزاء الجنائي على الشخص الذي يكون مسؤولا عن ارتكاب أحد الأفعال التي يجرمها القانون فعندما ترتكب جريمة الإرهاب بالوسائل الالكترونية فإنه يتوجب على المحكمة المختصة إيقاع العقوبة على مرتكب الجريمة حال ثبوتها، والقاعدة العامة : أنه لا تطبق العقوبة على مرتكب الجريمة إلا بعد اتخاذ الإجراءات الجنائية والتحقيق من قبل النيابة المختصة.

ولذلك سوف نتناول الإجراءات الجنائية في المبحثين الآتيين:

المبحث الأول : إجراءات التحقيق الابتدائي في جرائم الإرهاب بالوسائل الالكترونية.

المبحث الثاني: معوقات التحقيق في الجرائم الالكترونية.

المبحث الأول

إجراءات التحقيق الابتدائي في جرائم الإرهاب عبر الوسائل الالكترونية

عندما ترتكب الجريمة التقليدية فلابد من تحريك الدعوى الجنائية بحق المتهم ولابد من خضوع الدعوى للضوابط القانونية التي ترسمها قوانين أصول المحاكمات الجنائية وقانون الإجراءات الجنائية فهذه الإجراءات ليست مجرد وسائل فنية بحتة ، بل هي أعمال تمس الحرية الشخصية عند مباشرتها في مواجهة المتهم.[1]

فالإجراءات الحقيقية تعكس الصورة الحقيقية للحريات العامة ، فالمحقق يبحث عن الحقيقة بأية وسيلة ويفترض الدفاع الاجتماعي في أن الإجراءات الجنائية تدخل في وظيفة الدولة ، فهي ليست في نزاع شخصي ، فالتأكد من الحقيقة بمعناها

١ د. محمد ياسر أبو الفتح ، خصائص وتصنيفات الجريمة المعلوماتية منتدى د. شيماء عطا الله- منتدى القانون الجنائي، ٢٠٠٨، www.shaimaaaatalla.com

المادي والشخصي يفترض وجود مناخ إجرائي يختلف عن مناخ النظام الاتهامي الذي لا يتيح للقاضي أن ينفذ إلى الحقيقة إلا من خلال حجج الخصوم ، وبذلك فإن الدعوى الجنائية سواء أكانت حول جريمة تقليدية أم معلوماتية فلابد أن تمر بمراحل التحقيق التي تصون حرية الفرد وحقوقه.

ولما كان أساس توقيع العقوبة على المتهم إثبات إدانته بإقامة الأدلة التي تثبت وقوع الجريمة، أو نسبتها إلى المتهم بحجة قاطعة، ووجود الأدلة الجازمة لدى القاضي بالحكم عليه من واقع الأدلة المعروضة عليه. لذلك فإن الإثبات موضوع غاية في الأهمية وبخاصة في جرائم الإرهاب المرتكبة عبر الوسائل الالكترونية عالية الكفاءة ، وترجع صعوبة إثبات تلك الجرائم إلى خصائص هذه التقنية ذاتها وبخاصة السرعة الفائقة التي ترتكب بها، وهو ما يسهل ارتكابها ويسهل طمس معالمها ومحو آثارها قبل اكتشافها ؛ إذ يستطيع الجاني أن يرتكب جريمة دون أن يترك وراءه أي أثر خارجي ملموس، وعدم ملاءمة الأدلة التقليدية في إثباتها ، ومن هنا تبدأ صعوبة البحث عن الدليل وجمع الأدلة ومدى قبولها إن وجدت ومدى مصداقيتها في إثبات وقائع الجريمة.[١]

وعلى هدى ما سبق فإننا سوف نقسم هذا المبحث إلى مطلبين على النحو الآتي :

المطلب الأول : صعوبة الإثبات في جرائم الإرهاب عبر الوسائل الإلكترونية.

المطلب الثاني: إجراءات التحقيق الابتدائي في مسرح الجريمة.

المطلب الأول

صعوبة الإثبات في جرائم الإرهاب عبر الوسائل الالكترونية

الإثبات الجنائي : هو نشاط إجرائي الغرض منه هو الوصول إلى اليقين القضائي طبقاً لمعيار الحقيقة الواقعية ، وذلك بشأن الاتهام أو تأكيد أو نفي آخر يتوقف عليه إجراء قضائي.[٢] وبمعنى آخر هو إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعل معين.[٣]

---

١ د. محمد السعيد رشدي ، حجية وسائل الاتصال الحديثة في الإثبات، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية محور المعاملات المدنية، دبي الامارات العربية المتحدة، ٢٦-٢٨ أبريل، ٢٠٠٣. ص٣٦١-٣٦٢.

٢ د. أمال عبد الرحيم عثمان: الإثبات الجنائي ووسائل التحقيق العلمية ، دار النهضة العربية، القاهرة، ١٩٧٥. ص٤

٣ د. محمود محمود مصطفى ، شرح قانون الإجراءات الجنائية ط١١-القاهرة-١٩٧٦-ص ٤١٤.

والهدف من الإثبات هو بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة ، فإنه في سبيل ذلك يستخدم وسائل معينة هي وسائل الإثبات، ووسيلة الإثبات هي كل ما يستخدم في إثبات الحقيقة – فهي نشاط يبذل في سبيل اكتشاف حالة أو مسألة شخص أو شيء ما أو ما يفيد في إظهار عناصر الإثبات المختلفة - أي الأدلة ونقلها إلى المجال الواقعي الملموس.[١]

وتشير مسألة الإثبات في نظام الحاسوب والإنترنت صعوبات كبيرة أمام القائمين على التحقيق وذلك لجملة مور نذكر أمثلة منها:[٢]

كالتخزين الالكتروني للمعطيات الذي يجعلها غير مرئية وغير مفهومة بالعين المجردة، ويشكل انعدام الدليل المرئي (المفهوم) عقبة كبيرة أمام كشف الجرائم، وقد يشكل تشفير البيانات المخزنة الكترونيا أو المنقولة عبر شبكات الاتصال عن بعد عقبة كبيرة أمام إثبات الجرائم الالكترونية والبحث عن الأدلة، كما أن سهولة محو الدليل في زمن قصير تعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسوب والإنترنت.

ومن الأمثلة الواقعية على ما تقدم ما حصل في دولة الإمارات العربية المتحدة، حيث قام مشغل حاسوب بتهديد المؤسسة التي يعمل لديها بتنفيذ مجموعة من مطالبه، وذلك بعد أن حذف كافة البيانات الموجودة على الجهاز الرئيسي للمؤسسة وقد رفضت المؤسسة الاستجابة لمطالبة ، فأقدم على الانتحار ووجدت المؤسسة صعوبة استرجاع البيانات التي كانت قد حذفت.[٣]

وتنعقد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بواسطة شبكات الاتصال عن بُعد، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثا عن الأدلة وتحقيقها.

فمن الصعب إجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية ، حيث إن هذا الإجراء يتعارض مع سيادة هذه الدولة الأخيرة ، ولما كانت الأدلة المتحصلة من التفتيش على نظم الحاسب الآلي الإنترنت تحتاج إلى خبرة

١ د. أمال عبد الرحيم عثمان، مرجع سابق. ص ٤٤

٢ د. سعيد عبد اللطيف حسن : الإثبات في جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت. ط١. دارا لنهضة العربية. القاهرة. ١٩٩٩. ص ٩٥.

٣ د. هشام محمد فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة. مكتبة الآلات الحديثة. اسيوط. ١٩٩٤ . ص ٢٣٥. وانظر د. عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي والإنترنت دار الكتب القانونية. القاهرة. ٢٠٠٢. ص ٤٦.

فنية ودراية فائقة في هذا المجال.[١] فإن نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكم قد يؤدي إلى ضياع الدليل بل تدميره أحيانا.[٢]

لذلك فإنه يجب أن يتزايد الإثبات بالخبرة القرائن بالنسبة لهذا النوع الجديد من الجرائم ، وهو ما يستوجب الاهتمام بالخبراء وتأهيلهم التأهيل العلمي الصحيح الذي يمكنهم من القيام بأعمال الخبرة ، وأن هذا الاهتمام بوسائل الإثبات، يُمكن القضاء من اللجوء إلى القرائن القضائية بجرأة أكبر في المسائل العلمية ويمكنهم من استنباط الأمور العلمية ذات البعد الجنائي أو القانوني بوجه عام من الأمور الثابتة ، وهذه هي فحوى القرائن ، لكي يتمكن القضاة من الوصول إلى الحقيقة ، من خلال القرائن القضائية بالذات . التي يعتبرها القضاء في بعض الأحيان من المسائل العلمية فيتوقف عند خبرة الخبراء ولا يلجأون إليها علمياً.

وهناك عدة طرق لجمع الأدلة عن الجرائم المرتكبة عبر الوسائل الالكترونية ، وهي في الوقت نفسه تعد من طرق الإثبات للوصول إلى حقيقتها ، ومن باب أولى تعد من أهم طرق الإثبات الجنائية ، وهي المعاينة والتفتيش والشهادة والخبرة في الجرائم المعلوماتية.

١ كمال الكركي، جرائم الحاسوب ودور مديرية الأمن في مكافحتها ورقة عمل مقدمة إلى ندوة قانون حماية المؤلف . نظرة إلى المستقبل المنعقدة في عمان بتاريخ ١٩٩٩/٧/٥ - ص١٠ وما بعدها.

٢ اسامة أحمد المناعسة، جرائم الحاسب الآلي والإنترنت – دراسة تحليلية مقارنة – ط١، دار وائل – عمان، ٢٠٠١، ص٢٨٩-٢٩٧.

المطلب الثاني

إجراءات التحقيق الابتدائي في مسرح الجريمة

إجراءات التحقيق هي عبارة عن مجموعة من الأعمال التي يرى المحقق وجوب أو ملاءمة القيام بها لكشف الحقيقة بالنسبة لواقعة معينة.[١]

وأولى الخطوات التي يجب أن تؤخذ عند مسرح الجريمة هي صيانة الأدلة بما يمنع إتلافها أو تغيرها على أن تكون الإجراءات وفقا لقواعد القانون وجمع الأدلة في الجرائم الالكترونية يتطلب الدقة والحذر ؛ لكونه يملك قيمة إثبات في الجريمة.[٢]

وهناك أنواع معينة من أدلة الحاسوب يتطلب جمعها بدقة ونقلها بطريقة خاصة لكي لا تكون عرضة للتلف أو التبديل ، ويعتبر التحقيق الابتدائي المرحلة الأولى في الخصومة الجنائية من أجل إثبات حق الدولة في العقاب ، فهو يهدف إلى تحديد مدى جدوى تقديم المتهم إلى المحاكم الجنائية لإقرار هذا الحق في مواجهته ، ولقد أدت خطورة الجزاء الجنائي إلى أن يعهد إلى نوع معين من القضاة وهم قضاة التحقيق.[٣]

والبحث عن الأدلة الجنائية لإثبات سلطة الدولة في العقاب أونفيه، هو أمر يتوقف على مدى إثبات وقوع الجريمة ونسبتها إلى المتهم.

