مدى حجية أدلة الإثبات الجنائي التقليدية في إثبات جرائم الإرهاب المعلوماتي.

عبد العزيز خنفوسي

أستاذ محاضر قسم - ب-

كلية الحقوق والعلوم السياسية

جامعة سعيدة.

الملخص باللغة العربية:

يتميز الإرهاب الالكتروني عن الإرهاب التقليدي بالطريقة العصرية المتمثلة في استخدام المواد المعلوماتية والوسائل الالكترونية التي جلبتها تقنية عصر المعلومات، ولذلك نجد أن الأنظمة الالكترونية والبنية التحتية المعلوماتية هي هدف الارهابين.

ومن هنا يمكن القول بأن العصر الجديد للإرهاب تميز بالدور المركزي الذي تلعبه شبكة الانترنت في تشكيلها ونقل الأفكار والخبرات عبرها، أي بين التنظيمات الإرهابية والأفراد الذين يشكلونها، فقد بات واضحا خلال الخمسة أعوام الأخيرة النمو الواسع والملحوظ لظاهرة لجوء الجماعات الإرهابية إلى الانترنت كوسيلة رئيسية لبث دعايتها وأفكارها.

وعليه فقد جاء هذا المقال البحثي من أجل استعراض مدى كفاية وسائل الإثبات الجنائي التقليدية في كشف أفعل وسلوكيات الإرهاب المعلوماتي.

الكلمات المفتاحية الدالة: الإرهاب الالكتروني، الإرهاب التقليدي، عصر المعلوماتية، الإثبات الجنائي التقليدي، الإثبات الجنائي الرقمي، الفضاء الافتراضي، الجريمة الإرهابية الرقمية.

Abstract in English:

Featuring electronic terrorism from the traditional way of modern terrorism in the use of information materials and electronic means which brought the era of information technology, therefore, we find that the electronic and IT infrastructure systems is the goal of the terrorists.

Hence it can be said that the new age of terrorism characterize the central role that the Internet plays in the formation and transfer of ideas and experiences across it, that is, between terrorist organizations and individuals who pose, it has become clear over the last five years the broad and significant growth of the phenomenon of asylum terrorist groups to the Internet as a major means to broadcast propaganda and ideas.

And it was this research came from the article to review the adequacy of the traditional means of proof in criminal detection and behavior do informational terrorism.

Keywords function:

Electronic terrorism, conventional terrorism, the information age, the traditional criminal prosecution, criminal prosecution digital, virtual space, digital terrorist crime.

- مقدمة:

إن التحديات الدولية التي فرضتها العولمة في مجالات التنافسية الاقتصادية والسوق الحرة، قد حتمت على المنتظم الدولي أن يندمج سريعا وفورا في عالم المعلوماتية والتكنولوجيا الحديثة، وهذا باعتبارها خيارا استراتيجيا لا يمكن للمجتمعات الإنسانية أن تحيد عنه ولو لبرهة يسيرة، والسبب في ذلك أنها ستجد نفسها قابعة في مكانها، وعاجزة عن مواكبة المتغيرات السريعة والمتنامية للتنمية الاقتصادية والاجتماعية والثقافية.

في سبيل ذلك، فقد أدى التطور المذهل الذي عرفته تكنولوجيا الاتصالات والرقمنة الذكية إلى اختصار المسافات بين الدول والإلغاء شبه الكلي للحدود القائمة بينها، خصوصا وأن الثورة المعلوماتية قد مست جميع مناحي الحياة، وأصبحت أشبه ما يكون بالثورة في حياة البشرية وأسلوب حياة الناس، وهذا لارتباطها الوثيق بجميع القطاعات الحيوية، واحتلالها مكانة متميزة في مجال تنمية الإدارة والقطاع الخاص، نظرا للتغييرات الجوهرية التي أحدثتها في نمط وأسلوب العمل الذي أصبح يتم عبر نظم المعلوماتية وشبكات الاتصال المتطورة، كما ساهمت أيضا هذه الثورة في تأمين عمليات جمع البيانات من مصادرها المتنوعة، ومعالجة معطياتها الآلية وتخزين المعلومات المرتبطة بها وتحديثها وإيصالها إلى الجهات المستفيدة منها.

غير أن هذه النقلة النوعية في مجال المعلوماتية لم تقتصر فقط على الجانب الايجابي المرتبط بالثورة العلمية والتكنولوجية، وإنما كانت لها انعكاسات جانبية أوجدت أنماطا سلوكية مشوبة بعدم الشرعية، والتي تغذت من الاستعمال المعيب والتدليسي لوسائل الاتصال المتطورة، وهذا خصوصا أمام حتمية انفتاح المنظومة الرقمية على بعضها البعض، والسماح للآخر بالاطلاع عليها واستخدامها، والإسقاط شبه التام لحواجز الأمن المادية والالكترونية المعتمدة لحماية المعلومات، والتي أصبحت في متناول الجميع، بما في ذلك العصابات الإجرامية والتنظيمات الإرهابية.

- الإشكالية الرئيسية للورقة البحثية:

لقد أثبتت التجربة الأمنية في مجال مكافحة الإرهاب شيوع استخدام وسائل التكنولوجيا الحديثة داخل المجموعات الأصولية، بحيث تم اعتمادها في تنظيم الهياكل الداخلية، وفي توجيه التعليمات سواء أفقيا بين مجموع الخلايا المكونة للتنظيم أو عموديا بين الزعامة والقاعدة المرتبطة بها، بل تم استخدامها حتى في تنفيذ المخططات التخريبية، كالمتفجرات المتحكم بها عن بعد بواسطة أجهزة الهواتف النقالة، واعتمادها أيضا كمورد للتزود بالمعلومات المتعلقة بكيفية تصنيع المواد المتفجرة وغيرها...

