تحديات الإجراءات التحقيقية
والبحث في مسرح جريمة الإرهاب الإلكتروني
(دراسة في القانون القطري)

الدكتور
أيمن أحمد الكريمين
أستاذ العلوم الشرطية المساعد
كلية الشرطة – قطـــــر
الدكتور
رامي عبدالحميد المجالي
أستاذ علم الجريمة المساعد
جامعة البلقاء التطبيقية/ كلية عجلون الجامعية – الأردن

ملخص البحث

يعتبر مسرح جريمة الإرهاب الإلكتروني من أخطر مسارح الجريمة وأكثرها تعقيدا، لإختلاف تلك الجريمة عن الأنماط الأخرى من الجرائم التقليدية، سواء كان ذلك من ناحية الإجراءات التحقيقية والبحث فيها (التحديات الأمنية)، أو من ناحية تطبيق نصوص القوانين (التحديات القانونية).

وعليه تظهر أمام الجهات التحقيقية الأمنية أو القضائية صعوبات تعرقل أو تؤثر على قدرة المحققين الفنية في كيفية التعامل مع الدليل الرقمي الموجود في مسرح الجريمة الإلكترونية من حيث طرق ووسائل المعاينة أو إجراءات التفتيش، وكذا أمام رجال القضاء في تطبيق القانون، وذلك لعدم وجود قانون خاص بتلك الجريمة ينظم عملية الإجراءات التحقيقية الفنية من لحظة البلاغ عن القضية ولغاية توديعها للمحكمة المختصة. وهذا يتطلب من الجهات المعنية بذل المزيد من الجهد في تدريب القوى العاملة في مجال البحث والتحقيق الجنائي على كيفية التعامل مع الدليل الرقمي في مسرح الجريمة، والعمل على تشريع قانون خاص تنظم نصوصه المفاهيم المتعلقة بالجريمة والإجراءات التحقيقية والعقوبة المترتبة على ذلك الفعل.

الكلمات المفتاحية: التحديات، إجراءات التحقيق، الإرهاب الإلكتروني، مسرح الجريمة الإلكتروني، الدليل الرقمي.

Challenges of investigation procedures of electronic crime terrorism

(Studying The Qatari Law)

Dr: Ayman Ahmed AL-Krimeen\ Assistant Professor of Police Science
Police College - Qatar
Dr: Rami Abedalhameed Amajali\ Assistant Professor of Criminology
Balqa Applied University\ College of Ajloun University

Abstract

The electronic crime is considered as the most dangerous and complicated crime besides it's different from the traditional crime at two levels the first one is the investigation procedures (security challenges) and the second one is the level of applying the rules (law challenges) As a result security investigators face challenges regarding dealing with the available digital evidence of electronic crime. And the same thing is happening with the court of law specially when applying rules of the digital crime. Because there is no specific rule that enable the security administration to deal with such crime technically from the moment of the acknowledgement of the crime to the moment of delivering the case to the court of law.

So the security administration should train investigators of ways how to deal with a digital crime evidence and create a rule that punish electronic violators fairly.

Key words (Electronic crime, Security procedures, challenges, Digital evidence, Electronic terrorism)

مقدمة

الأمن الإلكتروني أصبح ضرورة في حياتنا لأنه مرتبط بوسائل الإتصال الحديثة إرتباطا وثيقا بمختلف طرق التواصل وبكافة أشكاله، لهذا فإنه لا يمكن لأي بلد في هذا العصر أن يبقى معزولا عن التطورات السريعة والهائلة في مجال التقنية المعلوماتية، وما ينجم عنها من مخاطر إجتماعية وإقتصادية وأمنية. لذلك بات من الضروري على كل بلد حماية أفراده ومقدراته ومؤسساته من الآثار المترتبة على هذا الإنفتاح [١].

تختلف إجراءات المعاينة والتفتيش في الجرائم التقليدية عنها في الجرائم الإلكترونية، حيث أن البحث عن الدليل في مسرح الجريمة الإلكتروني هو دليل رقمي، يحتاج إلى خبرة فنية عالية من محققين ذوو خبرة، وذلك لسهولة إتلاف الأدلة من قبل الجناة، كما أن مرتكبيها من بين فئات متعددة، حيث تجعل التنبؤ بالمشتبه بهم أمرا صعبا، كما أنها جريمة عابرة للحدود لا تعترف بعنصر الزمان والمكان.

هناك فجوة واسعة بين المتخصصين التقنيين وممارسي المهن القانونية في نظام العدالة الجنائية، حيث أن كثيرا من ممارسي المهن القانونية يعلم ويدرك بأنهم بحاجة للحصول على دراية وخبرة بالأدلة الرقمية وممارسات الجنائيات الرقمية، إلا أنهم مع ذلك يعتبرون أن الإجراءات التقنية والحصول على المعرفة صعبة التعلم أو حتى المتابعة بالنسبة لهم، علما بأنهم لا يحتاجون إلى فهم الإجراءات الجنائية الرقمية للقرص الصلب المستخدم في الكمبيوتر، هم فقط بحاجة إلى معرفة ما إذا كانت البيانات (الأدلة الرقمية) المتحصل عليها ذات حجة قانونية. ولهذا وجدوا أنفسهم تائهين في التفاصيل دون فهم المباديء الأساسية في إجراءات التحقيقات الجنائية الرقمية[٢].

مشكلة الدراسة:

تسعى أجهزة العدالة الجنائية في معظم دول العالم إلى السرعة والدقة في الكشف عن الأدلة الجرمية في مسرح الجريمة مستندة في ذلك على ما تنص عليه أجهزتها التشريعية في تلك الدول ومن أجل وضع الحلول المناسبة والوقائية لمنع

---

[١] د/ بن يحيى ناعوس - مكافحة الإرهاب الإلكتروني: ضرورة بشرية وفريضة شرعية، منتدى الألوكة، السعودية، http://www.Alukah.net/ ، تاريخ الإضافة ٢٠١٥/١/٦، عدد الصفحات٢٨، عدد المجلدات١، تاريخ الإطلاع ٢٠١٨\١١\١٠م.

[٢] Losavio M, Adams J., (٢٠٠٦) *Gap analysis: judicial experience and perception of electronic evidence*, Journal of Digital Forensic Practice; ١:١٣-, ٢٠٠٦.

إنتشار مثل هذه الجرائم مستقبلا، إلا أن العديد من الدول ما زالت تعاني من الضعف في إكتشاف هذه الجرائم، ومن بينها جرائم الإرهاب الإلكتروني نتيجة أوجه القصور في التشريعات الوضعية التي لا تتماشى مع التطور التكنولوجي على مستوى العالم، لذلك تكمن مشكلة الدراسة في بعض التحديات الفنية التي تتمثل في معاينة وتفتيش مسرح جريمة الإرهاب الإلكتروني، التي تظهر أمام رجال الضابطة العدلية في مرحلتي البحث والتحقيق تحول دون إتمام الإجراءات التحقيقية اللازمة، وذلك لما تنطوي عليه كل مرحلة من المراحل إجراءات فنية دقيقة في كشف ملابسات وغموض الجريمة، والسبب في هذا أنه يتطلب في الجرائم الإلكترونية وجود محققين متخصصين ومن ذوي الخبرة في مجال تلك التقنية، من أجل عملية الإستقصاء والإستدلال على الأدلة المطلوبة في مسرح الجريمة الإلكتروني.

أسئلة الدراسة:

تسعى الدراسة للإجابة على الأسئلة التالية:

السؤال الأول:ما هي التحديات الفنية المتعلقة بالمعاينة في الإجراءات التحقيقية والبحث في مسرح جريمة الإرهاب الإلكتروني؟

السؤال الثاني: ما هي التحديات الفنية المتعلقة بالتفتيش في الإجراءات التحقيقية والبحثفي مسرح جريمة الإرهاب الإلكتروني؟

السؤال الثالث: ما دور التشريع القطري في مواجهة جريمة الإرهاب الإلكتروني؟

أهداف الدراسة:

تهدف الدراسة إلى التعرف على التحديات التي تواجه الإجراءات التحقيقية والبحث في مسرح جريمة الإرهاب الإلكتروني من خلال:

١. التعرف على التحديات الفنية المتعلقة بالمعاينة في إجراءات البحث والتحقيق الجنائي في مسرح جريمة الإرهاب الإلكتروني.
٢. التعرف على التحديات الفنية المتعلقة بالتفتيش في إجراءات البحث والتحقيق الجنائي في مسرح جريمة الإرهاب الإلكتروني.
٣. التعرف على دور التشريع القطري في مواجهة جريمة الإرهاب الإلكتروني.