وفي هذه المرحلة يقوم قضاة التحقيق بدور إيجابي في جمع أدلة الإثبات أو النفي للوصول إلى الحقيقة.

وتبدو أهمية مرحلة التحقيق الابتدائي إلى تحضير الدعوى ومدى قابليتها للنظر أمام قضاء الحكم، ونظرا إلى أنها تتم على أثر وقوع الجريمة فإنها تتاح لها جمع الأدلة قبل ضياعها ؛ لأن كل تأخير في تحقيق هذه المهمة قد يؤدي إلى تشويه صورة الحقيقة ، كما أن الحاجة تبدو مهمة في تأكيد حق الدولة في العقاب الذي يدعو إلى اتخاذ بعض الإجراءات الماسة بحرية المتهم.[٤]

---

١ د. أحمد حسني طه، مبادئ قانون الإجراءات الجنائية في التشريع المصري، مطبعة بهجت للطباعة، الجزء الأول، بدون تاريخ، ص٤٠٦.

٢ حسن رجب الزهراني، إثبات جرائم تقنية المعلومات، بحث تكميلي مقدم لنيل درجة الماجستير، السعودية، جامعة الإمام محمد بن سعود الإسلامية، ٢٠٠٥، ص ٢ ww.imamu.edu.sa

٣ د. أحمد فتحي سرور، الوسيط في قانون العقوبات، دار النهضة العربية، الطبعة الأولى ص ٣٦١.

٤ د. أحمد فتحي سرور، مرجع سابق، ص ٨٨

ويعتبر من ضمن أعمال التحقيق الابتدائي أعمال التحقيق الخاصة بجمع الأدلة، حيث يتم الانتقال إلى موقع الحادث للمعاينة وندب الخبراء والتفتيش وضبط الأشياء المتعلقة بالجريمة وسماع الشهود والحبس الاحتياطي، فإن توافرت الأدلة الكافية لدى سلطة التحقيق تأمر بإحالتها إلى المحكمة المختصة.

الفرع الأول

المعاينة في جرائم الإرهاب الالكتروني

يقصد بالمعاينة مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها أو محوها أو تعديلها.(١)

وعرفها البعض الآخر بأنها : إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها ، وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة.(٢)

ويرى آخر أنها « رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة.(٣)

والمعاينة في جوهرها ملاحظة وفحص حسي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة.(٤)

والمعاينة قد تكون إجراء تحقيق أو استدلال، ولا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد ، فإذا جرت المعاينة في مكان عام كانت جراء استدلال ، إذا اقتضت دخول مسكن أو مكان له حرمة خاصة كانت إجراءً تحقيقيًا.(٥)

---

١ د. محمد أبو العلا عقيدة ، التحقيق وجمع الأدلة في مجال الجريمة الالكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية المنعقد بمركز البحوث والدراسات بأكاديمية شرطة دبي، بتاريخ ٢٦ أبريل ٢٠٠٣ منشور على موقع كلية الحقوق جامعة المنصورة. http://www.f-low.net

٢ د. مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري دار النهضة العربية، سنة ٢٠٠٠، ص ٦٤٢.

٣ د. محمد زكي ابو عامر، الإجراءات الجنائية . دار المطبوعات الجامعية. الإسكندرية. ١٩٨٤، ص ٦٧٩.

٤ د. طه السيد أحمد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق في النظام الجزائي المصري والسعودي، دار الكتب والدراسات العربية، ٢٠١٦، الإسكندرية، ص ٧٧

٥ د. سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت دار النهضة العربية، ٢٠١٣، ص ٢٨٧.

والانتقال إلى محل الواقعة من أهم إجراءات جمع الأدلة فهو لازم لمعاينة حالة الأمكنة والأشياء والأشخاص ووجود الجريمة ماديا وكل ما يلزم إثبات حالة (المادة ٩٠ من قانون الإجراءات الجنائية المصري).[١]

وتظهر أهمية المعاينة عقب وقوع الجرائم التقليدية حيث يوجد مسرح فعلي للجريمة يحتوي على آثار مادية فعلية يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لفحصها لبيان مدى صحتها في الإثبات.

ولكن الحال ليس كذلك بالنسبة للجرائم المرتكبة بالوسائل الإلكترونية ؛ حيث إن المجرم الالكتروني لا يترك بعد ارتكابه للجريمة آثاراً مادية وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها.

لذلك يرى البعض أن أهمية المعاينة تتضاءل في الجريمة الالكترونية ، وذلك لندرة تخلف آثار مادية عند ارتكاب الجرائم الإرهابية عبر الوسائل الالكترونية ، كما أن طول الفترة بين وقوع الجريمة أو ارتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو التلف أو المحو لتلك الآثار.[٢]

وفي كل الأحوال عند تلقي بلاغ عن وقوع إحدى الجرائم الالكترونية ، وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته ومسرح الجريمة الالكترونية يختلف عن مسرح الجريمة التقليدية ، كالقتل والسرقة ، والجريمة الالكترونية قد تكون جريمة مستمرة كما في حالة الجرائم الاقتصادية والسرقة الاحتيال ، وقد يكون مسرحها كالجرائم الأخرى كما في التزوير وإتلاف البرامج وتفجير المباني والمنشآت ، ففي حالة الجريمة المستمرة ذات الأهداف الاقتصادية تكون المعاينة هدفها المداهمة وضبط الأدلة على الطبيعة ، وفي الحالة الثانية وبعد وقوع الجريمة فالأمر متوقف على اعترافات المتهمين متى تم القبض عليهم ، وكذلك شهادة الشهود والقرائن وعند إجراء المعاينة في المجال الالكتروني يجب مراعاة الضوابط الآتية:[٣]

١ د. سامح السيد جاد ، الإجراءات الجنائية في القانون المصري ، طبعة دار الوزان ، ١٩٨٩ ، ص ٢٢٢.

٢ د. هشام فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية مكتبة الآلات الحديثة – أسيوط – ١٩٩٤ - ص ٥٩.

3 Robert taylor: computer crime, in criminal investigation edited by Charles swanson. N. Chamelin and I. territto, Hill inc. 5 th edition, 1992-p 450

تصوير الحاسب والأجهزة الطرفيه المتصلة به على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.

إعداد خطة المعاينة ، موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.

العناية البالغة بالطريقة التي تم بها إعداد النظام والآثار الالكترونية الخاصة بالتسجيلات الالكترونية التي تتزوج بها شبكات المعلومات بموافقة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع.

ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكنهم إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء.

عدم نقل أي معلومة من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

التحفظ على المعلومات الموجودة بسلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة وفحصها، وترفع من عليها البصمات ذات الصلة بالجريمة.

التحفظ على مستندات الإدخال والمخرجات الورقية ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد بها من بصمات .

قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في مجال المحاسبات.

١٠- قصر مباشرة المعاينة على فئة معينة من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسب الآلي ونظم المعلومات واسترجاع المعلومات والذين تلقوا تدريبا كافياً على التعامل مع نوعية الآثار والأدلة التي يحتويها مسرح الجريمة المعلوماتية.

الفرع الثاني

التفتيش في جرائم الإرهاب الالكتروني

التفتيش : هو البحث في مستودع أسرار المتهم وهو إجراء من إجراءات التحقيق يتطلب أوامر قضائية لمباشرته.[١]

ويجب على المحقق الجنائي المبادرة لإجراء التفتيش وذلك قبل قيام الجاني بطمس معالم الجريمة وإخفاء كل ما يتعلق بها، وهو يستطيع ذلك إذا اتسع له الوقت وأتيحت له الفرصة.[٢]

والتفتيش في مدلوله القانوني بالنسبة للجرائم الالكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية ، فيقصد به أنه إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها.[٣]

إلا أنه توجد بعض الصعوبات الإجرائية التي تعيق خضوع البيانات المخزنة آلية لقواعد التفتيش التقليدية والتي منها تعدد الأماكن التي يوجد بها النظام المعلوماتي داخل أو خارج الدولة وهناك صعوبات في تحديد الأشياء التي يهدف إلى ضبطها من عملية التفتيش، وغيرها من الصعوبات مثل عدم اكتمال المعرفة المعلوماتية والتقنية لتنفيذ عملية التفتيش كما ينبغي أن تكون.[٤]

تفتيش وضبط البيانات المعلوماتية المخزنة:

قضت المادة (١٩) من الاتفاقية الأوربية بودابست المتعلقة بالإجرام الإلكتروني.

---

١ د. رمزي رياض عوض ، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها ، دراسة تحليلية تأصيلية مقارنة – دار الفكر العربي، القاهرة، سنة ٢٠٠٠، ص ٨٥.

٢ د. نبيل عبد المنعم جاد، أسس التحقيق والبحث الجنائي العلمي مطبعة كلية الشرطة، ٢٠٠٦، ص ١١٢.

٣ د. هلالي عبد اللاه أحمد. تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي. دار النهضة العربية، القاهرة، ١٩٩٧، ص ٢٣٧.

٤ د. عفيفي كامل عفيفي، جرائم الحاسب الآلي وحقوق المؤلف والمصنفات الفنية، دراسة مقارنة، منشأة المعارف، الإسكندرية، ٢٠٠٠، ص ٣٤٤.

يجب على كل دولة طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة التفتيش أو الولوج بطريقة مشابهة:

لنظام معلوماتي أو لجزء منه وكذلك للبيانات المعلوماتية المخزنة فيه ، وعلى أرضه.

ب- لدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية.

يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل التأكد مما إذا كانت سلطاته تقوم بالتفتيش أو الولوج بطريقة مشابهة لنظام معلوماتي معين أو جزء منه، وفقا للفقرة « ١ » بند « أ » وأنها تملك أسبابا تدعو للاعتقاد بأن البيانات التي تسعى إليها مخزنة في نظام معلوماتي آخر أو في جزء منه على أرضه ، وأن هذه البيانات يمكن الوصول إليها بشكل قانوني سواء من خلال النظام الآتي أو من خلال كونها مهيأة من أجله ، وأن هذه السلطات المذكورة ستكون قادرة على التوسع العاجل لنطاق التفتيش أو الولوج بطريقة مشابهة لنظام آخر... الخ).