وكمثال على هذا الطرح، فإن العديد من التنظيمات الإرهابية التي تم تفكيكها بعدة دول عربية، أثبتت التحريات والأبحاث التمهيدية المنجزة بشأنها أنها كانت تعتمد التواصل المعلوماتي عبر مواقع إلكترونية في شبكة الانترنت مع نظيراتها في بعض الدول الأجنبية الشيء الذي مكنها من توحيد منهجها العقائدي ومرتكزاتها الإيديولوجية بهدف

إعلان البيعة لأمير واحد بغية الانصهار التام ضمن تنظيم جهوي أو إقليمي، وهذا في انتظار إعلان البيعة المطلقة والنهائية لزعيم واحد على الصعيد العالمي.

هذا وقد ساهمت الوسائل التكنولوجية المتطورة في تقديم خدمة عرضية غير مقصودة للتنظيمات الإرهابية، وذلك عن طريق إشاعة تسمياتها وإذاعة بياناتها سواء تلك المقرونة بالتهديد أو التي تتبنى من خلالها بعض الأعمال الإرهابية، وهو ما يحقق أهم أهداف الجريمة الإرهابية المتمثل في الأثر النفسي الذي ينجم عنها، والذي يتجلى عادة في حالة عارمة من الخوف والرعب، ويعطي في أغلب الأحيان لتلك التنظيمات حجما أكبر من حجمها المعتاد، وهذا لأنه ينطوي على نوع من التضخيم والمغالاة لتحسيس المجتمع بقدرة هذا التنظيم على استهداف جميع المواقع الحساسة في أي مكان وزمان.

وبالتالي نجد أن الأمر لا يقف عند حد استخدام التنظيمات الإرهابية لوسائل التقنية الحديثة في تنفيذ مخططاتها التخريبية، بل يتعداه إلى أبعد من ذلك، فقد أدى التطور المتنامي للظاهرة الإرهابية وتعقد شبكاتها الدولية إلى البحث في أحدث التقنيات والاختراعات العلمية لتسخيرها كوسيلة وكهدف خدمة لمشروعها الإجرامي، ولا شك أن نظم المعالجة الآلية للمعطيات كانت على قائمة هذه الأولويات، الشيء الذي أفرز نمط جديد من الإرهاب يمكن تسميته بالإرهاب المعلوماتي أو الالكتروني.

ولما كان الإرهاب الالكتروني لا يختلف عن الإرهاب التقليدي، إلا من حيث الوسيلة المستخدمة في ارتكابه، وهي شبكة المعلومات الدولية، فهل يمكن الجزم بأن نصوص قانون العقوبات كافية لمواجهة جرائم الإرهاب الالكتروني، وهذا في ظل قصور قواعده، وعدم مواكبتها لمستجدات هذه الجرائم؟

وحتى وإن سلمنا نسبيا بأننا نستطيع رصد الأفعال المكونة لجرائم الإرهاب المعلوماتي، فإنه سيعترضنا لا محال صعوبة الإثبات الجنائي لجريمة الإرهاب الالكتروني، الأمر الذي يؤدي بنا إلى طرح التساؤل الرئيسي التالي:

هل تعد وسائل الإثبات الجنائي التقليدية كافية وملائمة من أجل إثبات أركان جريمة الإرهاب الالكتروني؟

- تصميم هيكل الورقة البحثية:

من أجل الإجابة على الإشكالية الرئيسية المطروحة في خضم ورقتنا هذه المقدمة إلى مؤتمر ليبيا الدولي حول (الإرهاب الالكتروني ومخاطره وسبل مكافحته)، فإنه يتوجب علينا الأمر أن نناقش مدى حجية أدلة الإثبات الجنائي التقليدية في إثبات جرائم الإرهاب المعلوماتي وفق الخطة التالية:

المحور الأول: المعاينة كدليل إثبات جنائي في جرائم الإرهاب الالكتروني.

أولا: أهمية المعاينة في جرائم الشبكات الالكترونية.

ثانيا: أسلوب المعاينة من خلال العالم الافتراضي.

ثالثا: صور المعاينة من خلال الشبكات الالكترونية.

رابعا: الخطوات الواجب إتباعها قبل الانتقال لمعاينة الجريمة من خلال الشبكات الالكترونية.

المحور الثاني: الضبط والتفتيش في مجال جرائم الإرهاب الالكتروني.

أولا: معنى التفتيش في جرائم الإرهاب الالكتروني.

ثانيا: شروط التفتيش في العالم الافتراضي الرقمي.

المحور الثالث: ضبط الأدلة الرقمية.

أولا: معنى الضبط في البيئة الرقمية.

ثانيا: الإشكالات التي يثيرها ضبط البيانات الالكترونية المتحصل عليها من التفتيش.

المحور الأول: المعاينة كدليل إثبات جنائي في جرائم الإرهاب الالكتروني.

تعتبر المعاينة إجراء قانوني صالح لكشف الحقيقة في بعض الجرائم، والذي تكون غايته الكشف عن العناصر المادية التي تتعلق بالجريمة وتفيد في التحقيق الجاري بشأنها.

أولا: أهمية المعاينة في جرائم الشبكات الالكترونية.

لا تتمتع المعاينة في مجال الكشف عن جرائم الشبكات الالكترونية بنفس الدرجة من الأهمية التي يمكن أن تلعبها في مجال الجريمة التقليدية، ويرجع الأمر في ذلك للأسباب التالية:

1- إن الجرائم التي ترتكب من خلال الشبكات الالكترونية قلما يترتب على حدوثها آثارا مادية.

2- الأعداد الكبيرة للمتعاملين على الانترنت، والذين يترددون على مسرح الجريمة ما بين اقتراف الجريمة والكشف عنها، الأمر الذي قد يسمح بحدوث تغيير أو عبث بآثار الجريمة أو محوها، وهو ما يلقي ظلال من الشك على الدليل المستقي من المعاينة (1).

