١

البحث والتحقيق الجنائي في الإرهاب الإلكتروني
في القانون البحريني المقارن

إعداد دكتور

محمود صالح العادلي

أستاذ القانون الجنائي

كلية الحقوق - جامعة البحرين

نشر هذا البحث بدعم من

عمادة البحث العلمي بجامعة البحرين

مقدمة

- **مدخل الدراسة :**

مع بزوغ فجر التكنولوجيا الحديثة تم ميلاد علم جديد هو علم البحث الجنائي الرقمي . فالاستخدام غير المشروع لآليات وتقنيات التزاوج الذي تم بين تكنولوجيا الاتصالات وتكنولوجيا الكمبيوتر الحاسب الآلي هو الدافع المحرك لميلاد هذا العلم الذي يهتم بالآثار الرقمية الجنائية التي يتركها المتهم إذا ما استخدم الكمبيوتر أو الشبكة العالمية للمعلومات أو الإنترنت فهو علم يبحث إذن في مسرح الجريمة الرقمي.

وإذا كان البحث والتحقيق الجنائي في مجال الجريمة الرقمية – بوجه عام يصادف مخاطر وتحديات جمة ، فإن الأمر يزداد صعوبة فيما يتعلق بالإرهاب الإلكتروني نظرا لأنه مرتكبيه – في الغالب الأعم – يرتكبون جرائمهم من خلال تنظيم إرهابي مما يدخل في نطاق الجرائم المنظمة .

- **تساؤلات الدراسة :**

وفي واقع الأمر وحقيقته أن البحث والتحقيق الجنائي في الإرهاب عبر الفضاء الإلكتروني تكتنفه الكثير من الصعوبات والمخاطر والتحديات ، ولعل سر هذه الصعوبة يكمن في ذوبان فكرتي المكان والزمان في الجرائم الإلكترونية، فمحل وقوع الجريمة يصعب تحديده ، وكذا زمان وقوعها ، كما أن المجرم المعلوماتي يتميز بقدرات فنية وذهنية تجعله يفلت من العدالة بسهولة ، زد على ذلك أن تكنولوجيا المعلومات تتيح لمرتكبي الجرائم الإلكترونية بوجه عام –والإرهابية بصفة خاصة – طمس الأدلة الجنائية الرقمية التي يمكن أن تثبت اقترافهم هذه الجرائم .

ومن هنا تبرز بوضوح عدة أسئلة ، هي :

١. هل النصوص أو القواعد القانونية التقليدية في البحث الجنائي والتحقيق الجنائي كافية بذاتها لمواجهة الإرهاب الإلكتروني ؟ .
٢. وإذا كانت الإجابة بالنفي ، هل يمكن تعديل أو تطويع هذه القواعد التقليدية لتمتد مظلتها لتغطي المواجهة الإجرائية للإرهاب الإلكتروني ؟ أم أن الأمر يفرض إيجاد نصوص قانونية أو قواعد قانونية جديدة تتيح للقائمين على البحث والتحقيق الجنائي المرونة الكافية للقيام بمهامهم ووظائف في البحث والتحقيق الجنائي ؟.

- **أهداف الدراسة :**

وتهدف هذه الدراسة إلى تحديد المفاهيم الرئيسية للبحث الجنائي الرقمي وكيفية استخلاص دليل رقمي يمكن استخدامه في مجال الإثبات أمام أجهزة العدالة الجنائية وتحديد طرق جمع واستخلاص وتحقيق الأدلة الرقمية .

- **أهمية الدراسة :**

تكمن أهمية البحث في أنه يقدم دراسة نظرية وعملية عن البحث والتحقيق الجنائي في مجال الجرائم الإرهابية التي ترتكب عبر الفضاء الإلكتروني ، بحسبان أن هذه الجرائم من أخطر – إن لم تكن أخطر على الإطلاق – جرائم العصر .

- **محددات و مصطلحات الدراسة :**

تدور هذه الدراسة في فلك مصطلحات قانونية عدة من أهمها ما يلي : الإرهاب الإلكتروني ، العلوم الجنائية للحاسب الآلي ، الاستخبارات الجنائية البحث الجنائي الرقمي ، التحقيق الجنائي الرقمي ، الدليل الرقمي .

- **مشكلات الدراسة :**

وتنبع المشكلات الإجرائية الجنائية ـ في مجال مكافحة الإرهاب عبر الفضاء الإلكتروني – من كون أنها تتصل – في الغالب الأعم ـ ببيانات معالجة إلكترونياً وكيانات منطقية غير مادية. الأمر الذي يصعب معه كشف هذه الجرائم، ويصعب – أو يكاد يستحيل ـ جمع الأدلة بشأنها في بعض الحالات ، كما يواجه التفتيش وجمع الأدلة عوائق كثيرة في هذا المجال، ومما يضاعف من هذه الصعوبات أن التفتيش وجمع الأدلة قد يتعلقان ببيانات مخزنة في أنظمة أو شبكات إلكترونية موجودة بالخارج، كما يثير مسألة الدخول إليها ومحاولة جمعها وتحويلها إلى الدولة التي يجري فيها التحقيق، مشكلات تتصل بسيادة الدولة أو الدول الأخرى التي توجد لديها هذه البيانات.

الأمر الذي يمكن التغلب عليه من خلال التعاون الدولي في مجالات البحث والتفتيش والتحقيق وجمع الأدلة، كما قد يمتد هذا التعاون ليشمل تسليم المجرمين وتنفيذ الأحكام الأجنبية الصادرة في الدعاوي الناشئة عن جرائم الإرهاب عبر الفضاء الإلكتروني.

زد على ذلك أن بعض المجرمين يلجئون إلى تخزين البيانات أو المعلومات المتعلقة بالجريمة بالخارج، مما يصعب إثباتها، كما أن التساؤل يثور حول حرية تدفق المعلومات.

ومما يثار بصدد الإجراءات التي قد تتخذ بمناسبة ارتكاب جريمة إرهابية عبر الفضاء الإلكتروني – خصوصاً بالنسبة لإجراءات التفتيش و الضبط و المصادرة – ضرورة فض الاشتباك بين المصالح المتعارضة ولاسيما مصالح المجتمع في إقامة العدالة من جهة ومصالح الأفراد المتعلقة بحقوقهم وحرياتهم العامة وخصوصا الحرية الفردية وحرمة الحياة الخاصة للأفراد، فعلى المشرع أن يفض هذا التنازع بما يحقق المعادلة الصعبة بين الفاعلية والضمانات ، أي فاعلية الإجراءات المطلوبة للأجهزة الأمنية، وسلطات التحقيق في كشف غموض الجريمة وضبط فاعليها والتحقيق معهم وتقديمهم للمحكمة، وضمانات المتهمين التي تكفل لهم عدم المساس بحقوقهم وحرياتهم إلا لضرورة ، والضرورة تقدر بقدرها.

ومن المشكلات الإجرائية التي تثار بمناسبة الإرهاب الإلكتروني مدى التزام الشهود، أو المشتبه فيهم بكشف الرموز أو الأرقام أو كلمات السر المتعلقة بالبيانات أو البرامج ذات الصلة بالجريمة. كما يثور التساؤل عن مدى حجية المخرجات الإلكترونية في الإثبات، نظرا لطبيعتها الخاصة التي تميزها عن وسائل الإثبات التقليدية [١] .

- **خطة الدراسة :**

وترتيباً على ما تقدم ، فإننا سنعرض لموضوع هذا البحث من خلال ثلاثة مباحث ، هي :

المبحث الأول : في البحث الجنائي في جرائم الإرهاب عبر الفضاء الإلكتروني .

المبحث الثاني : في التحقيق الجنائي في جرائم الإرهاب عبر الفضاء الإلكتروني .

المبحث الثالث :مخاطر وتحديات البحث والتحقيق الجنائي في جرائم الإرهاب عبر الفضاء الإلكتروني.

على أن يعقب ذلك خاتمة تتضمن نتائج البحث وتوصياته .

---

١ للمزيد حول المشكلات الإجرائية للجرائم المعلوماتية بوجه عام ؛ راجع :

Sicber (U.) : Les crimes informatiques et d' autres crimes dans le dommaine de la technologie informatique, Rev. int. dr. pen. 1993, p.291,spec.p.307 et s.

Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age ,by Tom Douglas Brian Loader , Thomas Douglas,1st edition, Routledge, 2000

Digital Evidence and Computer Crime, by Eoghan Casey, 1st edition Academic Pr. 2000.

Criminal Profiling: An Introduction to Behavioral Evidence Analysis,by Brent E. Turvey, Diana Tamlyn, Jerry Chisum , 1 edition , Academic Press Limited 1999.

Fighting Computer Crime: A New Framework for Protecting Information, by Donn B. Parker, 1 edition, John Wiley & Sons 1998.

Information Warfare Principles and Operations, by Edward Waltz 1998.

Cyber Crime: How to Protect Yourself from Computer Criminals by Laura E. Quarantiello, Tiare Publications, 1996.

وانظر أيضاً : د. أحمد ، هلالي عبد اللاه ، تفتيش نظم الحاسب الآلي ، ط١ ، دار النهضة العربية ، القاهرة ١٩٩٧ . ولنفس المؤلف حجية المخرجات الكمبيوترية في المواد الجنائية مصر ، ١٩٩٩. د. رستم ، هشام الجوانب الإجرائية للجرائم المعلوماتية أسيوط مصر، ١٩٩٤.

المبحث الأول

البحث الجنائي في مجال الإرهاب الإلكتروني

- **توطئة :**

قبل أن نعرض للبحث الجنائي في مجال الإرهاب عبر الفضاء الإلكتروني ، يتعين علينا أولاً أن نعرف المقصود بهذا الإرهاب، والمقصود بالعلوم الجنائية للحاسب الآلي . و يقصد بالإرهاب الإلكتروني – أو عبر الفضاء الإلكتروني – كل استخدام للتقنيات الرقمية لإخافة وإخضاع الآخرين. أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية [٢] .

أما العلوم الجنائية للحاسب الآلي فهي فرع من العلوم الجنائية القانونية المتعلقة بالأدلة الجنائية التي يعثر عليها في أجهزة الكمبيوتر والوسائط الرقمية المخزنة للحاسب الآلي والمعروفة أيضا باسم العلوم الجنائية للأجهزة الرقمية Digital Forensics [٣] .

- **التعريف بالبحث الجنائي :**

البحث الجنائي هو مجموعة من الإجراءات والأعمال التي يقوم بها رجال البحث الجنائي ، وهي تستهدف منع ارتكاب الجريمة فضلا عن البحث والتحري عن كافة الجرائم المعلومة والمجهولة وجمع الأدلة والقرائن والشهود والبراهين ، علاوة على اكتشاف الأدوات المستخدمة في ارتكاب الجريمة وكل ما يتعلق بها ، مما قد يؤدي في النهاية إلى ضبط الجناة أو المتهمين وتقديمهم للعدالة لينالوا عقابهم عما اقترفت أيديهم [٤] ، أو بالأحرى لاستيفاء حق الدولة في العقاب .

وبتعبير آخر البحث الجنائي هو : " إدراك مدلولات الآثار المادية وتفسير بعض الوقائع أو السلوكيات والملاحظة وجمع المعلومات التي تدور بين الناس " [٥] ، وبعبارة موجزة البحث

---

٢ راجع : . ويكيبيديا، الموسوعة الحرة ، إرهاب إلكتروني ، ١٦ ديسمبر ٢٠١٤، زيارة ٢٥ ديسمبر ٢٠١٤ : http://ar.wikipedia.org/wiki/%D8%A5%D8%B1%D9%87%D8%A7%D8%A8_%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A .

٣ راجع : ويكيبيديا، الموسوعة الحرة ، علوم جنائية رقمية ، ٣٠ أغسطس ٢٠١٤ ، زيارة ٣٠ ديسمبر ٢٠١٤ : http://ar.wikipedia.org/wiki/%D8%B9%D9%84%D9%88%D9%85_%D8%AC%D9%86%D8%A7%D8%A6%D9%8A%D8%A9_%D8%B1%D9%82%D9%85%D9%8A%D8%A9 .

٤ في هذا المعنى : الغضوري ، بدر محمد عقيد بالشرطة الكويتية ، ١٨ أكتوبر، ٢٠١٢ ،البحث الجنائي التحريات السرية :

http://balghadouri.blogspot.com/2012/10/blog post.html

٥ الدكتور/ إبراهيم ، حسين – التحقيق الجنائي في مواجهة التقنيات والمتغيرات المدنية – مجلة كلية الدراسات العليا – أكاديمية مبارك للأمن – مصر – العدد الثامن – يناير ٢٠٠٣م – ص ٢١٨ . وأنظر أيضاً : الدكتور عبد المطلب ، ممدوح عبد الحميد البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت – دار الكتب القانونية – مصر – ٢٠٠٦م – ص ٢٩ .

الجنائي – أو ما يطلق عليه ـ في بعض الأنظمة القانونية ـ الاستخبارات الجنائية Criminal intelligence عبارة عن المعلومات التي يتم جمعها و/أو تحليلها و/أو نشرها في محاولة لتوقع أو منع أو مراقبة الأنشطة الجنائية [٦] .

وتُعرّف الشرطة العسكرية بجيش الولايات المتحدة الاستخبارات بشكل أكثر تفصيلاً: الاستخبارات الجنائية عبارة عن المعلومات التي يتم جمعها أو فحصها أو تحليلها أو تسجيلها/رفع تقارير بها ونشرها من خلال وكالات فرض القانون فيما يتعلق بأنواع الجرائم والمجرمين المحددين والمجموعات الجنائية المعروفة أو المشتبه بها [٧] [٨] .

- **البحث الجنائي قبل وبعد وقوع الجريمة :**

البحث الجنائي يدور في فلك الجريمة ، فهو يسبق وقوعها بالفعل ، كما أنه يتحرك بفاعلية أكثر بعد وقوعها بالفعل .

- **أ البحث الجنائي قبل وقوع الجريمة:**

يهدف البحث الجنائي في هذه المرحلة :

١ـ التقليل من فرص ارتكاب الجريمة، من خلال اتخاذ تدابير ترمي إلى منع وقوع الجريمة .

٢ـ زيادة الوعي الأمني لدى الجمهور، الأمر الذي قد يدفعهم إلى اتخاذ إجراءات وقائية أو بالأحرى تتسم بالحيطة والحذر .