كما نصت الاتفاقية العربية لمكافحة جرائم التقنيه الحديثة في المادة ٢٦ فيها على أنه « تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:

تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها.

ب- بيئة أو وسيط تخزين معلومات تقنية والذي قد تكون معلومات التقنية مخزنة فيه أو عليه».

وبذلك أقرت الاتفاقيات المختلفة حق الدول في تفتيش نظام الحاسب للوصول إلى البيانات المخزنة فيه.

وإذا كانت الاتفاقيات السابقة قد أقرت حق الدول الأعضاء في تفتيش نظم الحاسب الآلي والشبكات إلا أنها بينت في الوقت ذاته ان النصوص الإجرائية التقليدية قد تحول دون هذا التفتيش ، ومن ثم أوجبت على الدول الأعضاء أن تراجع قوانينها بما يسمح لهذا الإجراء.

و اتخذت التشريعات المختلفة في هذا الشأن اتجاهين:[١] الأول : ينكر تطبيق القواعد التقليدية عند تفتيش الحاسوب والشبكات وأنه يتعين النص صراحة على هذا التفتيش.[٢]

والاتجاه الثاني : يرى أعماله تلك القواعد ولو لم ينص عليه صراحة باعتباره مما يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه.[٣]

الاتجاه الأول :

يجسد هذا الاتجاه التشريع الانجليزي حيث نص قانون إساءة استخدام الحاسب الصادر في٢٩ يونيو ١٩٩٠ بشأن الجرائم المدرجة في القسم الأول ، وهي جرائم الولوج غير المصرح به لنظام الحاسب - والتي يعاقب عليها بالحبس لمدة لا تجاوز ستة أشهر، فإن التفتيش فيها لا يكون إلا بناء على إذن قضائي يستند إلى أسباب منطقية للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها في أماكن خاصة ، وأن بعض الأدلة المتعلقة بهذه الجريمة يمكن الحصول عليها في هذه الأماكن.[٤]

كذلك يمثل الاتجاه الأول المشرع الفرنسي حيث رأي الفقه في فرنسا أن النبضات الالكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة ، وبالتالي لا تعتبر شيئاً مادياً بالمعنى المألوف.

وقد استجاب المشرع الفرنسي لهذه التغيرات وعدل نصوص التفتيش وذلك بإضافة عبارة المعطيات المعلوماتية وذلك في المادة ٩٤ من قانون الإجراءات الجنائية ؛ حيث نصت على أن « يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على الأشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة.[٥]

---

١ راشد بشير إبراهيم: التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على إمارة ، أبو ظبي ، ، مركز الإمارات للدراسات والبحوث والاستراتيجية، ط١، ٢٠٠٨٧، ص ٥٨.

٢ نبيلة هبة هروال : الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دار الفكر الجامعي الاسكندرية، ٢٠٠٧، ص ٢٢٥.

٣ د. هشام فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة. أسيوط، ١٩٩٢، ص ٦٤.

4 Ferbrache (David) : pathology of coputer viruses springer- verlog London- LTD. 1992 p. 233.
Edward (martin) : computer crimes and other crimes aginst information technology in united kingdom R. I.. D. 1993 m,p. 640.

5 Philippe baumard:la cyber ciminalit e copart ementale, revue francaise de criminalogie et de droit penal, vol. 3 , November 2014.

الاتجاه الثاني:

ويمثل هذا الاتجاه التشريع الكندي إذ تجيز المادة ٤٨٧ من القانون الجنائي الكندي إصدار أمر قضائي لتفتيش وضبط (أي شيء) تتوافر بشأنه أسس أو مبررات معقولة للاعتقاد بأن جريمة قد وقعت أو يشتبه في وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة، أو أنه سيتيح دليلا على وقوع الجريمة. وحتى الآن ورغم أن الركيزة أوالوعاء المادي للبيانات كالأقراص والاسطوانات الممغنطة ، وهو الذي يتم ضبطه فإن تفسير الفقه لهذه المادة يوسع من نطاقها إلى حد يسمح بتفتيش وضبط بيانات الحاسب غير المحسوسة.(١)

في التشريع المصري لم يتعرض قانون الإجراءات الجنائية المصري لتفتيش الحاسب الآلي وشبكة المعلومات وذلك لا يعني أنه أباح تفتيشها بدون إذن، ذلك لأن المشرع الدستوري قد أقر حق الإنسان في الخصوصية بصفة عامة، وفق نص في المادة ٥٧ من الدستور الصادر عام ٢٠١٤ والتي نصت على أنه « للحياة حرمة خاصة ، وهي مصونة لا تمس).

وتنص المادة ٩١ من قانون الإجراءات الجنائية المصري على أن : « تفتيش المنازل عمل من أعمال التحقيق ، ولا يجوز الالتجاء إليه إلا بمقتضى أمر من قاضي التحقيق بناء على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة ، ولقاضي التحقيق أن يفتش أي مكان وفي جميع الأحوال يجب أن يكون أمر التفتيش مسبباً.

وطبقا للمادة ١٩٩ من قانون الإجراءات الجنائية المصري تباشر النيابة العامة التحقيق في مواد الجنح والجنايات طبقاً للأحكام المقررة لقاضي التحقيق ، وذلك مع ملاحظة ما نصت عليه المادة ٢٠٦ من أنه يشترط لقيام النيابة بتفتيش غير المتهم أو بتفتيش منزل غير منزله الحصول على أمر مسبب بذلك من القاضي الجنائي بعد اطلاعه على الأوراق.

يتضح من النصوص السابقة أنه يشترط لصح التفتيش الشروط الآتية:

1 Donald k.piragaff. computer crimes and other crimes against inf or mation technology in cand a, R. I . D . P. 199., p. 241.

أولا : يجب أن يكون هناك اتهام موجه إلى الشخص الذي يراد تفتيشه أو تفتيش مسكنه أو وردت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة.

ثانياً: يجب أن يكون التفتيش وفقا لنص المادة (٩١) إجراءات مصري بصدد جناية أو جنحة وقعت فعلاً فلا يجوز التفتيش في المخالفات.

ثالثا: يجب أن يهدف التفتيش إلى ضبط الأشياء المتعلقة بالجريمة أو التي تفيد في كشف الحقيقة ، فإن لم يكن هناك فائدة ترجى لصالح التحقيق من مباشرة التفتيش كان إجراءاً تحكيمياً ويخضع المحكم في تقدير مدى الفائدة من التفتيش لرقابة محكمة الموضوع.

والتفتيش في الجرائم الرقمية المعلوماتية يكون محله كل مكونات الحاسب الآلي سواء كانت مادية أو معنوية ، وكذلك شبكات الاتصال الخاصة به ، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش وتشمل جميع مكوناته المادية والمكونات المعنوية التي تشمل برنامج النظام وبرامج التطبيقات سابقة التجهيز طبقاً لاحتياجات العميل ، ويستلزم تفتيش الحاسب الآلي مجموعة من الأشخاص لديهم الخبرة ومهارة تقنية في نظم الحاسب الآلي ، كمشغلي الحاسب الآلي وخبراء البرامج ومديري النظم المعلوماتية.[1]

١ د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الحاسب والإنترنت دار الكتب القانونية، المحلة الكبرى - مصر ٢٠٠٧. ص ٢٨٨. انظر كذلك د. عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات. بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية الأمنية للعمليات الإلكترونية - محور القانون الجنائي - دبي - خلال الفترة من ٢٨/٢٦ أبريل ٢٠٠٣. ص ٦١٠.

الفرع الثالث

الشهادة في الجرائم الإرهابية باستخدام الوسائل الالكترونية.

الشهادة في مجال الجريمة المرتكبة بالوسائل الإلكترونية لا تختلف من حيث ماهيتها عنها في الجريمة التقليدية ، وأمر سماع الشهود متروك لفطنة المحقق ومرتبط بظروف التحقيق، والأصل أن يطلب الخصوم سماع من يرون من الشهود، وللمحقق أن يدعو للشهادة من يقدر أن لشهادته أهمية، وله أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه.

والشاهد في الجريمة الالكترونية : هو ذلك الشخص التقني صاحبه الخبرة والتخصص في تقنية وعلوم الحاسب الآلي ، والذي تكون لديه معلومات جوهرية أو مهمة لازمة للدخول – الولوج – في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذا الشاهد اسم الشاهد المعلوماتي وذلك تمييزا له عن الشاهد التقليدي.[1] والشاهد المعلوماتي بهذا المفهوم قد يكون واحدا من عدة طوائف أهمها:

مشغلو الحاسب الآلي : وهم الخبراء الذين تكون لهم الدراية التامة بتشغيل جهاز الحاسب الآلي إلى وحدات منفصلة واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.[2]

المحللون: والمحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين وتحليلها إلى وحدات منفصلة واستنتاج العلاقات الوظيفية منها، كما يقوم كذلك بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

المبرمجون: وهم الأشخاص المتخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين: الفئة الأولى: هم مخططو برامج التطبيقات ويقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقومون بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات.

---

١ د. هلالي عبد اللاه ، التزام الشاهد بالإعلام في الجرائم المعلوماتية – دراسة مقارنة، دار النهضة العربية، القاهرة، سنة ٢٠٠٠، ص٢٣.

٢ د. محمد فهمي ، الموسوعة الشاملة لمصطلحات الحاسب الالكتروني . مطابع المكتب المصري الحديث القاهرة، سنة ١٩٩١.