3- إمكانية التلاعب في البيانات عن بعد، وهذا من خلال وجود طرف آخر على معرفة ودراية بالجاني (2).

ثانيا: أسلوب المعاينة من خلال العالم الافتراضي.

يمكن القول أن المحقق أو ضابط الشرطة القضائية يستطيع الانتقال إلى العالم الافتراضي لمعاينته من خلال الحاسب الآلي بمكتبه، أو من خلال مكتب الخبراء المعتمدين لدى الجهات القضائية، أو من خلال الخبير الاستشاري إذا كان ذلك جائزا بحسب نصوص قانون الإجراءات الجنائية (أو قانون الإجراءات الجزائية)، بل وتجوز المعاينة كذلك من خلال اللجوء إلى مقر متعهد الإيواء، وهذا باعتباره أفضل مكان يمكن من خلاله إجراء المعاينة (3).

ثالثا: صور المعاينة من خلال الشبكات الالكترونية.

نستطيع القول أن المعاينة قد تتم عن طريق تصوير شاشة الحاسوب، سواء باستخدام آلة تصوير تقليدية أو عن طريق تجميد مخرجات الشاشة، أو عن طريق حفظ الموقع باستخدام خاصية الحفظ الموجودة في نظام التشغيل، كما يمكن إجراء المعاينة بالنسبة لشبكة الانترنت عن طريق إنزال نسخة من المصنف محل الاعتداء في حالة جرائم الاعتداء على الملكية الفكرية، أو التحفظ على نسخة في حالة الصور والعلامات لطباعتها على ورقة مثلا (4).

رابعا: الخطوات الواجب إتباعها قبل الانتقال لمعاينة الجريمة من خلال الشبكات الالكترونية.

1- الحصول على معلومات عن مكان الجريمة ونوع الأجهزة وعددها، وهذا تمهيدا لتحديد إمكانيات التعامل معها فنيا من حيث التأمين والضبط وحفظ المعلومات.

2- إعداد خريطة بالموقع وخطة للهجوم.

3- توفير برامج واسطوانات للاستعانة بها في الفحص والتشغيل.

4–تأمين التيار الكهربائي بحيث لا يتم التلاعب أو التخريب عن طريق قطع التيار.

5–عدم مغادرة مسرح الجريمة قبل إجراء اختبارات على ما تم ضبطه، والتأكد من خلو موقع الحاسب الآلي من أي مجالات لقواعد مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.

6–البحث عن خادم الملف لتعطيل حركة الاتصالات (5).

7–التحفظ على محتويات سلة المهملات، وفحص الوراق والشرائط والأقراص الممغنطة المتواجدة فيها، ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

8–الاستعانة بأهل الخبرة.

هذا ونجد أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، والتي صادق عليها المشرع الجزائري بموجب المرسوم الرئاسي رقم 14- 252 المؤرخ في 08 سبتمبر 2014 قد أشارت في مادتها 15 إلى الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، وقالت بأن جريمة الإرهاب المعلوماتي هي تلك الجريمة التي تستخدم فيها تقنية المعلومات الحديثة من أجل نشر أفكار ومبادئ جماعات إرهابية والدعوة لها، وكذا تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية. هذا بالإضافة إلى أن هذه الجريمة تقوم كذلك على نشر طرق صناعة المتفجرات بغية استخدامها في العمليات الإرهابية، وكذا نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

وبالرجوع إلى المادة 23 من نفس الاتفاقية نجد أنها أشارت بصورة صريحة إلى إجراء التحفظ العاجل على البيانات المخزنة في تقنية المعلومات في حالة معاينة الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، وعليه فقد اشترطت نفس المادة السابقة الذكر جملة من الإجراءات يجب القيام بها تتمثل في:

1–تبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة، بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية المعلومات، خصوصا إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل.

2–ضرورة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته، وكذا إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، وهذا من أجل تمكين السلطات المختصة من البحث والتقصي.

3–تبني جملة من الإجراءات الضرورية، وهذا لإلزام الشخص المسؤول عن حفظ تقنية المعلومات من أجل الإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الجنائي الداخلي.

المحور الثاني: الضبط والتفتيش في مجال جرائم الإرهاب الالكتروني.

أولا: معنى التفتيش في جرائم الإرهاب الالكتروني.

إن التفتيش بالمعنى الفني هو إجراء تحقيقي ووسيلة للإثبات المادي، وهذا لأنه إجراء يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، وهو ما يتنافر مع الطبيعة غير المادية لبرامج وبيانات الحاسبات الآلية، وكذا شبكة الشبكات الالكترونية، وهذا لأنها مجرد برامج وبيانات إلكترونية ليس لها أي مظهر مادي محسوس في

العالم الخارجي، وعلى ذلك فلا يرد عليها تفتيش أو ضبط، مما يتعين معه إخضاعها لأحكام مستقلة تتلائم وطبيعتها الخاصة.

وعليه يعتبر تفتيش نظام معلومات الحاسب الآلي ووسائط وأوعية حفظ وتخزين البيانات المعالجة إلكترونيا، إجراء يندرج ضمن التفتيش بمعناه القانوني ويخضع بالتالي لأحكامه، ويجوز الضبط المادي لهذه المعلومات كالأقراص والأسطوانات الممغنطة (6).

ثانيا: شروط التفتيش في العالم الافتراضي الالكتروني.

يخضع التفتيش في العالم الافتراضي الالكتروني لمجموعة من الشروط الموضوعية وأخرى شكلية تتمثل فيما يلي:

1- بالنسبة للشروط الموضوعية: فهي تتمثل في السبب والمحل والسلطة المختصة بالقيام به.