---

٦ في هذا المعنى :

Department of Justice DOJ , National Criminal Intelligence Sharing Plan 2003 . Retrieved fromhttp://www.fas.org/irp/agency/doj/ncisp.pdf

International Association of Chiefs of Police IACP Criminal Intelligence Sharing: A National Plan for Intelligence Led Policing At the Local, State and Federal Levels 2002 .

Retrieved from : http://www.ncirc.gov/documents/public/supplementaries/intel_sharing_report.pdf

٧ في هذا المعنى :

Field Manual FM 3 19.50 Police Intelligence Operations 2006 . Retrieved fromhttps://rdl.train.army.mil/soldierPortal/atia/adlsc/view/public/22739 1/FM/3 19.50/chap4.htm;jsessionid=2Dp2J7GTSyJPCJpXR821z1Mvh17s0z9VsGLgtBMJLwv2DTyngKbZ!99557122

٨ للمزيد حول هذا الموضوع ؛ راجع :

Criminal intelligence , Wikipedia, the free encyclopedia ,5 November 2014 , Visit December 30, 2014 ,http://en.wikipedia.org/wiki/Criminal_intelligence .

٣ـ تحقيق التواجد الأمني ، بالشكل الذي يساعد على بث الرهبة في نفوس كل مَنْ تسول له نفسه الإقدام على سلوك إجرامي [٩] .

- **ب مرحلة البحث الجنائي بعد وقوع الجريمة:**

تستهدف هذه المرحلة : كشف غموض الجريمة ، من خلال إجراءات متعددة منها : معاينة مسرح الجريمة ، وجمع الآثار المادية ، والتحفظ على المشتبه بهم وشهود الواقعة ، والربط بين الوقائع والأحداث السابقة أو المعاصرة أو اللاحقة على الجريمة، والترتيب المنطقي وإعمال العقل لكشف الغموض الذي يكتنف الجريمة [١٠] .

- **البحث الجنائي والإرهاب عبر الفضاء الإلكتروني :**

والبحث الجنائي في جرائم الإرهاب عبر الفضاء الإلكتروني بنوعيه – أي السابق على ارتكاب الجريمة واللاحق لها – له طبيعته الخاصة التي تجعل إجراءاته تختلف كثيراً أو قليلاً – بحسب الأحوال – عن تلك الإجراءات في الجرائم التقليدية ؟

ومن هنا نستطيع أن نقول بأن القواعد الإجرائية الجنائية التقليدية للبحث الجنائي لمواجهة الإرهاب عبر الفضاء الإلكتروني غير كافية لمواجهة جرائم الإرهاب عبر الفضاء الإلكتروني . ولقد كان المجتمع الغربي سباقاً في ذلك ، حيث ظهرت هناك علوم جديدة تتعلق بالطب الشرعي الإلكتروني وغيره من العلوم التي أفرزت مجموعة من القواعد الفنية والإجرائية القانونية التي تسهل على المحقق طريقه للوصول للحقيقة أو الحصول على دليل . وصدرت قوانين عدة لتواجه هذا النوع من الجرائم .

ولما كان الإرهاب الإلكتروني يمثل خطورة على المجتمع الداخلي والخارجي في آن واحد ، كما أن الجرائم الإرهابية الإلكترونية يسهل ارتكابها ، كما أن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، علاوة عن أن آثار الجريمة يمكن محوها بسهولة وإتلاف أدلتها حيث يلجأ مرتكبي هذه الجرائم إلي محو آثار جرائمهم ، وخصوصاً في مجال الجريمة المنظمة كما أنهم يلجئون إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية في أنظمة الكترونية مع استخدام شفرات أو رموز سرية لإخفائها عن أعين أجهزة العدالة، الأمر الذي يثير مشكلات كبيرة في جمع الأدلة الجنائية وإثبات هذه الجرائم في حقهم .

- **١٤ـ تقسيم :**

ولما كانت إجراءات الانتقال لمسرح الجريمة و المعاينة والضبط – وهي إجراءات متداخلة بشكل أو بآخر – في مرحلتي البحث الجنائي والتحقيق الجنائي ، فإننا سنرجئ الحديث عنها –

---

٩ قرب هذا المعنى : د. عبد المطلب ، ممدوح عبد الحميد مرجع سابق – ص ٢٩ .

١٠ للمزيد حول هذا الموضوع ؛ راجع : المرجع السابق – ص ٣٤ وما بعدها .

ومعها إجراء التفتيش للمبحث الثاني من هذه الدراسة ، وسنكتفي هنا بعرض موضوعين : الأول هو ضرورة القائمون على البحث الجنائي والإلمام بأنظمة الحاسب الآلي والتعامل مع الإنترنت ، والثاني يتعلق بالحث الجنائي والوقاية من الإرهاب عبر الإنترنت ، وسنخصص لكل موضوع مطلب مستقل .

المطلب الأول

القائمون على البحث الجنائي والحاسب الآلي والإنترنت

- **خصائص جرائم الإرهاب عبر الفضاء الإلكتروني والحاسب الآلي والإنترنت:**

إذا كانت الجرائم ذات الصلة بالحاسب الآلي تتسم بخصائص عدة من أبرزها : حداثة أساليب ارتكابها، وسرعة تنفيذها، وسهولة إخفائها، و دقة وسرعة محو آثارها. فإن الإرهاب الإلكتروني يتسم بهذه الخصائص مجتمعة ، بل أنه قد يتفوق على الجرائم الإلكترونية الأخرى في هذه الخصائص ، نظراً لأنه يصدر – في الغالب الأعم – عن جماعة إرهابية منظمة تخطط بدقة لكل خطواتها .

- **المواجهة الإجرائية والمعرفة بأنظمة الحاسب الآلي:**

لذا فإن المواجهة الإجرائية لهذا الإرهاب يتطلب أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وكيفية تشغيلها، وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها و ضبط الأدوات التي استخدمت في ارتكابها والتحفظ على البيانات أو الأجهزة التي استخدمت في ارتكابها أو تلك التي تكون محلا للجريمة [١١] ، هذا فضلاً عن ضرورة الإلمام بالتعامل مع شبكة الإنترنت ومواقع التواصل الاجتماعي ، مثل الفيس بوك وتويتر ، فضلاً عن طرق اختراق

---

١١ هذا ولقد صادفت أجهزة الشرطة والتحقيق صعوبات جمة في بداية تصديها للجرائم الإلكترونية ، سواء فيما يتعلق بكشف غموضها أم فيما يتصل بإجراءات التفتيش والضبط اللازمين، أم فيما يختص بالتحقيق في هذه الجرائم ؛ ومن هنا ظهرت الحاجة إلى ضرورة إعداد برامج تدريب وتأهيل لرجال الشرطة والمحققين يمكنهم من الوقوف على النواحي الفنية لهذه الجرائم ؛ جدير بالذكر أنه في بداية ظهور هذا النوع من الجرائم، وقعت الشرطة في أخطاء جسيمة أسفر عنها الكثير من الإضرار بالأجهزة أو الملفات، أو الأدلة الخاصة بإثبات الجريمة، ومن الأمثلة التي تضرب في هذا الصدد : ما حدث في الولايات المتحدة الأمريكية ؛ حيث طلبت إحدى دوائر الشرطة هناك من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي حتى تتمكن الشرطة من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، وقد نجم عن ذلك أن تسببت دائرة البوليس بدون قصد في إتلاف ما كان قد سلم لها من الملفات والبرامج . راجع :

الدكتور / رستم هشام : المرجع السابق – ص ٢٩ . وأيضاً الدكتور / عقيدة محمد أبو العلا – التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية – أكاديمية شرطة دبي ، مركز البحوث والدراسات تاريخ الانعقاد: ٢٦ ٢٨ إبريل /نيسان ٢٠٠٣ دبي الإمارات العربية المتحدة – ص ٤ .

المواقع الهاكرز ، وكل ما يفيد في كشفهم للحقيقة ولحصولهم على أدلة تفيد في إثبات الجريمة في الإرهاب عبر الفضاء الإلكتروني .

وحتى يؤتي التدريب ثماره يتعين أن يشتمل على كيفية تشغيل الحاسبات، بعد التعرف على أنواعها ونظمها المختلفة، لاكتساب مهارات ومعارف تتصل ببرمجة الحاسبات، والمعالجة الإلكترونية للبيانات والجرائم التي تقع على الحاسبات، أو تستخدم الحاسبات وسيلة لارتكابها، وأساليب ارتكاب هذا النوع من الجرائم، فضلا عن أمن الحاسبات، ووسائل اختراقها، مع دراسة حالات تطبيقيه لجرائم وقعت بالفعل ، وكيفية مواجهتها .

وهذا ما دفع الكثير من بلدان العالم إلى عقد الدورات التدريبية المتخصصة لكل القائمين على مكافحة جرائم الإرهاب عبر الفضاء الإلكتروني، من رجال الشرطة وأعضاء النيابة العامة، سواء في مراكز تابعة لوزارة الداخلية أو في المراكز المتخصصة التابعة لوزارة العدل، كما هو الحال في أمريكا وانجلترا، وكندا.

- **الخير والشر وأدوات العصر :**

وملاك القول فيما تقدم أن الصراع بين الخير والشر ـ أي بين المجتمع الذي يريد أن يفرض قانون للحياة السلمية بين أفراده وبين الفئة الضالة من المنحرفين والمجرمين والإرهابيين ـ هو في جانب منه صراع بين ذكاء القائمين على تنفيذ القانون وذكاء الخارجين عنه ، بين أدوات القائمين على تنفيذ القانون وأدوات الخارجين عنه ، فإذا كان ذلك كذلك فإن طبيعة جرائم الإرهاب عبر الفضاء الإلكتروني تقتضي تزويد القائمين على نفاذ القانون بمعرفة متميزة بنظم الحاسبات، وكيفية تشغيلها، ووسائل إساءة استعمالها من قبل مستخدميها، ولن تتحقق هذه المعرفة التقنية إلا من خلال تدريب القائمين على أعمال التحري، والمباشرين للتحقيق في مجال الجرائم الإلكترونية.

ولعل ذلك ما دفع البعض إلى المناداة بضرورة وجود شرطة متخصصة، ونيابة متخصصة في هذا المجال [١٢] .

١٢ هذه المعلومة شائعة بين كثير من المراجع والكتابات المتعلقة بهذا الموضوع ؛ ويمكن الرجوع – على سبيل المثال في هذا الشأن إلى : موقع جريدة الوحدة السورية : الجريمة الإلكترونية من أخطر جرائم العصر وأعقدها ٢٠١١/١٠/١٠ – زيارة ٢٠١٥/٥/١ :

http://wehda.alwehda.gov.sy/_archive.asp?FileName=31557433120111009185502

المطلب الثاني
التحريات وكشف غموض الإرهاب عبر الفضاء الإلكتروني

- **البحث الجنائي والوقاية من الإرهاب عبر الفضاء الإلكتروني :**

يثور التساؤل حول مدى جواز قيام السلطات المختصة بالبحث الجنائي أن تتخذ إجراءات وقائية تستهدف منع الإرهاب عبر الفضاء الإلكتروني .

والإجابة على هذا التساؤل - لدينا - بالايجابي ، شريطة إلا تمس هذه الإجراءات الوقائية الحقوق والحريات العامة إلا لضرورة والضرورة تقدر بقدرها .

وتفصيلا لذلك نقول أن من حق السلطات المختصة وقاية المجتمع من الإرهاب عبر الفضاء الإلكتروني من خلال مراقبة الإنترنت، وخاصة وسائل التواصل الاجتماعي.

- **موقف بعض الدول من الإجراءات الاحتياطية لمنع الإرهاب عبر الفضاء الإلكتروني:**

وما نذهب إليه ليس بدعة ، بل هو أمر معمول به في كثير من دول العالم ، بهدف وقاية المجتمع من الجريمة بوجه عام ، والجرائم الإرهابية بصفة خاصة . إذ توجد العديد من الدول حول العالم تستخدم التكنولوجيا في التضييق على الحريات، حيث تمنع مواطنيها من استخدام الإنترنت والوصول لشبكات التواصل الاجتماعي، ومنها من تحجبه عن سكانها وتتيحه لمسئوليها، والبعض الآخر يحجمها ويراقبها عن كثب.

وسنعرض لذلك فيما يلي ، وقد اخترنا بعض الدول الغربية والشرقية والآسيوية ، بجانب دول مجلس التعاون الخليجي ومصر . [١٣]

وذلك على التفصيل التالي :

- **أولاً : الدول الغربية :**

١ ألمانيا :

في ألمانيا كشفت مجلة «دير شبيجل» الألمانية في يونيو ٢٠١٣، أن جهاز المخابرات الألماني يعتزم إنفاق ١٠٠ مليون يورو على توسيع مراقبة الإنترنت، وفي مايو ٢٠١٣م قالت تقارير إعلامية نقلتها كل من صحيفة «زود دويتشه تسايتونج» وشبكتا «إن آر دى» و«دبليو دى آر» التليفزيونيتين الألمانيتين: «إن القطاع الخارجي بأمن الدولة سيراقب مواقع تويتر

---

١٣ أنظر في الموضوع : كساب ، محمد : مراقبة الشبكات الاجتماعية في دول العالم: التكنولوجيا تضيق على الحريات تقرير ، موقع جريدة المصري اليوم ، ٣يونيو ٢٠١٤ ، زيارة ٣٠ ديسمبر ٢٠١٤ :

http://www.almasryalyoum.com/news/details/457780#

وراجع أيضاً: محمد حسن عامر دول العالم تراقب شبكات التواصل.. والمبرر: مواجهة الإرهاب.. بريطانيا: الملكة دافعت عن قانون المراقبة لمواجهة التطرف.. والرقابة مكنت الصين والسعودية من كشف خلايا إرهابية ، ٣ يونيه٢٠١٤ ؛ زيارة ٢٩ ديسمبر ٢٠١٤ ، الموقع الإلكتروني للجريدة الوطن المصرية :

http://www.elwatannews.com/news/details/496671

وفيس بوك وغيرها خلال الزمن الحقيقي، بمعنى الفترة التي يكون فيها رواد هذه المواقع أمام أجهزتهم يمارسون عملية التواصل» [١٤] .

وفي ديسمبر ٢٠١٣، قالت شبكة «دويتشه فيله» الألمانية: «إن وزارة الداخلية الألمانية تسعى لاستثمار ١٣٠ مليون يورو، لزيادة فعالية الرقابة على الإنترنت منعاً للنشاطات الإرهابية التي تتوزع على أكثر من ٤٥٠٠ موقع» .