الفئة الثانية: هم مخططو برامج النظم ويقومون باختيار وتعديل وتصحيح برامج نظام الحاسب الداخلية وادخال أية تعديلات أو إضافات لها.[١]

مهندسو الصيانة والاتصالات: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.[٢]

مديرو النظم: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.[٣]

الفرع الرابع

الخبرة في جرائم تقنية المعلومات

أولا : ماهية الخبرة : الخبرة هي إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لإمكان استخلاص الدليل منه.[٤]

كما عرفها البعض بأنها : الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه ،والخبرة الفنية تعتبر إجراء من إجراءات التحقيق بحسب الأصل والخبرة – كدليل في الإثبات تنصرف إلى رأي الخبير الذي يثبته في تقريره.[٥]

وبما أن تقرير الخبير يعتبر من الأدلة الفنية فإن إجراء ندب الخبير هو من إجراءات جمع الأدلة فللمحقق الاستعانة بالخبراء ليستطلع رأيهم في بعض الأمور التي تعرض له أثناء تأدية مهمته في التحقيق الذي ينتهي بإصدار قرار بأن لا وجه لإقامة الدعوى أو بإحالتها إلى محكمة الموضوع ، وأما الخبرة في مرحلة المحاكم ، فإنها تساعد القاضي في تكوين عقيدته للفصل في القضية.[٦]

ثانياً: أهمية الاستعانة بالخبراء:

إذا كان للخبرة أهمية في الجرائم التقليدية فإن أهميتها تزداد وتصبح ضرورية بل وحتمية في إثبات الجرائم الالكترونية ، فالخبرة وسيلة من وسائل الإثبات التي

١ د. هلالي عبد الله أحمد: التزام الشاهد بالإعلام في الجريمة المعلوماتية – دار النهضة العربية، القاهرة، سنة ٢٠٠٠ ص، ص ٢٤.
٢ د. عبد الله علي محمود: إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات . بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية – محور القانون الجنائي – دبي – خلال الفترة من ٢٨/٣٦ أبريل ٢٠٠٣، ص ٦١٦.
٣ د. خالد محمد المهيري: التحقيق الجنائي العملي في الجريمية التقليدية والمعلوماتية – الطبعة الثانية – دار العزيز – للطباعة والنشر ، دبي، بدون تاريخ نشر، صـ٥٠.
٤ د. مأمون محمد سلامة : الإجراءات الجنائية في التشريع المصري – الجزء الأول، دار النهضة العربية، القاهرة، سنة ٢٠٠١، ص ٦٤٥.
٥ د. أمال عثمان: الخبرة في المسائل الجنائية – رسالة دكتوراه ، كلية الحقوق جامعة القاهرة. ١٩٦٤، ص ٢٨، وما بعدها.
٦ د. مامون سلامة: مرجع سابق ص ٦٤٦.

تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية.[١]

وهي بحث لمسائل مادية أو فنية يصعب على المحقق أن يشق طريقه فيها ، ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات.[٢]

وفي حقيقة الامر أنه منذ بدء ظهور الجرائم ذات الصلة بالحاسب الآلي تستعين الشرطة وسلطات التحقيق أو المحاكم بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي ، وذلك بغرض كشف غموض الجريمة ، أو تجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق، فإذا كانت الاستعانة بخبير فني أمر جوازي للمحقق أو لجهة التحقيق ، إلا أنه في المسائل الفنية البحتة التي لا يمكن للقاضي أن يقطع فيها برأي دون استطلاع رأي أهل الخبرة ، يجب عليه أن يستعين بخبير فإذا تصدى للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير كان حكمه معيباً مستوجباً نقضه ، وهذا المبدأ استقر عليه قضاء محكمة النقض المصرية.[٣]

وبناء عليه فإذا كانت الاستعانة بخبير في المسائل الفنية البحتة أمر واجب على جهة التحقيق والقاضي ، فهي أوجب في مجال الجرائم الالكترونية، حيث تتعلق بمسائل فنية آية في التعقيد ومحل الجريمة فيها غير مادي والتطور في أساليب ارتكابها سريع ومتلاحق ولا يكشف غموضها إلا متخصص على درجة كبيرة من التمييز في مجال تخصصه ، فإجرام الذكاء والفن لا يكشفه ولا يبغله إلا ذكاء وفن مثله .[٤]

وأهمية الاستعانة بالخبير في مجال الجرائم الالكترونية تظهر عند غيابه ، فقد تعجز الشرطة عن كشف غموض الجريمة ، وقد تعجز هي أو جهة التحقيق عن جمع الأدلة حول الجريمة ، وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه.[٥]

١ د. خالد محمد المهيري: التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية . الطبعة الثانية. دار الغرير للطباعة والنشر. دبي . بدون سنة نشر. بحث منشور بالإنترنت، ص ٤٨٩.

٢ د. علي محمود علي حمودة : الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائية. بحث منشور ضمن أبحاث المؤتمر العلمي الأول. حول الجوانب القانونية والأمنية للعمليات الإلكترونية - مركز البحوث والدراسات أكاديمية شرطة دبي - محور القانون الجنائي في الفترة من ٢٦-٢٨ أبريل ٢٠٠٣ ، ص ٢٨٥.

٣ نقض ١٩٦٥/٣/٢١ - مجموعة القواعد القانونية رقم ٥٢ صـ ٣١.

نقض ١٩٧٧/٦/٢٢ - مجلة ، المحامون ، سنة ٤٢، رقم ٧٥٩. ص ٥٨٣

٤ د. طه السيد أحمد الرشيدي: مرجع سابق. ص ١٢٢.

5 Robert taylor:computer crime: in criminal investigation editied by Charles swanson. N. chamelin and l. territto hill. Ine, 5 th edition 1992.p.1

المبحث الثاني

معوقات التحقيق في الجرائم الالكترونية

التحقيق في الجرائم المتعلقة بالإنترنت وملاحقة مرتكبيها جنائياً يتسم بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق ، بل يمكن أن يؤدي بها إلى الخروج بنتائج سلبية ينعكس على نفسية المحقق بفقدانه الثقة في نفسه وفي أدائه وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون الغير قادرة على حمايته من هذه الجرائم وملاحظة مرتكبيها وانعكاسها أيضا على المجرم نفسه، حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره ، وأن خبرة القائمين على المكافحة والتحقيق لا تجاري خبرته وعلمه ، الأمر الذي يعطيه ثقة كبيرة في ارتكاب المزيد من هذه الجرائم التي قد تكون أكثر فداحة وأشد ضرراً على المجتمع المحلي أو المجتمعات الأخرى.[١]

ومن أهم المعوقات التي قد تواجه القائمين على مكافحة الجرائم الإرهابية عبر الوسائل الإلكترونية والتحقيق فيها عوائق تتعلق بالأحجام عن الإبلاغ عن الجريمة وعوائق تتعلق بعدم توافر الكفاءة البشرية المؤهلة للتحقيق وعوائق تتعلق بخفاء الجريمة المعلوماتية وغياب الدليل المرئي وعوائق تتعلق بصعوبة التعاون الدولي في مكافحة الجريمة المعلوماتية.[٢]

لذلك فإننا سوف نقسم هذا المبحث إلى مطلبين.

المطلب الأول : عوائق تتعلق بالجريمة والجهات المتضررة.

المطلب الثاني: عوائق تتعلق بجهات التحقيق.

---

١ د. عبد الرحمن بحر، معوقات التحقيق في جرائم الإنترنت . دراسة مسحية على ضباط الشرطة بدون البحرين. رسالة ماجستير جامعة نايف للعلوم الأمنية. الرياض. ١٩٩٩، ص ٥١.

٢ د.حسين بن سعد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت بحث منشور بالإنترنت.

المطلب الأول

عوائق تتعلق بالجريمة والجهات المتضررة

أولا : عوائق تتعلق بالجريمة :

خفاء الجريمة وغياب الدليل المرئي:-

خفاء الجريمة وغياب الدليل المرئي وافتقاد أكثر الآثار التقليدية وصعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية ، كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والاطلاع عليها أو استنساخها ؛ وذلك لسهولة محو الدليل أو تدميره في زمن قصير جدا ، فالجاني يمكنه أن يمحو الأدلة التي تتمكن السلطات من كشف الجريمة إذا ما علمت بها ، وفي هذه الحالة فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده ، وبالتالي تنصله من مسؤولية هذا الفعل. وإرجاعه إلى خطأ في نظام الحاسب الآلي أو الشبكة أو في الأجهزة .[1]

ويعزز ذلك الضخامة البالغة لكم المعلومات والبيانات المتعين فحصها وإمكانية خروجها عن نطاق أقليم الدولة والبعد الجغرافي بين مرتكب الجريمة والضحية بالإضافة إلى عدم المعرفة بمكونات الجريمة المتعلقة بشبكة الإنترنت من قبل بعض الأطراف المعنية.[2]

ثانياً: عوائق تتعلق بالجهات المتضررة :

الأحجام عن الإبلاغ : من أهم وأخطر المشكلات التي تتعلق بعملية الإبلاغ عن جرائم الإنترنت، حيث يحجم البعض عن إبلاغ السلطات المختصة عن الجرائم التي ارتكبت بحقهم خاصة المؤسسات والشركات التجارية حتى في الدول المتقدمة من الناحية التقنية والتي ترتفع فيها معدلات هذا النوع من الجرائم.

ففي دراسة للمعهد الوطني للعدالة التابع لوزارة العدل الأمريكية شملت ١٢٧ من العاملين في مجال التحقيق في جرائم الحاسوب والإنترنت يمثلون ١١٤ وكالة رسمية

١ د. هشام محمد فريد رستم ، الجرائم المعلوماتية أصول التحقيق الجنائي الفني. مجلة الأمن والقانون، العدد ٢، ١٩٩٩، ص ٤٣٠.

٢ سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات رسالة ماجستير في العلوم الشرطية. كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية. الرياض، ٢٠٠٣، ص ١١٤.

كان غالبية المشاركين في الدراسة يعتقدون أن معظم جرائم الحاسوب CSI بالاشتراك مع مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية إلى أن حوالي ٧٠٪ من الجرائم التي يتم اكتشافها لا يتم البلاغ عنها لسلطات إنفاذ العدالة.

ويمكن أن يعزي إحجام البعض عن الإبلاغ لعدة أسباب:

عدم إدراك الأفراد أو مدراء الأنظمة الحاسوبية ومسؤول الشركات أن مثل هذه الأفعال والهجمات تعتبر جرائم يمكن معاقبة مرتكبيها بموجب التشريعات والأنظمة المطبقة ضمن إقليم الدولة أو المطبقة دوليا.[١]

خوف الجهات التي وقعت عليها الجرائم خاصة المؤسسات والشركات المالية من أن يؤثر انتشار خبر الحادث على سمعتها ومصداقيتها وظهورها بمظهر مشين أمام الآخرين[٢]، لأن تلك الجرائم ارتكبت ضدها، مما قد يترك انطباعاً بإهمالها أو قلة خبرتها أو عدم وعيها الأمني[٣]، ولم تتخذ الاحتياطات الأمنية اللازمة لحماية معلوماتها، الأمر الذي قد ينعكس سلباً على أرباحها وقيمة أسهمها.

خوف المؤسسات والشركات التجارية من أن تؤدي أعمال التحقيق إلى احتجاز حواسبها أو تعطيل شبكاتها لفترة طويلة، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق عطفاً على ما قد تسببت الجريمة خسارتها أصلاً.

بعض الضحايا قد تساورهم الشكوك حول مقدرة رجال إنفاذ القانون على التعامل مع هذا النوع المستحدث من الجرائم.

