جامعة نايف العربية للعلوم الأمنية
المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي
www.nauss.edu.sa
http://ajfsfm.nauss.edu.sa

مقال أصلي

إجراءات البحث والتحقيق في جرائم الإرهاب الإلكتروني وتحدياتها (دراسة في النظام السعودي)

نهاد فاروق عباس*

كلية العدالة الجنائية جامعة نايف العربية للعلوم الأمنية

ص.ب: 6830، الرياض 11452، المملكة العربية السعودية

الوصول الحر

المستخلص

يشكل التقدم السريع في تقنية المعلومات عصب تطوير نظم الحياة وبناء المجتمع المعلوماتي، ويزداد الاهتمام به في العصر الحاضر نظراً لاتساع نطاق استخدام تقنية المعلومات في أغلب مناحي الحياة، وإزاء هذا التطور فإنه يفتح مجالاً جديداً للجريمة ومسرحاً من أخطر مسارح الجريمة وأدقها وأكثرها تعقيداً، بخلاف ما كان عليه الحال في الجريمة التقليدية من جميع الجهات سواء على الصعيد الأمني، أو الجغرافي الواسع واللامحدود.

وعليه تظهر أمام الجهات القضائية المختصة في الدولة مجموعة من التحديات والمخاطر تعرقل عملها، وتؤثر على قدرتها الفنية في القيام بالمهام المنوطة بها بصفة خاصة في مرحلتي البحث والتحقيق، لما تنطوي عليه كل مرحلة من إجراءات فنية دقيقة مفيدة في كشف حقيقة الجريمة تطلب جهداً مضاعفاً في حالة الجريمة الإلكترونية لما فيها من خصائص فنية أدق وأصعب، وهذا يتطلب توافر خبرة متميزة في هذا المجال بخلاف ما تتولى القيام به جهة البحث أو التحقيق، ما يستدعي معرفتهم بتلك التقنية حتى تستطيع كل جهة إنجاز مهامها النظامية المنوطة بها بنص النظام للوقوف على حقيقة الجريمة والتوصل إلى الجاني الحقيقي في الجريمة، وذلك لا يتأتى إلا عن طريق ندب أحد الخبراء المسجلين لدى المحاكم وحضوره لجميع إجراءات البحث والتحقيق لتسهيل الوصول إلى دليل دقيق ومحاكمة عادلة.

الكلمات المفتاحية: إجراءات البحث والتحقيق، الجرائم الإلكترونية، الإرهاب الإلكتروني، أمن المعلومات، الأدلة الجنائية.

Investigation Procedures in Terrorist Electronic Crimes and it's Challenges: A study in the Saudi legal system

Nehad Farouk Abbas Mohamed

College of Criminal Justice, Naif Arab University of Security Science, Riyadh, Kingdom of Saudi Arabia

Rapid advances in information technology (IT) form the backbone of the development of everyday life and a knowledge based society. At present, there is more and more attention being paid to IT because of its extensive use in all spheres of life. Due to this massive cyber development, new type of crimes with complex and multifaceted nature have evolved. This is in contrast to traditional crimes from all angles,

* Corresponding author: Nehad Farouk Abbas Mohamed
Email: nehadfarouk2008@yahoo.com

doi: 10.12816/0011262

الإصدار والاستضافة ـ جامعة نايف العربية للعلوم الأمنية

whether security or geographical based. Due to this, a number of challenges and dangers or threatening specialist judicial authorities and hamper their work and technical abilities in performing the tasks entrusted to them, particularly in crime investigation and prosecution.

Because of the complex nature and detailed technical procedures applied at each stage of crime investigation, much greater efforts are required to reveal the hidden realities of an electronic crime. Therefore, investigation authorities, judiciary and other relevant bodies require an uptodate knowledge of new technologies to be able to perform their allocated tasks precisely according to defined rules and regulations, and identify the perpetrator correcly.

Key words: Information technology, Crime investigation, Electronic crimes, Terrorism, Saudi legal system

مقدمة

تعد الجريمة التقليدية النموذج الطبيعي لتطبيق قواعد ونصوص الأنظمة والتشريعات، بالإضافة إلى أنها قد تحدث بعض الخلاف في تطبيق بعض قواعد الأنظمة الشكلية أو الإجرائية كنظام الإجراءات الجزائية فما بالنا والجريمة الإلكترونية نموذج مختلف نوعاً ما في مجال تطبيق القواعد الإجرائية من عدد من النواحي الإجرائية لما فيها من مخاطر محو أو إفساد الدليل، وبصفة خاصة أن الدليل فيها دليل رقمي له مسرح مختلف يعرض فيه، ويحتاج إلى خبرة فنية عالية من الخبير المطلع عليه، وبخاصة في جرائم الإرهاب التي غالباً ما تكون مشفرة، أو يعبرون عنها بعبارات ويستخدمون فيها أدوات غير معلومة غالباً، أو غير مفهومة للشخص العادي، وعليه فإن إجراءات البحث والتحقيق في مثل هذه الجرائم تعترضها تحديات عدة منها الأمنية ومنها الفنية، ومنها صفة المتضرر من الجريمة، وبصفة خاصة في الجرائم الإرهابية سواء كان من الداخل أو من الخارج .

وعليه يثار التساؤل الرئيسي وهو: ما هي مخاطر وتحديات إجراءات البحث والتحقيق في جرائم الإرهاب الإلكتروني؟

مفاهيم ومصطلحات الدراسة

إجراءات البحث: هي مجموعة الإجراءات القانونية التي يباشرها مأمورو الضبط الجنائي، وتكون سابقة لارتكاب الجريمة أو معاصرة أو لاحقة [1].

التحقيق: هو مجموعة إجراءات تهدف إلى البحث عن حقيقة الجريمة وتحديد شخصية مرتكبها [2].

الجرائم: الجريمة هي كل فعل أو ترك ضار، له مظهر خارجي، ليس استعمالاً لحق ولا قياماً بواجب، يحرمه القانون ويفرض له عقاباً، يؤديه إنسان أهل لتحمل المسئولية الجنائية [3].

الإرهاب: ورد في القرار الصادر عن مجمع الفقه الإسلامي الدولي في دورته الرابعة عشرة المعقودة في الدوحة في شهر كانون الثاني من العام 2003 م بشأن حقوق الإنسان والعنف الدولي أن الإرهاب يعني: العدوان أو التخويف أو التهديد المادي المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض [4].