٢ الولايات المتحدة الأمريكية [١٥] :

كشفت صحيفة «جارديان» البريطانية في تقرير نشر في يونيو من العام الماضي أن: الحكومة الأمريكية أبلغت شركات تكنولوجيا المعلومات والاتصال العالمية سراً، ببرنامج حكومة الولايات الخاص بالرقابة على بعض البيانات على شبكة الإنترنت، ومنها الرقابة الحكومية على المحادثات الخاصة على موقع التواصل الاجتماعي «فيس بوك». والبرنامج يتيح الرقابة على الرسائل القادمة من خارج الولايات المتحدة على خدمات «فيس بوك» و«جوجل».

وفجرت صحيفة «واشنطن بوست» الأمريكية، في أغسطس ٢٠١٣، فضيحة تجسس أمريكية عبر الإنترنت، إذ نشرت تقريراً يكشف أن وكالة الأمن القومي ومكتب التحقيقات الفيدرالي الأمريكي FBI، يتنصتان مباشرة على الحواسيب المركزية الخاصة بتسع من شركات الإنترنت الأمريكية العملاقة، لمواجهة الإرهاب. وأوضحت أنهما– أي الوكالة والمكتب المذكورين- تستخرج بيانات صوتية من خلال الفيديو والدردشة التي تتم بين المستخدمين، والصور، ورسائل البريد الإلكتروني، والاتصالات الهاتفية عبر الإنترنت، وحفظ سجل الاتصالات، مما يتيح لمحللي الاستخبارات الأمريكية مراقبة وملاحقة أهداف أجنبية يشتبه في كونها أهدافاً إرهابية.

٣ بريطانيا :

في أبريل ٢٠١٢ قالت صحيفة «واشنطن بوست» الأمريكية: «إن الحكومة البريطانية ستتقدم بمشروع قانون للرقابة على الرسائل النصية، ومواقع التواصل الاجتماعي، لمواجهة الإرهاب والتهديدات الأخرى في عصر الميديا الاجتماعية وفق مسئولين حكوميين». غير أن بعض المعارضين لمشروع القانون، وفقاً للصحيفة، رأوا أنه «ربما يجعل بريطانيا تتجاوز أيران في الرقابة على الإنترنت». [١٦]

---

١٤ راجع : عامر ، محمد حسن مرجع سابق .

١٥ أنظر في الموضوع : عامر ، محمد حسن مرجع سابق .

١٦ المرجع السابق .

- **ثانياً : الدول الشرقية والآسيوية :**

١ آسيا الوسطى :

تسود الرقابة على الإنترنت في دول آسيا الوسطى، خاصة في جمهوريات الاتحاد السوفيتي المجاورة لإيران، مثل «تركمانستان، أوزبكستان، طاجيكستان»، حيث تحظر الشبكات الاجتماعية وتراقب المواقع حماية للدولة وأنظمة الحكم [١٧] .

٢ كوبا :

تفرض كوبا رقابة مشددة على الإنترنت وترفع تكاليف استخدامه، ولا يمكن الوصول للإنترنت إلا لحوالي ٥ ٪ فقط من السكان، ويستخدم ٢٣٪ آخرون «إنترنت الحكومة»، ولا يمكن الوصول للإنترنت إلا في المرافق العامة بشرط تسجيل هوية مستخدميه [١٨] .

٣ الصين [١٩] **:**

هناك أكثر من ٥٠٠ مليون مستخدم صيني للإنترنت، لكنهم يتعاملون مع الرقابة المفروضة على شبكات التواصل عن طريق خوادم الـ«بروكسي». وتراقب السلطات وسائل الإعلام الاجتماعية المحلية وتتبع المحتوى الإباحي أو «التخريبي» و«السياسي» وتحذفه.. وتحظر العديد من المواقع، بما في ذلك «يوتيوب، فيس بوك، تويتر، نيويورك تأيمز». ففي يوليو ٢٠٠٩ حجبت «فيس بوك» بعد اشتباكات بين الشرطة ومواطنين في مدينة «أورماتشي». وتفرض الصين منذ ذلك الوقت رقابة صارمة على مواقع التواصل الاجتماعي بعد أن بدأت مجموعات إرهابية تنشر فيديوهات لكيفية صنع متفجرات [٢٠] .

وفي ديسمبر ٢٠١١، أصدرت السلطات الصينية قواعد جديدة تفرض على مستخدمي مواقع التدوين المصغرة «ميكروبلوجز» تسجيل بياناتهم الشخصية، وأصبح على مستخدمي شبكات «ويبو» للتدوين المصغر، الخدمة الصينية الموازية لخدمة «تويتر»، تقديم أسماءهم الحقيقية، كما فرض على المستخدمين القدامى تسجيل بياناتهم خلال ثلاثة أشهر.. ومن يرفض القيام بذلك من المستخدمين سيفقد القدرة على نشر أية تعليقات جديدة [٢١] .

وفي مايو ٢٠١٤ أعلنت السلطات تفكيك ٢٣ خلية إرهابية، بمتابعة مواقع الإنترنت تبين أنهم كانوا يتبادلون خبرات صنع المتفجرات من خلال غرف الدردشة والرسائل النصية [٢٢] .

---

١٧ المصدر السابق .

١٨ أنظر : كساب ، محمد مقال سابق .

١٩ أنظر في الموضوع : كساب ، محمد مقال سابق .

٢٠ أنظر : عامر ، محمد حسن مقال سابق .

٢١ أنظر : كساب ، محمد مقال سابق .

٢٢ أنظر : عامر ، محمد حسن مقال سابق .

٤ روسيا :

اتخذت روسيا سلسلة من الإجراءات الصارمة على الإنترنت لمواجهة الإرهاب، ففي أبريل ٢٠١٤، نشرت وزارة التربية الروسية مشروع قرار حول حماية المدارس من الإرهاب عبر فرض رقابة على الأنشطة الإلكترونية للطلاب. وبحسب نص المشروع، فإن على المسئولين عن المدارس والجامعات، تحليل المواقع الإلكترونية الخاصة بالطلاب والعاملين، وكذلك وضع ملفات خاصة بهؤلاء الذين يتجهون إلى انتهاك القواعد، وينص مشروع القانون على وجوب مراقبة المسئولين للإنترنت باستمرار، بهدف جمع المعلومات حول الأنشطة الإرهابية في مناطقهم. وذكرت صحيفة «ازفيستيا» الروسية، في يناير الماضي أن: مجلس النواب الروسي سيناقش مجموعة من مشاريع القوانين المتعلقة بمكافحة الإرهاب. وأشارت الصحيفة إلى أن: المقترحات تشمل الأمن المعلوماتي والقانون الفيدرالي حول الاتصالات وتكنولوجيا المعلومات بإرغام أصحاب المواقع الإلكترونية والشركات، التي تقدم خدمات الإنترنت على حفظ المعلومات الخاصة بالمستخدمين لمدة ٦ أشهر [٢٣]، ومؤخراً وقع الرئيس الروسي فلاديمير بوتين مؤخراً قانونا يسمح للسلطات بمطالبة مقدمي خدمات الإنترنت بمنع مواقع معينة.وفي مايو الماضي، استولى مؤيدون لبوتين على مقر شركة شبكة «في كونتاكتي» الاجتماعية الشهيرة في روسيا، وهي خدمة شبيهة بـ«فيس بوك»، وطردوا مديرها من مكتبه، لرفضه الإفصاح عن بيانات طلبتها الحكومة منه [٢٤].

٥ كوريا الشمالية :

يتم استخدام الإنترنت على نحو محدود للغاية في كوريا الشمالية البالغ عدد سكانها ٢٤ مليون شخص، غير قادرين على استخدام الإنترنت.. إلا أنه يمكن لبعض الكوريين الوصول إلى شبكة الإنترنت الداخلية التي تتصل بها وسائل الإعلام الرسمية، ويسمح للنخبة والأجانب المقيمين في فنادق معينة بالوصول الكامل إلى الإنترنت [٢٥].

٦ إيران :

وفيها يتم حظر معظم مواقع وسائل التواصل الاجتماعي، مثل «فيس بوك، تويتر»، ومواقع المعارضة السياسية والمواقع الجنسية، وفي المقابل يستخدم الإيرانيون طرقًا بديلة ونطاقات أخرى للإنترنت للالتفاف على القيود الرسمية [٢٦].

---

٢٣ أنظر : عامر ، محمد حسن مقال سابق .

٢٤ أنظر في الموضوع : كساب ، محمد مقال سابق .

٢٥ أنظر: كساب ، محمد مقال سابق .

٢٦ أنظر في الموضوع : كساب ، محمد مقال سابق .

٧ تركيا :

في مارس ٢٠١٤، حجبت تركيا موقعي «تويتر، يوتيوب» ، كما أنها فرضت رقابة صارمة على الإنترنت، حتى حجبت «فيس بوك» و«تويتر» و«يوتيوب» بهدف حماية نظام الحكم [٢٧] .

٨ روسيا :

صعدت الحكومة الروسية محاولاتها لرصد ومراقبة شبكة الإنترنت، وتستهدف المدونين.. ومؤخراً وقع الرئيس الروسي فلاديمير بوتين مؤخراً قانونا يسمح للسلطات بمطالبة مقدمي خدمات الإنترنت بمنع مواقع معينة.وفي مايو الماضي، استولى مؤيدون لبوتين على مقر شركة شبكة «في كونتاكتي» الاجتماعية الشهيرة في روسيا، وهي خدمة شبيهة بـ«فيس بوك»، وطردوا مديرها من مكتبه، لرفضه الإفصاح عن بيانات طلبتها الحكومة منه [٢٨] .

- **ثالثاً : الدول الأفريقية :**

- اريتريا :

تقيد الحكومة الوصول إلى الإنترنت وتراقب عن كثب الشبكات الاجتماعية.. وفرضت الحكومة على مستخدميها استخدام إنترنت أحد مقدمي خدماته الثلاث المملوك مباشرة من قبل الحكومة للسيطرة عليها من خلال أعضاء رفيعي المستوى من الحزب الوحيد في البلاد.. ولكن الغالبية العظمى من الناس لا يمكنهم الوصول إلى الإنترنت [٢٩] .

- **رابعاً : الدول العربية :**

١ مصر:

في الواقع أن اهتمام وزارة الداخلية بمصر بجرائم الإنترنت تمتد جذوره لعام ٢٠٠٢ حيث أصدر وزير الداخلية القرار رقم ١٣٥٠٧ لسنة ٢٠٠٢ بإنشاء إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق للأخذ بزمام المبادرة لمواجهة تلك الجرائم والحد من خطورتها وضبط مرتكبيها وتقديمهم للعدالة . وتُجمل الأهداف من تكوين الإدارة في : ضبط مختلف صور الخروج علي الشرعية فيما يمس الأمن القومي وأمن الأفراد باستخدام الحواسب الآلية في مصر، ويأتي قرار إنشائها مع المرحلة المقبلة والتي تسعي الدولة فيها لتنفيذ الحكومة

---

٢٧ أنظر في الموضوع : عامر ، محمد حسن مقال سابق .

٢٨ أنظر في الموضوع : كساب ، محمد مقال سابق .

٢٩ للمزيد أنظر : كساب ، محمد مقال سابق .

الإلكترونية حيث ستظهر تداعيات كثيرة مع بدء ميكنة العمل بالحاسبات في مختلف الوزارات ومصالح وهيئات الدولة مما سيترتب عليه وجود العديد من أنماط القضايا المختلفة [٣٠] .

٢ المملكة العربية السعودية :

تستهدف الرقابة المحدودة – في المملكة ـ لمواقع التواصل الاجتماعي « رصد الحسابات التي تحرض على الكراهية وأعمال مخالفة للنظام»..نظرا لأن «فئة ضالة» تستخدم شبكات التواصل في بث رسائل تحريضية مستغلة أنها خدمة مفتوحة وعامة للجميع . فقد أوضح المتحدث الأمني لوزارة الداخلية معالي اللواء منصور التركي، ذلك بقوله : " نحن لا نتابع كل من يستخدم هذه

---

٣٠ وتضم إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق ثلاثة أقسام هي : قسم العمليات وقسم التأمين وقسم البحوث والدراسات . ويهمنا أن نشير هنا إلى اختصاصات قسم العمليات – التي تُجمل في الآتي :

١ مكافحة الجرائم التي تقع باستخدام أجهزة الحاسب الآلي في مجالات نظم وشبكات وقواعد البيانات .

٢ إخطار الأجهزة النوعية المختصة بأعمال المكافحة بالبيانات والمعلومات المتعلقة بالجرائم الجنائية التي يمكن التوصل إليها من خلال الاتصال بشبكات المعلومات والتنسيق معها .

٣ إعداد قاعدة بيانات بجرائم المعلومات التي تدخل في نطاق اختصاص الإدارة والأحكام الصادرة فيها .

وخطة عمل هذه الإدارة تشمل :

- ضبط ومكافحة جرائم الانترنت بشتى صورها وأنماطها.
- تقديم المساعدات الفنية والأدلة المادية لضبط جرائم الانترنت لأجهزة الشرطة النوعية .
- حصر و متابعة مقاهي الانترنت ووضع الضوابط لها لتسجيل بيانات مستخدمي الشبكة العالمية وإعداد قاعدة بيانات لخدمة أغراض المتابعة .

إعداد البحوث الفنية والقانونية في مجال جرائم الحاسبات مع الأجهزة المختصة بوزارة الداخلية .

- وضع خطة تأمين ووقاية نظم وشبكات المعلومات لأجهزة وزارة الداخلية
- إعداد أرشيف متكامل للمعلومات التي تخدم أعمال الإدارة وإنشاء الملفات والسجلات والبطاقات اللازمة لذلك .
- إعداد قاعدة بيانات بجرائم المعلومات التي تدخل في نطاق اختصاص الإدارة .
- راجع : وزارة الداخلية المصرية ، إدارة مكافحة جرائم الحاسبات وشبكات المعلومات ؛ د. ت ، زيارة ٣ سبتمبر ٢٠١٤م ، موقع وزارة الداخلية المصرية :

http://citizen service.moiegypt.gov.eg/crimes_web/main.htm

وفي سبتمبر ٢٠١٠، أنشأت وزارة الداخلية المصرية قسمًا جديدًا خاص بمراقبة ما يكتب على «فيس بوك» بقرار إداري رقم ٧٦٥ صدر في أول يوليو من نفس العام.. ويضم القسم الجديد ثلاث ورديات، تعمل كل منها ٨ ساعات،وتتكون كل وردية من ١٥ فردًا، مقسمة إلى ضابطين وعشرة أمناء شرطة وثلاثة مهندسين، ويتم العمل طوال الوردية على رصد جميع المجموعات والصفحات وغرف الدردشة، وكتابة تقارير وافية عن هذه الدردشات . أنظر في الموضوع : كساب ، محمد مرجع سابق .