أ- وبالنسبة للسبب: فيجب أن تكون هناك جناية أو جنحة قد وقعت بالفعل، واتهام شخص أو أشخاص معنيين بارتكابها أو المشاركة فيها، وكذا قيام قرائن وأمارات قوية على وجود أشياء تفيد في كشف الحقيقة سواء مع شخصه أو مسكنه أو مع شخص أو مسكن غيره.

فطالما كان هدف التفتيش هو جمع الأدلة التي تثبت وقوع الجريمة وتكشف عن هوية فاعلها، فإن هذه الجريمة قد تقع على الشبكة ذاتها أو تقع باستخدامها.

ب- وفيما يتعلق بمحل التفتيش: فيقصد به المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، وهو المسكن أو الشخص أو الرسائل أو السيارة، وهي التي تكون محلا للتفتيش.

ومحل التفتيش في جرائم الشبكات الالكترونية هو الحاسب الآلي الذي يعتبر النافذة التي تطل بها الانترنت على العالم، والشبكة التي تشمل في مكوناتها الخادم والمزور الآلي والمضيف وملحقاته الفنية.

وجدير بالذكر أن مثل هذا المحل لا يمكن أن يكون قائما بذاته، وإنما يشمله مكان أو عقار ما، أو يكون بصحبة مالكه أو حائزه، أي أن الحرز الذي يوجد فيه الحاسب الآلي هو بطبيعته حرز مادي كالمترل أو شخصه، كما هو الشأن في الحاسوب المحمول سواء كان شخصيا أو هاتفيا نقال (7)، ولهذا يجب على ضابط الشرطة القضائية عند استصداره إذن التفتيش أن يحدد محل ذلك الإجراء تحديدا دقيقا وكذا الغرض منه، وأن يتأكد من أنه مما يجوز تفتيشه، وإلا كان هذا الإجراء باطلا، فمقر الهيئات الدبلوماسية مثلا لا يمكن تفتيشها (8).

ويشترط في إذن التفتيش أن يكون محددا خصوصا في محله والأشياء المراد البحث عنها لضبطها، كما لو تضمن الإذن تحديد القطع الصلبة المكون منها الحاسوب، وكما لو صدر الإذن بتفتيش ذاكرة الحاسب الآلي والأدوات الأخرى لتخزين البيانات (9).

وتجدر الإشارة إلى ان تحقيق هذا الشرط أمر صعب جدا، وهذا لأنه يتطلب من مصدر الاذن أن يحدده تحديدا فنيا، وهو ما يتجاوز ثقافته الفنية في مجال الشبكات الالكترونية.

- وبناءا عليه، وفي إطار جرائم الانترنت (والتي منها جرائم الإرهاب الالكتروني)، فإن التفتيش يقع على موضوعين هما:

- مكونات الحاسب الآلي المادية والمعنوية.
- الشبكة وما تتضمنه من مكونات.

فبالنسبة للحاسب الآلي فهو جهاز إليكتروني يقوم بمعالجة البيانات، وله كيان مادي يتكون من: وحدات الإخراج، وحدة الذاكرة الرئيسية، وحدة الإدخال، وحدة الحساب والمنطق، وحدة التحكم، وحدات التخزين الثانوية، وتشمل كل وحدة من هذه الوحدات على مجموعة من المفردات المعلوماتية.

أما بخصوص الكيان المعنوي، فإنه يشمل البرمجيات الجاهزة والبيانات والمعلومات المنطقية.

وفيما يتعلق بقابلية المكونات المادية للحاسوب للتفتيش، فإن الولوج إلى المكونات المادية للحاسب الآلي يخضع للإجراءات القانونية الخاصة بالتفتيش، أي أنه يجب مراعاة مكان وجود الحاسب أثناء مباشرة التفتيش، فقد يكون في مكان عام أو خاص، كما ان لصفة المكان أهمية خاصة في مجال التفتيش، حيث أنه إذا كان متواجدا في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنه يأخذ حكمه، فلا يجوز تفتيشه إلا في الحالات وبالضمانات التي يجوز فيها تفتيش المسكن، وهي الحصول على الإذن أو الرضاء بالتفتيش من حائزه، ويجب التمييز داخل ذلك المكان بين ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحواسيب الأخرى أم انها متصلة بحاسوب أو بنهاية طرفيه في مكان آخر كمسكن الغير مثلا، ففي هذه الحالة الأخيرة يتعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش تلك الأماكن (10).

أما إذا كانت المكونات المادية للحاسوب متواجدة في أماكن عامة كمحل بيع البرامج، فإن إجراءات التفتيش تخضع للقواعد المقررة الخاصة بتفتيش تلك الأماكن، وذات الشيء يقال إذا كانت المكونات المادية في حوزة شخص سواء كان مبرمجا أو عامل صيانة أو موظفا في شركة تنتج برامج الحاسب الآلي، إذ تطبق حينئذ أحكام تفتيش الشخص وبذات الضمانات.

وفي حالة اتصال حاسب المتهم بنهاية طرفية موجودة في مكان آخر داخل الدولة، فإن البعض (11) يرى أن التفتيش يمكن أن يمتد إلى سجلات البيانات التي تكون في موقع آخر، خاصة إذا كانت البيانات الخاصة به ضرورية لإظهار الحقيقة.

أما في حالة اتصال حاسب المتهم بنهاية طرفية موجودة في مكان آخر خارج الدولة، فإن التشريع الهولندي ينص على إمكانية تفتيش نظم الحاسب الآلي المرتبطة حتى ولو كانت موجودة في دولة أخرى، لكن بشرط أن يكون هذا التدخل مؤقتا وأن تكون البيانات محل التفتيش لازمة لإظهار الحقيقة حسب ما نصت عليه المادة 01/125 من الاتفاقية الأوروبية لجرائم الانترنت.