أهمية الدراسة:

تأتي أهمية الدراسة من ناحيتين:

الناحية الأولى: حداثة هذا النوع من الجرائم وإنتشاره على نطاق واسع، وذلك في ظل إفتقاد النصوص التشريعية التي تتناول ذلك الفعل بالتجريم في قانون خاص بالإرهاب الإلكتروني في دولة قطر، حيث يرتبط فعل الإرهاب الإلكتروني بإستخدام شبكة الإنترنت ومواقع التواصل الاجتماعي. وقد تتمثل تلك الأفعال في جرائم الإرهاب والتدمير والخراب والترويع.

الناحية الثانية : عدم وجود دراسات سابقة على حد علم الباحثين إلى مسألة تحديات الإجراءات التحقيقية والبحث في مسرح جريمة الإرهاب الإلكتروني فيما يتعلق بالمعاينة والتفتيش، حيث جاءت الدراسة لبيان ابرز هذه التحديات ووضع صانعي القرار في الدولة القطرية أمام الآثار السلبية الناجمة عن خطر الإرهاب الالكتروني والعمل على تعديل النصوص التشريعية في القانون القطري.

التعريفات المفاهيمية والإجرائية:

التحديات:

لا يوجد تعريف واحد متفق عليه يصلح أن يكون جامعا وشاملا لمفهوم التحديات، ويعود ذلك لإختلاف نظرة كل باحث للفهوم.

التحديات هي متغيرات أو متطورات أو مشكلات أو صعوبات أو عوائق نابعة من البيئة المحلية أو الإقليمية أو العالمية[1].

تعرف إجرائيا في هذه الدراسة بأنها تلك الصعوبات التي تحيط بجريمة الإرهاب الإلكتروني وتواجه المحقق الجنائي في كشف غموض وملابسات حقيقة الجريمة، والمتعلقةفي الصعوبات التي تواجه الجهات المناطة بإجراءات التحقيق متمثلة في معاينة وتفتيش مسرح جريمة الإرهاب الإلكتروني من ناحية، والقصور التشريعي في مواجهة جرائم الإرهاب الإلكتروني من ناحية أخرى.

التحقيق الجنائي:

هو الإجراءات القانونية والإدارية والفنية التي تتخذها سلطة رسمية ذات إختصاص بقصد كشف الجريمة والتعرف على الجناة والمتضررين من الجريمة وجمع الأدلة التي تحقق العدالة الجنائية[2]. وفي تعريف آخر فقد عرف التحقيق الجنائي بأنه عبارة عن مجموعة الإجراءات القانونية التي يباشرها مأمورو الضبط الجنائي، وتكون سابقة لإرتكاب الجريمة أو معاصرة أو لاحقة[3].

أما إجرائيا فيقصد بالتحقيق الجنائي في هذه الدراسة: مجموعة الإجراءات أو الخطوات القانونية التي يباشرها المحقق الجنائي أثناء إجراء المعاينة والتفتيش في مسرح جريمة الإرهاب الإلكتروني.

---

[1] **د/ فتحي أنيس- الإمارات إلى أين... إستشراف التحديات والمخاطر على مدى ٢٥ عام، مركز الإمارات للدراسات، أبوظبي.٢٠٠٥م.**

[2] **د/ سعد محجوب- أساليب البحث الجنائي في الوقاية من الجريمة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض. ٢٠٠٠م.**

[3] **د/ عبدالكريم الردايدة- الجامع الشرطي: في إجراءات التحقيق الجنائي وأعمال الضابطة العدلية، الطبعة١، دار اليراع للنشر والتوزيع، عمان. ٢٠٠٦م.**

الجريمة الإلكترونية:

هي أي فعل ينطوي على إستخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون[١]، وقد ذهب البعض إلى تعريف آخر للجريمة الإلكترونية، ألا وهو "موضوع هذه الجريمة، والمتمثل بالمعلومات والبيانات محل الجريمة، ذلك عندما يتجه قصد الجاني إلى الإعتداء عليها كإتلافها أو تخريب البرامج أو تزويرها"[٢].

أما إجرائيا فيقصد بالجريمة الالكترونية في هذه الدراسة بأنها: هي تلك الجرائم التي يتم تنفيذها بإستخدام التقنية الرقمية، أو بإستخدام الأجهزة الرقمية لتنفيذ الجرائم التي تكون فيها الأجهزة الرقمية هي المستهدف، أو الجرائم التقليدية التي تلعب التقنية دورا رئيسيا في كشفها.

الإرهاب الإلكتروني:

عرف الإرهاب الإلكتروني بأنه: العدوان أو التخويف أو التهديد ماديا أو معنويا بإستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات والأفراد على الإنسان أو دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق يسند صوته وصور الإفساد في الأرض[٣]. وذهب جانب آخر من الفقه لتعريفه بأنه: " ممارسة العنف بشكل فردي أو جماعي أو تيار أو جمعية أو تنظيمات دينية سواء كانت إسلامية أو غير إسلامية أو ينتمي إلى نظام معين يؤيد الإرهاب والإرهابيين وذلك وفقا لإستراتيجية محددة"[٤]. كما تم تعريفه بأنه: تعبير يشمل مزج مصطلح التهديد بنظام المعالجة الآلية للمعلومات بإستخدام تقنية الإتصالات الحديثة (الإنترنت)[٥].

وإجرائيا فيعرف الإرهاب الإلكتروني بأنه كل سلوك أو نشاط غير مشروع يصدر عن شخص لديه الإلمام الكافي بإستخدام تقنية المعلومات بهدف الإعتداء على النفس أو المال أو المعلومات بأي طريقة كانت وبغض النظر عن الدافع وراء إرتكاب تلك الجريمة أو الجهة التي ينتمي إليها الجاني.

---

[١] د/ سلمان القحطاني- علوم الأدلة الجنائية الرقمية. كلية الملك فهد الأمنية-مركز الدراسات والبحوث، الطبعة١، الرياض، ٢٠١٢م.

[٢] د/ فينوص السعدي- المعلوماتية ودورها في الهيمنة الأمريكية، رسالة ماجستير مقدمة إلى كلية العلوم السياسية – جامعة النهرين، ٢٠٠٩م.

[٣] د/ عبدالرحمن السند- وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، جامعة الإمام محمد بن سعود، ٢٠٠٤م.

[٤] د / عبدالرحمن؛ وآخرون- الإرهاب الإلكتروني: الظاهرة والمواجهة، مركز بحوث الشرطة- أكاديمية الشرطة، الإصدار الحادي والستون، مطابع الشرطة، مصر، ٢٠١٦م.

[٥] د/ عبد الفتاح حجازي- مبادىء الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م.

المبحث الأول

سنتناول في هذا المبحث الاطار العام للإرهاب الالكتروني في مطلبين مستقلين.

المطلب الأول: الإرهاب الإلكتروني ماهيته (أولا) وخصائصه وأهدافه التي تقتضيها طبيعته (ثانيا).

أما المطلب الثاني فسنستعرض فيه بعض الدراسات التي تناولت جريمة الإرهاب الإلكتروني.

المطلب الأول

ماهية الإرهاب الإلكتروني

يتفق المتخصصون في قضايا الإرهاب والجماعات المتطرفة على أن الإرهاب الإلكتروني يزداد خطورة وفتكا كلما زاد التقدم في المجال المعلوماتي، وهو لا يقل خطرا عن الإرهاب الواقعي الذي يحدث عن طريق التفجير والتخويف والخطف، فالتطور التقني يقابله التجسس والتخلف والهدم، والدمار الذي يلحقه الهجوم الإرهابي بأنظمة المعلومات التي تتحكم في كل مرافق ومناحي الحياة في المجتمع الذي يعتمد على الكمبيوتر والإنترنت إعتمادا مطلقا قد يعطل حياة مجتمع بأكمله[1].

بدأت علاقة الإرهاب بالشبكة العنكبوتية فعليا في منتصف التسعينات من القرن الماضي، وبدأ إستغلال جماعات الإرهاب الإلكتروني إستغلال الإنترنت بإنشاء مواقع خاصة بهم تبرر أفكارهم التكفيرية مستغلين بذلك زيادة إقبال الشباب على التكنولوجية الإلكترونية، وفي بداية الألفية الثانية خاصة بعد إطلاق "فيس بوك" في عام ٢٠٠٤م شكل الجهاديون علاقات دولية مرتبطة إلكترونيا بنظيراتها في كل دول العالم، تهدف إلى التخطيط لعمليات إرهابية دولية، لا يمكن تعقب صفحاتها الإرهابية في الدولة، ولا يمكن تعقبها في الدول الأخرى التي يتواجد بها الأطراف الأخرى[2].