الشبكات ولكن نرصد فقط المواقع التي تحرض على الكراهية أو على أعمال مخالفة للنظام، ونسعى لتنفيذ الأنظمة بحق من يقفون وراء هذه المعرفات والمواقع» [٣١] .

٣ دولة الإمارات العربية المتحدة :

في مايو ٢٠١٢، كشف مسئول بالشرطة الإماراتية، عن قيام الشرطة بمراقبة الإنترنت ومواقع التواصل الاجتماعي على مدار الساعة، وذلك تزامنًا مع حملة ضد نشطاء سياسيين. [٣٢] .

٤ قطر :

رغم تأكيد الحكومة القطرية على أنها لن تحجب أي موقع للإنترنت، وأنها لن تراقب المواد المتوافرة على الشبكة خاصة بعد إعلانها قطر "منطقة معلومات مفتوحة" [٣٣] غير أن هذه الإعلانات الرسمية لا تتوافق مع الواقع حيث أن هناك الكثير من الحالات والتقارير التي تؤكد قيام شركة "كيوتل" بمنع تصفح الكثير من صفحات الإنترنت [٣٤] وتقول بعض التقارير أيضا أن الشركة القطرية المزودة للخدمة قامت بتطوير برمجيات خاصة تمنع المحتوى "غير اللائق" وتقوم بمراقبة استخدام الشركة لدى المزودين الآخرين [٣٥] ، وهم في حالة قطر "مقاهي الإنترنت" العامة.

كما تمارس شركة "كيوتل" عمليات حجب المواقع، ولا تذكر الشركة عبر موقعها الرسمي أي إجراءات أو خطوط عريضة لسياستها في الحجب، وتقول بعض تقارير حقوق الإنسان أن شركة "كيوتل" تتجسس على الرسائل التي تمر عبر مزوداتها [٣٦] .

---

٣١ أنظر: الشهري ، منصور الداخلية: لا نتابع مستخدمي مواقع التواصل بل نرصد من يهدد الوطن – خبر منشور بصحيفة عكاظ السعودية العدد : ٤٤٣٧ – الصادر في ١٤٣٤/١٠/٠٣ هـ الموافق ١٠ أغسطس ٢٠١٣ م الداخلية: لا نتابع مستخدمي مواقع التواصل بل نرصد من يهدد الوطن . أنظر الموقع الإلكتروني للصحيفة :
http://www.okaz.com.sa/new/mobile/20130810/Con20130810626858.htm

٣٢ أنظر في الموضوع : كساب ، محمد مقال سابق . للمزيد حول هذا الموضوع ؛ راجع :
http://old.openarab.net/ar/node/90

٣٣ منظمة الخصوصية الدولية، إسكات قطر، ٢٠٠٣/٩/٢١:
http://www.privacyinternational.org/article.shtml?cmd[347]=x 347 103775. زيارة ٢٠٠٦/٦/١

٣٤ المصدر السابق.

٣٥ المصدر السابق.

٣٦ صحفيون بلا حدود، الانترنت تحت المراقبة، قطر،
http://www.rsf.org/article.php3?id_article=10765. زيارة ٢٠٠٦/٦/٢
للمزيد حول هذا الموضوع ؛ أنظر : الزلاقي ، إيهاب خصم عنيد الإنترنت والحكومات العربية تقرير منشور بموقع المبادرة العربية لإنترنت حر – عن الدول العربية – تقرير قطر . راجع :

http://old.openarab.net/ar/node/101

فعلى سبيل المثال أعلن موقع [٣٧] Boing Boing في ٢٧ فبراير ٢٠٠٦ أنه تم حظر الوصول إليه من داخل قطر، وهذا الموقع يعمل كدليل مفتوح لعرض الكثير من الموضوعات المختلفة والمتنوعة التي تظهر على شبكة الإنترنت، وهو موقع مفيد للغاية في الكثير من المعلومات المتنوعة وليس من نوعية المواقع التي يمكن أن تقع تحت طائلة الحجب لأسباب تقليدية ترتبط بالإباحية، وأكد بيان على الموقع أنه تعرض للحجب داخل دولة قطر وأيضا داخل الإمارات [٣٨] ، وأكد البيان أن شركة "كيوتل" القطرية تستخدم برنامج الحجب المسمى Smart Filter الذي تنتجه شركة أمريكية هي Secure Computing وهذا البرنامج تستخدمه العديد من الدول العربية التي تمارس حجب المواقع مثل الإمارات [٣٩] [٤٠] .

٥ الكويت :

منذ أن بدأت خدمة الانترنت في الدخول للكويت، لم تضع الحكومة رقابة مركزية صارمة عليها، ومع ذلك فقد حددت الدولة بوضوح شديد القواعد التي يلزم تقديم هذه الخدمات من خلالها، وتركت للشركات المزودة اتخاذ الإجراءات الفنية لحجب المواقع تحت رقابة وزارة المواصلات الكويتية التي تختص بالنظر في الطلبات المقدمة لوزارة التجارة والصناعة بشأن تأسيس مؤسسات فردية أو شركات بغرض تقديم خدمات الانترنت للجمهور [٤١] .

---

٣٧ موقع بوينج بوينج :

Boing Boing banned in UAE, Qatar, elsewhere ،27/2/2006

http://boingboing.net/2006/02/27/boingboing banned in.html

زيارة ٣ سبتمبر ٢٠١٤ الساعة ٥٤ر ٩ مساءً بتوقيت مملكة البحرين .

٣٨ المصدر السابق .

٣٩ المصدر السابق.

٤٠ للمزيد حول هذا الموضوع ؛ أنظر : الزلاقي ، إيهاب المصدر السابق .

٤١ راجع : القرار الوزاري الكويتي رقم ٧٠ لعام ٢٠٠٢ بشان أسس وضوابط الترخيص لمقدمي خدمة الانترنت ؛ ومن هذه الضوابط ما نصت عليه المادة ٤ من هذا القرار التي تقول : يلتزم مزودي خدمة الانترنت بما يلي :

١ـ الالتزام بتركيب وتشغيل أنظمة الرقابة الكفيلة بمنع المواد والمواقع الإباحية أو المخالفة للدين والعادات والأمن وبالوسائل المختلفة مثل صفحات الانترنت أو برامج المحادثة أو البريد الالكتروني أو سواها. مع التحديث المستمر لمواكبة التغيير في المواقع والعناوين الجديدة. وعلى أن يتم اعتماد كفاءة النظام من قبل وزارة المواصلات.

٢ـ تقديم خدمة الانترنت بأي وسيلة كانت لأي من مقدمي خدمة الانترنت دون حصول الأخير على ترخيص صالح من قبل وزارة المواصلات.

٣ـ تقديم كشف شهري بجميع مقدمي خدمة الانترنت المرتبطة مع المزود. شاملا الاشتراكات القائمة والجديدة والمنتهية .

غير أنه إزاء إساءة استخدام مواقع التواصل الاجتماعي عبر الفضاء الإلكتروني ، اضطرت دولة الكويت أن تلجأ إلى حجب المواقع الإسلامية التي تحرض على العنف كجزء من حرب شاملة على الإرهاب عقب الاشتباكات الأخيرة مع الأصوليين الذين خططوا لمهاجمة الأمريكيين وقوات الأمن في البلاد – الكويت [٤٢] ، وبعبارة أخرى قد أكدت مصادر أمنية كويتية أن وزارة الداخلية تراقب بعض حسابات شبكات التواصل الكويتية في موقع التواصل الاجتماعي تويتر والتي تتعاطف وتدعم توجه داعش وتحث على إثارة القلاقل بهدف زعزعة أمن واستقرار الكويت وإثارة الفتن وبصدد تطبيق القانون عليهم بعد توثيق الدلائل والبراهين [٤٣] .

هذا ولقد شهد شهر فبراير ٢٠٠٥ حملة واسعة لإغلاق العديد من المواقع الإسلامية التي وصفت بالمتطرفة، وجاءت هذه الحملة بعد صدام عنيف حدث بين قوات الأمن وجماعات إرهابية في الكويت، وأعلن "حامد خاجة" وكيل وزارة الاتصالات أن السلطات أغلقت بالفعل ثلاثة مواقع كويتية وأنها تعمل بالتعاون مع مسئولي الأمن وشركات تزويد الانترنت على منع الوصول للمواقع غير الكويتية ولكنه رفض تحديد عدد أو أسماء هذه المواقع [٤٤] [٤٥] .

---

٤٢ أنظر :

Elias Diana , Associated Press, Kuwait blocks sites that incite violence.http://usatoday30.usatoday.com/tech/news/techpolicy/2005 02 08 kuwait websites_x.htm

زيارة ٤ أغسطس ٢٠١٤ الساعة ١٠ر١١ مساءً .

٤٣ أنظر موقع البوابة نيوز : الكويت تشن حملة مراقبة على شبكات التواصل الاجتماعي بعد تغريدة زعيم داعش .

http://www.albawabhnews.com/719988

حيث ذكر هذا الموقع أن أبو بكر البغدادي – أي زعيم داعش هدد باحتلال دولة الكويت من أجل محاربة أمريكا.

الجدير بالذكر، أن البغدادي قال في تغريدة له على حسابه الشخصي على موقع التواصل الاجتماعي "تويتر"، "نحن لدينا تصفية حساب مع أمريكا، لكن لا نستطيع الوصول لها، بل ستأتي إلينا، وذلك يتم بدخول الكويت، بعدها ستأتينا أمريكا ونقاتلها وننتقم" .

٤٤ أنظر : Elias Diana : op.cit.

٤٥ ومن الأمثلة التي تضرب في هذا المضمار حجب الموقع الشخصي لمحمد الجاسم رئيس التحرير السابق لجريدة "الوطن" الكويتية . أنظر : موقع المحامي محمد عبد القادر جاسم :

http://www.aljasem.org/default.asp?opt=2&art_id=88

زيارة ٤/٩/٢٠١٤ الساعة ١٠ر١ صباحاً .

وقد تم تصعيد قضية حجب هذا الموقع إلى مجلس الأمة حيث وجه النائب "أحمد السعدون" سؤالا لوزير الداخلية حول ملابسات حجب الموقع خاصة وأن الخطوات التي اتخذتها الداخلية لا تستند إلى قانون، وطالب النائب بالحصول على بيانات مفصلة بكل الحالات التي طالبت فيها الداخلية بحظر مواقع على شبكة الانترنت والأسانيد القانونية الداعمة لهذه الإجراءات.

راجع :

زيارة ٨/٩/٢٠٠٦ . http://www.alommah.org/home/index.php?option=com_content&task=view&id=10

ورغم هذه المجهودات إلا أن الخاجة اعترف أن وسائل الرقابة والحجب لا يمكنها منع كل المستخدمين عن الوصول لهذه المواقع، وأوضح أنهم يبذلون أقصى ما بوسعهم لمنع المواطنين من فتح هذه المواقع التي تنشر أفكارا مدمرة، وأنهم لو نجحوا فقط في منع ٩٠٪ من الزوار لها فسيكون هذا الأمر إنجازا ملحوظا [٤٦].

٦ الوضع في مملكة البحرين :

وجه وزير الدولة لشؤون الاتصالات البحرينية، الشيخ فواز بن محمد آل خليفة، لإنشاء مكتب للمتابعة والتنسيق بوزارة الدولة لشؤون الاتصالات يباشر أعماله اعتبارًا من ١ أغسطس ٢٠١٣، بتنفيذ ما جاء في توصية المجلس الوطني لتفعيل الإجراءات القانونية ضد كل من يسيء استخدام وسائل الاتصال الاجتماعي والعبث بأمن المملكة واستقرارها [٤٧].

ويتضح أن مبررات مراقبة شبكة التواصل – في مملكة البحرين حماية المجتمع من الإرهاب الإلكتروني الذي يستخدم المواقع الإلكترونية والحسابات والرسائل للتحريض والترويج للعنف والأعمال الإرهابية على شبكات التواصل الاجتماعية مما يمس أمن المواطنين والمقيمين ويضر بالمصالح العامة، كما يستهدف الوحدة الوطنية ويؤثر على الأمن والسلم الأهليين [٤٨].

=كما تم حجب موقع شخص آخر هو "حامد العلى" الذي نشرت جريدة الرأي العام في ٢٠٠٥/٨/٨ أن السلطات المختصة حجبت الوصول إليه من داخل الكويت عن طريق طلبات لمزودي خدمات الإنترنت الرئيسيين في البلاد

راجع : موقع الرأي الحر، ٢٠٠٥/١٠/٢،تعليقا على قرار السلطات بإغلاق موقع "حامد العلى":

http://www.raihur.com/index.php?p=87 . ٢٠١٤/٩/٤ زيارة

وقيل في أسباب حجب الموقع إنه يروج لفكر الإرهاب . أنظر : الزلاقي ، إيهاب خصم عنيد الإنترنت والحكومات العربية تقرير منشور بموقع المبادرة العربية لإنترنت حر – عن الدول العربية – تقرير الكويت . للمزيد حول هذا الموضوع ؛ راجع :

http://old.openarab.net/ar/node/102

٤٦ أنظر : Elias Diana : op.cit.

٤٧ نقلا عن وكالة أنباء البحرين ؛ راجع الموقع الإلكتروني :

http://www.bna.bh/portal/mobile/news/574939

٤٨ هذا ما أكده معالي الشيخ فواز بن محمد آل خليفة وزير الدولة لشئون الاتصالات .

أنظر : وكالة أنباء البحرين :http://www.bna.bh/portal/mobile/news/574939

المبحث الثاني

التحقيق الجنائي في جرائم الإرهاب عبر الفضاء الإلكتروني

- **تقسيم :**

سنعرض هنا لأهم إجراءات التحقيق في جرائم الإرهاب التي ترتكب عبر الفضاء الإلكتروني، وهي : المعاينة ، والاستعانة بخبير ، والتفتيش ، والضبط . وقبل أن نعرض لهذه الإجراءات سنعرض للمقصود بمسرح الجريمة فيما يتعلق بالإرهاب عبر الفضاء الإلكتروني. وعليه سينشطر هذا المبحث إلى مطلبين: الأول في التعريف بالتحقيق الجنائي وبمسرح الجريمة والإرهاب عبر الفضاء الإلكتروني، والثاني في المعاينة ، والاستعانة بخبير ، والتفتيش ، والضبط .