التحديات: تلك الصعوبات التي تواجه كشف حقيقة الجريمة، ومنها:

- صعوبة العلم بوقوع الجريمة.
- صعوبة تعيين الجاني.
- صعوبة القبض على الجاني.
- التطور الإلكتروني السريع والمضطرد.

مخاطر وتحديات إجراءات البحث والتحقيق في جرائم الإرهاب الالكتروني

قبول البلاغ

من أعمال الاستدلال التي نص عليها نظام الإجراءات الجزائية السعودي ما ورد بنص المادة السابعة والعشرين من نظام الإجراءات الجزائية السعودي الصادر في 22/1/1435هـ؛ حيث حدد فيها أعمال الاستدلال التي يحق لرجل الضبط الجنائي القيام بها. وقد بدأ النص بـ (على) مما يظهر منه أنه واجب لا يجوز لمأمور الضبط الجنائي التخلي عنه، أو الامتناع عن القيام به؛ حيث إنه من أولى الاختصاصات القانونية الملقاة على عاتقه تقبل البلاغات والشكاوى، وفي كل الجرائم التي تمس الحق الخاص ولم يتوصل إليها والعلم بها، والحاجة لتدخل السلطة المختصة لا يصح قيام مأمور الضبط الجنائي بأي من الإجراءات الجنائية المنوط به القيام بها من خلال نص النظام فيما عدا حالات التلبس.

ويجب على رجل الضبط الجنائي قبول ما يصله أو يوجه إليه من بلاغ بخصوص الجرائم التي نص عليها النظام، وأن يبعث بها فوراً إلى سلطة الاتهام، وإن لم يفعل ما يمليه عليه واجبه، أو رفض قبول البلاغ،

وجب مساءلته تأديبياً من ذوي الاختصاص [4].

تحديات البلاغ

وفي مجال الجرائم عبر الفضاء الإلكتروني يكون القيام بالجريمة عبر التقنيات الحديثة؛ حيث يستخدم البريد الإلكتروني تلك الخدمة التي تسمح بتبادل الرسائل والمعلومات مع الآخرين عبر الإنترنت، وتعد هذه الخدمة من أبرز الخدمات التي تقدمها شبكة الإنترنت، لما تمثله من سرعة في إيصال الرسالة وسهولة الاطلاع عليها في أي مكان، فلا ترتبط الرسالة الإلكترونية المرسلة بمكان معين، بل يمكن الاطلاع عليها وقراءتها في أي مكان من العالم، وعلى الرغم من أن البريد الإلكتروني أصبح أكثر الوسائل استخداماً في مختلف القطاعات، وخاصة قطاع الأعمال لكونه أكثر سهولة وأمناً وسرعة لإيصال الرسائل إلا أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني من خلال استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيراً من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني ووسائل التواصل الاجتماعي الحديثة فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها، وكذلك يقوم الإرهابيون باستغلال هذا الفضاء التقني في نشر أفكارهم والترويج لها والسعي لتوسعة الرقعة الجغرافية للأتباع والمتعاطفين معهم عبر المراسلات الإلكترونية، ومما يقوم الإرهابيون به أيضاً اختراق البريد الإلكتروني للآخرين وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية [5]، فلا نرى مانعاً من تلقي البلاغ عبر البريد الإلكتروني كذلك.

ومع ذلك فإنه في مجال الجرائم الإرهابية بصفة عامة لا يشترط وجود البلاغ أو الشكوى من صاحب الشأن ولا يتوقف عمل السلطة المختصة على وجوده لما ورد بنص المادة الخامسة عشرة من نظام مكافحة الإرهاب الصادر في 24/2/1435هـ، فقد يحجم البعض عن التبليغ نظراً لعدم إدراكهم خطورة الجريمة على هذا الشكل [6].

ورغم أنه قد استقر نظام مكافحة جرائم المعلوماتية، بالمرسوم الملكي رقم: م/17 وتاريخ: 8/3/1428 هـ، والذي يهدف إلى الحد من نشوء جرائم المعلوماتية وذلك بتحديد تلك الجرائم والعقوبات المقررة لها، إلا أنه من التحديات التي تقابل الجريمة الإرهابية عبر الفضاء الإلكتروني صعوبة العلم ببداية بالجريمة، فقد لا يتوافر العلم بوقوعها حتى بالنسبة للمجني عليه لكي يستطيع تقديم البلاغ للسلطة المختصة.

كما أن هيئة الاتصالات وتقنية المعلومات مسئولة عن تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها، وكذلك أثناء المحاكمة، وذلك نص المادة الرابعة عشرة من نظام مكافحة الجرائم المعلوماتية. وقد يضبط المجرم بالجرم المشهود، ويمكن اكتشافها من طرف مديري النظام [6]، ومن خلال تقدم المدعي إلى مركز الشرطة المختص مع ما يثبت دعواه من أدلة وقرائن وإثباتات وتحديد الوسيلة التي استخدمت في ارتكاب الجريمة التي تضرّر من جرائها سواءً أكانت من خلال تغريدة عبر أحد مواقع التواصل الاجتماعي، أو مقال في موقع ما أو غير ذلك، ولا يمنع من أن يصطحب المدعي في بعض الأحيان جهاز الحاسب الآلي الخاص به حال ارتباطه بالجريمة التي ارتكبت طالباً من رجل الضبط الجنائي ضبط ما فيه وإثباته في محضر إثبات البلاغ كإجراء من إجراءات الاستدلال، مع الإدلاء بمعلومات وافية عن حال المتهم من حيث كونه معروفاً لديه كاسمه وعمره وعنوانه وصلته به أو غير معروف لديه، ليتمكن رجل الضبط الجنائي من خلالها من طلب حضوره وسماع أقواله حيال التهمة المنسوبة إليه، وضبط محل الجريمة وجميع ما له علاقة بها، تمهيداً لبعثها إلى هيئة الاتصالات وتقنية المعلومات التي تتولى وفقاً لاختصاصها واستناداً للمادة الرابعة عشرة من نظام مكافحة جرائم المعلوماتية، والتي بدورها تقوم بإعداد تقرير فني حيال ما رفع لها وتحيله إلى الجهة المختصة.