لكن قد نجد أن البعض يتحفظ على هذا الاتجاه، وحجته في ذلك أن تفتيش نظم الحاسب الآلي المرتبطة والموجودة في دولة أجنبية يعتبر انتهاكا لسيادة الدولة الأجنبية (12).

أما بالنسبة للاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، فنجد أنها سايرت التشريع الهولندي من خلال نصها في المادة 26 على إمكانية تفتيش المعلومات المخزنة، وأكدت على ضرورة تبني مجموعة من الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية

معلومات معينة أو جزء منها، وهذا إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها، وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الولى، فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.

ج- وفيما يتعلق بالسلطة المختصة بالتفتيش: فهي من اختصاص النيابة العامة، والتي يمكن لها أن تندب إما عون او ضابط الشرطة القضائية في هذا الشأن، مع مراعاة قواعد الاختصاص المكاني والنوعي.

- وبخصوص التفتيش في بيئة الانترنت بناءا على القبض على الأشخاص، فإننا نتعرض فيه لحالتين هما:

- الحالة الأولى: وجود أجهزة استدعاء إلكترونية في حوزة الشخص المقبوض عليه، وفي هذه الحالة تسمح المحاكم إما لعون أو ضابط الشرطة القضائية بالاطلاع على هذا الجهاز (13).

- الحالة الثانية: وجود أجهزة تخزين إلكترونية تحتوي على معلومات أكثر من جهاز الاستدعاء في حوزة الشخص المقبوض عليه، وفي هذه الحالة يرى البعض (14) أنه بالقياس على الأشياء المادية، فإنه يجوز لعون أو ضابط الشرطة القضائية تفتيش نظائرها الالكترونية، وهذا بدون استصدار إذن.

وعليه يقصد بشخص المتهم المعلوماتي كمحل للتفتيش: " تحسس جسمه وملابسه وفحصه بدقة وإخراج ما يخفيه فيه من محصلات جريمة الانترنت، وإذا كانت معه أمتعة جاز تفتيشها بحثا عن أجزاء تتعلق بوحدات معلوماتية محل البحث، سواء أكانت بين يديه أو كانت في سيارته" (15).

- التفتيش في بيئة الانترنت بناءا على حالة التلبس بالجريمة: لما كانت جرائم الانترنت كغيرها من الجرائم يمكن أن تتوافر فيها شروط الجريمة المتلبس فيها، كان من الجائز لعون أو ضابط الشرطة القضائية تفتيش شخص المشتبه فيه، وما قد يحمله من حاسوب نقال أو هاتف محمول، ولكن لا يجوز له تفتيش مسكنه، وما به من موجودات من بينها الحاسب الآلي، فلقد سبق وأن قضت المحكمة الدستورية العليا المصرية بعدم دستورية المادة 47 من قانون الإجراءات الجنائية المصري التي كانت تجيز تفتيش المساكن في حالة التلبس.

وبالتالي فمن مظاهر التفتيش في حالة التلبس أن يكون عون أو ضابط الشرطة القضائية في أحد مقاهي الانترنت يمارس هوايته في الإبحار عبر شبكة الانترنت، ويشاهد شخص آخر يعبر أحد المواقع العسكرية للدولة بالشبكة، ويقوم بطباعة مجموعة من الصور للأماكن الموجود فيها السلاح، ففي هذه الحالة نجد أن حالة التلبس تتحقق ويكون لعون أو ضابط الشرطة القضائية أن يقوم بإلقاء القبض على هذا الشخص وتفتيشه (16).

كما يجوز تفتيش المتهم بناءا على رضائه، وهذا كما لو قام أحد مستخدمي الانترنت بترديد عبارات أمام عون أو ضابط الشرطة القضائية تفيد بأنه مشترك بالبريد الالكتروني مع أحد الأشخاص الناشطين في تنظيم إرهابي معين، وأنه يتبادل معه الرسائل الالكترونية في كل ما يتعلق بنشر أفكار ومبادئ هذا التنظيم الإرهابي، فيطلب منه عون أو ضابط الشرطة القضائية أن يقوم بتفتيش جهازه، فإن وافق فإن التفتيش والضبط يكون صحيحا.

ويرى البعض كذلك (17) أنه يمكن إجراء التفتيش من خلال الجهاز الموجود بمكتب عون أو ضابط الشرطة القضائية، وهو ما يطلق عليه التفتيش على المباشر، وفي النهاية فإنه يجب تحرير محضر يثبت فيه ما تم من إجراءات بصدور التفتيش، وما أسفر عنه من أدلة، ويجب أن يكون هناك شخص متخصص في الشبكات الالكترونية

يصاحب من يقوم بإجراء التفتيش، وهذا من أجل الاستعانة به في مجال الخبرة الفنية، وفي صياغة مسودة محضر التفتيش.

المحور الثالث: ضبط الأدلة الرقمية.

أولا: معنى الضبط في البيئة الرقمية.

إن الدليل الرقمي هو عبارة عن معطيات مخزنة في نظام إلكتروني يمكن استخدامها في قضية ما.

وبالتالي، فإن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها، ويقصد بالضبط وضع اليد على شيء يتصل بالجريمة التي وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبيها، والضبط لا يرد إلا على الأشياء المادية دون القيم المعنوية، وفي هذا الصدد يرى البعض أن الضبط لا يرد على الأدلة الرقمية لانتفاء الكيان المادي عنها، وبالتالي لا يتم ضبطها إلا إذا تجسدت في دعامة مادية، كما لو كانت مطبوعة في مخرجات الحاسوب أو في أي وعاء آخر بالبيانات كالأسطوانة الليزيرية أو على فلاشه (18).

في حين يرى البعض الآخر أنه لا مانع من ورود الضبط على البيانات الالكترونية (19).

أما الاتجاه الثالث، فيدعو المشرع للتدخل لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط، وهذا لتشمل إلى جانب الأشياء المادية البيانات الالكترونية.