أصبحت المنظمات الإرهابية تستخدم الإنترنت كوسيلة مهمة للإتصال في إستقدام عناصر جديدة لتجنيدها وضمها لتلك المنظمات من أجل المحافظة على وجودها وإستمرارها، وكذلك لترويج الفكر الإرهابي وإستخدامه كمنابر إعلامية لهم[3].

---

[1] د/ مصطفى موسى- الإرهاب الإلكتروني: دراسة قانونية-أمنية-نفسية-إجتماعية، دار الكتب والوثائق القومية المصرية، الطبعة١، القاهرة، ٢٠٠٩م.

[2] د/ زكريا أبو دامس- أثر التطور التكنولوجي على الإرهاب، عالم الكتب الحديث، الأردن، ٢٠٠٥م.

[3] د/ هند الخليفة- الحاسب الجنائي في الدول العربية، دراسة إستطلاعية، مؤتمر المعلومات والأمن الوطني، الرياض، ٢٠٠٧م.

يسعى إرهابي الإرهاب الإلكتروني إلى عمل تغييرات أساسية في الأنظمة العاملة، وتدمير حالة الرفاه المجتمعي والمعرفة، وتدمير البنية المعلوماتية التحتية وتعريض المجتمعات العالمية إلى مخاطر غير محتملة وغير متوقعة، وخاصة فيما يتعلق بأنظمة الإتصالات الأمنية والعسكرية، من خلال إستغلال موارد العالم المادي والإفتراضي مستهدفا بذلك التقنية التي تؤثر على قوة الإنتاجية والثقة بالمجتمعات ما بعد الصناعية [١].

يعتبر هذا المصطلح حديث النشأة، فلم يستقر الباحثون والمتخصصون على تعريف معتمد للإرهاب الإلكتروني، حيث وجدت عدة تعريفات لهذا المصطلح؛ إتفقت في الوسائل المستخدمة في هذه النوعية من الإرهاب، التي تستخدم شبكة المعلومات (الإنترنت) والوسائل الإلكترونية في تنفيذ غاياتها وأهدافها الإرهابية[٢].

ثانيا: خصائص وأهداف الإرهاب الإلكتروني

خصائص الإرهاب الإلكتروني:

يتميز الإرهاب الإلكتروني بعدد من الخصائص تميزه عن غيره من الجرائم التقليدية، وتحول دون إختلاطه بجرائم الإرهاب العادي، حيث تعتبر جريمة الإرهاب الإلكتروني من الجرائم العابرة للحدود، وغير خاضعة لنطاق إقليمي محدود. فهي لا تحتاج للقوة والعنف في إرتكابها، وإنما وجود جهاز حاسوب متصل بالشبكة المعلوماتية ومزود ببعض البرامج. فالشخص مرتكب جريمة الإرهاب الإلكتروني من الأشخاص ذوي الإختصاص في مجال تقنية المعلومات أو لديه المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية.ومن ناحية أخرى نجد أن هناك صعوبة في إكتشاف جرائم الإرهاب الإلكتروني، وذلك لنقص الخبرة لدى المحققين في بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم، وكذا صعوبة إثبات جريمة الإرهاب الإلكتروني، نظرا لسهولة تدميره وإتلافه من قبل الإرهابيين[٣].

أهداف الإرهاب الإلكتروني:

يهدف الإرهاب الإلكتروني إلى تحقيق عدد من الأهداف غير المشروعة تتمثل في: إلحاق الضرر بالبنى المعلوماتية التحتية وتدميرها، والإضرار بوسائل الإتصالات وتقنية المعلومات أو بالأموال والمنشآت العامة والخاصة. والإخلال بالنظام العام، والأمن المعلوماتي، وزعزعة الطمأنينة. كما تسعى إلى تعريض

---

[١] د/ فايز الشهري – التطرف الإلكتروني رؤية تحليلية لإستخدامات شبكة الإنترنت في تجنيد الأتباع، ورقة علمية مقدمة لمؤتمر تقنية المعلومات والأمن الوطني، ٢٠٠٧م.

[٢] لواء طارق عطية- شبكة المعلومات الدولية (الإنترنت) والإرهاب، بحث منشور بمجلة الأمن العام، العدد ٢٠٧، القاهرة، أوكتوبر، ٢٠٠٩م.

[٣] د/ عبدالله العجلان- حماية أمن المعلومات والخصوصية في قانون الإنترنت، بحث مقدم إلى المؤتمر الدولي الأول حماية أمن المعلومات، القاهرة من ٢-٤ يونيو ٢٠٠٨م.

سلامة المجتمع وأمنه للخطر ونشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة، وتهديد السلطات العامة والتنظيمات الدولية وإبتزازها.وقد يكون بدافع الإنتقام من الخصوم أو جمع الأموال والإستيلاء عليها، أو قد يكون من أجل إستقطاب الشباب للإنخراط ضمن صفوف تلك الجماعات الإرهابية، أو قد يكون الهدف منها جذب الإنتباه والدعاية والإعلان أو إثارة الرأي العام [1].

المطلب الثاني

الدراسات التي تناولت جريمة الإرهاب الإلكتروني

أجرى (عبدالرحمن؛ وآخرون، ٢٠١٦) دراسة هدفت إلى الوقوف على ماهية الإرهاب الإلكتروني وبيان أشكاله ووسائله، حيث إتبعت الدراسة المنهج الوصفي التحليلي، وقد توصلت الدراسة إلى عدد من النتائج من أبرزها ما يتعلق بدوافع إنتشار الإرهاب الإلكتروني أنه يتمثل في ضعف بنية الشبكات المعلوماتية وقابليتها للإختراق وغياب الحدود الجغرافية وتدني مستوى المخاطرة وسهولة الإستخدام، إضافة غلى الفراغ التنظيمي والقانوني على الشبكات المعلوماتية[2].

كما قام (موسى، ٢٠٠٩) بإجراء دراسة هدفت إلى معرفة مدى موضوعية ومصداقية ما تنشره التنظيمات السرية الإرهابية على مواقعها عبر شبكة الإنترنت، حيث إستخدم الباحث المنهج التحليلي، على المواقع الإلكترونية والبريد الإلكتروني وغرف الدردشة خلال الفترة من عام ١٩٩٢-٢٠٠٨م، وقد توصلت الدراسة إلى عدد من النتائج من أهمها: أنه يرجع سبب ظهور الإرهاب الإلكتروني وإنتشاره إلى قابلية البنية التحتية للشبكات المعلوماتية للإختراق، وغياب الحدود غلى أرض الواقع في الشبكة المعلوماتية والإجتماعية[3].

وفي دراسة قام بها (عباس، ٢٠١٥) هدفت إلى معرفة مخاطر وصعوبات التحقيق في جرائم الإرهاب الإلكتروني في نظام الإجراءات الجزائية السعودي، خلصت غلى عدة نتائج منها: عدم الخبرة التقنية لدى سلطات البحث والتحقيق قد يتسبب في فقدان الدليل[4].

ومن جانبنا نرى أن الإرهاب الإلكتروني هو كل نشاط إيجابي أو سلبي، يقوم به فرد أو مجموعة لديهم الإلمام الكافي بتقنية المعلومات، وبغض النظر عن إنتمائهم السياسي أو الديني أو العرقي، بالإعتداء على إنسان أو مال، أو بيانات

---

[1] راجع د/ عبدالرحمن؛ وآخرون- المرجع السابق-ص٢٩.

[2] د/ عبدالرحمن؛ وآخرون- الإرهاب الإلكتروني: الظاهرة والمواجهة، مركز بحوث الشرطة- أكاديمية الشرطة، الإصدار الحادي والستون، مطابع الشرطة، مصر، ٢٠١٦م.

[3] د/ مصطفى موسى- الإرهاب الإلكتروني: دراسة قانونية-أمنية-نفسية-إجتماعية، دار الكتب والوثائق القومية المصرية، الطبعة١، القاهرة، ٢٠٠٩م.