وإذا كان المتهم مجهول الهوية وغير معروف للمدعي، فإن جهة الضبط الجنائي ممثلة في الشرطة تقوم بمخاطبة هيئة الاتصالات وتقنية المعلومات لإكمال اللازم حيال ذلك، ولما لها من خبرات فنية تمكنها من التعرف على مرتكب الجريمة وجمع أكبر قدر من المعلومات عنه التي بناءً عليها يقوم مأمور الضبط الجنائي بالبحث عن المتهم والقبض عليه وضبط كل ما له علاقة بالجريمة المرتكبة كجهاز الحاسب الخاص به ونحو ذلك، وكافة الأدلة والقرائن الرقمية التي تفيد القضية محل البحث، ثم سماع أقوال المتهم، فالإحالة إلى هيئة التحقيق والادعاء العام لمباشرة دراسة كافة أوراق القضية للوقوف على مدى تشكيلها جريمة من عدمه وفي حال كونها تشكل جريمة داخلة في اختصاصها المكاني والنوعي فإنها تباشر إجراءات التحقيق مع المتهم من استجواب ومواجهة ونحوهما وفقاً للتهمة المنسوبة إليه؛ حيث لكل جريمة هيئة إجرامية ومسار تخصص فني أو تقني يحتاج إلى فريق على دراية بخباياها [7].

ونظراً لما لتمويل الإرهاب من خطورة إجرامية أولى بالاهتمام عن فعل الإرهاب ذاته؛ حيث إنه إذا لم يجد الإرهاب من يموله فلا إرهاب نص النظام بموجب نص المادة الرابعة والثلاثين على أنه (تقوم لجنة طلبات المساعدة القانونية المتبادلة في وزارة الداخلية بتلقي طلبات المساعدة القانونية المتبادلة المتعلقة بجرائم تمويل الإرهاب).

ولمزيد من سبل المكافحة والتتبع الدقيق ولمواجهة تحديات الجريمة الإرهابية الإلكترونية نص على تولي أمر البلاغات والتحريات المالية لوحدة التحريات المالية في وزارة الداخلية بموجب نص المادة الخامسة

والثلاثين من نظام مكافحة الإرهاب ولها تبادل المعلومات مع الجهات النظيرة وفقاً لأحكام المادة الخامسة والعشرين من نظام مكافحة غسل الأموال.

المعاينة

المعاينة أحد إجراءات التحقيق الابتدائي التي يعتمد عليها في البدء بالتحقيق مع المتهم في جريمة ما، ولا يختلف الأمر على اعتبار المعاينة محل الدراسة تناقش المعاينة في جريمة إلكترونية، فبطبيعتها كإجراء لا تختلف من الجريمة التقليدية للجريمة الإلكترونية، كما سنرى رغم الاختلاف الذي سيظهر في المحتوى الفني للمسرح الإلكتروني [6].

والجدير بالذكر أن النص على إجراء المعاينة ورد بنظام الإجراءات الجزائية السعودي الجديد الصادر في 2/ 1435 هـ ضمن أعمال التحقيق بموجب نص المادة التاسعة والسبعين. وعليه وبمقتضى النص يظهر لنا أن هناك سلطة تقديرية للمحقق في القيام بإجراء المعاينة لما ورد بالنص السالف ذكره عند الاقتضاء فيجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة، وليس هناك أي التزام آخر على المحقق في إجراء المعاينة في حضور أي من أطراف الدعوى أو وكلائهم [8]. وبصفة خاصة في الجرائم الإلكترونية؛ حيث تظهر أهمية المعاينة فور وقوع جريمة من الجرائم التقليدية؛ لوجود مسرح في مكان مادي ظاهر يحتوي على آثار مادية واقعية مترجمة إلى أحداث وأدوات ومظاهر خارجية ملموسة واضحة، ويهدف القائم بالمعاينة إلى التحفظ عليها تمهيداً لفحصها لبيان مدى صحتها فقط [9].

أما في الجرائم الإلكترونية وبصفة خاصة الإرهابية؛ فنادراً ما يتخلف عن ارتكابها آثار مادية، وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، ما يعرض هذه الآثار للمحو أو التلف؛ لذا ينبغي العمل على إتمام المعاينة على وجه السرعة حتى لا تعطى الفرصة لأن تمتد يد العبث لأي من الأدلة قبل معاينتها وضبطها.

محل المعاينة موضوعياً

بشكل موضوعي تكون المعاينة للآثار التي يتركها مستخدم الإنترنت، وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الجهاز المستخدم والبيانات المحفوظة فيه أيّاً كان نوع الجهاز، أو حجمه [10].

تحديات المعاينة

يتمثل التحدي الأول في أن الدليل محل المعاينة، والمسرح محل المعاينة بصفة عامة من الطبيعة الرقمية التي تحتاج لذاتها لمن كان لديه من الخبرة الفنية في الضبط والإثبات لمثل هذه الرقميات الفنية الدقيقة فإن كان هناك تصوير لمسرح الجريمة في الجريمة التقليدية فالتحدي هنا أن التصوير للجهاز الذي من خلاله تمت ممارسة السلوك المادي المرتب للنتيجة، وكذلك كل ما يتصل بالجهاز من ملحقات وأجهزة أخرى [11].

والتحدي الآخر في هذا تسجيل التاريخ والوقت، وهذا في حد ذاته من المخاطر؛ حيث إنه قد يكون الجهاز مضبوطاً بتوقيت مختلف يظهر على الصورة فقط، والكاميرا بها توقيت مخالف وهو ما يحتاج أيضاً إلى الخبير الفني فيما بعد لمحاولة المقابلة بينهما بفحص الجهاز والتأكد من ذلك، كلها مخاطر وتحديات تقابل المحقق في إجراء المعاينة.

والتحدي الثالث بيان مكان التصوير؛ حيث المكان المفترض مكان وجود الجهاز وما بالجهاز من صور ورسائل فالجهاز هو مكان وجودها الذي يثبت بالمحضر، ومكان وجود الجهاز هو مكان الجاني الذي قد يتصل منه وقت المعاينة [11].

والتحدي الرابع وهو طريقة إعداد نظام الجهاز، فهذا التحدي فيه من المخاطر الفنية على سير القضية؛ لما في طريقة الإعداد من آثار على الإثبات من حيث المحتوى وطريقة الكتابة، وإعداد البرامج، ما يحتاج إلى ندب الخبير الفني المختص للعناية بدقة ملاحظة لما بالجهاز من أمور فنية ودقيقة تحتاج إليها عملية المعاينة، وكذلك حالة التوصيلات وقت المعاينة، والكابلات المتصلة بالجهاز محل المعاينة [12].