المطلب الأول
التعريف بالتحقيق الجنائي
وبمسرح الجريمة والإرهاب عبر الفضاء الإلكتروني

- **تقسيم :**

سيتوزع موضوع هذا المطلب إلى فرعين : الأول في التعريف بالتحقيق الجنائي والإرهاب عبر الفضاء الإلكتروني ، والثاني في مسرح الجريمة والإرهاب المذكور .

الفرع الأول

التعريف بالتحقيق الجنائي والإرهاب عبر الفضاء الإلكتروني

- **أولاً : التعريف بالتحقيق الجنائي بوجه عام :**

التحقيق Instruction F. /Instruction –Briefing-Examination of a case E. الجنائي هو – حسب اعتقادنا ـ مجموعة من الإجراءات الجنائية تستهدف الوصول للحقيقة أو الحصول على دليل بمناسبة وقوع جريمة جنائية ما . أو هو مرحلة من مراحل الدعوى الجنائية أو الجزائية ـ سمها ما شئت ـ تشكل نوعاً من مرحلة تحضيرية تسمح بالتثبت من اقتراف الجرم وتحديد ما إذا كانت التهم الموجهة ضد الأشخاص الملاحقين كافية لإحالة الدعوى إلى قضاء

الحكم ، وهذه المرحلة اختيارية بالنسبة للجنح ما لم ينص القانون على خلاف ذلك ، في حين أنها إلزامية أو وجوبية بالنسبة للجنايات [٤٩] .

خصائص التحقيق الجنائي :

ويتميز التحقيق الجنائي بخصائص عدة ، هي : أن يكون كاملاً ، وله طابع بوليسي ، وهو إجراء عادي وليس استثنائياً ، علاوة على أنه في شق منه له طبيعة قضائية .

وهذا ما سنعرضه فيما يلي :

١ـ **شمولية التحقيق الجنائي** : بمعنى أنه يشمل كافة الجوانب الإجرائية للتهمة أو للواقعة الجنائية . وبمعنى آخر يجب أن يكون كاملاً – شأنه في ذلك شأن التحقيق النهائي أمام القضاء ـ بقدر المستطاع ومستمراً حتى القبض أو توقيف المتهم [٥٠] [٥١] ـ وهو كل مَنْ تشير أصبع الاتهام إلى تورطه في الجرم محل التحقيق – وتشمل إجراءات التحقيق الجنائي كافة الوسائل القانونية التي تساهم في الوصول للحقيقة أو الحصول على دليل ، ومن ذلك : الانتقال إلى مسرح الجريمة أو غيره من الأماكن ذات الصلة بالجريمة ، المعاينة ، سماع الشهود ، سؤال المتهم واستجوابه ، الاستعانة بالخبراء ، والقبض والضبط والإحضار ، والحبس الاحتياطي .

٢ـ **الصفة البوليسية** : تنصرف هذه الصفة للتحقيق الجنائي الذي تجريه الشرطة ، لتلبية مقتضيات التحريات الجزائية ، نظراً لأن القانون يسند لرجال الشرطة – وخصوصاً من لهم صفة الضبطية القضائية – ملاحقة المتهمين حتى أقصى الحدود ، وكل مَنْ تحوم حوله شبهات تورطه في ارتكاب جريمة ، وفي حدود مدد قانونية معينة ، ويتيح القانون لرجال الشرطة التوسل بوسائل بوليسية معينة كالتخفي في ملابس معينة أو استخدام الحيل والخدع ، والتنصت على الهاتف [٥٢] بضوابط قانونية معينة .

---

٤٩ في هذا المعنى : منعم ، لينا وآخرون – مفردات اللغة القانونية – فرنسي ؛ عربي؛ إنجليزي – مترجم من أصل فرنسي – الناشر دالوز وهاشيت أنطوان – بيروت – ٢٠١٠ م – ص ٣٢٢ .

٥٠ في هذا المعنى : نخلة ، موريس وآخرون – القاموس القانوني الثلاثي قاموس قانوني موسوعي شامل ومفصل – عربي / فرنسي / إنجليزي – منشورات الحلبي الحقوقية – بيروت الطبعة الأولى – ٢٠٠٢م – ص ٤٤٩ .

٥١ إن كان للقبض أو لتوقيف المتهم مقتضى ؛ ووفقاً للضوابط المقررة لهذين الإجراءين .

٥٢ في هذا المعنى : نخلة ، موريس وآخرون – المرجع والموضع السابقين . ويراعي أن هذه الصفة البوليسية لا تتعارض مع الصفة القضائية ؛ لأن المقصود بالصفة البوليسية هو استخدام وسائل الشرطة المختلفة للإجراءات التي يتخذها مأموري الضبط القضائي بمناسبة التحقيق الجنائي ؛ أما الصفة القضائية فهي مستمدة من الطبيعة القضائية لإجراءات هذا التحقيق على النحو المشار إليه بالمتن .

٣- **الصفة العادية** : أن التحقيقات الجنائية فورية ومؤقتة وشخصية وعينية ، فهي مجموعة إجراءات ليست لها صفة استثنائية ، أي تحكمها فكرة الشرعية الجنائية العادية – وليست الاستثنائية ، أي التي تسود في الظروف الطارئة – وتمتد مظلة هذه الشرعية الجنائية العادية لتشمل تلك الإجراءات التي يتخذها رجال الشرطة – بضوابط معينة – في حالة الجرم المشهود ، أو التلبس بالجريمة ، كما أن هذه الإجراءات يتم تفعيلها بصفة فورية بمجرد اقتراف الجريمة ، ويمارسها رجال الشرطة دون وساطة ، إذ يستمدون سلطاتهم من القانون ذاته ، فلا حاجة لأي شكليات أولية ، لممارسة إجراءات التحقيق الجنائي ، كندب سلطة التحقيق الابتدائي كالنيابة العامة، كما أن إجراءات التحقيقات الجنائية مؤقتة حيث يكون للنيابة العامة أن تنتقل لمكان الجريمة وتمارس اختصاصاتها فوراً بمجرد علمها بالواقعة ، علاوة على أن التحقيقات الجنائية لها نطاقها الشخصي والعيني أو الموضوعي فلمأمور الضبط القضائي سلطة ضبط الأشياء التي لها علاقة بالجريمة والتي تكون في حيازة المساهمين فيها أو الغير ، في حدود ما يقرره القانون وخصوصا فيما يتعلق بحرمة المسكن وسر المهنة وأسرار الحياة الخاصة . كما يمكن لمأمور الضبط القضائي أن يقبض على المتهم حتى ٢٤ ساعة ، متى اقتضت ضرورة التحقيق ذلك [٥٣] .

٤- الصفة القضائية : تستمد الطبيعة القضائية لإجراءات التحقيقات الجنائية من كون السلطة التي تمارسه لها هذه الصفة كالنيابة العامة وقاضي التحقيق ، علاوة على أن هذه الإجراءات تمهيدية لإجراءات المحاكمة التي تستهدف الفصل في النزاع الناشئ عن ارتكاب الجريمة الجنائية ، لتعلن كلمة الحق أو القانون أو – إن شئت – كلمة العدل في هذا النزاع .

الفرع الثاني
مسرح الجرائم الإرهابية عبر الفضاء الإلكتروني

- **أولاً : مسرح الجريمة في الجرائم التقليدية :**

لعل من أهم العناصر التي ترتبط بالجريمة هو مسرحها أو مكان وقوع أركانها [٥٤] ، وهو العنصر الرئيس لضبط وتحري الجريمة وملاحقة مرتكبيها . فمسرح الجريمة – بوجه عام - يحتوي مختلف الأماكن التي توجد بها أدلة ومؤشرات عن فعل جنائي ما، وهي تحتوي:

---

٥٣ في هذا المعنى : نخلة ، موريس وآخرون – المرجع والموضع السابقين .

٥٤ قد يقول قائل أن مسرح الجريمة هو المكان الذي يقع فيها الركن المادي باعتباره الركن المحسوس أو الملموس أو بالأحرى الركن الذي يمكن إدراكه بحاسة من الحواس ؛ أما الركن المعنوي فهو لا يمكن إدراكه ؛ وهذا القول مردود عليه بأن تقسيم الجريمة إلى أركان جاء على سبيل التبسيط للدراسة ؛ أما في الواقع لا يمكن الفصل بين الركنين فالقاتل– على سبيل المثال عندما يقتل يأتي بالركنين المادي والمعنوي معاً وفي وقت واحد ، وقس على ذلك .الأمر الذي يصح معه بأن مسرح الجريمة وهو مسرح ارتكاب الجريمة بكافة أركانها .

١ المكان الذي تم فيه العثور على الجريمة يقدر في بعض الأحيان بالكيلومترات، مثلا في حوادث الطائرات .

٢ المكان الفرعي الذي شهد فعل جنائي متصل بالجريمة والأماكن العامة المستغلة من طرفها.
والمكان الذي تم فيه العثور على الجريمة يقدر في بعض الأحيان بالكيلومترات، مثلا في حوادث الطائرات [٥٥] .

- **ثانياً : المقصود بمسرح الجريمة عبر الفضاء الإلكتروني :**

أما مسرح الجريمة الإلكترونية [٥٦] ـ بما في ذلك الجرائم الإرهابية عبر الفضاء الإلكتروني ـ فهو مسرح معنوي – يختلف عن المسرح المادي للجريمة التقليدية – فهو يشمل كل مكان تجول فيه الشخص في الشبكة العنكبوتية ، إذ يترك آثار أقدامه وبصماته المعنوية في الموقع الذي يزوره ، حيث يتم تحديد عنوان الـ ip الدائم له ويتم تحديد نوع الجهاز الذي يستخدمه والمكان الذي يدخل منه .

ويمكن تتبع هذه العناصر بطرق بسيطة أحيانا وبعضها متوفر للمستخدمين العاديين [٥٧] ، ومن خلال هذه العناصر يتم كشف معلومات المستخدم ويجعلها متاحة لأي شخص يود تتبع تحركات المجرم ، فضلا عن أن يقوم بذلك المتخصصون ، و حتى أن جهاز المجرم الشخصي نفسه يحتفظ بملفات الكوكيز للمواقع التي دخلها .

غير أن الأمر ليس بهذا القدر من البساطة ، صحيح أنه قد يمكن اكتشاف المجرمين البسطاء بمثل هذه الطرق ، أما المجرمين المتخصصين ـ بل وحتى الهواة منهم ـ فيحرصون على محو آثارهم التي تم تسجيلها من خلال عدة طرق منها مسح ملفات الكوكيز الموجودة على أجهزتهم و أيضا القيام بإخفاء IP الخاصة بأجهزتهم بطرق مختلفة ومنها ما هو متوفر للكافة أيضا [٥٨] .

---

٥٥ للمزيد حول مسرح الجريمة ؛ راجع : د. عبد المطلب ، ممدوح عبد الحميد، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية ، مصر ، ٢٠٠٦ ، ص ٦٩ وما بعدها .

٥٦ للمزيد حول هذا الموضوع ؛ راجع : د. عبد المطلب ، ممدوح عبد الحميد، مرجع سابق ، ص ٦٩ وما بعدها . وأيضاً: د. ممدوح ، خالد فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي – مصر ٢٠٠٩ .

٥٧ يمكن للمحقق أن يدخل بعض المواقع الخاصة مثل déjà news المتاح بسهولة للوقوف على ما قام به المتهم بارتكاب جريمة إرهابية عبر الفضاء الإلكتروني لمعرفة ما قام به على شبكة الإنترنت خلال الفترة الزمنية موضوع التحقيق ؛ حيث إن هذا الموقع – والمواقع المماثلة يحتوي على أرشفة لكل ما يقوم المستخدم بكتابته ضمن المجموعات الإخبارية ولفترات طويلة جدا . راجع : مصعب القطاونة الإجراءات الجزائية الخاصة في الجرائم المعلوماتية – بحث مقدم لشبكة قانوني الأردن LAWJO ص ٧ ؛ راجع موقع شبكة قانوني الأردن :www.lawjo.net

٥٨ توجد بعض المواقع مثل www.anonymizer.com تقوم بتوفير برمجيات تتيح للمستخدم الدخول للمواقع المختلفة دون أن يتم كشف الـ ip الخاصة بأجهزتهم وغيره الكثير جدا من البرامج التي تقوم بذات الوظيفة.

المطلب الثاني

الخبرة الفنية والمعاينة والتفتيش والضبط

والجرائم الإرهابية عبر الفضاء الإلكتروني

- **الاستعانة بالخبرة الفنية في الإرهاب عبر الفضاء الإلكتروني:**

الأصل أن الاستعانة بخبير فني أمر جوازي للمحقق أو لجهة التحقيق والحكم، غير أنه في المسائل الفنية البحتة التي لا يمكن للقاضي أن يقطع فيها برأي دون استطلاع رأي أهل الخبرة، يجب عليه أن يستعين بالخبير، فإذا تصدى للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير كان حكمه معيبا مستوجبا نقضه، وهذا المبدأ أستقر عليه قضاء محكمة النقض المصرية [٥٩] .

وهذا المبدأ تأخذ به محكمة التمييز البحرينية حيث قضت بعدم التزام المحكمة بالالتجاء إلى الخبراء إلا في المسائل الفنية التي يتعذر عليها أن تشق طريقها فيها [٦٠] .

وترتيباً على ذلك فإنه يجب على المحقق والقاضي ـ في مجال الجرائم الإرهابية التي تقع في الفضاء الإلكتروني – نظراً لأن هذه الجرائم تتصل بمسائل فنية غاية في التعقيد ومحل الجريمة فيها غير مادي، والتطور في أساليب ارتكابها سريع ومتلاحق، ولذا فإن الفني المتخصص هو أقدر من غيره على كشف غموضها .

- **أهمية الاستعانة بالخبيرة في مجال جرائم الإرهاب عبر الفضاء الإلكتروني :**

وتنبع أهمية الاستعانة بالخبيرة في مجال جرائم الإرهاب عبر الفضاء الإلكتروني ، من التطور السريع الذي تشهده تكنولوجيا المعلومات التي تجعل من الصعوبة بمكان على غير المتخصصين ملاحقة هذا التطور ، الأمر الذي يخشى معه أن تعجز الشرطة عن كشف غموض الجريمة، كما قد تعجز هي أو جهة التحقيق عن جمع الأدلة حول الجريمة ، بل قد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال لدى التعامل معه [٦١] .