[4] د/ نهاد عباس- إجراءات البحث والتحقيق في جرائم الإرهاب الإلكتروني وتحدياتها: دراسة في النظام السعودي، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠١٥م.

الغير، أو معلومات عن طريق إستخدام الكيان المعنوي للحاسب الآلي، أو أي جهاز إلكتروني آخر مرتبط به أو بنظام المعلومات العالمية (الإنترنت)، بقصد العدوان أو التخويف أو التهديد المادي والمعنوي، سواء كان ذلك بتعطيله أو إضعاف قدرته على أداء وظائفه بالنسخ أو بالإضافة أو الحذف أو بالمناقلة للخصائص الأساسية للبرامج أو المعلومات المخزنة أو الإتصال بها من غير وجه حق بأي وسيلة كانت.

المبحث الثاني

تحديات إجراءات البحث والتحقيق في مسرح الجريمة الإلكتروني

سيتناول هذا المبحث كل من التحديات الفنية (المطلب الأول). أما المطلب الثاني سنتناول فيه المواجهة التشريعية في القانون القطري لجريمة الإرهاب الإلكتروني

المطلب الأول

التحديات الفنية

تكمن التحديات الفنية لإجراءات البحث والتحقيق في مسرح الجريمة الإلكتروني في عدة مسائل أهمها المعاينة والتفتيش، وسنتناولها تباعًا:

أولا: المعاينة

المعاينة هي إحدى الإجراءات التحقيقية التي خول بها القانون رجال الضابطة العدلية إجرائها سواء كان ذلك في مسرح الجريمة العادي أو مسرح الجريمة الإلكتروني، فهي كإجراء لا تختلف وإنما يظهر الإختلاف في المحتوى الفني لمسرح الجريمة الإلكترونية [1].

إن أول مهمة يجب القيام بها من قبل المحقق الجنائي هي المحافظة على مكان الجريمة وحمايته قبل البدء بعملية جمع الأدلة ومعاينة مسرح الجريمة، في الجرائم الإلكترونية، فإن مكان الجريمة يمكن أن يكون جهاز حاسب أو مخدم (server) أو جهاز موبايل، علما بأن الحفاظ على الحالة الأصلية للتجهيزات التي تحوي على أدلة رقمية يعتبر من أهم خطوات التحليل الجنائي الرقمي[2].

تتضمن عملية جمع الأدلة الرقمية الجنائية من مسرح الجريمة الإلكتروني على عدد من الإجراءات الفرعية التي تشمل عملية البحث عن دليل رقمي عبارة عن بيانات رقمية مخزنة في وسائط رقمية مختلفة وتوثيقه والتي يعتقد أنها ذات قيمة وعلاقة وتفيد في القضية [3].

---

[1] د/ تركي، المويشير- التحقيق في الجرائم المعلوماتية: ملتقى الجرائم المعلوماتية، هيئة التحقيق والادعاء العام، الرياض، ٢٠٠٩م.

[2] د/ جميل طويله- التحليل الجنائي الرقمي: دليل عملي لطرق التحليل الجنائي الرقمي في الجرائم المعلوماتية، ٢٠١٦م.

[3] د/ عبدالفتاح حجازي-عالم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ٢٠٠٨م.

يتعين على المحقق الجنائي عند العلم بوقوع الجريمة الإنتقال مباشرة إلى مسرح الجريمة الذي يعتبر مكمن الآثار والأدلة المادية، حيث يتوجب عليه التعامل مع مسرح الجريمة على أنه مسرحين هما:مسرح تقليدي يتكون من مكونات مادية محسوسة للمكان الذي وقعت فيه الجريمة، فقد يترك الجاني آثارا عدة كالصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية. أما المسرح الثاني يقع داخل البيئة الإلكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الإنترنت، في ذاكرة الأقراص الصلبة الموجودة بداخله [١].

أ. محل المعاينة

تعتبر الآثار التي يتركها الجاني مستخدم الإنترنت محلا للمعاينة، كما تشمل جميع الاتصالات والرسائل المرسلة والمستقبلة على جهاز الحاسوب والبيانات المحفوظة فيه، بغض النظر عن نوع وحجم الجهاز المستخدم [٢].

ب. تحديات المعاينة

الدليل محل المعاينة في مسرح الجريمة من الطبيعة الرقمية وهذا يمثل التحدي الأول التي تحتاج لمن لديه الخبرة الفنية في الضبط والإثبات لمثل تلك الرقميات الفنية الدقيقة على أجهزة الكمبيوتر والأجهزة الإلكترونية الأخرى، لأنه من السهولة تغييرها وحذفها أو تدميرها، فلذلك يتعين على المحقق تأمين وتوثيق وتصوير الأدلة الرقمية في أسرع وقت ممكن في مسرح الجريمة الإلكتروني [٣].

والتحدي الآخر هو إتساع مسرح الجريمة الإلكتروني بخصوص المكونات الرئيسية لتقنية الإرتباطات (سلكية أو لاسلكية) بين أجهزة الحاسب والأجهزة التقنية الأخرى في جميع مواقع مسرح الجريمة، والتي عادة ما يدل وجود مكونات شبكية سواء من نقاط وصول سلكية أو لاسلكية إلى إحتمال وجود أدلة إضافية خارج نطاق مسرح الجريمة الرئيسي الذي تتم معاينته حاليا، وهذه المكونات الشبكية في حال وجودها يجب توثيقها بشكل منفصل عن مسرح الجريمة الرئيسي [٤].

ومن ناحية أخرى يكمن التحدي في توثيق الوقت والتاريخ، حيث أنه قد يكون الجهاز مضبوطا بتوقيت مختلف يظهر على الصورة فقط، وتوقيت مخالف للكاميرا، وهذا يحتاج إلى خبير متخصص لمحاولة المقابلة بينهما بفحص الجهاز والتأكد من ذلك [٥].

---

[١] د/ أشرف قنديل- الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الطبعة١، الإسكندرية، ٢٠١٥م.

[٢] د/ عمر يوسف- الجرائم الناشئة عن إستخدام الإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٤م.

[٣] راجع د/ نهاد عباس- المرجع السابق- ص١١

[٤] د/ سلمان القحطاني- أساسيات شبكات الإتصالات الحديثة، مطبعة الحميضي، الرياض، ٢٠١٠م.

[٥] Thomas L. Floyd, (٢٠٠٥), Digital Fundamentals, Prentice, Pp: ٨٧-٨٩.

كما يتمثل التحدي في عملية فقدان البيانات المخزنة أو تدميرها في حالة قطع مصدر الطاقة الكهربائية عن جهاز كمبيوتر أو أي جهاز إلكتروني في المسرح[١].

وفي حالة أخرى يظهر التحدي في تغير أو تلف البيانات أثناء عملية جمعها وتغليفها في حال تعرضها للحقول المغناطيسية المتولدة عن طريق الكهرباء الساكنة أو المغناطيس أو الأجهزة الإلكترونية الأخرى[٢].

وقد يقومالجاني وخوفا من إكتشافه يقوم بمحو البيانات من الملفات، والتخلص منها حتى من سلة المهملات [٣]، بالإضافة إلى إمكانية التلاعب في البيانات عن بعد ، أو محوها عن طريق التدخل من خلال وحدة طرفية من قبل الجاني، وهذا يؤدي إلى الشك بصحة الأدلة إذا ما تم تحصيلها من مسرح الجريمة المعلوماتية [٤].

ثانيا: التفتيش

التفتيش إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مسرح الجريمة، لذلك يعتبر من أهم إجراءات التحقيق، لأنه غالبا ما يسفر عن أدلة مادية تؤكد علاقة المتهم بالجريمة. فالتفتيش ليس غاية بحد ذاته وإنما وسيلة للوصول إلى أدلة مادية تسهم في كشف الحقيقة[٥].

يتناول التفتيش مكونات الكمبيوتر بالبحث عن الأدلة الرقمية الموجودة في نظام الحاسب الآلي وما يتم ضبطه في نطاق ذلك، حيث يقوم المحقق بفرز وتصفية البيانات وإستبعاد ما هو غير مفيد والإبقاء على البيانات ذات القيمة الاستدلالية المهمة في القضية من خلال إستخدام مجموعة من الأدوات والتقنيات المصممة لهذا الغرض، وتركز هذه العملية في الأساس على تحديد وإيجاد الأدلة الرقمية المحتملة سواء في مصادرها المعروفة أو ربما في مواقع غير معهوده (غير تقليدية)، أي أن عملية التفتيش تعنى بإكتشاف وتحديد وإستخراج وفحص البيانات المحتمل وجود أدلة بها [٦]. ولكن هنا يثور سؤالين هما:

١. ما هي المعلومات الرقمية الصالحة للتفتيش؟
٢. ما أهم البيانات الرقمية التي يجب تفتيشها؟

---

[١] د/ سلمان القحطاني- علوم الأدلة الجنائية الرقمية. كلية الملك فهد الأمنية-مركز الدراسات والبحوث، الطبعة١، الرياض، ٢٠١٢م.