وعليه يمكن تعريف الضبط في البيئة المعلوماتية بأنه وضع اليد على الدعائم المادية المخزنة فيها البيانات الالكترونية التي تتصل بالجريمة المعلوماتية (والتي منها جريمة الإرهاب الالكتروني)، وإن كانت الصعوبة تتمثل في عدم إمكانية وضع اليد على شبكات المعلومات الدولية، وهذا لأنها لا تخضع لسيطرة شخص معين، ولا تعمل في إطار دولة معينة.

ثانيا: الإشكالات التي يثيرها ضبط البيانات الالكترونية المتحصل عليها من التفتيش.

إن ضبط البيانات الالكترونية المتحصل عليها من التفتيش الناجم عن التحقيق في جرائم الإرهاب المعلوماتي يمكن أن يطرح عدة إشكالات للنقاش والتحليل تتمثل فيما يلي:

- الإشكال الأول: إنه ووفقا للمادة 45 في فقرتها الأخيرة من قانون الإجراءات الجزائية الجزائري المعدل والمتمم أنه لا يجوز لضابط الشرطة القضائية الاطلاع على الأوراق والمستندات قبل حجزها، وهذا إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم الإرهاب، وبالتالي فإن التساؤل يثور لمعرفة مدى سريان القيود الخاصة بضبط تلك الوراق على ضبط البيانات الالكترونية المتحصل عليها من تفتيش حاسوب المتهم المرتكب لجريمة الإرهاب المعلوماتي؟

وبالتالي نجيب على هذا التساؤل بالإيجاب لسببين هما:

– السبب الأول: أن العلة التي اقتضت حظر الاطلاع على الأوراق المكتوبة أو المستندات المغلقة تتوفر بالنسبة لمحتوى نظام المعالجة الآلية للبيانات، وهذا لأن الغلق والتغليف بالنسبة لتلك الوراق يضفي عليها مزيدا من السرية، ويفصح عن رغبة صاحبها في عدم إطلاع الغير على مضمونها بغير إذن، وهو ما يتحقق

بالنسبة للبيانات المخزنة في نظام معلوماتي، وهذا لأن محتواها لا يكون مكشوفا للغير، حيث لا يمكن الوصول أو الاطلاع عليها إلا بمعرفة كلمة السر أو الشفرة.

– السبب الثاني: هو أن المادة 45 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم ترسي قاعدة عامة وضمانة بالنسبة للأسرار التي تتضمنها سائر وسائط وأوعية حفظ وتخزين المعلومات، سواء ما كان منها تقليديا كالأوراق، أو مستحدثا كالأقراص المرنة والأشرطة الممغنطة والذاكرات الداخلية للحاسبات والفلاشة، ومتى توفر الغلق في تلك الأوعية كإحاطة محتوياتها بسياج أمني كالتشفير مثلا، فإنه لا يكون لعون أو ضابط الشرطة القضائية إزالة ذلك السياج سواء بنفسه أو بمعاونة أهل الخبرة للاطلاع على محتوياتها.

– الإشكال الثاني: يتعلق بتمتع المتهم بحق الصمت والامتناع عن الإجابة على الأسئلة الموجهة إليه، وعون أو ضابط الشرطة القضائية يحتاج عادة في شبكة المعلومات أو الحاسبات التي يتعامل معها إلى معرفة معلومات معينة حول بعض المسائل التي من شأنها تسهيل مهمته في التفتيش والضبط، كمعرفة نظام إدارة قواعد البيانات أو فك الشفرة، وبالتالي فهل يجوز للمتهم أن يمتنع عن الإدلاء بهذه المعلومات ويتمسك بحقه في الصمت؟

القاعدة العامة أنه لا يجوز إجبار المتهم على تقديم دليل إدانته، وهذا بإرغامه على الكشف عن كلمات السر أو الشفرة التي تمكن من الدخول إلى المعلومات المخزنة للحاسب الآلي أو الكشف عن مخرجات المعلومات.

وعلى خلاف ذلك يمكن إكراه غير المتهم على تقديم تلك المعلومات بالتعاون مع سلطات الضبط والتحقيق، وهذا كإلزام مقدم الخدمات بتقديم كلمة السر لعون أو ضابط الشرطة القضائية حتى يتمكن من تحديد المصدر أو مكان الوصول للاتصالات السابقة (20)، وبالتالي للتعرف على الأشخاص المشتبه فيهم والذين قاموا على سبيل المثال بتوزيع منشورات عدائية أو عقائدية ودينية تحرض على ارتكاب ما يسمى بجرائم الإرهاب الالكتروني.

- الإشكال الثالث: إذا كان قانون الإجراءات الجزائية الجزائري المعدل والمتمم قد أورد نصوص تجيز ضبط الرسائل والبرقيات، فهل تطبق أحكام هذه النصوص على المراسلات الالكترونية المستحدثة كالبريد الالكتروني؟

يقصد بالبريد الالكتروني:" جميع تقنيات الاتصال التي تقوم بتناقل المعلومات عبر الوسائل الالكترونية مثل:

– التيلتيكس أو نقل النصوص عن بعد.

– الفاكس ملي أو الناسخ الهاتفي.

– الفيديو تكس المتفاعل أو الفيوداتا.

– المحطات الطرفية أو الطرفيات التي تكون بشأن حاسبات ما يكرويه، أو بشكل محطة طرفية متسقة أو مرتبطة بذاكرة " (21).