ويعتبر القانون البلجيكي الصادر في ٢٣ نوفمبر سنة ٢٠٠٠ من أحدث التشريعات الحديثة التي نظمت أعمال الخبرة في مجال الجرائم الإلكترونية ، بما في ذلك الإرهاب عبر الفضاء الإلكتروني [٦٢] .

---

٥٩ أنظر : أحكام النقض المصرية – الدائرة الجنائية – نقض ١٩٦١/٦/١٣ – س ١٢ – رقم ١٣١ – ص ٦٧١ – نقض ١٩٧٤/٥/٩ – س ٢٥ – رقم ١٨٣ – ص ٤٨٩ – نقض ١٩٨٣/١/٤ – س ٣٤ – رقم ٥ – ص ٥٢ .

٦٠ أنظر : حكم محكمة التمييز البحرينية ٣ /١١/ ٢٠٠٣ الطعن رقم ١٧ جنائي لسنة ٢٠٠٣ – مجموعة القواعد القانونية التي قررتها محكمة التمييز في خمس سنوات ٢٠٠٣ ٢٠٠٧ ص ٥٥ .

٦١ أنظر : Taylor R. : op. cit. p. 1 .

٦٢ راجع :

Meunier C. : La loi du 28 Nov. 2000 relative a la criminalite informatique. Rev. Dr. pen. Crim. 2002, p. 611 et s.

وطبقا للمادة ٨٨ من القانون المذكور يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام، أو البحث فيه، أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق[٦٣] .

- **مهمة الخبير :**

وتُجمل مهمة الخبير – طبقاً للنص المشار إليه ـ في تشغيل النظام، و تقديم البيانات المطلوبة، وفقاً للطريقة التي تريدها جهة التحقيق، فقد تريد البيانات مسجلة على ديسك disqu أو على سيد يروم C-DROM، أو على الأقراص الممغنطة، أو على ورق[٦٤] .

ووفقا للقانون المذكور فإن الالتزام بتشغيل النظام واستخراج البيانات المطلوبة منه، يرجع إلى قاضي التحقيق بصفة أصلية، كما يجوز ذلك للنيابة العامة على سبيل الاستثناء في حالة التلبس بالجريمة، أو عند الرضاء بعملية التفتيش هذه[٦٥] .

ويلاحظ أن التزام الخبير هو التزام ببذل عناية، وعليه فإنه لا يُسأل الخبير متى لم يصل إلى النتيجة المطلوبة نتيجة ضعف خبرته، أو بسبب العقبات التي واجهته أثناء مباشرته لمهمته، غير أنه من الممكن أن تثور مسؤوليته الجنائية في حالة رفضه القيام بالمهمة المكلف بها، أو إذا قام بإتلاف عمدي للبيانات المطلوب منه التعامل معها، أو حفظها[٦٦] .

وغني عن البيان أن الخبير يلتزم – فضلاً عن التزامه بأداء مهمته التي حددتها له جهة التحقيق ـ كذلك بالمحافظة على سر المهنة، وفي حالة إفشائه السر، يعاقب بالعقوبة المقررة لهذه الجريمة[٦٧] .

- **ثانياً : المعاينة :**

يقصد بالمعاينة مشاهدة وإثبات الآثار المادية التي نتجت عن ارتكاب الجريمة، وتستهدف المحافظة علي هذه الآثار حتى لا تتعرض للإتلاف أو المحو أو التعديل .

---

٦٣ راجع : Meunier C. : art. Prec. P. 681.
٦٤ راجع : Meunier C. : art. Prec. P. 683.
٦٥ راجع : Meunier C. : art. Prec. P. 682 .
٦٦ راجع : Meunier C. : art. Prec. P. 683.
٦٧ راجع : Meunier C. : art. Prec. P. 684.

والمعاينة من إجراءات التحقيق الابتدائي- بمعناه الواسع ، أي بما يشمل مرحلة جمع الاستدلالات[٦٨] ، والتحقيق الابتدائي بمعناه الضيق ، الذي تجريه سلطات التحقيق [٦٩] - ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتصل بالتحقيق، والأصل أن يحضر أطراف الدعوى المعاينة، وقد يقرر المحقق أن يجريها في غيبتهم، ولا يلتزم المحقق بدعوة محامي المتهم للحضور [٧٠] ، ومجرد غياب المتهم عند إجراء المعاينة ليس من شأنه أن يبطلها [٧١] .

وإذ تظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجب مسرح فعلي للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لفحصها لبيان مدى صحتها في الإثبات، فليس الحال كذلك بالنسبة للجرائم الإلكترونية، حيث يندر أن يتخلف عن ارتكابها آثار مادية، وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها [٧٢] .

وإذا تمت المعاينة بعد وقوع جريمة إلكترونية – بما في ذلك الجرائم الإرهابية التي تقع عبر الفضاء الإلكتروني - يتعين مراعاة ما يلي : ١. تصوير الحاسب والأجهزة الطرفية المتصلة به، شريطة أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة. ٢ .الحرص على ملاحظة الطريقة التي تم بها إعداد النظام. ٣ .ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى تتاح الفرصة لإجراء عمليات المقارنة والتحليل عند عرض الأمر فيما بعد على المحكمة. ٤ . كما يتعين عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة. ٥ . التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة، وفحصها، ويرفع من عليها البصمات المتعلقة بالجريمة.

---

٦٨ وطبقاً لقانون الإجراءات الجنائية البحريني – الصادر بالمرسوم بقانون رقم ٤٦ لسنة ٢٠٠٢ لمأموري الضبط القضائي أثناء جمع الاستدلالات أن يحرروا المعاينات اللازمة م ٥٠ .

٦٩ وفقاً للمادة ٨٩ من قانون الإجراءات الجنائية البحريني على عضو النيابة العامة أن ينتقل إلى أي مكان ليثبت حالة الأشخاص والأماكن والأشياء المتصلة بالجريمة وكل ما يلزم إثبات حالته .

٧٠ د. حسني ، محمود نجيب شرح قانون الإجراءات الجنائية، ط ٣، ١٩٩٨ ص ٥٢٨ وما بعدها ؛ د.عقيدة ، محمد أبو العلا شرح قانون الإجراءات الجنائية، ط ٢٠٠١ . القاهرة ج ٢ ص ٦٤٤ وما بعدها .

٧١ نقض مصري ١٩٨٠/١/٣١ – مجموعة أحكام النقض – س ٣١ – رقم ٢٩ – ص ١٤٨ .

٧٢ د. رستم ، هشام الجوانب الإجرائية للجرائم المعلوماتية ١٩٩٤ – أسيوط – مصر – ص ٥٩.

٦ .التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما عساه أن يوجد عليها من بصمات. ٧ .قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات [٧٣] .

- **ثالثاً: التفتيش:**

التفتيش إجراء من إجراءات التحقيق، يهدف إلى البحث عن أشياء تتعلق بالجريمة، وكل ما يفيد بصفة عامة في كشف الحقيقة، سواء تعلق بالأشخاص أم بالأماكن.

- وللتفتيش شروط موضوعية تتعلق : أ – بسببه : وقوع جريمة بالفعل تعد جناية أو جنحة، وان يوجه اتهام إلى الشخص المراد تفتيشه أو تفتيش مسكنه. ب –الغاية منه : ضبط أشياء تفيد في كشف الحقيقة .

والشروط الشكلية تتحدد بـ:أـ أن يكون الأمر بالتفتيش مسببا. بـ حضور المتهم أو من ينيبه أو الغير أو من ينيبه التفتيش. جـ تحرير محضر بالتفتيش [٧٤] .

وفيما يخص محل التفتيش في حالة ارتكاب جريمة إرهابية عبر الفضاء الإلكتروني ، فإنه يتعين التفرقة بخصوص محل التفتيش بين فرضين : الأول أن يكون محل التفتيش يتجسد في المكونات المادية للحاسب الآلي وملحقاته ، والثاني على العكس أن يتمثل محل التفتيش في البيانات الإلكترونية .

- **الفرض الأول : تفتيش المكونات المادية للحاسب الآلي :**

وفيما يتعلق بالفرض الأول ـ أي عندما يرد التفتيش على المكونات المادية للحاسب الآلي وملحقاته – فلا شك في خضوع التفتيش والضبط طبقاً لقواعد قانون الإجراءات الجنائية ، بما في ذلك البيانات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية ،

---

٧٣ أنظر :

• Taylor R. : Computer crime, "in criminal investigation edited" by Charles Swanson, n. chamelin and L. Territto, Hill, inc. 5edition 1992.p.450.

د. رستم ، هشام – المرجع السابق – ص ٦٠ وما بعدها. وأيضاً : د. عقيدة ، محمد أبو العلا – بحث سابق ص ٨ .

٧٤ د.عقيدة ، محمد أبو العلا شرح قانون الإجراءات الجنائية، ط ٢٠٠١ – دار النهضة العربية بالقاهرة – ص٤٣١ وما بعدها.

وذلك تبعاً للمكان أو الحيز الموجودة فيه[٧٥] ، وعليه متى كانت موجودة بمسكن المتهم أو أحد ملحقاته فتحكمها القواعد ذاتها التي يخضع لها تفتيش المسكن ، حيث يجوز تفتيشها وضبطها متى كان تفتيش المسكن جائزاً ، والعكس بالعكس ، أما إذا كانت هذه المكونات المادية في مكان عام فيحكمها ما يحكم هذا المكان من أحكام إجرائية . في حين أنه إذا كان الحاسب في حوزة شخص خارج مسكنه ، فإن تفتيشه عندئذٍ يخضع للقواعد ذاتها التي يخضع لها تفتيش الشخص بوصفه أحد متعلقاته ، يستوي أن يكون الحائز هو مالك الجهاز أم سواه . وهكذا الشأن بالنسبة لسائر أحكام التفتيش في الحالات العادية ، أي التي لا تتعلق بالعالم الافتراضي أو بالفضاء الإلكتروني .

- **الفرض الثاني : تفتيش البيانات الإلكترونية :**

أما بالنسبة للفرض الثاني – أي حيث يرد التفتيش على البيانات الإلكترونية – فنظراً لأن البيانات الإلكترونية ليس لها بحسب جوهرها مظهر مادي ملموس في العالم الخارجي ، فإن التفتيش يرد على هذه البيانات ثم تحويلها إلى وسائط إلكترونية لحفظها وتخزينها كالأسطوانات والأقراص الممغنطة، ومخرجات الحاسب[٧٦] ؛ لأن البيانات في الفضاء الإلكتروني عبارة عن نبضات إلكترونية ، تقبل التخزين على أوعية أو وسائط مادية كالأشرطة الممغنطة والأقراص والأسطوانات، كذلك يمكن تقديرها وقياسها بوحدات قياس خاصة معروفة ، وترتيباً على ذلك تكون هذه البيانات صالحة كموضوع للضبط والتفتيش شأنها شأن الوسائط المادية ذاتها .

- **ردنا على الرأي القائل بعدم صلاحية المكونات المنطقية لأن تكون محلاً للتفتيش :**

وإذا قيل – بل قيل بالفعل ـ أن هذه المكوّنات المنطقية لا تصلح بطبيعتها لأن تكون محلاً للتفتيش ، نظراً لأن التفتيش يهدف في المقام الأول إلى ضبط أدلة مادية ، وهذا يستلزم وجود أحكام خاصة تكون أكثر ملائمة لهذه البيانات اللا محسوسة[٧٧] . فذلك مردود عليه – في نظرنا – بأن القانون يجب أن يحقق مصالح المجتمع ولا يتخلف عن ذلك ، فنصوص القانون ليست هدفاً في حد ذاته ، بل هي وسيلة لتحقيق أهداف معينة ، أبرزها تحقيق مصالح المجتمع وحماية مصالحه الجديرة بحماية القانون ، وأي تفسير لنصوص القانون لا يراعى هذه الحقيقة هو تفسير قاصر ، لأنه يقدس

---

٧٥ انظر : د. هشام رستم ، ص٦٤ وما بعدها ؛ أسامة المناعسة وآخرون ، ص٢٧٦ وما بعدها.

٧٦ راجع :

• Mohrenschlager M : computer crimes and others crimes aganiste information technology in the Germany. Rev. Int. dr. pen. 1993, p. 319,. Spec. p.349.

٧٧ بخصوص الجدل حول صلاحية الجانب المنطقي للحاسوب لأن يكون موضوعاً للتفتيش راجع : أسامة المناعسة وآخرون ، ص٢٧٨ وما بعدها ؛ د. هشام رستم ، ص٦٤ وما بعدها ؛ أ. عطية عثمان محمد بوحويش ، حجية الدليل الرقمي في إثبات جرائم المعلوماتية ، رسالة التخصص العالي الماجستير ، مقدمة إلى أكاديمية الدراسات العليا/فرع بنغازي ، للعام الجامعي ٢٠٠٩ ص٩٦ وما يليها .

عبارات النص على فحواه ومرماه وغايته . فالغرض من التفتيش هو التنقيب عن أدلة أو الوصول للحقيقة ، أيا كان المحل الذي يرد عليه ، أي سوء أكان مادياً أم معنوياً .

كما لا ينال من ذلك القول بأن " القواعد التي تحكم التفتيش والضبط إنما وُضعت في زمن مبكر وقبل ظهور الحاسوب وتطبيقاته ، وأيا كانت المبررات التي ساقها معتنقو المساواة بين الكيان المادي والمنطقي ، فإن طبيعة البيانات المعالجة تتطلب قواعد خاصة تحكمها بدلاً من محاولة تطويع القواعد التقليدية وتوسيع نطاقها ، وهذا يتأتّى من خلال إجراء تعديل عليها من شأنه توسيع نطاق الأشياء التي تكون مشمولة بالتفتيش والضبط وتضمينها من الأحكام بما يتلاءم ومتطلبات هذه التقنية الجديدة . فالنصوص الخاصة بالتفتيش بمعناه التقليدي لا ينبغي إعمالها بشأنها مباشرة ، باعتبار أن هذه النصوص تمثل قيداً على الحرية الفردية ، ومن ثم يصبح القياس على الأشياء المادية محظوراً لمنافاته الشرعية الإجرائية " [٧٨] .

إذ أن ذلك مردود عليه – في نظرنا – بأن النصوص الإجرائية التي تنظم التفتيش لا تتصادم مع هذا التفسير الواسع لعبارات هذه النصوص وألفاظها ، فلا خير في أي تشريع لا يواكب مستجدات العصر ، فالقانون – أي قانون – يجب أن يحقق مصالح المجتمع ، فإن تخلف عن إيقاع العصر ، فيجب تغييره ليحقق مصالح المجتمع بشكل أفضل ، ولا مفر في حالة غياب نصوص تشريعية جديدة تستوعب مستجدات العصر أن يمتد تفسير هذه النصوص ليشملها مظلة القانون .