والتحدي الخامس وجود مكونات تقنية تعمل على توفير خطر جسيم على المعلومات يتحقق بوجود مجال مغناطيسي يستخدم في محو البيانات، وهو من الأمور الفنية البحتة التي تحتاج إلى الفحص التقني الدقيق لتفادي مخاطر المحو.

والتحدي السادس هو احتمال أن يكون الجاني وخوفاً من اكتشافه قام بمحو البيانات من الملفات ولم يتمكن من محوها من سلة المهملات؛ فهنا وجب التحفظ على ما بسلة المهملات وتصوير المحتوى من شاشة الجهاز لبيان كونها محتوى سلة المهملات وإثبات ذلك رقمياً، كما أن هناك تقنيات حالياً تعمل على استرجاع البيانات حتى بعد محوها من الملفات لتفادي مخاطر المحو [11].

وأخيراً تتضمن المعاينة كل الأقراص المغنطة الموجودة بالمكان المستعملة أو غيرها للحصول على البصمات على الأقل، وكل أوراق سواء مكتوب عليها أم لا فقد تكون مما قام الجاني بالتسجيل عليها أو على غيرها بالغلط، وكل موجودات من أوراق كربون، أو أقراص من أي نوع [13].

تحديات جغرافية

يعد مسرح الجريمة هو النطاق الجغرافي للجريمة؛ لذا فإنه بموجب نص المادة الثالثة من نظام مكافحة الإرهاب السعودي يتضح أن مجال

الجريمة الإرهابية بصفة خاصة يخضع لمبدأ العينية الذي ينظر إلى عين الجريمة بغض النظر عن شخص ومكان وقوعها ما يعمل على اتساع المجال الجغرافي لها. وعليه يشمل مسرح الجريمة كل شيء أو محل أو وحدة من منشأة أو رقعة من الأرض تتضمن أي من أدوات، أو وسائل، أو بيانات تتعلق بالجريمة [10]، كما تشمل المعاينة أي مكان سواء كان عاماً أو خاصاً.

تحديات نوعية

نصت المادة الخامسة عشرة من نظام مكافحة الجرائم المعلوماتية السعودي على أنه (تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام)، ومن جانب آخر أكدت المادة الرابعة عشرة من نظام مكافحة الإرهاب 1435هـ على اختصاص رجال الضبط الجنائي بأعمالهم الأصلية المنصوص عليها، وكذلك جهة التحقيق المختصة، كما أكدته المادة الأربعون من نظام مكافحة الإرهاب.

وعليه من وجهة نظرنا ينبغي قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات؛ إلا أن ذلك لا يمنع نظراً لانشغال المحقق ببعض الأمور الفنية الأخرى في القضية أن يقوم المحقق بإجراء المعاينة بنفسه أو أن يندب أحد رجال الضبط الجنائي.

كما أنه حتى يمكن حصر الأدلة ونقلها بصفة خاصة وأنها أدلة رقمية وفنية، وغيرها، فإنه يتوجب على المحقق البدء بالمعاينة فور وصوله إلى المكان محل المعاينة، حتى لا يدع فرصة للعبث بالمحتوى المادي أو التقني في القضية.

ومع اختلاف التخصص القانوني عن التخصص التقني فللمحقق عند انتقاله إلى مكان وقوع الجريمة لإجراء المعاينة أن يصطحب معه من يرى الاستعانة بهم من الخبراء في مجال تقنية الحاسب والشبكات، وهذا لا يمنع أبداً من توفير الإسعاف للمصابين وفق ما نص عليه نظام الإجراءات الجزائية السعودي 1435هـ.

وفي النهاية نوضح أنه نظراً لما تتمتع به جريمة الإرهاب الإلكترونية من دقة وأمور فنية وعلمية عديدة ومتشابكة، فإنه يجوز للمحقق القيام بإعادة إجراء المعاينة إذا وجد لذلك مقتضى.

الخبرة

الخبرة هي: إبداء الرأي من مختص في أحد فروع المعرفة العلمية، ورجال الضبط الجنائي هم أول السلطات التي تملك تقدير الحاجة الفنية للاستعانة بالخبراء في قيامهم بمهام الاستدلال وجمع المعلومات لما نصت عليه المادة الثامنة والعشرون من نظام الإجراءات الجزائية السعودي الجديد 2 /1435هـ.

تحديات الخبرة

توجد تحديات تعترض عمل مأمور الضبط أو المحقق عند ضبط البيانات تحول دون إتمام الضبط للبيانات لكونها دليل ارتكاب جريمة ما في المجال الإلكتروني. والأصل أن الخبرة أحد إجراءات التحقيق وليس الاستدلال، كما ورد بنص المادة السادسة والسبعين من نظام الإجراءات الجزائية، كما أعطى النص كذلك سلطة تقديرية للمحقق على أن يقدر مدى حاجته إلى الخبرة الفنية في الجريمة محل التحقيق، وبصفة خاصة أنها من جرائم الإرهاب عبر الفضاء الإلكتروني، وغالباً ما تكون مرسلة بطريقة مختلفة عن الطرق العادية في الإرسال، وقد تكون مشفرة وبها من الألغاز ما يحتاج إلى خبرة من نوع خاص في تلك الجرائم فضلاً عن الخبرة التقنية التي يحتاج إليها الأمر؛ حيث يجب فحص الجهاز المرسل منه أو المستقبل وبناء علي ذلك إذا قام الشك في أي من الأمور الداخلة في إثبات الجريمة أو المحققة لأحد أدلتها وجب ندب خبير للوقوف على حقيقتها لاستمرار سير التحقيق، وذلك للاختصاص المنوط به.

إلا أنه وبصفة خاصة في الجرائم الإرهابية الإلكترونية؛ نظراً لحاجتها إلى الدقة والخبرة الفنية والتقنية؛ فإنه حسب نص المادة الثامنة والسبعين من نظام الإجراءات الجزائية لعام 1435هـ، للخصوم رد الخبير إذا شكّوا في ذمته وضميره أو أخلاقه المهنية إذا وجدت أسباب قوية تدعو لذلك.