[٢] د/ حسين الغافري- التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، منتدى كلية الحقوق، جامعة المنصورة، مصر، ٢٠١٥م، http://www.F-law.net/law/ تاريخ الإطلاع: ٢٠١٨\١\١٨م.

[٣] راجع د/ عبدالفتاح حجازي – المرجع السابق- ص٤٦.

[٤] م/ لينا الأسدي- مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية: دراسة مقارنة، ط١، دار الحامد للنشر والتوزيع، عمان-الاردن، ٢٠١٥م.

[٥] راجع د/ أشرف قنديل- المرجع السابق- ص٨٣.

[٦] د/ سلمان القحطاني- أساسيات شبكات الإتصالات الحديثة، مطبعة الحميضي، الرياض، ٢٠١٠م.

للإجابة على السؤال الأول: فإن المعلومات الرقمية الصالحة للتفتيش هي تلك الأجهزة والمعدات والبرامج التي تعالج المعلومات وتخزنها على هيئة رقمية ثنائية (٠ أو ١). وفي العصر الحالي تعد جميع الأجهزة الحديثة من أجهزة وإتصالات سواء كانت سلكية أو غير سلكية تعمل على هذا النسق وذلك لكفاءته وسرعة معالجته وقلة أخطائه [١].

أما إجابة السؤال الثاني فيما يتعلق بأهم البيانات الرقمية التي يجب تفتيشها، كما أشار إليها [٢] تشمل المكونات التالية:

١. إستكشاف جميع أنواع الملفات والتي تشمل على سبيل المثال لا الحصر: (برنامج الورد، برنامج إكسل، برنامج البوربوينت، الملفات النصية، ملفات pdf، ملفات الصور، ملفات الصوت، ملفات الفيديو).
٢. الملفات المؤقتة وملفات الكوكي.
٣. فحص البريد الإلكتروني وروابط الإنترنت.
٤. فحص ملفات التسجيل والمتابعة.
٥. فحص الملفات البيانات والملفات التنفيذية.
٦. إستكشاف زمن إرتكاب الجريمة.
٧. إستعادة وإستخراج الملفات المحذوفة

أ. محل التفتيش:

هو الحاسوب والشبكة التي تشمل في مكوناتها الخادم والمزود الآلي والمضيف والملحقات التقنية [٣].

ب. تحديات التفتيش:

هناك بعض التحديات التي تواجه المحقق الجنائي أثناء عملية التفتيش المتعلقة بجهاز الحاسوب ومكوناته تتمثل في مكان وجود الحاسوب، فقد يكون في منزل الجاني أو منزل شخص آخر ليس له علاقة بالقضية، وقد يكون له عدة ملحقات للحاسوب موجودة عند أكثر من شخص مشتركين في إرتكاب الجريمة. أو قد يتمثل التحدي الآخر في إتصال جهاز الحاسوب المستخدم في إرتكاب الجريمة بجهاز حاسوب آخر وفي مكان آخر، أو أن يكون متصلا بعدة أجهزة وفي أماكن مختلفة [٤].

---

[١] Thomas L. Floyd, (٢٠٠٥), Digital Fundamentals, Prentice, Pp: ٩٧-٩٩

[٢] د/ سلمان القحطاني- علوم الأدلة الجنائية الرقمية. كلية الملك فهد الأمنية-مركز الدراسات والبحوث، الطبعة١، الرياض، ٢٠١٢م.

[٣] راجع د/ أشرف قنديل- المرجع السابق- ص٩٥.

[٤] د/ حسين الغافري- التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، منتدى كلية الحقوق، جامعة المنصورة، مصر، ٢٠١٥م، http://www.F-law.net/law/ تاريخ الإطلاع: ٢٠١٨\١\١٨م.

أما التحدي الآخر الذي يواجه عملية التفتيش يتمثل في أنه قد لا يمكن إستعادة الملفات المحذوفة حتى بإستخدام برمجيات الإستعادة أو برمجيات الجنائيات الرقمية وذلك إذا تمت الكتابة عليها من قبل نظام التشغيل. وعادة ما يحصل ذلك للملفات المحذوفة منذ وقت طويل [١]

وفي بعض الأحيان يكون النظام المعلوماتي المراد تفتيشه مزودا بنظام حماية يمنع من الدخول إليه دون تدخل ومساعدة المسؤول عن ذلك، وهنا يثار التساؤل حول مدى إجبار أو إكراه المتهم على تزويد المحقق بمفاتيح المرور الخاصة بالنظام أو الإفصاح عن كلمة السر من أجل الوصول إلى البيئة المعلوماتية[٢].

ومن ناحية أخرى يكمن التحدي فيما يخص صدور الإذن لإجراء التفتيش، حيث أنه قد يستغرق بعض الوقت، مما قد يؤدي إلى تلاشي الدليل وإندثاره بالمحو والإتلاف، وقد يكون عائقا أمام تحصيل ذلك الدليل [٣].

ومن وجهة نظر الباحثان نجد أن الجرائم المعلوماتية هي جرائم غير ملموسة (مستترة)، وقد يمضي على إرتكابها وقت طويل حتى تصل إلى علم الجهات المختصة، أو أن الشخص أو المؤسسة أو الشركة المتضررين من الجريمة يحجموا عن الإبلاغ عن تلك الجريمة، لأي سبب كان، سواء تعلق بعدم الوعي الأمني في أخذ الإحتياطات الأمنية لحماية أمنها المعلوماتي، أو أن الإخبار عن الجريمة قد يؤدي إلى حرمان الشخص من خدمة معينة أو أن تتأثر وظيفته بذلك. هذا من جانب المجني عليه. أما جهات البحث والتحقيق الجنائي عن الجرائم المعلوماتية فإن هناك معوقات تواجه المحقق تتمثل في نقص الخبرة والتدريب في التعامل مع الجرائم التي تتعلق بالتقنية، وعدم توفر المعرفة بالأساليب التي يتم من خلالها إرتكاب الجرائم المعلوماتية.

كذلك هنالك أمور تتعلق بالأمور الإدارية والقوى البشرية، لدى جهات التحقيق المختصة، حيث يظهر النقص في أعداد المحققين في منطقة الإختصاص، أو عدم توفر وسيلة النقل أو نقصها نتيجة إشراكها في واجبات أخرى (إدارية أو عملياتية أو قضائية). وفيما يتعلق بالتشريعات الناظمة فإنه مع التطور السريع لتقنية المعلومات وظهور جرائم مستحدثة يبرز القصور التشريعي في مواكبة تلك الجرائم، مما يحدو بالقاضي إلى اللجوء إلى التفسير الضيق والخروج على مبدأ شرعية الجرائم (لا جريمة ولا عقوبة إلا بنص). والتحدي الهام أما المحققين هو

---

[١] John Baschab, Jon Piot, The Executives Guide to Information Technology, Wiley, ٢٠٠٧.

[٢] Volonino, Linda and Reynaldo, Anzaldua, (٢٠٠٨), computer forensics for Dummles/ Wily publishing- U.S.A.

[٣] Warren G. Kruse, computer forensics (incident response essentials), simultaneously – Canada. (٢٠٠٥).

عندما تكون الجريمة عابرة للحدود تصعب معها المعاينة والتفتيش. وبالتالي فقدان الدليل الرقمي في مسرح الجريمة. مما ينعكس سلبا على الإجراءات اللاحقة المتعلقة في كشف غموض وملابسات الجريمة.

المبحث الثالث

المواجهة التشريعية لجريمة الإرهاب الإلكتروني

من خلال هذا المبحث سوف نتطرق إلى أهم التشريعات التي صدرت في دولة قطر، والتي تم تجريم الإرهاب الإلكتروني فيها والإعتداءات التقنية بموجبها.