- الرغبة في إضفاء الأسلوب الذي ارتكبت به الجريمة؛ لكي لا يتم تقليديه من الآخرين مستقبلا.[٤]

- قد تكون بعض هذه الجرائم محدودة الأثر مما يدفع بعدم الإبلاغ عنها، فقد يقوم مخترق ما للنظام بإظهار رسالة تفيد بقيامه بهذه العملية، أو يقوم مجرم آخر

١ د. حسين بن سعيد الغافري: التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت. بحث منشور على موقع بالإنترنت ص ٨١ وما بعدها http://www.eastlaws.com

٢ د. طارق عبد الله الشدي: آلية البناء لنظم المعلومات. دار الوطن للطباعة والنشر، الرياض ١٤٢٣هـ، ص ٢١٠.

٣ باسم الحمادي: صعوبة إثبات جرائم الإنترنت. بحث منشور على شبكة الانترنت بتاريخ ٧ محرم ١٤٢٣ هـ. الرياض.

٤ د. زكي أمين حسونة: جرائم الكمبيوتر الجرائم الأخرى في مجال التكتيك المعلوماتي. المؤتمر السادس للجمعية المصرية للقانون الجنائي، ص ٤٧٦.

بإرسال فيروس حاسب آلي إلى جهاز المستفيد ، ويكون هذا الفيروس محدود الأثر أو تقوم برامج الحماية من الفيروسات بالقضاء عليه.

وقد يكون الإفصاح عن التعرض لجريمة معلوماتية من شأنه حرمان شخص من خدمات معينة تتعلق بالنظام المعلوماتي ، فقد يحرم الموظف في الجهة من خدمات معينة على الإنترنت أو قد يحرم من خدمات الإنترنت عموماً حين يتعرض لجريمة معلوماتية ناتجة عن الاختراق أو زيارته لأماكن غير مأمونة أو غير مسموح بزيارتها.

عدم معرفة الضحية بوجود جريمة أصلاً، وعدم القناعة أنها ممكن أن تحدث في مؤسسته.

المطلب الثاني

عوائق تتعلق بجهات التحقيق

عدم توافر الكفاءة البشرية المؤهلة للتحقيق تعتبر من العوائق التي تتعلق بجهات التحقيق ، فهناك معوقات ترجع إلى شخصية المحقق مثل التهيب من استخدام الحاسب الآلي والتهيب من استخدام شبكة الإنترنت، بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية.

وهناك معوقات تتعلق بالنواحي الفنية، كنقص المهارة الفنية المطلوبه للتحقيق في هذا النوع من الجرائم ونقص المهارة في استخدام الحاسب الآلي والإنترنت، وعدم توافر المعرفة بأساليب ارتكاب جرائم الحاسب الآلي ،والإنترنت، وقلة الخبرة في مجال التحقيق في جرائم الحاسب الآلي والإنترنت والمعرفة باللغة الانجليزية[١] ، كذلك فإن للعاملين في مجال الحاسب الآلي مصطلحات علمية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم ، وليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون : لديهم لغة عربية تعرف بلغة المختصرات وهي لغة متطورة ومتجددة.

ومن أجل ذلك فإنه لابد من إيجاد أسلوب خاص للتحقيق في هذه الجرائم يجمع بين الخبرة الفنية والكفاءة المهنية ومن الممكن حيال ذلك اتباع الخطوات التالية.[٢]

تبادل المعلومات بين المحقق وخبير الحاسب الآلي ، وذلك قبل البدء في التحقيق وأخذ أقوال الشهود والمشتبه فيهم أو استجواب المتهمين، بحيث يشرح المحقق للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم ، ومن جهة أخرى يقوم الخبير بشرح الأبعاد الفنية والنقاط التي ينبغي استجلاؤها من الأشخاص وكافة المصطلحات الحاسوبية التي يمكن استخدامها مع بيان معانيها ليتم الاستفادة منها عند الضرورة.

يتم حصر النقاط المطلوب استجداؤها من قبل الخبير والمحقق قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيب تلك النقاط.

---

١ سليمان بن مهجع العنزي، مرجع سابق ص ١١٩

٢ د. حسين بن سعيد الغافري ، مرجع سابق. ص ٢٠

يتم أخذ أقوال الشهود واستجوبات المتهمين من قبل المحقق وبحضور الخبير الذي يجوز له توجيه الأسئلة الفرعية أثناء الاستجواب وفق الكيفية التي تتم الاتفاق عليها مسبقا قبل بدء التحقيق.

التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في الحاسب الآلي وملحقاته الخاصة بالشاهد أو المتهم الذي تم التحقيق معه مع مراعاة أن هذا الأخير لا يجوز إجباره على تقديم دليل يدينه.

ولضمان نجاح التحقيق في الجرائم المرتكبة بالوسائل الالكترونية فهناك بعض القواعد التي ينبغي مراعاتها أهمها:

تفادي ضياع الوقت في التحقيق حول جرائم لا يمكن اكتشافها ، أو أن الأدلة اللازمة لاكتشافها وإثبات التهمة قد قضى عليها.

ضرورة مراعاة وجود نوع من التعامل بين المحققين وخبراء الحاسب الآلي العاملين في المؤسسة المجني عليها.

مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الالكتروني وغيرها من الحقوق.

العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسب الآلي وملحقاتها وبرامجها.

مراعاة حفظ الأدلة الجنائية بالطرق المناسبة كل حاله على حدا، وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي ضبطت عليها.

الاستعانة بالتقنيات المتطورة في المجال المعلوماتي في مواجهة الجرائم المعلوماتية ، ولا سيما وأن هذه التقنيات أثبتت جدارتها ونجاحها في جمع الأدلة الجنائية وصناعة البنية الاتهامية وتحليل القرائن واستنتاج الحقائق.

الخـاتمة :

بينا من خلال هذه الدارسة أن جرائم الإرهاب عبر استخدام الوسائل الإلكترونية أصبحت هاجساً يؤرق الدول التي أصبحت عرضه لهجمات الإرهابين والجماعات المتطرفة عبر الإنترنت، وقد أصبحت هذه الجماعات تمارس نشاطها الإرهابي من أي مكان في العالم، لأن التقنية الحديثة وحدها غير قادرة علي حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضراراً جسيمة علي الأفراد والمنظمات والدول إلي اتخاذ التدابير والاحترازات لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود قليلة ولاتزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهه هذا الجرم الخطير.

حيث إن القانون الدولي لم يعط تعريفاً واضحاً، ومنهجاً معيناً للتعامل مع هذا النوع الجديد من الإرهاب، علماً أنه عرف الإرهاب النووي وأصدر عدة قرارات يمكن الرجوع إليها، في حين أن الإرهاب الإلكتروني يمكن اعتباره أداة إرهابية مؤذية جداً.

إن هناك تحديا لعدم وجود اتفاق عالمي حول التعريف القانوني للسلوك الإرهابي ، وخاصة أن المجتمع الدولي إلى الآن لم يصل إلى تعريف واضح للإرهاب بشكلة التقليدي ناهيك عن الإرهاب عبر الإنترنت، والبعض الآخر يعتبر الإرهاب مقاومة مشروعة أو جريمة سياسية . وهناك تداخل لمفهوم الإرهاب عبر الإنترنت مع غيره من المفاهيم كالجريمة الإلكترونية والتجسس وحرب المعلومات وفرض ذلك إشكالية تحديد المعاملة القانونية الواضحة.

كما بينا أن الإرهاب الإلكتروني يشكل تهديداً قويا للدول والمجتمعات وهذا الإرهاب لم يتبلور بعد لكن يجب أن يؤخذ علي محمل الجد وان يتم الاستعداد لمواجهته وبينا أن الإرهاب الإلكتروني عبارة عنى عدوان أو تخويف أو تهديد مادى أو معنوي يصدر من الجماعات أو الأفراد على الأنسان ، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق ، باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتي صنوف العدوان وصور السلوك.

كما بينت الدراسة أن من أكثر الوسائل المستخدمة في الإرهاب الإلكتروني هو البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم ، بل إن كثيرًا

من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها.

وتبين لنا من خلال هذه الدراسة أن الجماعات الإرهابية أو المتطرفة تعتمد علي إنشاء وتصميم مواقع لهم علي شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلي مبادئهم، وتعليم الطرق التي تساعد علي القيام بالعمليات الإرهابية ، وكيفية اختراق وتدمير المواقع وكيفية الدخول علي المواقع المحجوبة وطريقة نشر الفيروسات وغير ذلك.

كما تبين لنا من مجمل هذة الدراسة أن نظم وقواعد الإثبات الجنائي التقليدية المعمول بها قاصرة وأن الفكر القضائي غير ملائم لعملية كشف ومكافحة وتحقيق مثل هذا النوع من الجرائم واشتقاق الدليل منها ، ثم الحكم فيها بل يحتاج ذلك لرجل أمن معلوماتي ومحقق معلوماتي وقاض معلوماتي فضلاً عن الخبير المعلوماتي .

توصيات ومقترحات لمواجهة جرائم الإرهاب الإلكتروني:-

السعي لحجب وإزالة المواقع الإلكترونية المشبوهة التي تسعي إلى نشر الإرهاب والأفكار المتطرفة، وتلك المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء علي الآخرين.

تفعيل الدور الوقائي الذى يسبق وقوع جريمة الإرهاب الإلكتروني ، وذلك من خلال تفعيل دور المؤسسات التربوية (المدرسة، الأسرة، دور العبادة ، أجهزة الأعلام) وذلك بالتوعية حول خطورة هذه الجرائم علي الأسرة والمجتمع.

سن القوانين أو التشريعات الخاصة التي تسد كافة الثغرات التي تكتنف جريمة الإرهاب الإلكتروني وسبل التحقيق فيها، كالقوانين المتعلقة بكيفية اكتشاف الأدلة الإلكترونية والأدلة التي تُقبل قانوناً لإثباتها.

استحداث هيئة وطنية من الخبراء والمختصين تعمل علي وضع وتطوير استراتيجية وطنية للأمن الإلكتروني ، تركز على حماية البنية التحتية لشبكات المعلومات والنظم البرمجية ،وتنسيق وتوحيد الجهود بين الجهات المختلفة في الدولة

الأمنية والتشريعية والقضائية والفنية ، وذلك من أجل الحد من جرائم الإرهاب الإلكتروني قدر المستطاع والعمل علي ضبطها ، وإثباتها بالطرق القانونية .

السعي لإيجاد منظومة قانونية دولية تحت مظلة الأمم التحدة يعهد إليها توثيق وتوحيد جهود الدول في مكافحة ومواجهة الإرهاب الإلكتروني.