ويتميز البريد الالكتروني عبر البريد العادي بالسرعة في نقل المعلومات وقلة التكاليف، ومع ذلك توجد هناك أوجه تشابه بينهما تتمثل في:

أن التعامل مع الرسالة الالكترونية لا يختلف عن التعامل مع الرسالة الورقية، إذ بمقدور المستخدم أن يطرحها جانبا أو يرد عليها أو ينقلها إلى شخص آخر أو يحفظها في حقل خاص، كما يتشابهان كذلك في عملية حفظ البريد، إذ بمقدور المستخدم أن يحفظ بريده الالكتروني بأحد الطرق الآتية:

- الحفظ في صناديق بريد خاصة.
- الحفظ في ملفات.
- طباعة الرسائل وحفظها في ملفات خاصة مع البريد الورقي التقليدي.

وعلى ذلك، فإن هناك من يرى أن مخرجات الحاسب الآلي تعتبر من قبيل المستندات المطلوبة، وذلك مسايرة منا للتقدم التقني الذي تجاوز المفهوم التقليدي للمستند باعتباره مجرد ورقة مطلوبة، ومن هذا الاتجاه نجد قانون العقوبات الفنلندي المعدل، والذي ماثل بين مخرجات الحاسوب والمستندات الورقية التقليدية.

ولكي يتم ضبط الرسائل الالكترونية المشكوك فيها، فعلى المحقق اختيار صندوق البريد الخاص بالمتهم محل التفتيش، فإذا كان يريد ضبط الرسائل الالكترونية الواصلة، كان عليه أن يختار خانة الرسائل الواردة، وإذا كان يريد ضبط الرسائل التي أرسلها المتهم، كان عليه أن يختار خانة الرسائل الصادرة، وفي حالة ما إذا كان يريد ضبط رسالة كان قد ألغاها المتهم من قبل، فعليه اختيار ملفات الحفظ أو سلة المهملات، وله في كل هذه الحالات طباعة الرسائل مع الأخذ في الاعتبار أحكام المادة 217 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم (22).

- الإشكال الرابع: يتعلق بالأشياء التي يتم ضبطها من خلال الشبكات الالكترونية، وكيفية المحافظة على الأدلة من التلف.

بالنسبة للأشياء التي يتم ضبطها من جراء التفتيش في جرائم النت، يعتبر ضبط الحاسوب كوسيلة لارتكاب الجريمة من أهم وسائل الضبط، بالإضافة إلى النسخ بإحدى أساليب الضبط المستخدمة في حالة عدم إمكانية ضبط القطع الصلبة المتضمنة للمواد غير المشروعة (23).

وهناك أسلوب آخر للضبط يتمثل في تجميد التعامل بالحاسوب أو إحدى القطع المكونة له، والتي استخدمت في ارتكاب الجريمة، وهذا مثل القرص الصلب، مع ملاحظة أن هذا الأسلوب من الضبط يصلح أن يتخذ في مواجهة الخوادم التي قد تحتوي على حلقات نقاش تدعو إلى الانضمام لتنظيمات إرهابية، كما يصلح إذا كان القرص الصلب المتضمن للمواد غير المشروعة مثلا يحتوي على ملفات مشفرة تحتاج إلى فك شفرتها، أو أن يحتاج الدخول إلى الحاسوب إلى كلمة مرور، أو أن تقوم بالحاسوب برمجية تسمح بمحو محتويات القرص الصلب عن بعد.

أما فيما يتعلق بتحريز المضبوطات المعلوماتية وتأمينها فنيا، فإنه من الضروري أن يكون المحقق في جرائم الإرهاب الالكتروني مؤهلا ومدربا على التعامل مع تلك الأدلة، وإلا فإن خطئه يؤدي إلى ضياع الأدلة، ولذلك فإن تأمين الأدلة وصيانتها من العبث يقتضي اتخاذ الإجراءات الآتية:

1–ضبط الدعائم الأساسية للبيانات وعدم الاختصار عن ضبط نسخها.

2–عدم ثني القرص، وهذا لأن ذلك قد يؤدي إلى تلفه وما عليه من معلومات.

3–عدم تعريض الأقراص والأشرطة الممغنطة لدرجة حرارة عالية ولا للرطوبة.

4–عدم تعريض الأقراص للأتربة.

5–عدم الضغط على الأقراص، وعدم الكتابة عليها بالقلم، لأن ذلك قد يفسد سطح القرص.

الخاتمة:

بناءا على ما تقدم ذكره في خضم محتوى هذه الورقة البحثية يتبين لنا أن وسائل الإثبات التقليدية في قانون الإجراءات الجنائية، لا تكفي لمواجهة الإرهاب الإلكتروني أو غيره من الجرائم التي قد ترتكب من خلال شبكة المعلومات الدولية.

وترجع صعوبة الإثبات حسب نظرنا، وبصفة خاصة للأسباب الآتية:

1 - صعوبة محو الدليل عن بُعد، وبالتالي إخفاء معالم الجريمة والتخلص من آثارها، الأمر الذي يؤدي إلى صعوبة التحقيق في هذه النوعية من الجرائم وتتبع مرتكبيها والقبض عليهم.

2- الحرفية الفنية العالية التي تتطلبها جرائم الإنترنت من أجل الكشف عنها، وهذا ما يعرقل عمل المحقق الذي تعود التعامل مع الجرائم التقليدية.

3 - تعتمد جرائم النت على التضليل في التعرف على مرتكبيها، وهذا لأنهم يعتمدون على التخفي عبر ضروب الإنترنت تحت قناع فني، كما تعتمد هذه الجرائم على قمة الذكاء والمهارة في ارتكابها.

4 - يلعب البُعد الزمني والمكاني والقانوني دورا مهما في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم.

5 - إن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسوب متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.

6 - يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود.

7- صعوبة اكتشاف جرائم الإرهاب الإلكتروني، ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم.

8- صعوبة الإثبات الجنائي في الإرهاب الإلكتروني، نظراً لسرعة غياب الدليل الرقمي، وسهولة إتلافه وتدميره.