إن التطور الملحوظ في الجرائم المعلوماتية والإرهاب الإلكتروني يحتم وجود إستراتيجية لمواجهة هذه الجرائم من خلال تحديث التشريعات القانونية والضرورية للتعامل مع تلك الجرائم الغير تقليدية، هذه المواجهة تتعامل مع التطور الحديث والمتقدم في جرائم الكمبيوتر المختلفة، سواء كانت تتعلق بالجرائم التقليدية التي تحدث عن طريق إستخدام الكمبيوتر أو الجرائم التي تحدث مباشرة من خلال الكمبيوتر.

يضطر القاضي في كثير من الأحيان إلى التفسير الضيق لنصوص القانون الجنائي، فيما يتعلق بالجرائم الإلكترونية، وهذا الإجراء يلتزم به القاضي في مواجهة نقص النص أو غموضه[1].

لذلك يتوجب على المشرع إخضاع الجرائم الإلكترونية بنصوص صريحة ومباشرة، وتحديد العقوبة اللازمة على الفعل الذي يتم إرتكابه من خلال التقنية الرقمية، وذلك خشية إفلات المجرم من المسائلة الجزائية عن الفعل الخطير الذي ترتب عليه إعتداء على الحياة الخاصة [2].

وقبل البدء في عرض المواجهة التشريعية لجريمة الإرهاب الإلكتروني في دولة قطر، فإننا سوف نقوم بإلقاء الضوء على بعض النصوص القانونية في تشريعات بعض الدول العربية والمتعلقة بالإجراءات التحقيقة (التفتيش) في الجرائم المعلوماتية.

المشرع العراقي أعطى في المادة (٧٢/ب) من قانون أصول المحاكمات الجزائية العراقي مهمة التفتيش لقاضي التحقيق أو المحقق أو عضو الضبط القضائي، في حين نجد أن المشرع الإماراتي أعطى لمأمور الضبط القضائي هذه المهمة وذلك في المادة (٥١) من قانون الإجراءات الجزائية لدولة الإمارات. وفي

---

[1] د/ أكرم نشأت- السياسة الجنائية: دراسة مقارنة، ط٣، بغداد، ٢٠٠٦م.

[2] د/ علي الزعبي- حق الخصوصية في القانون الجنائي: دراسة مقارنة، ط١، المؤسسة الحديثة للكتاب-طرابلس، ٢٠٠٦م.

النظـام الـسعودي لمكافحـة الجريمـة المعلوماتيـة لـم يـأتي فيـه نـص يحـدد الجهـة المسؤولة [1].

أما المشرع الأردني أجاز في المادة (١٢/أ) لموظفي الضابطة العدلية بعد الحصول على إذن من المدعي العام المختص أو المحكمة المختصة الدخول إلى أي مكان تشير الدلائل إلى إستخدامه لإرتكاب أي من الجرائم المنصوص عليها في قانون جرائم أنظمة المعلومات رقم (٣٠) لسنة ٢٠١٠، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل إلى إستخدامها لإرتكاب أي من تلك الجرائم [2].

أما فيما يتعلق بموقف التشريع القطري بالجرائم المعلوماتية فقد تم إصدار قانون الجرائم الإلكترونية رقم (١٤) لسنة ٢٠١٤م متضمنا العديد من النصوص والإجراءات الهامة في مكافحة الجرائم التي تقع عبر شبكة الإنترنت مع بيان أوجه القصور من قبل الباحثين ومنها:

١. الدخول غير المشروع:

إن الدخول إلى الشبكة المعلوماتية يأتي في باديء الأمر بنشاط محسوس يتمثل في الضغط على أحرف لوحة المفاتيح أو أرقامها، وهذا التصرف ينتج عنه إحداث تصرفات مخالفة للقانون عن هذا السلوك أو النشاط، نتيجة تحويل تلك الحروف أو الأرقام إلى بيانات تعالج داخل النظام المعلوماتي ينتج عنه سلوك تقني ذا تأثير سلبي يسبب ضررا أو خسارة غير مشروعة للضحية في الجريمة المعلوماتية[3].

هنا نجد أن المشرع القطري قد جرم في المادة الثانية منه الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها، وتضاعف العقوبة في حال الدخول والحصول على معلومات تمس الأمن الداخلي أو الخارجي للدولة أو إقتصادها الوطني. وكذلك أيضا قد جرم في المادة الثالثة من ذات القانون بدون وجه حق بأي وسيلة على موقعا إلكترونيا أو نظاما معلوماتيا أو وسيلة تقنية معلومات أو جزء منها وترتب على الدخول حذف أو إلغاء أو إضافة أو إفشاء أو نقل أو إلتقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية ... إلخ.

---

[1] م/ لينا الأسدي- المرجع السابق- ص٦٧.

[2] أنظر المادة (١٢/أ) من قانون جرائم أنظمة المعلومات الأردني رقم (٣٠) لسنة ٢٠١٠

[3] د/ عبدالرازق سندالي- التشريع المغربي في الجرائم المعلوماتية، بحث مقدم إلى الندوة الإقليمية حول الجرائم المتعلقة بالكمبيوتر، المملكة المغربية، المنعقد في الفترة ١٩-٢٠/نيسان/٢٠٠٧، ص٦٩.

٢. جريمة التنصت وإلتقاط الرسائل الإلكترونية:

يدخل ضمن الجريمة المعلوماتية التقاط الرسائل الإلكترونية المرسلة بين الأشخاص على شبكة الويب العالمية مع توافر العلم والإرادة (القصد الجنائي بعنصريه) فإن مثل هذه الجريمة تتحقق[١].

فقد جاء نص المادة (٤) من قانون الجرائم الإلكترونية القطري حول تجريم إعتراض أو إلتقاط أو التنصت العمد دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات أو على بيانات المرور[٢]

ولهذا نعتقد بأن المشرع كان موفقا في هذه المادة بخصوص حماية الإتصالات من التنصت والمراسلات وبكافة الطرق والوسائل العادية والإلكترونية.

٣. التزوير المعلوماتي:

يقصد بالتزوير المعلوماتي هو الذي يرد على مخرجات الحاسب الآلي سواء كانت مخرجات مرسومة عن طريق الراسم أو ورقية مكتوبة كتلك التي تخرج عن طريق الطابعة [٣]. وفي إطار هذه الجريمة يدخل أيضا قيام الموظف بتغيير الحقيقة في البيان البنكي مثلا، أو إذا كان هنالك السلوك الإجرامي المتمثل بفعل الإستعمال ومحل هذا الإستعمال يرد على المحرر المزور[٤].

وهذا ما ذهب إليه المشرع القطري في تجريم التزوير الإلكتروني الذي يقع على محرر إلكتروني، حيث جاء في نص المادة [٥](١٠): تجريم التزوير إذا وقع على محرر إلكتروني غير رسمي وإستعمله مع علمه بتزويره.

٤. إنتحال الشخصية والإحتيال الإلكتروني:

غالبا ما تكون هذه الجريمة بصورة إستخدام هوية شخصية أخرى وبطريقة غير شرعية وذلك من أجل الإستفادة من هوية المجني عليه أو إخفاء هوية الجاني لتسهيل عملية إرتكاب الجريمة. كما تعدت الجرائم المعلوماتية إلحاق الأذى بالأشخاص إلى الإعتداء على الأموال أو الذمة المالية للغير، حيث يدخل في نطاقها

---

[١] م/ لينا الأسدي- المرجع السابق- ص٨٢.

[٢] أنظر المادة الرابعة من قانون الجرائم الإلكترونية القطري رقم (١٤) لسنة ٢٠١٤م.

[٣] د/ عبدالفتاح حجازي - الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية-المحلة الكبرى، مصر، ٢٠٠٥م

[٤] د/ عبدالفتاح حجازي- جرائم الكمبيوتر والإنترنت في التشريعات العربية، ط١، دار النهضة العربية- القاهرة، ٢٠٠٩م.

[٥] أنظر المادة العاشرة من قانون الجرائم الإلكترونية القطري رقم (١٤) لسنة ٢٠١٤م. والتي نصت على: تجريم التزوير إذا وقع على محرر إلكتروني غير رسمي وإستعمله مع علمه بتزويره.

كل حق ذي قيمة إقتصادية ويدخل في إطار التعامل. وبالتالي يكون أحد عناصر الذمة المالية للشخص[1].

لقد جرم المشرع القطري تلك الجريمة وأفرد لها عقوبة، كما جاء في الفقرة الأولى من المادة (١١) من قانون الجرائم الإلكترونية وعلى النحو التالي: يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات وبالغرامة التي لا تزيد عن (١٠٠,٠٠٠) ريال أو بإحدى هاتين العقوبتين في حال[2]:

أ. إستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في إنتحال هوية شخص طبيعي أو معنوي.