كما لا يصلح دفاعاً عن وجهة النظر المغايرة الاحتجاج بالحريات الفردية والشرعية الجنائية ، لأن مثل هذا الاحتجاج ليس هنا موطنه فنحن نتحدث عن جرائم إرهابية ترتكب عبر الفضاء الإلكتروني ، تهدد كيان المجتمع ووحدته وسلامته ، فالشرعية الجنائية العادية – بأفكارها التقليدية – لا تصلح لمواجهة خطر العصر ، ألا وهو الإرهاب ، فلابد أن نقر بوجود شرعية جنائية غير عادية لمواجهة الخطر الجديد على الحياة وعلى الإنسانية وعلى الدول . فالإرهاب الذي نوجهه هو إرهاب عدمي [٧٩] ، أي يريد أن يرتد بالمجتمعات إلى مرحلة العدم ، أي مرحلة المربع رقم الصفر ، فهو يريد هدم كافة الأنظمة القائمة في أي مجتمع أي نظام القضاء – ونظام الجيش –

---

٧٨ د. ارحومة ، موسى مسعود – الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية – بحث مقدم إلى المؤتمر المغاربي الأول حول : المعلوماتية والقانون – الذي نظمته أكاديمية الدراسات العليا – طرابلس – ليبيا – خلال الفترة ٢٨ ٢٩ /١٠/٢٠٠٩ – ص٧ .

٧٩ للمزيد حول الإرهاب العدمي ؛ راجع : سيدر برج بيتر . سي أساطير إرهابية – بين الوهم والمغالاة والواقع – ترجمة معروف ، عفاف – ١٩٩٢ القاهرة – ص ٨٠ وما بعدها . د. العادلي ، محمود صالح – موسوعة القانون الجنائي للإرهاب – الجزء الأول : المواجهة الجنائية للإرهاب – دار الفكر الجامعي بالإسكندرية – مصر – ٢٠٠٢م – بند ٢٢٩ ص ٢٨٠ .

ونظام الحكم ، ليبدأ بعد ذلك ببناء أنظمة أخرى استمدت أفكارها من كتب صفراء ، وآراء متطرفة ، تم تلقينها للجماعات الإرهابية عبر كهوف مظلمة من خلال تنظيماتهم السرية .

ولذا فإن مواجهة هذا الفكر المتطرف والإرهابي لا يجب أن يخضع للشرعية الجنائية العادية ، بل لشرعية جنائية غير عادية ، تستمد مبادئها وأحكامها من منطلق أن التهاون مع الأفكار المتطرفة أو الإرهابية معناه انهيار مؤسسة القانون ذاتها ، والعودة بالمجتمعات إلى عصر ما قبل الدولة، وليس أدل على ذلك من أن الدول التي دهسها قطار الإرهاب ، انزلقت لمستنقع التفكك والتشرذم ، ودفعت هذه الدول فواتير غالية من دماء الأبرياء ، ومن انهيار لكثير من مؤسساتها ، بل انتكست هذه الدول عبر كافة الأصعدة ، فعادت إلى عصر الفوضى والهمجية واللادولة .

- **موقف المشرع البحريني :**

وحسبنا ما فعل المشرع البحريني حينما سمح للنيابة العامة أن تجري على نظام تقنية المعلومات المتصل بالجريمة، إذ تنص المادة ١٥ من قانون جرائم تقنية المعلومات ـ القانون رقم ٦٠ لسنة ٢٠١٤ [٨٠] ـ على أنه :

" ١ للنيابة العامة أن تصدر أمراً مسبباً بالدخول إلى ما يلي وتفتيشه:

أ نظام تقنية المعلومات المتصل بالجريمة أو أي جزء منه وأية بيانات لوسيلة تقنية المعلومات مخزنة فيه.

ب أي من وسائط تخزين بيانات وسيلة تقنية المعلومات التي من المحتمل أن يكون مخزناً عليها بيانات متصلة بالجريمة.

٢ إذا قامت لدى النيابة العامة أثناء تنفيذ الأمر المشار إليه في البند أ من الفقرة ١ من هذه المادة أمارات قوية بأن البيانات المتصلة بالجريمة مخزنة في نظام تقنية المعلومات آخر أو في جزء منه، وكانت هذه البيانات قابلة لأن يتم الدخول إليها من خلال نظام تقنية المعلومات الأول أو متاحة من خلاله على نحو مشروع، فإن للنيابة العامة أن تصدر أمراً مسبباً بمد الدخول والتفتيش إلى النظام الآخر " .

- **٥٧ـ خامساً : الضبط :**

ضبط الأشياء المتعلقة بالجريمة هو إجراء قانوني يتمثّل في وضع كل ما يحتمل أن يكون قد استعمل في ارتكاب الجريمة أو نتج عنها أو أن تكون الجريمة وقعت عليه أو ما من شأنه أن يفيد في

٨٠ المنشور بالجريدة الرسمية – العدد ٣١٧٨ – الصادر في ٢٠١٤/١٠/٩ .

كشف الجريمة على ذمّة التحقيق[٨١] ، وبعبارة أخرى ضبط الأشياء هو وضعها تحت يد السلطة العامة للتحفظ عليها حتى يتم انتهاء الإجراءات في الدعوى الجنائية سواء بإصدار قرار بحفظ الأوراق أو أمرا بأن لا وجه لإقامة الدعوى أو حكم في موضوعها[٨٢] .

إذ يتعين على رجل الضبط القضائي عند ضبط الشيء أن يسلمه للمحقق فورا باعتباره صاحب الاختصاص في هذا الشأن. وللمحقق أن يعيده لمن ضبط لديه أو أن يأمر بالتحفظ عليه لحين حفظ الدعوى أو صدور أمر بأن لا وجه لإقامة الدعوى أو حكم في موضوعها.

وتحرص قوانين الإجراءات الجنائي على النص على أحوال الضبط والجهات المختصة باتخاذه والإجراءات الواجب إتباعها. وأهمية ضبط الأشياء تنبع من كونها تجسد أدلة الواقعة الجنائية ويدور في فلكها معظم إجراءات البحث والتحقيق الجنائي والمحاكمة .

فالأدلة الجنائية هي الأعمدة التي ترتكز عليها الأحكام الجنائية سواء بالإدانة أم البراءة .وللمحقق أن يستعين بالخبراء لتحديد ماهية الأشياء المضبوطة ، إذ يقوم بتحريزها عقب ضبطها ويرسلها لهم بكتاب يتضمن طلباته فيما يتعلق بهذه الأشياء.

والتساؤل الآن: هل يمكن ضبط الاتصالات والمراسلات عبر شبكة الإنترنت وغير ذلك من نشاط يمارس عبر وسائل التواصل الاجتماعي مثل الفيس بوك و تويتر ؟ .

- **الوضع في القانون المقارن :**

وهذا الإجراء تنص عليه قوانين العديد من الدول الأخرى بما فيها الولايات المتحدة الأمريكية وفرنسا وكندا واليابان وهولندا .

ففي **الولايات المتحدة الأمريكية** ـ على سبيل المثال ـ يجيز القانون اعتراض الاتصالات الإلكترونية بصفة عامة بما في ذلك شبكات الحاسب الآلي ، شريطة الحصول على إذن من المحكمة .

ووفقا للقانون الفرنسي الصادر في ١٠ يوليو سنة ١٩٩١ يجوز اعتراض الاتصالات البعدية ومنها شبكة المعلومات ، ونفس الحال في القانون الهولندي الذي يجيز إجراء التنصت على شبكة الحاسب الآلي بموجب أمر أو إذن من قاضي التحقيق ، في حالة ثبوت ضلوع المتهم في جرائم خطيرة ، ويشمل ذلك كل وسائل الاتصال بما في ذلك التلكس Telex ، والفاكس Tele fax ونقل البيانات .

---

٨١ راجع : المركز العربي للبحوث القانونية والقضائية التابع لجامعة الدول العربية القانون العربي الاسترشادي للإجراءات الجزائية : http://www.carjj.org/node/1742

٨٢ قارن : د. حسن المرصفاوى شرح قانون الإجراءات والمحاكمات الجزائية الكويتية ط ٧٠ ص٣١٣ .

وفي اليابان سبق القضاء المشرع ، إذ أجاز القضاء الياباني هذا الإجراء بالرغم من أن القانون هناك لم ينص صراحة على السماح به ، فقد أقرت إحدى المحاكم هناك – هي محكمة مقاطعة Kofu سنة ١٩٩١ ـ مشروعية التنصت على شبكات الحاسب الآلي في سبيل البحث عن الدليل [٨٣] .

ويمكن تبرير ذلك – في نظرنا ـ بأن القضاء الياباني أخذ بروح النصوص وفحواها ، وليس بحروفها ومبناها .

- **الوضع في القانون البحريني :**

١ ضبط الرسائل في قانون الإجراءات الجنائية البحريني :

طبقاً للمادة ٢٩ من قانون حماية المجتمع من الأعمال الإرهابية ـ الصادر بالمرسوم رقم ٥٨ لسنة ٢٠٠٦ ـ للمحامي العام أو من يقوم مقامه أن يأمر بضبط الرسائل بجميع أنواعها والمطبوعات والطرود والبرقيات، وبمراقبة الاتصالات بجميع وسائلها، وتسجيل ما يجرى في الأماكن العامة أو الخاصة، متى كان لذلك فائدة في كشف الحقيقة في الجرائم التي تنطبق عليها أحكام هذا القانون .وفي جميع الأحوال يجب أن يكون أمر الضبط أو المراقبة أو التسجيل مسبباً ولمدة لا تجاوز ستين يوماً، ولا يجوز مد هذه المدة إلا بأمر من المحكمة الكبرى.

صحيح أن هذا النص لم يذكر صراحةً مراقبة وضبط الاتصالات الإلكترونية بجميع صورها وأشكالها بما في ذلك الرسائل الإلكترونية ، غير أن عبارات النص جاءت مطلقة فهي تتحدث عن الرسائل بجميع أنواعها و الاتصالات بجميع وسائلها ، الأمر الذي نرى معه أنه يمكن اعتبار هذا الأمر جائزاً ومشمولاً بالنص المشار إليه بصورة ضمنية ، إذ يتسع مفهوم الرسائل والاتصالات إلى أبعد من المفهوم التقليدي لها .

٢ ضبط الرسائل ـ وما يتصل به من إجراءات تمهيدية أو تكميلية للضبط ـ في قانون جرائم تقنية المعلومات البحريني :

وفقاً للمادة ١٢ من قانون جرائم تقنية المعلومات البحريني ـ الصادر بالقانون رقم ٦٠ لسنة ٢٠١٤ [٨٤] ـ للنيابة العامة أن تأمر أي شخص بالقيام على وجه السرعة بالحفاظ على سلامة بيانات معينة لوسيلة تقنية المعلومات، بما في ذلك بيانات خط السير المخزنة داخل نظام تقنية

---

٨٣ ـ د. أحمد ، هلالي عبد اللاه ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ـ دراسة مقارنة ، ص٧٩ ـ ٨٠؛ المناعسة ، أسامة وآخرون ، ص٢٨٣ ـ ٢٨٥ . وأيضاً : د. ارحومة ؛ موسى مسعود – بحث سابق – ص ١٣ .

Yamaguchi Atsushi : "Computer crimes and others crimes against information Technology in Japan، Rev. int. de dr. pén. 1993. P. 448.

٨٤ تم نشر هذا القانون بالجريدة الرسمية – العدد ٣١٧٨ – الصادر في ٢٠١٤/١٠/٠٩ .

المعلومات، تكون في حيازته أو تحت سيطرته وبالإبقاء على سلامة هذه البيانات متى رأت الحاجة لذلك لإظهار الحقيقة في أية جريمة وتوافرت لديها دلائل تحملها على الاعتقاد بأن هذه البيانات عرضة للفقد أو التغيير. كما أن للنيابة العامة أن تأمر الشخص المشار إليه في الفقرة ١ من هذه المادة بالحفاظ على البيانات والإبقاء على سلامتها لمدة لا تزيد على تسعين يوماً، وللمحكمة الكبرى الجنائية منعقدة في غرفة المشورة أن تأذن للنيابة العامة، بناء على طلب مشفوع بالمبررات يقدم قبل انقضاء المدة المشار إليها بثلاثة أيام، مد هذه الفترة لمدة أو لمدد متعاقبة لا يزيد مجموعها على تسعين يوماً أخرى، وعلى المحكمة – كلما أمكن ذلك ـ سماع أقوال الشخص المشار إليه. فضلا عن ذلك يجوز للنيابة العامة أن تأمر الشخص المشار إليه في الفقرة ١ من هذه المادة بالمحافظة على سرية الأمر الصادر له وفقاً لأحكام أي من الفقرتين ١ و ٢ من هذه المادة لمدة لا تزيد على تسعين يوماً، قابلة للتجديد لمدة أو لمدد متعاقبة لا يزيد مجموعها على تسعين يوماً أخرى وبالإجراء المنصوص عليه بالفقرة ٢ المشار إليها.

أما المادة ١٣ من نفس القانون فقد أجازت للنيابة العامة أن تأمر أي شخص يكون حائزاً أو تحت سيطرته بيانات معينة لوسيلة تقنية المعلومات بتقديمها على وجه السرعة بما في ذلك البيانات المخزنة داخل نظام تقنية معلومات أو أية وسيلة تقنية المعلومات. كما أن للنيابة العامة أن تأمر أي مزود خدمة بتقديم أية معلومات تكون في حيازته أو تحت سيطرته عن أي مشترك في خدماته أو مستخدم لها، سواء كانت هذه المعلومات في صورة بيانات وسيلة تقنية المعلومات أو في أية صورة أخرى ولا يدخل في ذلك بيانات خط السير والمحتوى.وذلك كله متى رأت النيابة العامة الحاجة لذلك لإظهار الحقيقة في الجريمة.

في حين أن المادة ١٤ من ذات القانون فقد أجازت لقاضي المحكمة الصغرى، بناء على طلب النيابة العامة، وبعد اطلاعه على الأوراق أن يأمر بما يلي:

أ القيام على وجه السرعة بالحفاظ على بيانات خط السير المتصلة بالجريمة سواء كان الإرسال قد تم بثه من خلال مزود خدمة واحد أو أكثر.