ومن التحديات التي تقابلها الخبرة في جرائم الإرهاب الإلكتروني أنه على الخبير المنتدب للقيام بمهام الخبرة أن ينجز عمله خلال مدة محددة سلفاً عليه إتمام عمله خلالها وتقديم تقريره الفني بخصوصها؛ حيث إن تحدي الزمن عامل مؤثر وبقوة في الجرائم الإلكترونية بصفة خاصة ؛لما لها من سرعة إتمام ففي لحظة تمحى كل البيانات دون تحديد زمن معين؛ حيث عدم وجود الدليل المرئي [14]، ونظراً لعلم الخبير بما تحتاج إليه هذه النوعية من الجرائم إلى السرعة الفائقة في الإنجاز فعليه الالتزام بما حدد له من موعد لتقديم تقريره، وإلا كان متواطئاً مع الجناة، ذلك وإلا كان للمحقق أن يستبدله بغيره من الخبراء لإنجاز العمل في الوقت اللازم وفق نص المادة السابعة والسبعين من نظام الإجراءات الجزائية السعودي لعام 1435هـ.

وإذا كان أمراً تقديرياً للسلطة المختصة فينبغي أن يكون محتملاً في الجرائم الإلكترونية، بل ووجوبياً إذا كانت من نوعية جرائم الإرهاب، لما فيها من مخاطر ومشكلات فنية قد يترجمها، أو يحللها الخبير الفني بخلاف الآخر في هذا الأمر وفي النهاية الأمر يتعلق بأمن الدولة وكذلك مساس بحقوق المتهم أو الجناة بصفة خاصة فيجب عدم إهدارها أو المساس بها إلا بناء على يقين فالأصل في الإنسان البراءة، والأصل افتراض مبدأ البراءة في المتهم، ومن هنا تتحرى المحكمة الدقة وبصفة

خاصة في جرائم الإرهاب فتناقش الخبير في تقريره الذي قدمه في الجريمة محل التحقيق بموجب نص المادة الثانية عشرة من نظام مكافحة الإرهاب.

وتحد آخر نظراً لهذه الدقة الفائقة في تقرير الخبير وما يحيط به من مخاطر فنية وتقنية، وتحديات متطورة وتخصصية محترفة؛ فلابد من تحقيق مستوى تقني عالٍ الجودة في الخبرة؛ وعليه فبموجب نص المادة الرابعة عشرة من نظام مكافحة المعلوماتية السعودي (تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة)؛ حيث إننا بصدد نوع من الجرائم يحتاج إلى دقة فنية لها قوتها في الإثبات [15].

ومن التحديات التي يقابلها تقرير الخبير أن الإرهاب الإلكتروني يتسم بكونه جريمة إرهابية متعدية الحدود، وعابرة للقارات، وغير خاضعة لنطاق إقليمي محدود يصعب على الأنظمة الداخلية مواجهتها بمفردها [16]، لما لها من أهداف مباشرة وأخرى غير مباشرة [17].

كما يتوافر تحد آخر في صعوبة اكتشاف جرائم الإرهاب الإلكتروني، ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم [16،18]، والتي قد تستخدم فيها الاستراتيجيات العسكرية في التخطيط [17].

كما تمثل صعوبة الإثبات في الإرهاب الإلكتروني تحدياً خطيراً، نظراً لصعوبة توفير الخبرة الكافية والأدوات اللازمة لاستخلاص الدليل، ولسرعة غياب الدليل الرقمي، وسهولة إتلافه وتدميره لدى المتخصصين [16].

التفتيش

بموجب نصوص المواد (55-41) من نظام الإجراءات الجزائية السعودي يكون الهدف من القيام بإجراء التفتيش في جرائم الإرهاب الإلكتروني هو البحث عن حقيقة شخص، وأدوات وأجهزة الجريمة، ويكون محله ما يتعلق بخضوع مكونات الكمبيوتر للتفتيش، ومكان وجوده يتم التفتيش فيه وفق أحكام تفتيش المنازل مع توافر الضمانات المقررة قانونا لمثل هذا النوع من التفتيش [19]، كما يشمل ماديات الجهاز التي استعملت في الجريمة [7].

محل التفتيش

تفتيش نظام الحاسب الآلي: بما أن التفتيش إجراء يهدف إلى البحث عن شيء يتصل بجريمة وقعت بالفعل ويفيد في كشف حقيقتها وحقيقة شخص مرتكبيها. فقد يقتضي الأمر التفتيش في مكان خاص له الحرمة الخاصة به كالمسكن، ولكن بما أن الدراسة الحالية هدفها التركيز على مخاطر وتحديات البحث والتحقيق في جرائم الإرهاب عبر الفضاء الإلكتروني، فإن إجراء التفتيش هنا يتناول بالبحث التفتيش الوارد على النظام المعلوماتي وما يتم ضبطه من دلائل في نطاق ذلك [19]

ولكن هنا نتساءل ما المكونات الصالحة للتفتيش؟

من المعروف أن الحاسب الآلي يتكون من مكونات مادية ومكونات منطقية، كما أن له شبكة اتصالات سلكية ولاسلكية سواء كان ذلك على المستوى المحلي أو المستوى الدولي. وفيما يتعلق بإمكانية التفتيش وضبط الأدلة فإن الفقه الجنائي اختلف حول مدى قابلية البيانات المعلوماتية المكونات المنطقية للحاسب من عدمها لأن تكون موضوع تفتيش طبقا للنصوص التقليدية، وهو ما يستدعي سن أنظمة إجرائية جديدة تنص على السماح بإمكانية تفتيش أجهزة الكمبيوتر والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكتروني والبريد الصوتي والبريد المنقول عن طريق الفاكس.

تحديات التفتيش

من المخاطر التي تصادف هذه النوعية من الجرائم فيما يتعلق بإجراء التفتيش كون الجهاز موجوداً بمنزل المتهم، أو أنه موجود بمنزل المتهم وله وصلة أخرى، أو يتصل بجهاز آخر، أو عدة أجهزة في منزل آخر، أو عدة منازل، وقد يكونون شركاء له، وقد لا يكون لهم أي علاقة بالجريمة. في مثل هذه الحالات إذا أخذنا باتباع ما يجب القيام به في التفتيش فإنه يتم تفتيش الجهاز وما يتصل به وما يحتويه من مكونات مادية، كما أنه وبحسب الحال لا تصح الأدلة الناتجة عن ذلك، إلا إذا كان التفتيش قد تم بناء على أمر مسبب من الجهة المختصة؛ تطبيقاً لنص المادة الثانية والأربعين من نظام الإجراءات الجزائية السعودي.