عقد الاتفاقيات بين الدول بخصوص جرائم الإرهاب الإلكترونية وتنظيم كافة الإجراءات المتعلقة بالوقاية من هذه الجريمة وعلاجها وتبادل المعلومات والأدلة في شأنها ، بما في ذلك تفعيل إتفاقيات تسليم الجناة في جرائم الإرهاب الإلكتروني .

تعزيز التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية التخريبية الإلكترونية الواقعة في أراضيها ضد دول وجهات أخرى خارج هذه الأراضي.

قيام مزودي خدمة الإنترنت بالإبلاغ عن النشاط الإرهابي الملموس إن شعروا بأنه يتضمن التهديد لأي شخص أو مؤسسة .

وضع برنامج وطني شامل لرعاية الشباب وحمايتهم وتوجيه طاقتهم وإبداعهم لما فيه ضد المجتمع ، وأن يكون هذا البرنامج خارج الإطار التقليدي وأن تشارك في وضعه مؤسسات الدولة المختصة والمجتمع الأهلي والجامعات ومراكز البحوث ، ومن المهم الانتباه إلى تنفيذ البرنامج ، وضرورة التواصل إلى نتائج ملموسة.

الدفع بعناصر أمنية للانضمام إلى هذه المواقع بهدف إفساد خططها أو تدميرها، أو نشر تصحيح المعلومات الدينية الواردة فيها، حتي لا يثق علي الأقل فيها من يدخل هذه المواقع ، فلا يدرى هل هم أهل فكر أم جهات أخرى، حيث ستفقد هذه المواقع مصداقيتها وبريقها.

إدراج نصوص جنائية توفر الحماية الكاملة ضد الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات والأفعال التي تعتبر أفعالاً إرهابية التي تهدف إلى المساس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف ، وكذلك كل الأفعال التي يمكن أن تقترف في إطار ما يسمي بالإرهاب الإلكتروني.

قائمة المراجع

أولا : باللغة العربية :

١. د. أحمد محمد يوسف حربه: الإرهاب والأمن الجنائي (الظواهر الإجرامية، جامعة نايف للعلوم الأمنية، الرياض، ٢٠٠٧، ص ١٠.

٢. د. أحمد رشاد سلام: جريمة الإرهاب الدولي والتعويض عنها والقانون الواجب التطبيق عليها، دار النهضة العربية، القاهرة، ٢٠١٧، ص٩٥.

٣. د. أحمد فتحي سرور: القانون الجنائي الدستوري، دار الشروق، الطبعة الثانية، ٢٠٠٢، نبذ ٨، ص١٩٨.

٤. د. أحمد فتحي سرور: المواجهة القانونية للإرهاب، الطبعة الثانية، دار النهضة العربية، ٢٠٠٨، ص٢٣٢.

٥. د. أحمد فتحي سرور: الوسيط في قانون العقوبات، القسم العام، طبعة ١٩٨٥، ص ٢١٢.

٦. أ. د. أحمد عوض بلال: مبادي قانون العقوبات المصري، القسم العام، دار النهضة العربية، طبعة ٢٠٠٥، ٢٠٠٦، ص٢٥٩.

٧. د. إبراهيم حامد طنطاوي: شرح الأحكام العامة لقانون العقوبات، الجزء الأول ، النظرية العامة للجريمة، دار النهضة العربية، ٢٠١٧ ،ص ٥٥.

٨. د. إبراهيم عيد نايل: السياسة الجنائية في مواجهة الإرهاب، دار النهضة العربية، القاهرة، ١٩٩٦، ص ٥٨.

٩. د. ايسر محمد عطية القيس: بحث بعنوان «دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته» الملتقي العلمي ، الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية. منشور بالإنترنت، الاردن ـ ٢٠١٤ ، www.assakina.com

١٠. أمينة نشناش: « الركن المفترض في الجريمة المعلوماتية بين الوقاية والمكافحة» محاضرة ألقيت بتاريخ ٢٠١٥/١١/١٦ ، حقوق جامعة محمد خيصرة ، بسكرة ، الجزائر، ص١٥٦.

١١. د. أمال عثمان: فكرة الخطر في الجرائم الاقتصادية بصفة عامة، دار النهضة العربية، بند ١٧، ص٤٥.

١٢. د. أمال عثمان: الإثبات الجنائي ووسائل التحقيق العلمية ، دار النهضة العربية، القاهرة، ١٩٧٥م، ص٤.

١٣. د. أمال عثمان: شرح قانون العقوبات الاقتصادي في جرائم التموين ١٩٨٣، دار النهضة العربية، بند ١٥، ص ٤٣.

١٤. د. أمال عثمان: الخبرة في المسائل الجنائية – رسالة دكتوراه، كلية الحقوق جامعة القاهرة، ١٩٦٤، ص ٢٨، وما بعدها.

١٥. د. أحمد محمد مصطفى: الإرهاب ومواجهته جنائيا دار الفتح للطباعة والنشر، القاهرة، ط١، ٢٠٠٦، ص ١٥٦.

١٦. أحمد سامي الرواشدة : مكافحة الجريمة المعلوماتية بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة، الأردن، المجلد (١) العدد ٣ ، ٢٠٠٩، ص ١٢٨.

١٧. أحمد خليفة الملط : الجرائم المعلوماتيه ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الثانية ، ٢٠٠٦ ، ص١٨٧.

١٨. أسامة أحمد المناعسة : جرائم الحاسب الآلي والإنترنت – دراسة تحليلية مقارنة – ط١، دار وائل – عمان، ٢٠٠١، ص٢٨٩-٢٩٧.

٩١. د. أحمد حسني طه : مبادئ قانون الإجراءات الجنائية في التشريع المصري، مطبعة بهجت للطباعة، الجزء الأول ، بدون تاريخ، ص٤٠٦.

٢٠. القاضي كاظم عيد جاسم جبر: مكافحة الإرهاب في التشريع العراقي، موسوعة القوانين العراقية، بغداد، ط١، ٢٠١٠، ص٨٦.

٢١. باسم الحمادي: صعوبة إثبات جرائم الإنترنت، بحث منشور على شبكة الإنترنت بتاريخ ٧ محرم ١٤٢٣ هـ، الرياض.

٢٢. د. جميل عبد الباقي الصغير: القانون الجنائي والتكنولوجية الحديثة للجرائم الناشئة عن استخدام الحاسب الآلي ، دار النهضة العربية القاهرة، ١٩٩٢، ص١١.

٢٣. د. جلال محمد الزعبي : جرائم الحاسوب الآلي والإنترنت. دراسة تحليلية مقارنة، ط١، دار وائل، عمان، ٢٠٠١م، ص٢٨٩-٢٩٧.

٢٤. د. حسين بن سعيد الغافري: التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، بحث منشور على موقع بالإنترنت ص ٨١ وما بعدها //:http www.eastlaws.com

٢٥. حسن رجب الزهراني : إثبات جرائم تقنية المعلومات، بحث تكميلي مقدم لنيل درجة الماجستير، السعودية، جامعة الإمام محمد بن سعود الإسلامية، ٢٠٠٥، ص ٢ ww.imamu.edu.sa

٦٢. د. حسن تركي عمير: الإرهاب الالكتروني ومخاطرة في العصر الراهن، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، بحث منشور على الإنترنت، ص٢٧٥.

٢٧. د. حسن عثمان: الإرهاب الدولي مظاهره القانونية، مرجع منشور بالإنترنت ، ص١١٢.

٢٨. د. حسنين ابراهيم صالح عبيد: دروس في قانون العقوبات. القسم العام دار النهضة العربية، ١٩٩٩. ص٢١٨.

٢٩. د. حيدر علي نوري: الجريمة الإرهابية، دراسة في ضوء قانون مكافحة الإرهاب، منشورات زين الحقوقية، لبنان، ط١، ٢٠١٣، ص ١٩٩.

٣٠. د. خالد حامد مصطفى: المسؤولية الجنائية المباشرة، الخدمات التقنية ومقدميها بحث منشور بالإنترنت، ٢٠١٦، ص ٩٥.

٣١. د. خالد محمد المهيري: التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية – الطبعة الثانية – دار العزيز – للطباعة والنشر ، دبي، بدون تاريخ نشر، ص٥٠٨.

٣٢. د. خالد المهيري: جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية ، معهد القانون الدولي ، دبي ، ٢٠٠٤ ، ص١٨٥ .

٣٣. د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، ٢٠٠٩، دار الفكر، الإسكندرية، ط١، ص٨٥.

٣٤. راشد بشير إبراهيم: التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على إمارة « أبو ظبي»، مركز الإمارات للدراسات والبحوث والاستراتيجية، ط١، ٢٠٠٨٧، ص ٥٨.

٣٥. د. رمزي رياض عوض : مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة – دار الفكر العربي، القاهرة، سنة ٢٠٠٠، ص ٨٥.

٣٦. رحماني منصور: الوجيز في القانون الجنائي العام، دار العلوم للنشر والتوزيع، عناية الجزائر، ٢٠٠٦، ص ١٠٨-١١٠.

٣٧. رائد العدوان : المعالجة الدولية لقضايا الإرهاب الالكتروني دورة تدريبية بعنوان توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب ٢٠١٣ صـ٢٥.

٣٨. د. زكي أمين حسونة: جرائم الكمبيوتر الجرائم الأخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، ص ٤٧٦.

٣٩. سامي على حامد عياد : استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، دار الفكر . الإسكندرية. ٢٠٠٨. ص ٧٣.

٤٠. د. سيد شوربجي عبد المولى: تأثير الجريمة على خطط التنمية الاجتماعية والاقتصادية في الوطن العربي، بحث منشور بالإنترنت، صـ ١٦٦-١٦٧.

٤١. د. سعيد على النقبي: المواجهة القانونية للإرهاب، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠١١، صـ١٦٩.

٤٢. د. سامر سعدون عبود: التحريض على ارتكاب الجرائم الإرهابية باستخدام وسائل التقنية الحديثة، كلية القانون جامعة بغداد، بحث منشور بالإنترنت، ٢٠١٦، ص ٥٧٩.

٤٣. د. سعيد عبد اللطيف حسن: الإثبات في جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، ١٩٩٩، ص٩٥ وما بعدها.

٤٤. د. سعد صالح الجبوري: الجرائم الإرهابية في القانون الجنائي، دراسة مقارنة في الأحكام الموضوعية، المؤسسة الحديثة للكتاب، ط١، ٢٠١١، ص ٦٦.

٤٥. سليمان بن مهجع العنزي: وسائل التحقيق في جرائم نظم المعلومات رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٣، ص ١١٤.