ب. تمكن عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات من الإستيلاء لنفسه أو لغيره على مال منقول، أو على سند أو التوقيع عليه بطريق الإحتيال، أو بإتخاذ إسم كاذب، أو بإنتحال صفة غير صحيحة (م١١/٢).

- العقاب بالحبس مدة لا تتجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٢٠٠,٠٠٠) ريال أو بإحدى هاتين العقوبتين كل من إرتكب أي فعل يتعلق بجرائم بطاقة التعامل الإلكتروني كما جاء في المادة (م١٢/فقرة١-٥).
- تجريم التعدي على حقوق الملكية الفكرية بأي وسيلة وفي أي صورة على حقوق المؤلف أو الحقوق المجاورة... إلخ المحمية وفقا للقانون المادة (م١٣).

وفي موضوع الجريمة الإرهابية من خلال الشبكة المعلوماتية، فقد أشار إليها القانون في المادة الخامسة منه والتي جاء فيها: كل من أنشأ أو أدار موقعا لجماعة أو تنظيم إرهابي على الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو سهل الإتصال بقيادات تلك الجماعات أو أي من أعضائها، أو الترويج لأفكارها، أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أي أداة تستخدم في الأعمال الإرهابية، يعاقب بالحبس مدة لا تزيد عن ثلاث سنوات وبالغرامة التي لا تزيد على (٥٠٠,٠٠٠) ريال.

أما موقف التشريع القطري فيما يتعلق بالتفتيش في الجرائم الإلكترونية فقد حدد في الباب الثالث من قانون مكافحة الجرائم الإلكترونية الأدلة وإجراءات التحقيق ضمن المواد من (١٤-٢٠).

وبموجب نصوص المواد (١٤-٢٠) من قانون مكافحة الجرائم الإلكترونية القطري رقم (١٤) لسنة ٢٠١٤ فإننا نلاحظ أنه في المادة (١٤) قد أجاز للنيابة العامة أو من تندبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن وأنظمة المعلومات ذات الصلة بالجريمة[3] .

---

[1] د/ محمد الشوا- الجريمة المنظمة وصداها على الأنظمة العقابية، دار النهضة العربية-القاهرة، ١٩٩٨م.

[2] أنظر المادة (١١) الفقرة١ و٢، والمادة (١٢ و١٣) من قانون الجرائم الإلكترونية القطري رقم (١٤) لسنة ٢٠١٤م.

[3] أنظر المادة (١٤) من قانون مكافحة الجرائم الإلكترونية القطري رقم (١٤) لسنة ٢٠١٤م.

كما أن المشرع أوجب أن يكون أمر التفتيش مسبباً ومحدداً، وأجاز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة. وإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي عرضها على النيابة العامة لاتخاذ ما يلزم بشأنها.

التفتيش بصورة عامة يعتبر من أخطر الحقوق التي منحت للمحقق وذلك لمساسها بالحريات التي تكفلتها الدساتير، لذا نجد أن المشرع يضع لها ضوابط عديدة فيما يتعلق بالجهة التي تباشره أو تأذن بمباشرته والأحوال التي تجوز فيها مباشرته بما يضمن الحرية الفردية أو حرمة المسكن[١].

فالشخص المراد تفتيشه لا بد أن يكون هناك مجموعة من المظاهر أو الأمور المعينة التي تؤدي إلى الإعتقاد بأنه قد إرتكب أو ساهم بإرتكاب الجريمة المعلوماتية [٢].

وبما أننا في نطاق تفتيش مسرح الجريمة الإلكترونية، فلا بد من التطرق إلى مكونات البنية التحتية لتقنية المعلومات بناء على طبيعة عملها والتقنيات المستخدمة بها كما أشار إليها[٣].

١. منظومة أجهزة الحواسيب: وهي منظومة تتعلق بالأجهزة التي لها خاصية معالجة البيانات (المحوسبة) من حيث إمكانية إستقبالها للبيانات (المدخلات) ومعالجتها، ومن ثم إخراجها وما يتبع هذه الأجهزة من ملحقات.
٢. منظومة أنظمة التشغيل: عبارة عن أنظمة برمجية مطورة خصيصا لكي تقوم بمهام تشغيل وتسهيل إستخدام مكونات التقنية والتي تسمى (أنظمة التشغيل).
٣. منظومة التطبيقات البرمجية: برمجيات متخصصة في أداء المهام التي يرغب المستخدم في تنفيذها من خلال أجهزة الحواسيب.
٤. إدارة البيانات وتخزينها: هي عملية التحكم المنظمة والمباشرة للبيانات إبتداء من تحصيلها وإدخالها مرورا بمعالجتها ومن ثم إخراجها وتخزينها.
٥. منظومة الشبكات والإتصالات: منظومة معنية بكل ما له علاقة مباشرة بعمل الشبكات والإتصالات وتشمل الأجهزة والمعدات والبرامج المعنية بتوفير تراسل البيانات ووصولها إلى أماكن بعيدة وتوفير الوصول إلى المعلومة من أي مكان وفي أي زمان.

---

[١] القاضي عبود صالح التميمي- التحقيق الجنائي العملي، ط١، بغداد، ٢٠٠٦.

[٢] د/ خالد إبراهيم- فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار الفكر الجامعي- الإسكندرية، ٢٠٠٩م.

[٣] Ken Laudon and Jane Laudon ،Management Information Systems (١١th Edition), Prentice Hall, ٢٠٠٩.

٦. منظومة الإنترنت: منظومة متكاملة تشتمل على البرامج التطبيقية الخاصة بالإنترنت مثل المتصفحات والأجهزة اللازمة لترابط الحواسيب مع بعضها البعض للوصول إلى بينات مخزنة في أماكن محددة.

لقد أشار في المادة الرابعة من قانون مكافحة الجرائم الإلكتروني إلى أنه: يجب إتباع إجراءات التفتيش المنصوص عليها في قانون مكافحة الجريمة الإلكترونية في حال أسفر عن التفتيش ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة يتعين ضبطها وعرضها على النيابة العامة لإتخاذ ما يلزم بشأنها.

ويكون هدف إجراء التفتيش في الجرائم الإلكترونية هو البحث عن حقيقة الجاني، والأدوات والأجهزة التي تم إستخدامها في الجريمة. وفقا لأحكام تفتيش الأشخاص والأماكن وأنظمة المعلومات ذات الصلة بالجريمة.

ونصت المادة (١٥) على أنه لا يجوز استبعاد أي دليل ناتج عن وسيلة من وسائل تقنية المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية بسبب طبيعة ذلك الدليل[١].

كما أنه لا يجوز استبعاد أي من الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، لمجرد ذلك السبب، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي. وهذا ما أكدته المادة (١٦) من ذات القانون.

ولهذا فإنه يتعين على المحقق إتباع ضوابط معينة، تتمثل في وجود جريمة قد تم إقترافها من قبل شخص أو أشخاص معينين بإرتكاب جريمة معلوماتية أو بالإشتراك فيها، بإستخدام الحاسب الآلي كأداة، سواء كانت تلك الجريمة جناية أو جنحة [٢].

كما يجب أن يتضمن إذن التفتيش الإجازة بالبحث عن كيان البرنامج وأنظمة تشغيله والسجلات التي تثبت إستخدام الأنظمة الآلية لمعالجة البيانات والسجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات [٣].

وفيما يخص الإذن بتفتيش البيانات أو المعلومات الإلكترونية فجاءت المادة (١٧) تبين الإذن للسلطة المختصة من خلال النيابة العامة أن تأمر بالجمع والتسجيل الفوري لأية بيانات أو معلومات إلكترونية أو بيانات مرور أو معلومات المحتوى التي تراها لازمة لمصلحة التحقيقات.

---

[١] أنظر المادة (٤) و المادة (١٥) من قانون مكافحة الجرائم الإلكترونية القطري رقم (١٤) لسنة ٢٠١٤م.

[٢] د/ محمد البشري- التحقيق في الجرائم المستحدثة، ط١، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٤م.

[٣] م/ لينا الأسدي-مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية: دراسة مقارنة، ط١، دار الحامد للنشر والتوزيع، عمان-الاردن، ٢٠١٥م.