وتشمل المكونات المادية للنظام المعلوماتي:

1- الحاسبات الآلية: هي بدورها تتكون من مكونات مادية ومعنوية. كما عرفتها المادة الأولى من نظام مكافحة الجرائم المعلوماتية؛ حيث عرفت أن الحاسب الآلي هو: (أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له).

2- المكونات الرئيسية: وتشمل وحدة الإدخال ووحدة الذاكرة الرئيسية ووحدة الحساب والمنطق ووحدة الإخراج.

3- استخدامات النظام.

4- وحدات التخزين الخارجي: كالأقراص المرنة و الصلبة وأقراص الليزر.

5- الأجهزة الملحقة: مثل الأجهزة التي يتم ربطها بالكمبيوتر و يتم

تشغيلها آلياً وفق برنامج معين كماكينات الخياطة والروبوت وغيرها.

أما العنصر الثاني المكون لنظام المعلوماتية فهو المكونات المنطقية أو البرامج وتنقسم إلى الكيانات المنطقية الأساسية أو برامج النظام والكيانات المنطقية أو برامج التطبيقات [20].

الضبط

وفق نص المادة السادسة والعشرين من نظام الإجراءات الجزائية يجوز لرجال الضبط الجنائي ضبط الأوراق وكل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج عنها وكذلك ما وقعت عليه الجريمة وكل ما يفيد في كشف الحقيقة بوجه عام، وكذلك وفق نص المادة الرابعة عشرة من نظام مكافحة الإرهاب 4 /1435هـ. كما أنه بموجب نص المادة الأربعين منه (تطبّق أحكام نظام الإجراءات الجزائية فيما لم يرد فيه نص خاص في هذا النظام)، وقد بينت المادة التاسعة والأربعون إجراءات أهمية التحريز للموجودات، ووفق نص المادة الخمسين بين النظام كيفية حفظ الأشياء محل الضبط.

تحديات الضبط

تعد هذه النصوص وما تحويه في مجال البحث في جرائم الإرهاب الإلكتروني ضمانات لسلامة الإجراءات ولها أهميتها الخاصة في تلك الأنواع من الجرائم لدقة ما يتم التوصل إليه من أدلة قد تكون أجهزة دقيقة وحساسة، أو جزئيات من أجهزة، الجزئيات الفعالة، أو التي تحمل البيانات فقط من أقراص ما أصغر حجمها، ودقة حساسيتها، مع العلم بضرورة الضبط لكل صغيرة وكبيرة موجودة بمسرح هذه الجريمة ماديّاً ومعلوماتيّاً، وإلا تعد هذه الإجراءات الضبطية معرضة لخطر المحو، أو الإتلاف. كما يعد إجراء الضبط هنا من التحديات التي تواجه جهة الضبط؛ لما لتلك الأدوات والأشياء المضبوطة من دقة فنية في التركيب وفي شدة حساسية التعامل معها إذا كان من يقوم بالضبط لا يعلم بتلك الحساسية العالية التي تعمل على تلف الملفات أو الأوراق والبيانات المعلوماتية المضبوطة نتيجة خدش أو لاستخدام القوة في الضبط، أو العنف في التعامل معها [6] ،نظراً لنقص الخبرة [16].

وأوجب النظام على رجل الضبط الجنائي وأعوانه المحافظة على سرية ما عثروا عليه وعدم استغلاله لمصلحتهم الخاصة؛ وفق نص المادة الحادية والستين اجراءات. وعليه كل ما يتعلق بالقضية المعروضة يعد من الأسرار الوظيفية التي لا يجوز إفشاؤها؛ حيث أصبحت المعلومات في هذه النوعية من الجرائم هي سلاح الجاني الذي يحارب به المجني عليه سواء كان فرداً أو جماعة، أو دولة [21] ، ما يدل على أنه من الشخصيات ذات الذكاء والخبرة العالية [12].

كما تشمل السرية حالة الجهاز محل الضبط وكونه كان بمفرده أو أنه متصل بالغير مع أحد الجيران، أو أنه كانت التوصيلات على شكل شبكة، أو كان في حالة مراقبة من جهة اتصال معينة أو أي من المعلومات التي تعرض لها رجل الضبط أو عرضت له أثناء التفتيش، أو الضبط، وأصل ذلك ما نصت عليه المادة الأربعون من النظام الأساسي للحكم السعودي. ومع ذلك ورغم أن النظام يحمي كل الاتصالات من الاطلاع إلا أن هذه الحماية من جانب آخر تعتمد على أن المحل موجود فعليا ليتم ضبطه.

إلا أنه في مجال الجريمة الإرهابية عبر الفضاء الإلكتروني نجد تحدياً آخر هو سرعة الإخفاء والمحو كعائق بين وجود أدلة ونجاح القضية، كما تعوق إجراء الضبط في حد ذاته؛ حيث ينعدم المحل [16]، لذا فهناك حاجة إلى برمجيات خاصة لنجاح تلك الإجراءات، وإنتاج أدلة تكشف حقيقة الجريمة ومنها برمجيات النسخ الاحتياطي الجنائي، وبرمجيات البحث عن المفردات النصية، وفك الشفرات، وبرمجيات كسر كلمة السر، استعادة البيانات المحذوفة، والتي تم قصها، استعراض الصور، وبرمجيات تتبع الاتصال الشبكي، وعرض محتوى الملفات، وبرمجيات الضغط والفك، وبرمجيات استراق ضربات لوحة المفاتيح [6].

الشهادة

إن طائفة الإرهابيين عبر الفضاء الإلكتروني من الفئات ذات الأفكار المتطرفة، كما لهم من أساليب التعامل أشكال غير متعارف عليها في الجريمة التقليدية؛ حيث يعملون على توظيف المواقع الإلكترونية في نشر أفكارهم، ويعملون على استخدام أكبر قدر ممكن من المساحة المعلوماتية للدخول إلى مواقع مهمة بالدولة تتعلق بالأمن سواء بالداخل، أو بالخارج، وللتحريض على الإرهاب، وكذلك تمويله [22]، ما يعمل على صعوبة إتمام إجراءات البحث وكذلك التحقيق ومنها استماع الشاهد المعلوماتي.