٤٦. سميرة المعاشي: ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، الجزائر، ٢٠١١، ص ٢٨٠.

٤٧. صغير يوسف: الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير منشورة بالإنترنت، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١٣، ص ٦٥.

٤٨. صالح مختاري : كيف تستخدم الجماعات الإرهابية الإنترنت لهندسة جرائمها المنظمة، مقال منشور بالإنترنت، ص ٣٥.

٤٩. طاهر سليمان خليل : مكافحة الإرهاب وتأثيره على حقوق الإنسان المدنية (دراسة مقارنة) مكتبة الصباح، بغداد، ٢٠١٤ ، ص ٢٠.

٥٠. د. طارق عبد الله الشدي: آلية البناء لنظم المعلومات ، دار الوطن للطباعة والنشر، الرياض ١٤٢٣هـ، ص ٢١٠.

٥١. د. عبد الله سليمان: شرح قانون العقوبات الجزائري ، القسم العام ، الجزء الأول (الجريمة) ، ديوان المطبوعات ، الجامعية ، الطبعة السابعة ، الجزائر ، ٢٠٠٩ ، ص٢٩.

٥٢. د. عبد الجبار رضاحي عواد : جرائم تقنية المعلومات وإثباتها جامعة النهرين، بغداد، مرجع منشور بالإنترنت، ص ١٧.

٥٣. د. عارف عيد: جرائم الإنترنت : مجلة جامعة الشارقة للعلوم الشرعية والقانونية المجلد العدد ٣ أكتوبر ٢٠٠٨ ، صـ٧٣.

٥٤. د. علي سعيد عبد اللطيف: الجرائم الناشئة عن استخدام الحاسب الآلي ، كلية الشريعة والقانون، القاهرة. بحث منشور بالإنترنت، صـ٩٣.

٥٥. عبد الله بن عبد العزيز فهد العجلان : الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، المنعقد بالقاهرة، في المدة من ٢-٤ يونية ٢٠٠٨. بحث منشور بالإنترنت، صـ٣٥. www.shaimaaatalla.com

٥٦. د. على سالم محمد: جرائم الارهاب الالكتروني ، قسم القانون الجنائي ، الجامعة الخليجية. ٢٠١٠، الناشر الجامعة الخليجية قسم القانون ، ص ٢٨٦، ص ٣٢٠. بحث منشور على الإنترنت.

٥٧. د. عبد الرحمن جلهم حمزة: جرائم الإنترنت من منظور شرعي وقانوني، دراسة مقارنة، بدون تاريخ نشر. ص٨٤.

٥٨. د. عثمان حسن: الإرهاب الدولي ومظاهره القانونية والسياسية، دار الكتب القانونية. الطبعة الأول ى، ٢٠١١، صـ١١١-١١٢.

٥٩. د. عادل عبد الصادق : الإرهاب الإلكتروني - القوة في العلاقات الدولية ، نمط جديد وتحديات مختلفة ، المركز العربي لأبحاث الفضاء الإلكتروني ، الطبعة الثانية ، ص١٦٧ .

٦٠. عبد الحميد إبراهيم محمد العريان: مكافحة الجرائم الإرهابية المعلوماتية بحث منشور بالإنترنت، ٢٠٠٦، المغرب، ص ١١٥

٦١. د. عبد الحميد إبراهيم محمد العريان:العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة، بحث منشور بالإنترنت. http;www.nauss.edu.sa

٦٢. د. عبد الرحمن بن عبد الله السند: وسائل الإرهاب الالكتروني حكمها في الإسلام وطرق مكافحتها، مقال منشور على موقع السكينة الالكتروني، ص ٩.

٦٣. عبد الحق باسو : الإرهاب المعلوماتي في القانون المغربي والدولي ، المؤتمر العام لمكافحة الجرائم الإرهابية المعلوماتية بالمغرب خلال الفترة من ١١ــ ١٥ /٢٠٠٦/٣ م صـ ٢١ .

٦٤. د. عمر عبد العزيز موسي: آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية. بحث مقدم لمؤتمر مركز جيل البحث العلمي ١٤ الجرائم الإلكترونية منشور بالإنترنت. www.jiL.cemt er/Ham .

٥٦. د. عبد الفتاح مصطفي الصيفي: القواعد الجنائية. الإسكندرية. ١٩٦٧. ص٣٥.

٦٦. د. عبد الفتاح بيومي : عالم الجريمة والمجرم المعلوماتي، منشأة المعارف : الإسكندرية. ٢٠٠٩. ص١٧.

٦٧. د. عبد الفتاح بيومي : الاحداث والإنترنت، أثر الإنترنت في انحراف الإحداث، دار الفكر العربي، الإسكندرية. ٢٠٠٧، ص١٩.

٦٨. د عبدالفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأول ي ، ٢٠٠٦ ، ص٣٦٦.

٦٩. د. عبد الفتاح بيومي حجازي : التزوير في جرائم الكمبيوتر والإنترنت دار الكتب القانونية، القاهرة، ٢٠٠٨ ، ص ١١٤.

٧٠. د. عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الحاسب والإنترنت دار الكتب القانونية، المحلة الكبرى – مصر ، ٢٠٠٧، ص ٣٨٨.

٧١. د. عبد الفتاح بيومي حجازي : الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٢م ص ٤٦.

٧٢. عبد الله دغمش العجمي: المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، ٢٠١٤م، ص ٤٥.

٧٣. د. عطا عبد العاطي محمد السنباطي: موقف الشريعة الإسلامية من جرائم الحاسب الآلي والإنترنت، دراسة مقارنة، دار النهضة العربية ١٤٢٢هـ- ط١ ، ٢٠٠٢، ص ٣٥.

٧٤. د. عبدالله محمد النويسه: جرائم تكنولوجيا المعلومات «دارسة تحليلية مقارنة». دار وائل للطباعة و النشر و التوزيع. ص ٩.

٧٥. د.على عدنان الفيل : الإجرام الإلكتروني ، دراسة مقارنة. لبنان ، الطبعة الأول ى ، ٢٠١٠، ص٧٤.

٧٦. د. علي محمود علي حمودة : الأدلة لمتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائية، بحث منشور ضمن أبحاث المؤتمر العلمي الأول ، حول الجوانب القانونية والأمنية للعمليات الإلكترونية – مركز البحوث والدراسات أكاديمية شرطة دبي – محور القانون الجنائي في الفترة من ٢٦-٢٨ أبريل ٢٠٠٣ ، ص ٢٨٥.

٧٧. د. علي محمود علي حمودة : شرح قانون العقوبات القسم العام، الجزء الأول ، دار الهاني للنشر، ٢٠٠٣، صـ٤٥٦.

٧٨. د. علي حامد عيد: تمويل الإرهاب، دار الفكر الجامعي ، الإسكندرية، الطبعة الأول ى، ٢٠٠٧، ص ١١٥.

٧٩. د. عفيفي كامل عفيفي: جرائم الحاسب الآلي وحقوق المؤلف والمصنفات الفنية، دراسة مقارنة، منشأة المعارف، الإسكندرية، ٢٠٠٠، ص ٣٤٤.

٨٠. د. عبد الرحمن بحر: معوقات التحقيق في جرائم الإنترنت «دراسة مسحية على ضباط الشرطة بدون البحرين، رسالة ماجستير جامعة نايف للعلوم الأمنية، الرياض، ١٩٩٩، ص ٥١.

٨١. د. عبد الله علي محمود: إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية – محور القانون الجنائي – دبي – خلال الفترة من ٢٨/٢٦ أبريل ٢٠٠٣، ص ٦١٦.

٨٢. د. فتوح أبو دهب هيكل: التدخل الدولي لمكافحة الإرهاب وانعكاساته على السيادة الوطنية، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ط١، ٢٠١٤، صـ٦٧.

٨٣. فتحية رصاع : الحماية الجنائية للمعلومات علي شبكة الإنترنت ، رسالة ماجستير، كلية الحقوق والعلوم الانسانية ، جامعة تلمسان ،٢٠١٢ ، ص٥٦ .

٨٤. د. كاظم عيد جاسم جبر: مكافحة جرائم الإرهاب في التشريع العراقي، دار الكتب والوثائق، بغداد، ٢٠١٠، ط١، بحث منشور بالإنترنت، ص ٣٤.

٥٨. كمال الكركي: جرائم الحاسوب ودور مديرية الأمن في مكافحتها ، ورقة عمل مقدمة إلى ندوة قانون حماية المؤلف ، نظرة إلى المستقبل المنعقدة في عمان بتاريخ ١٩٩٩/٧/٥- ض١٠ وما بعدها.

٨٦. د. مدحت رمضان : جرائم الاعتداء على الأشخاص عبر الإنترنت ، دار النهضة العربية، الطبعة الأول ى، ٢٠٠٠، ص ٨٧.

٨٧. منير محمد الجهيني : ممدوح محمد الجهيني: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها. دار الطباعة الجامعي. الإسكندرية. ٢٠٠٦ صـ٧٥.

٨٨. د. محمد سامي الشوا: الجريمة المنظمة وصداها على الأنظمة العقابية، دار النهضة العربية، القاهر، بدون تاريخ نشر، الطبعة الأول ى، ص ١٧٠.

٨٩. د. مايا حسن ملا خاطر: الإطار القانوني لجريمة الإرهاب الإلكتروني ، السعودية ،٢٠١٥ ، ص ١٣٢

٩٠. د. محمد السعيد رشدي: الإنترنت والجوانب القانونية لنظم المعلومات بحث مقدم إلي مؤتمر الإعلام والقانون، كلية الحقوق جامعة حلوان، من ٩-١٠ مارس ١٩٩٩.

١٩. د. محمد محمد شتا: فكرة الحماية الجنائية لبرامج الحاسب الآلي . دار الجامعة الجديدة للنشر، الإسكندرية. ٢٠٠١ ص٧٥.

٩٢. د. محمود صالح العدلي: الفراغ التشريعي في مجال مكافحة الجريمة الالكترونية،٢٠٠٩، جامعة طنطا، بحث منشور على الإنترنت، ص ٣٥.

٩٣. معتز محيي الدين: الإرهاب وتكنولوجيا المعلومات، مقال متاح على الإنترنت.

٩٤. د. مأمون محمد سلامة: قانون العقوبات. دار الفكر العربي. ١٩٩٦. ص٣٢١.

٩٥. د. مأمون محمد سلامة : قانون العقوبات. القسم العام، مطبعة جامعة القاهرة. ١٩٩١/٩٠. ص١٠٨.