9- يتميز الإرهاب الإلكتروني بأنه يجري عادة بتعاون أكثر من شخص على ارتكابه.

9–أن مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسوب والشبكة المعلوماتية .

التوصيات:

1. حجب المواقع الالكترونية المشبوهة التي تسعى إلى نشر الإرهاب والأفكار المتطرفة، وتلك المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء على الآخرين.

2. تفعيل الدور الوقائي الذي يسبق وقوع جريمة الإرهاب الالكتروني، وذلك من خلال تفعيل دَور المؤسسات التوعوية (المسجد، الأسرة، دُور التعليم، أجهزة الإعلام)، وذلك من خلال التوعية بخطورة هذه الجرائم على الأسرة والمجتمع، والسعي في تقوية الوازع الديني.

3. سَنّ القوانين والتشريعات الخاصَّة التي تسدُّ كافَّة الثغرات التي تكتنف جريمة الإرهاب الالكتروني أو سبل التحقيق فيها، كالقوانين المتعلقة بكيفية اكتشاف الأدلة الإلكترونية، وحفظها، والأدلة التي تقبل الإثبات قانونا.

4. تنسيق وتوحيد الجهود بين الجهات المختلفة في الدولة: التشريعيّة، والقضائيّة، والضبطية، والفنية، وذلك من أجل سد منافذ جريمة الإرهاب الالكتروني قدر المستطاع، والعمل على ضبطها وإثباتها بالطرق القانونية والفنيّة.

5. إيجاد منظومة قانونية دولية متكاملة تحت مظلة منظمة الأمم المتحدة يعهد إليها توثيق وتوحيد جهود الدول في مكافحة ومواجهة الإرهاب الالكتروني، ويتفرع منها جهة أو هيئة محايدة تتولَّى التحقيق في هذه الجرائم، ويكون لها سلطة الأمر بضبط وإحضار المجرم للتحقيق معه أياً كان مكان وجوده وجنسيته وبلده.

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

7. تعزيز التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية التخريبية الإلكترونية الواقعة في أراضيها ضدّ دول أو جهات أخرى خارج هذه الأراضي.

الهوامش والمراجع:

(1)- أنظر: نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات " دراسة مقارنة "، دار الفكر الجامعي، 2007، ص: 217.

(2)- أنظر: جميل الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، مصر، 2002، ص: 29.

(3)- أنظر: عمر أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، مصر، 2004، ص: 859.

(4)- أنظر: عمر أبو بكر بن يونس، نفس المرجع، ص: 896.

(5)- أنظر: محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، المجلة العربية للدراسات الأمنية والتدريب، العدد الثلاثون، أكاديمية نايف العربية للعلوم المنية، السعودية، 2000، ص: 114.

(6)- أنظر: هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية " دراسة مقارنة "، مكتبة الآلات الحديثة، أسيوط، مصر، 1994، ص: 680.

(7)- أنظر: عمر أبو بكر يونس، المرجع السابق، ص: 865.

(8)- أنظر: سامي حسين الحسيني، النظرية العامة للتفتيش في القانون المصري والقانون المقارن، دار النهضة العربية، القاهرة، مصر، 1972، ص: 210

(9)- أنظر: هشام محمد فريد رستم، المرجع السابق، ص: 690.

(10)- أنظر: نبيلة هبة هروال، المرجع السابق، ص: 237.

(11)- أنظر: هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي " دراسة مقارنة "، ط1، دار النهضة العربية، القاهرة، مصر، 1997، ص: 88.

(12)- أنظر: هلالي عبد اللاه أحمد، نفس المرجع، ص: 78.

(13)- أنظر: عمر أبو بكر يونس، المرجع السابق، ص: 109.

(14)- أنظر: عمر أبو بكر يونس، المرجع السابق، ص: 111.

(15)- أنظر: هلالي عبد اللاه أحمد، نفس المرجع، ص: 157.

(16)- أنظر: نبيلة هبة هروال، المرجع السابق، ص: 248.

(17)- أنظر: سهير عثمان عبد الحليم، الإرهاب والانترنت" دراسة حالة في ضوء التجربة المصرية "، ورقة عمل مقدمة إلى المؤتمر الدولي الأول حول: حماية أمن المعلومات والخصوصية في قانون الانترنت "، المنعقد في القاهرة خلال الفترة الممتدة من 02 إلى 04 يونيو 2008، ص: 15.

(18)- أنظر: هشام محمد فريد رستم، المرجع السابق، ص: 94.

(19)- أنظر: هشام محمد فريد رستم، المرجع السابق، ص، ص: 95، 96.

(20)- وهذا ما نصت عليه المادة 17 من الاتفاقية الأوروبية لجرائم الانترنت بقولها: -

1- من أجل ضمان التحفظ على البيانات المتعلقة بالمرور في تطبيق المادة 16، يجب على كل طرف اتخاذ الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل:

أ- التأكد على أن التحفظ العاجل لهذه البيانات المتعلقة بالمرور تتوافر بعض النظر عما إذا كان هناك مقدم خدمة واحد أو عدة مقدمين للخدمة قد ساهموا في نقل الاتصال.

ب- ضمان الإفشاء السريع للسلطة المختصة للطرف أو للشخص المعين من قبل هذه السلطة عن كمية بيانات مرور كافية، تسمح بتحديد هوية مقدمي الخدمات والطريق الذي تم الاتصال من خلاله ".

(21)- أنظر: ربح مصطفى عليان، البريد الالكتروني، مجلة الأمن والحياة، العدد 234، س21، 2003، ص: 66.

(22)- أنظر: تنص المادة 217 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم على ما يلي: " لا يستنبط الدليل الكتابي من المراسلة المتبادلة بين المتهم ومحاميه ".

(23)- أنظر: عمر أبو بكر بن يونس، المرجع السابق، ص، ص: 71، 72.