القواعد التي يخضع لها إجراء الاستماع إلى الشهود

وفق نص المادة الخامسة والتسعين إجراءات: يجب على المحقق الاستماع لأقوال الشهود الذين يطلب الخصوم شهادتهم ما لم ير المحقق فائدة من ذلك، وبناء على نص المادة الثامنة والتسعين: (يستمع المحقق لكل شاهد على انفراد، وله أن يواجه الشهود بعضهم ببعض وبالخصوم)، وذلك بهدف ألا يؤثر بعض الشهود على بعض.

ويمكن القول بأن الشاهد المعلوماتي ينحصر في عدة فئات هي:

1- مشغلو الحاسب الآلي: عامل تشغيل الحاسب الآلي هو ذلك الشخص المسئول عن تشغيل الجهاز والمعدات المتصلة به. ولا بد من أن تكون لديه خبرة كبيرة في مجال استخدام الكمبيوتر عن طريق استخدام هذه البيانات وكيفية إدخال البيانات ثم استخراجها، وهو يقوم بنقل البيانات من الوثائق إلى وسائط

التخزين التي تجري معالجتها بواسطة الحاسب الآلي.

2- خبراء البرمجة: وهم الأشخاص المتخصصون في كتابة أوامر البرامج.

3- المحللون: المحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع البيانات الخاصة بنظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقة الوظيفية بين هذه الوحدات.

4- مهندسو الصيانة والاتصالات: وهم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

5- مديرو النظم: وهم الذين توكل إليهم أعمال الإدارة في النظم المعلوماتية.

التزامات الشاهد المعلوماتي

بما أن نظام مكافحة الإرهاب نص على تطبيق قواعد نظام الإجراءات الجزائية في جرائم الإرهاب حسب النص فإن الشاهد المعلوماتي عليه عدد من الالتزامات كما هو الحال بالنسبة للشاهد في الجريمة التقليدية، متى كان الشاهد المعلوماتي حائزاً لمعلومات جوهرية تفيد سير التحقيق فإنه يكون مطالباً بأن يعلم بها سلطات التحقيق على سبيل الإلزام وإلا تعرض للعقوبات المقررة للامتناع عن الشهادة، وذلك في غير الأحوال التي يجيز له القانون فيها ذلك، وعليه يقع على الشاهد المعلوماتي عبء مساعدة هيئة التحقيق في كشف حقيقة الجريمة بالإدلاء بما لديه من معلومات تتعلق بالجريمة مهما كانت كبيرة أو صغيرة [6]، ومنها :

1- طبع ملفات البيانات المخزنة في ذاكرة الحاسب الآلي أو الدعامات الأخرى على أن يقوم بطبعها و تسليمها إلى سلطات التحقيق.

2- الإفصاح عن كلمات السر.

3- الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة [14].

الاستجواب

الاستجواب هو مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق، ومطالبته له بإبداء رأيه في الأدلة القائمة ضده إما تفنيدا أو تسليما، وذلك قصد محاولة كشف الحقيقة واستظهارها بالطرق القانونية. ونظراً لخطورة الاستجواب بالنسبة للمتهم فقد أحاطته التشريعات بعدة ضمانات وأوردها المنظم السعودي في نص المادتين الأولى والثانية بعد المائة.

ومن خلال هذين النصين يتبين قدر من الضمانات التي يتمتع بها المتهم في الاستجواب في الجرائم التقليدية وعليه تنطبق كذلك على المتهم في الجرائم الإلكترونية وفق نص المادة الخامسة عشرة من نظام مكافحة المعلوماتية السابق ذكرها، ونص المادة الأربعين من نظام مكافحة الإرهاب.

ومن التحديات وكذلك المخاطر التي يواجهها الاستجواب في هذه النوعية من الجرائم عدم خبرة المحقق في استخدام الحاسب الآلي، أو عدم إجادة الدخول على الإنترنت، ما يتطلب التدريب الكافي، وإعداد الكوادر الكافية.

كما أنه من المخاطر ضعف الخبرة الفنية بمعاني المصطلحات المستخدمة في الجريمة في الإرسال أو الاستقبال أو في التسجيلات والتي قد توجه التحقيق إلى غير مساره، ما يتطلب الإلمام الكامل بها من قبل المحقق.

والجدير بالذكر أنه من الضروري أن يتفق الخبير والمحقق على خطة التحقيق في مثل هذه الجرائم وللمحقق الاستعانة بالخبير في التعريف بكل ما يصعب عليه في التحقيق من أمور فنية تتطلب وجود الخبير الفني، فلابد من جلسة بينهما تسبق أي إجراء، وإلا تعرض التحقيق بل القضية برمتها لمخاطر عدة لأسباب فنية تخرج عن اختصاص المحقق.

ويعد عامل الزمن من التحديات والعوامل الهامة والمؤثرة في مجرى التحقيق؛ حيث إن النوعية الحالية من الجرائم تتمتع بسرعة الإنتاج والإنجاز للمهام المختلفة على أوسع نطاق جغرافي، فبالمقابل لابد من أن تتخذ إجراءات الاستجواب ذات النمط من السرعة في الانتهاء منها واستجلاء الحقيقة المنتظرة.

ومن المخاطر المساس بالحرمات؛ ففي ذات الوقت لا يجوز الاعتداء على الحرمات نتيجة السرعة فلكل حق حماية والحقوق مصانة بالنصوص الشرعية والنظامية.

ونظراً لما لطبيعة جريمة الإرهاب الإلكتروني فإن الاستجواب فيها يكون شائكاً بصفة خاصة وأنها من الجرائم التي قد يغيب فيها الدليل المرئي الكافي للاتهام [23]، ويشكل بذلك عدم توفر الدليل المرئي تحدياً أمام جهة الاستجواب ما قد يضعف جودة العمل ودقة النتائج المستخلصة، كما يواجه الاستجواب بعض التحديات الهامة ومنها صعوبة التواصل بين الدول التي مرت بها عناصر الجريمة [24].