كما أعطى المشرع القطري للنيابة العامة في المادة (١٨) من خلال السلطة المختصة أن تأمر كل ذي صلة بتسليم الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو معلومات المحتوى ذات الصلة بموضوع الجريمة أو ما يفيد في كشف الحقيقة. وكذلك للنيابة العامة أنت تأمر بالتحفظ على الأجهزة أو الأدوات أو الوسائل المستخدمة في ارتكاب الجريمة.

وفي المادة (١٩) أعطى المشرع القطري الجهة المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على الأجهزة أو الأدوات أو وسائل تقنية المعلومات، أو الأنظمة المعلوماتية أو البيانات أو المعلومات الإلكترونية محل التحفظ، لحين صدور قرار من الجهات القضائية المعنية بشأنه [١].

وفيما يتعلق بمعاينة مسرح الجريمة فإننا نجد المشرع القطري قد أورد في نص المادتين (٣١ و ٣٤) من قانون (الإجراءات الجنائية القطري رقم ٢٤ لسنة ٢٠٠٩) على إجراء المعاينة ضمن أعمال التحقيق الجنائي، حيث جاء في نص المادة (٣٤): "لمأمور الضبط القضائي أثناء جمع الإستدلالات أن يجروا المعاينة اللازمة"، كما جاء في نص المادة (٣١) من ذات القانون يجب على مأموري الضبط القضائي أن يحصلوا على جميع الإيضاحات اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم، أو التي يعلمون بها بأي كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة [٢].

وعليه وبمقتضى نص المادتين يظهر لنا أن هناك سلطة تقديرية للمحقق في إجراء المعاينة، فيجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة، وبالتالي ليس هناك أي إلتزام على المحقق فيما يتعلق بحضور معاينة مسرح الجريمة من قبل أي طرف من أطراف الدعوى أو وكلائهم خصوصا في الجرائم الإلكترونية، وذلك للحفاظ على مسرح الجريمة بما يحتويه من آثار مادية وأدوات ومظاهر خارجية ملموسة.

معاينة مسرح الجريمة الإلكتروني تعد من المسائل الجديدة لأن الإنتقال هنا لا يكون بالضرورة عبر العالم المادي وإنما من خلال طرق الشبكة المعلوماتية، حيث يستطيع المحقق أو مأمور الضبط القضائي أن ينتقل إلى الفضاء الإلكتروني عن طريق مقر عمل مزود بخدمة الإنترنت والذي يعتبر أفضل مكان لإجراء المعاينة من خلال مقر مكتب الخبير التقني المختص [٣].

من خلال إستعراض نصوص القانون المتعلق بالجرائم الإلكترونية القطري لاحظ الباحثان أنه لا يوجد في التشريع القطري نصوص قانونيه خاصة بجرائم الإرهاب الإلكتروني،أيضا أن هذا القانون لم تتضمن نصوصه كيفية إجراء التفتيش

---

[١] أنظر المواد (١٧، ١٨، ١٩) من قانون مكافحة الجرائم الإلكترونية القطري رقم (١٤) لسنة ٢٠١٤م.

[٢] أنظر المواد (٣١، ٣٤) من قانون الإجراءات الجنائية القطري رقم ٢٤ لسنة ٢٠٠٩.

[٣] د/ خالد إبراهيم- فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار الفكر الجامعي- الإسكندرية، ٢٠٠٩م.

والمعاينة المتعلقة بالجريمة الإلكترونية. كما أنه خلت النصوص القانونية في التشريع القطري من تعريف الإرهاب الإلكتروني.

إلا أنه حسنا فعل المشرع القطري بإصدار القانون رقم (١٤) لسنة ٢٠١٤م لمكافحة الجرائم الإلكترونية. والذي وضح فيه الجرائم التي ترتبط بتقنية المعلومات، كما أنه أيضا أشار في بعض نصوص المواد إلى الإجراءات الجنائية المتعلقة بالتفتيش والمعاينة، وقد تضمن القانون النص على الجرائم المستحدثة عبر النظم المعلوماتية لم تكن مجرمة من قبل وكانت تترك لتقدير سلطة قاضي الموضوع.

وأخيرا يجد الباحثان أن هذا القانون يجب الإستفادة من نصوصه في وضع نصوص أخرى تتعلق بالإرهاب الإلكتروني تهدف إلى مكافحة تلك النوعية من الجرائم.

الخاتمة

إن الإرهاب الإلكتروني من أهم المخاطر التي تواجه دول العالم في المرحلة الحالية، ولما تتيحه الشبكة العنكبوتية من مكنات واسعة سهلت للإرهابيين تواصلهم مع بعضهم البعض، وهذا بدوره صعب من إمكانية كشف الأنشطة الإرهابية وتعقب مرتكبيها والمتدخلين والمحرضين فيها. وبالرغم من الجهود الكبيرة التي تبذل للتصدي لهذه الظاهرة إلا أنها ما زالت دون الطموح المنشود.نظرا لتسارع وتيرته يوما بعد يوم.

أما فيما يتعلق بإجراءات البحث والتحري المتمثلة بمعاينة وتفتيش مسرح الجريمة بهدف إستجلاء حقيقة الجريمة وبصفة خاصة في جرائم الإرهاب الإلكتروني تنطوي على قدر عال من الدقة الفنية بما فيها من تحديات لسلطة التحقيق أثناء جمع الأدلة من مسرح الجريمة بالطرق التقنية.

من خلال المتابعة المتأنية لهذا الموضوع الذي تناول تحديات البحث والتحقيق الجنائي في مسرح الجريمة الإلكترونيوالدراسة العلمية الدقيقة ، فقد توصلنا لجملة من النتائج نجملها في النقاط التالية:

- الإرهاب الإلكتروني هو إستخدام التقنيات الرقمية لممارسة أنشطة إرهابية ضد الأفراد أو الدول لتحقيق أهداف إرهابية لجماعات أو تنظيمات إرهابية على إختلاف الدوافع سواء كانت سياسية أو دينية أو عرقية.
- قصور في التشريع فيما يخص بالنص صراحة على تجريم الإرهاب الإلكتروني بإستخدام التقنيات العلمية الحديثة للإضرار بأمن الدولة الداخلي والخارجي.
- لم يرد نص واضح وصريح في كيفية إجراء معاينة وتفتيش مسرح الجريمة الإلكترونية.
- أن هناك ضعف في الخبرة لدى رجال الضابطة العدلية في إستخدام التقنيات والتعامل مع الأدلة من حيث معاينتها والتفتيش عنها في مسرح الجريمة الإلكتروني.
- صعوبة التوصل إلى الأدلة الرقمية والتحفظ عليها.

التوصيات:

- **إعداد وتدريب العاملين في مجال البحث والتحقيق على كيفية التعامل مع مسرح الجريمة الإلكتروني.**
- **الإستفادة من التقنيات الحديثة في متابعة الإنترنت وبخاصة في مجال مكافحة الإرهاب الإلكتروني.**
- **إصدار قانون يتعلق بجرائم الإرهاب الإلكتروني على أن يشمل جرائم الإنترنت بشقيها الموضوعي بحيث يجرم الأفعال غير المشروعة ويعاقب مرتكبها، والإجرائي يوضح إجراءات تفتيش الحاسب وضبط المعلومات التي يحويها ومراقبة المعلومات أثناء إنتقالها والسماح للجهات القائمة على التفتيش ضبط برامج الحاسب والمعلومات الموجودة بالبرامج.**
- **توسيع سلطات الجهات المعنية بإجراء التفتيش في مسرح الجريمة الإلكتروني دون الحصول على إذن عند الضرورة ، إذا كان من شأن الإنتظار ضياع الدليل.**
- **التنسيق وتبادل المعلومات والخبرات مع الأجهزة الأمنية المعنية بمكافحة الإرهاب الإلكتروني على المستوى الدولي.**
- **نشر الوعي العام من خلال وسائل الإعلام المختلفة بجرائم الكمبيوتر، والعقوبات المترتبة عليها.**
- **إستحداث إدارات أمنية متخصصة بجرائم الإرهاب الإلكتروني تتبع لوزارة الداخلية، تعمل على التنسيق والتعاون بين الدول للوقاية من هذه الجريمة.**
- **إجراء دراسات أخرى تبحث في التحديات التي تواجه المحققين الجنائيين في مسرح الجريمة الإلكتروني تشمل مثلا: تحديد هوية الجاني، ضبط وتحريز الأدلة الرقمية، إستجواب ومناقشة الشهود.**