٩٦. د. مأمون محمد سلامة : قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العامة، دار الفكر العربي، ١٩٩٦، ص ١٦٨.

٩٧. د. مأمون محمد سلامة : الإجراءات الجنائية في التشريع المصري – الجزء الأول ، دار النهضة العربية ، القاهرة ، سنة ٢٠٠١، ص ٦٤٥.

٩٨. د. محمد فهمي : الموسوعة الشاملة لمصطلحات الحاسب الالكتروني ، مطابع المكتب المصري الحديث القاهرة، سنة ١٩٩١.

٩٩. د. محمد مصطفي القللي: شرح قانون العقوبات في جرائم الأموال. دار الياس للطباعة ، الطبعة الأول ي، ١٩٤٧. ص٢٦.

١٠٠. د. محمد أبو العلا عقيدة : التحقيق وجمع الأدلة في مجال الجريمة الالكترونية بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية المنعقد بمركز البحوث والدراسات بأكاديمية

شرطة دبي، بتاريخ ٢٦ أبريل ٢٠٠٣ منشور على موقع كلية الحقوق جامعة المنصورة. http://www.f-low.net

١٠١. د. محمد السعيد رشدي : حجية وسائل الاتصال الحديثة في الإثبات ، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية محور المعاملات المدنية ، دبي الإمارات العربية المتحدة، ٢٦-٢٨ أبريل، ٢٠٠٣، صـ٣٦١-٣٦٣.

١٠٢. د. محمود نجيب حسني: شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، ١٩٨٨. فيه ١٨٥. ص٢٧٥.

١٠٣. د. محمود نجيب حسني: علاقة السببية في قانون العقوبات، نادي القضاة، ١٩٨٤، صـ٤٥.

١٠٤. د. محمد عبد اللطيف عبدالعال: الجرائم المادية وطبيعة المسؤولية الناشئة عنها، دار النهضة العربية. القاهرة ١٩٩٧. ص٣.

١٠٥. محمد صالح كريدي: الأفعال غير المشروعة في الجرائم المعلوماتية ، كلية الحقوق جامعة عنابة ، ٢٠٠٠ ، ص٢٠.

١٠٦. د. محمود أبو اليزيد: الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية . رسالة دكتوراه. حقوق القاهرة ٢٠١٦، صـ٤٤٤.

١٠٧. د. محمد ياسر أبو الفتح : خصائص وتصنيفات الجريمة المعلوماتية منتدى د.شيماء عطا الله- منتدى القانون الجنائي،٢٠٠٨، www.shaimaaaatalla.com

١٠٨. د. محمود محمد مصطفى: شرح قانون العقوبات، القسم العام الطبعة العاشرة، ١٩٨٣، مطبعة جامعة القاهرة، صـ٢٨٠.

١٠٩. د. محمد محمد شتا: فكرة الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠١، ص ٧٥.

١١٠. د. محمود داوود يعقوب: المفهوم القانوني للإرهاب، دراسة تحليلية تأصيلية مقارنة، منشورات أين الحقوقية، الطبعة الثانية، ٢٠١٣، تونس، ص ٧٠.

١١١. د. مصطفى محمد موسى: دليل التحري عبر شبكة الإنترنت ، دار الكتب القانونية، القاهرة، ٢٠١٠، ص ١٤٣.

١١٢. محمود داوود يعقوب: المفهوم القانوني للجرائم الإرهابية ، دراسة تحليلية تأصيلي، مقارنة، منشورات زين الحقوقية، الطبعة الثانية، ٢٠١٢، تونسن بحث منشور صـ٣٧١.

١١٣. د. محمد العفيف : جرائم الإرهاب في التشريع المقارن ، المكتبة الوطنية، عمان، ٢٠٠٧، ص ١٢٥.

١١٤. مصطفى سعد حمد خلف: جريمة الإرهاب الالكتروني، دراسة مقارنة بين التشريعين الأردني والعراقي، كلية الحقوق جامعة الشرق الأو سط، ٢٠١٧، رسالة ماجستير، صـ٢٨٢.

١١٥. نبيلة هبة هروال : الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات دار الفكر الجامعي الاسكندرية، ٢٠٠٧، ص ٢٢٥.

١١٦. د. نبيل عبد المنعم جاد: أسس التحقيق والبحث الجنائي العلمي مطبعة كلية الشرطة، ٢٠٠٦، ص ١١٢.

١١٧. نورا بنداري عبدالحميد فايد: دور وسائل التواصل الإجتماعي في تجنيد ، أعضاء التنظيمات الإرهابية «دراسة حالة داعش» المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسة والاقتصادية. ٢٠١٧ ، ص٤٥.

١١٨. د. نهلا عبد القادر المؤمن: الجرائم المعلوماتيين، دار الثقافة للنشر والتوزيع، الطبعة الأول ي، عمان، ٢٠٠٨، ص٥١.

١١٩. نسرين عبد الحميد نبيه :الجريمة المعلوماتية والمجرم المعلوماتي ، منشأة المعارف، الإسكنرية، ٢٠٠٥، ص ٢١٢.

١٢٠. د . نائلة عادل محمد فريد قورة : جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، ص٣٦٤

١٢١. د. هدى حامد قشقوش: جرائم الحاسب الآلي في التشريع المقارن. دار النهضة العربية. القاهرة. ١٩٩٢. ص ٢٠.

١٢٢. د. هاشم الزهراني: الإرهاب المعلوماتي. كلية الملك فهذا الأمنية. مركز البحوث، ندوه المجتمع والأمن والجرائم الإلكترونية، الرياض٢٠٠٧. ص٣٧٩.

١٢٣. د. هشام محمد فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة، مكتبة الآلات الحديثة، اسيوط، ١٩٩٤ ، ص ٢٣٥ .

١٢٤. د. هشام محمد فريد رستم : الجرائم المعلوماتية أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، العدد ٢، ١٩٩٩، ص ٤٣٠.

١٢٥. د. هلالي عبد اللاه أحمد. تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ١٩٩٧، ص ٢٣٧.

١٢٦. د. هلالي عبد اللاه: التزام الشاهد بالإعلام في الجرائم المعلوماتية – دراسة مقارنة، دار النهضة العربية، القاهرة، سنة ٢٠٠٠، ص٢٣.

١٢٧. يونس محمد عرب : استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابين، ط١، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠١٢، ص١٦٦-١٦٧.

١٢٨. د. يوسف الصغير: الجريمة المرتكبة عبر الإنترنت ، مذكرة لنيل درجة الماجستير في القانونية كلية الحقوق والعلوم السياسية جامعة مولود المعمري- الجزائر، ٢٠١٣، ص١٢، بحث منشور بالإنترنت.

١٢٩. د. يسر أنور علي: شرح قانون العقوبات. النظرية العامة، دار الثقافة الجامعية. ١٩٩١، ص٧٨٢.

١٣٠.ثانياً : أحكام المحاكم :-

١. نقض جنائي ١٩٩٩/٧/٤ مجموعة القواعد القانونية لأحكام محكمة النقض – ١٤٢٩-س٦٧ ق .

٢. نقض ١٩٦٥/٣/٢١ – مجموعة القواعد القانونية - رقم ٥٢ صـ ٣١.

٣. نقض ١٩٧٧/٦/٢٢ – مجلة المحامون، سنة ٤٢، رقم ٧٥٩، ص ٥٨٣

٤. نقض ١٩٨٠/٢/٧ مجموعة أحكام محكمة النقض – الدائرة الجنائية – س ٤٩ ق – رقم ٨٧٧ – ص ٢٠٠.

ثالثاً :- مراجع أجنبية :-

- مراجع باللغة الانجليزية :-

1. Bruce Hoffman: the inside terrorism edition 2006, Columbia university 2/ sbn o- p 231. -
2. - Donald k.piragaff. Computer crimes and other crimes against information technology in canda, R. I. D. P. 199., p. 241.

3. - Edward (martin) : computer crimes and other crimes against information technology in united kingdom R. I.. D. 1993 m,p. 640.

4. - Ferbrache (David): pathology of computer virus's springer-verlog London- LTD. 1992 p. 233.

5. - However, uradnik, Kathleen: cyber terrorism. 2011. California, Greenwood Retrieved, 4 December, 2016. p. 140-149.

6. - Matusitz, Jonathan: cyber Terrorism crimes, April 2005. American foreign policy interests.

7. - Robert Taylor: computer crime, in criminal investigation edited by Charles Swanson. N. Chamelin and I. territory, Hilling. 5 th edition, 1992-p 450

8. - Robert Taylor: computer crime: in criminal investigation edited by Charles Swanson. N. chameleon and I. territory hill. Ine, 5 Th edition 1992.p1.

9. - Suzan w. BRENNER: "At Light Speed" Attribution and Response to Cybercrime, terrorism / Warf are. 2007. Journal of criminal law criminology, P390.

- مراجع باللغة الفرنسية :-

1. Andria decoc: Droit penal general- Dalloz. Paris 2.5 eme. 1971. P185. -

2. Alice yatopaulous-Marangop oulos: les mobiles du delet decriminalogyet de droit penal- Bibliotheque de sciences criminelles. Tome xvll. 2004.p. 103.

3. - Bernard bauloc: le terrorisme problèmes actuels de science criminelle, presses. Universitaires, Marseille, 1989,p. 65.

4. - Philippe baumard:la cyber ciminalit e copart ementale, revue francaise de criminalogie et de droit penal, vol. 3 , November 2014.

5. - Sotile: Le terrorisme international, recveil discours de l'académie de droit international, vol. 65, 1983, p. 96.

Crimes of terrorism through electronic means

"A comparative study"

Dr: yasser fissal amin

Abstract

Developing computers has led to a change in the form of life in the world. Financial, educational establishments and public utilities dependence on the new means of information technology increased day after day. In spite of the unlimited advantages and benefits of the new electronic means, the abuse of such new techniques represented by cyber terrorism has become a threat to the world. Cyber terrorism is considered as a weapon which is easily used and has severe effects and terrorist acts while being in his house, office, cafe or one in his room in hotel.

Cyber terrorism has become on obsession that□□□ scares the world that has become vulnerable to attacks by the terrorists who perform their subversive activity via internet from anywhere in the world. These risks increase day by day because the new technique by itself is unable to protect people from the electronic crimes which resulted in serious disadvantages against individuals, organizations and countries many countries have taken measures and precaution to confront the cyber terrorism. Yet, these efforts are not enough and we are still in needed more efforts to face dangerous weapon.

Keywords:cyberterrorism-electroniccrimes-criemsterrorism - cyber crim – ports – «world virtual» - Virtual private networks works. Threat – hackers.