النتائج

إن إجراءات البحث والتحري ابتداءً باستقبال البلاغ وانتهاءً بإجراءات التحقيق بهدف استجلاء حقيقة الجريمة وبصفة خاصة في جرائم الإرهاب الإلكتروني تنطوي على قدر عال من الدقة الفنية بما فيها من تحديات لسلطة جمع الاستدلالات وسلطة التحقيق، ومخاطر

على الأدلة المستقاة بالطرق التقنية المتحصل عليها. وعليه نتوصل إلى عدة نتائج نجملها فيما يلي:

- يشترط أن يكون الخبير المنتدب في الأصل من الخبراء المسجلين في سجل الخبراء لدى المحاكم.
- في حال ندب خبير من قبل المحقق المختص يحق له الاطلاع على الأوراق والمستندات المتعلقة بطلب الخبرة.
- عدم الخبرة التقنية لدى سلطات البحث والتحقيق قد يتسبب في فقدان الدليل.
- حضور الخبير جميع إجراءات البحث والتحقيق من ضرورات كشف حقيقة الجريمة.
- خبرة المحقق التقنية تعمل على سهولة الوصول إلى المحاكمة العادلة المبنية على حقيقة فنية ومادية واضحة.

التوصيات

حتى تؤتي تلك النتائج ثمارها على أرض الواقع فإنه من الضروري العمل على سد بعض الثغرات النظامية والعملية التي نجمل توضيحها من خلال عدد من التوصيات هي:

- سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، على أن يكون شاملاً للقواعد الموضوعية والإجرائية في نظام واحد.
- الاعتراف بالأدلة الرقمية واعتبار أن لها حكم الأدلة المادية.
- تطوير نظام تقادم الجريمة الإلكترونية.
- إعداد أنظمة ضبطية وقضائية مؤهلة للتعامل مع الجرائم الإلكترونية
- إعداد وتدريب الكوادر التقنية بسلطات البحث والتحقيق والمحاكمة للوصول إلى محاكمة عادلة.

المقترحات

و في سبيل العمل على تحقيق تلك التوصيات نقدم بعض المقترحات التي تعمل على تدعيم التوصيات السابقة وتحقيقها عملياً وهي كما يلي:

- إضافة الخبراء والفنيين المختصين بالحاسب الآلي إلى جهات الضبط المنصوص عليها بموجب المادة السادسة والعشرين من نظام الإجراءات الجزائية السعودي.
- تطبيق باقي نصوص نظام الإجراءات الجزائية بمعناها الواسع على الجرائم الإلكترونية بصفة عامة.
- استعانة المحقق بخبير مختص لإبداء الرأي في مسالة متعلقة بالتحقيق يعد من الأمور الاختيارية التي يخضع ضرورة القيام بها من عدمه لتقدير المختص حسب نص النظام، ولكن يجب أن يكون المحقق ذاته بل ورجال الشرطة والضبطية الجنائية على قدر من الخبرة والكفاءة الفنية في أمر الضبط وجمع المعلومات والبيانات، قدر الإمكان بطريق التدريب التقني لهم وإعداد الكوادر الفنية التي تفي بالغرض من حيث العدد، والعدة.

قائمة المراجع

1. سعد، محجوب حسن (1421هـ). أساليب البحث الجنائي في الوقاية من الجريمة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية.
2. كامل، محمد فاروق (1999م). القواعد الفنية الشرطية للتحقيق والبحث الجنائي، الرياض، جامعة نايف العربية للعلوم الأمنية.
3. العتيبي، معجب بن معدي الحويقل (1413هـ). حقوق الجاني بعد صدور الحكم في الشريعة، الرياض، مطبعة سفير.
4. الغويري، شارع بن نايف (1431هـ). الضبطية الجنائية في المملكة العربية السعودية، الرياض، كلية الملك فهد الأمنية.
5. السند، عبد الرحمن بن عبد الله (2004م). وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، الرياض، جامعة الإمام محمد بن سعود.
6. المويشير، تركي بن عبد الرحمن (2009م). التحقيق في الجرائم المعلوماتية، ملتقى الجرائم المعلوماتية، الرياض، هيئة التحقيق والادعاء العام.
7. السرحاني، محمد بن نصير محمد (2004م). مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت – دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، الرياض، جامعة نايف العربية للعلوم الأمنية.
8. حسني، محمود نجيب (1998م). شرح قانون الإجراءات الجنائية، ط3، القاهرة، دار النهضة العربية.
9. عقيدة، محمد أبو العلا (2001م). شرح قانون الإجراءات الجنائية، القاهرة، دار النهضة العربية.
10. ممدوح، خالد (2009م). فن التحقيق الجنائي في الجرائم الإلكترونية، الإسكندرية، دار الفكر الجامعي.

11. حجازي، عبد الفتاح بيومي (2006م). مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الإسكندرية، دار الفكر الجامعي.

12. رستم، هشام (1994م). الجوانب الإجرائية للجرائم المعلوماتية، الإسكندرية، دار الفكر الجامعي.

13. آل ثنيان، ثنيان ناصر (2012م). إثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية، رسالة ماجستير، الرياض، جامعة نايف العربية للعلوم الأمنية.

14. حموده، علي (2003م). الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث لمؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، شرطة دبي.

15. حسين، عبد الرحمن جميل محمود (2008م). الحماية القانونية لبرامج الحاسب الآلي، دراسة مقارنة، رسالة ماجستير، فلسطين، جامعة النجاح الوطنية.

16. الكعبي، محمد عبيد (2005م). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، القاهرة، دار النهضة العربية.

17. العموش، أحمد فلاح (2006م). مستقبل الإرهاب في هذا القرن، الرياض، جامعة نايف العربية للعلوم الأمنية.

18. موسى، مصطفى محمد (2005م). أساليب إجرامية بالتقنية الرقمية – ماهيتها ومكافحتها، القاهرة، دار الكتب القانونية.

19. أحمد، هلالي عبد اللاه (1997م). تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، القاهرة، دار النهضة العربية.

20. الغافري، حسين بن سعيد، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، منتدى كلية الحقوق، جامعة المنصورة، مصر. http://www.f-law.net/law/، تاريخ الاطلاع: 1/4/2015م.

21. يوسف، صغير (2013م). الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، تيزي وزو، جامعة مولود معمري .

22. الشهري، فايز عبد الله (2010م). ثقافة التطرف على شبكة الإنترنت الملامح والاتجاهات، الندوة العلمية عن استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، الرياض، جامعة نايف العربية للعلوم الأمنية.

23. حجازي، عبد الفتاح بيومي (2009م). الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت، القاهرة، بهجت للطباعة والتجليد.

24. الكواري، محمد علي أحمد (2007م). مسرح الجريمة ودوره في كشف غموض الجريمة، الرياض، جامعة نايف العربية للعلوم الأمنية.