ب الكشف عن قدر كاف من بيانات خط السير لتمكين النيابة العامة من تحديد مزود الخدمة والمسار الذي تم إرسال هذه البيانات من خلاله، متى كان ذلك يساهم في إظهار الحقيقة في جريمة معاقب عليها بموجب هذا القانون أو أي قانون آخر. ويصدر القاضي أمره في هذه الحالة مسبباً.

وفي سبيل وقوف النيابة العامة على الحقيقة في الجرائم الإلكترونية أجازت المادة ١٥ – من قانون تقنية المعلومات مدار البحث ـ للنيابة العامة أن تصدر أمراً مسبباً بالدخول إلى ما يلي وتفتيشه:

أ نظام تقنية المعلومات المتصل بالجريمة أو أي جزء منه وأية بيانات لوسيلة تقنية المعلومات مخزنة فيه.

ب أي من وسائط تخزين بيانات وسيلة تقنية المعلومات التي من المحتمل أن يكون مخزناً عليها بيانات متصلة بالجريمة.

و إذا قامت لدى النيابة العامة أثناء تنفيذ الأمر المشار إليه في البند أ من الفقرة ١ من هذه المادة أمارات قوية بأن البيانات المتصلة بالجريمة مخزنة في نظام تقنية المعلومات الآخر أو في جزء منه، وكانت هذه البيانات قابلة لأن يتم الدخول إليها من خلال نظام تقنية المعلومات الأول أو متاحة من خلاله على نحو مشروع، فإن للنيابة العامة أن تصدر أمراً مسبباً بمد الدخول والتفتيش إلى النظام الآخر.

و للنيابة العامة– وفقاً للمادة ١٦ من قانون تقنية المعلومات سالف البيان ـ سلطة الضبط والتحفظ على بيانات وسيلة تقنية المعلومات التي يتم الدخول إليها استناداً إلى أحكام المادة ١٥ من هذا القانون، ويشمل ذلك ما يلي:

أ الضبط والتحفظ على نظام تقنية المعلومات، أو أي جزء منه، أو أي من وسائط تخزين بيانات وسيلة تقنية المعلومات.

ب استنساخ بيانات وسيلة تقنية المعلومات والاحتفاظ بالنسخة.

ج المحافظة على سلامة بيانات وسيلة تقنية المعلومات.

د رفع بيانات وسيلة تقنية المعلومات من نظام تقنية المعلومات الذي تم الدخول إليه أو جعل الدخول إليها غير متاح.

ولا تشمل سلطة الضبط والتحفظ المشار إليها في الفقرة ١ من هذه المادة ما يكون قد وضعه المتهم تحت تصرف المدافع عنه أو الخبير الاستشاري لأداء المهمة التي عهد إليهما بها ولا المراسلات المتبادلة بينهما في القضية.

وأسند قانون جرائم تقنية المعلومات لقاضي المحكمة الصغرى– وفقا للمادة ١٧ ـ بناءً على طلب النيابة العامة، وبعد اطلاعه على الأوراق أن يأمر أي شخص مختص أو على دراية بكيفية عمل نظام تقنية المعلومات وبالتدابير المطبقة لحماية البيانات المخزنة في هذا النظام بأن يوفر لها، وبالقدر المعقول، المعلومات اللازمة لتمكينها من تنفيذ الإجراءات المنصوص عليها في المادتين ١٥ و ١٦ من هذا القانون. ويقدر القاضي – إن كان لذلك مقتضى – أتعاب من قام بتكليفه بأداء الأمر.

مع مراعاة الضوابط المنصوص عليها في البند ب من المادة ١٤ من هذا القانون، يجوز للنيابة العامة – طبقا للمادة ١٨ ـ بعد الحصول على إذن من قاضي المحكمة الصغرى القيام بما يلي:

أ تكليف أي شخص مختص بالقيام بجمع وتسجيل بيانات خط السير وبيانات المحتوى، أو أي منهما، المتعلقة باتصالات محددة يتم إرسالها بواسطة نظام تقنية المعلومات، وذلك حين حدوث هذه الاتصالات.

ب تكليف أي مزود خدمة، بالقيام بالأعمال المشار إليها في البند أ أو تقديم المساعدة اللازمة لمن كلفته النيابة العامة القيام بهذه الأعمال.

ج تكليف أي شخص مختص للقيام بحجب بيانات محتوى أية وسيلة تقنية المعلومات أو أي جزء منها ارتكبت بواسطتها أي من جرائم تقنية المعلومات.

وفي جميع الأحوال يجب أن يكون الإذن لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمدة أو مدد أخرى مماثلة.

و يحظر على من تم تكليفه وفقاً لأحكام الفقرة ١ من هذه المادة الكشف دون مسوغ في القانون لأي شخص آخر عن هذا التكليف أو بأية معلومات ذات صلة به أو الانتفاع بها بأية طريقة.

وفي سبيل تحقيق الفاعلية للإجراءات المشار إليها ادخرت المادة ١٩ من هذا القانون عقوبة الحبس مدة لا تزيد على سنتين وبالغرامة التي لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين لكل من لم يمتثل، قبل انقضاء المهلة التي حددها قاضي المحكمة الصغرى أو النيابة العامة بحسب الأحوال، لأمر أو تكليف صدر له وفقاً لحكم أي من الفقرتين ١ أو ٢ من المادة ١٢ ، أو أي من المادتين ١٣ أو ١٤ ، أو الفقرة ١ من المادة ١٨ من هذا القانون، كما يعاقب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين كل من خالف:أ الأمر المشار إليه في الفقرة ٣ من المادة ١٢ من هذا القانون.

ب حكم الفقرة ٢ من المادة ١٨ من هذا القانون.

وتكون العقوبة السجن مدة لا تزيد على خمس سنين إذا كان الجاني موظفاً عاماً أو مكلفاً بخدمة عامة.

ولست بحاجة إلى إيضاح أن هذه الإجراءات تشمل إجراء الضبط ذاته ، وما يتصل به من إجراءات تمهيدية تسهل الضبط أو تعرقل وصول الغير لبيانات محتوى أية وسيلة تقنية المعلومات أو أي جزء منها ارتكبت بواسطتها أي من جرائم تقنية المعلومات .

- **ضوابط تنظيم أحكام الضبط والتفتيش في الجرائم الإرهابية عبر الفضاء الإلكتروني :**

جلي مما تقدم أن مصالح المجتمع تفرض ضرورة سن التشريعات التي تضع النقاط مع الحروف بالنسبة لجوانب الضبط والتفتيش فيما يتعلق بالجرائم الإلكترونية بوجه عام وجرائم الإرهاب عبر الفضاء الإلكتروني بوجه خاص .

ولست بحاجة إلى التذكير بأن مهمة المشرع – أو المقنن – جد عسيرة فهو مطالب بعقد موازنة دقيقة بين مصالح المجتمع ومصالح الأفراد ، ومصالح المجتمع تتمثل في حمايته من خطر داهم قد يصل مداه إلى هدم الدولة والنظام في حد ذاتهما ، لأن جرائم الإرهاب عبر الفضاء الإلكتروني خطرها على المجتمع أشد خطرا من خطر الحروب العادية ، إذ تستهدف هذه الجرائم إلى محو الدول من على الخريطة أو هدم الدول والأنظمة لصالح مخابرات ،أجهزة مخابراتية عالمية أو بالأقل لصالح أفكار مستمدة من القرون المستمدة كتبها أصحابها في ظل ظروف مغايرة أو بناء على فهم ضيق لنصوص دينية هي بريئة من هذا الفهم الضيق براءة الذئب من دم ابن يعقوب .

أما مصالح الأفراد فتتجسد في احترام الحقوق والحريات العامة وحماية حقهم في الخصوصية .

وما لاشك فيه أنه ليس معنى ذلك أن المشرع يتقيد بالشرعية الجنائية العادية ، كلا وألف كلا ليس هذا هو المطلوب ، فالمطلوب على العكس أن يتحرر المشرع من الأحكام التقليدية للشرعية الجنائية ، دون أن يخرج عن فكرة الشرعية في حد ذاتها ، صحيح مطلوب من المشرع أن يحترم حقوق وحريات الأفراد بحيث لابد أن تكون إجراءات الضبط والتفتيش صادرة من سلطة قضائية وأن تكون موجهة ضد متهم أو مشتبه فيه ، غير أن هذه القيود يجب أن تكون في إطار شرعية جنائية غير عادية ، شرعية تتسم بالسرعة والفاعلية ، تتلاءم مع طبيعة الخطر الداهم من جرائم الإرهاب عبر الفضاء الإلكتروني ، وتتوافق مع سرعة التخلص من الأدلة الرقمية ، وضخامة المعلومات أو البيانات محل التفتيش والضبط ، وتتناسب مع أن مرتكبي مثل هذه الجرائم هم – في الغالب الأعم – على درجة عالية من الذكاء ، ولديهم خبرات فنية تجعلهم يستطيعون تضليل العدالة .

كما نأمل أن يكون تنظيم المشرع – أو المقنن – لأحكام الضبط والتفتيش تراعي البُعد الدولي لجرائم الإرهاب عبر الفضاء الإلكتروني ، يراعى فيه طبيعة التنظيمات الإرهابية ، وتعدد خلاياها التي يغلب عليها التنظيم العنقودي ، أي كعنقود العنب أي أن كل مجموعة منفصلة عن غيرها من المجموعات ، وذلك بهدف تفادي الاعتراف على كل التنظيم الإرهابي حال القبض على أحد أفراد الخلية .

ناهيك عن ضرورة أن يكون تقنين أحكام الضبط والتفتيش يراعي ارتباط مادة جرائم الإرهاب عبر الفضاء الإلكتروني أو وسيلتها بأنظمة أطراف أخرى لا صلة لهم بها أو بشبكات ونظم معلومات خارج الحدود .

كما يتعين على المشرع أن يحترم ضمانات المتهم وما توجبه قرينة البراءة المقررة له .

ولا مراء في أن المعيار الذي سينتهي إليه المشرع في تنظيمه لأحكام القبض والتفتيش ، لن يدفعه إلى تقييد الحريات والحقوق العامة إلا في أضيق نطاق ، فحده الأعلى يتجسد في تحقيق مصلحة المجتمع وأمنه وحدها الأدنى هو الضرورة ، والضرورة تقدر بقدرها ، فلا مساس بهذه الحقوق وتلك الحريات إلا بصفة استثنائية ، والاستثناء – كما هو معلوم ـ لا يجوز التوسع فيه ولا القياس عليه .

- **خلاصة القول :**

ومن هنا نستطيع القول بأن المشرع البحريني كان موفقاً تماماً حينما نص في قانون جرائم تقنية المعلومات البحريني ـ سالف البيان – على العديد من إجراءات التحقيق المتعلقة بالجرائم الإلكترونية على النحو السالف بيانه ، وهو ما يسري بطبيعة الحال على الإرهاب الرقمي ، فهذه الإجراءات كافية في حد ذاتها لمواجهة الجرائم الإلكترونية ومنها جرائم الإرهاب عبر الفضاء الإلكتروني .

المبحث الثالث

تحديات وصعوبات البحث والتحقيق الجنائي عبر الفضاء الإلكتروني

- **توطئة :**

الصعوبات[٨٥] والتحديات[٨٦] في البحث والتحقيق الجنائي المتعلق بالإرهاب عبر الفضاء الإلكتروني عديدة ، ومن أبرزها : البعد الدولي ، والصعوبات المتعلقة بالحصول على الدليل ، علاوة على الصعوبات الفنية ، وسنعرض ذلك فيما يلي :-

المطلب الأول

البعد الدولي في جرائم الإرهاب عبر الفضاء الإلكتروني

- **المقصود بالبعد الدولي:**

لاشك في أن تنامي ظاهرة الجرائم المعلوماتية عبر الوطنية ، وتخطي آثارها حدود الدول ، أفرز صعوبات وعقبات سلطات التحقيق والبحث الجنائي في مجال جرائم الإرهاب عبر الفضاء الإلكتروني بخصوص ممارسة بعض الإجراءات عبر الحدود كالمعاينة والتفتيش والضبط في نطاق البيئة الافتراضية . يضاف إلى هذا وذاك مشكلة تنازع الاختصاص بصدد هذه الجرائم باعتبار أن آثارها تتجاوز حدود الدول ، الأمر الذي يجعل الحلول الوطنية غير مجدية ، وتظل مشوبة بالقصور . الأمر الذي يفرض ضرورة التعاون الدولي لمواجهة هذه الصعوبات ، من خلال الاتفاقيات الدولية ، وتعاون الأجهزة المعنية في كل دولة مع نظيرتها في الدول الأخرى .

فجرائم الإرهاب عبر الفضاء الإلكتروني يمكن أن ترتكب عبر عدة دول ، إذ يمكن لأحد الإرهابيين أن يقوم بالنفاذ إلى أنظمه الحاسوب في أحد البلدان ويتم التلاعب بالبيانات في بلد آخر وتسجّل النتائج في بلد ثالث، فضلاً عن أنّه يمكن تخزين أدلة الجريمة الإرهابية عبر الفضاء

---

٨٥ الصعوبة هي الأمر العسير . راجع : مجمع اللغة العربية – المعجم الوجيز – القاهرة ٢٠٠٠م كلمة صَعُبَ – ص ٣٦٤ . وهي أيضاً العقبة . راجع :

http://www.arabdict.com/عربي عربي/D8%A7%D9%84%D8%B5%D8%B9%D9%88%D8%A8%D8%A9

٨٦ التحديات يقصد بها التصدي أو مواجهة الأمور المهددة لوجود الشئ ، وفي فلسفة التاريخ وجدت نظرية تحت مسمى التّحدّي والاستجابة مؤدّاها: أنّ الحضارة تنشأ عندما يواجه شعب ما تحدّيًا يهدّد كيانه فيواجه هذا التحدّي ببذل جهد مضاعف استجابة لحبّ البقاء. راجع :

http://www.arabdict.com/%D8%B9%D8%B1%D8%A8%D9%8A%D8%B9%D8%B1%D8%A8%D9%8A/%D8%AA%D8%AD%D8%AF%D9%8A%D8%A7%D8%AA

الإلكتروني في جهاز حاسوب موجود في بلد غير الذي ارتكب فيه المجرم فعله، الأمر الذي يتيح الفرصة للإرهابي إخفاء هويته، ونقل المواد من خلال قنوات موجودة في بُلدان مختلفة، في قارات مختلفة قبل الوصول إلى المرسَل إليهم، نتيجة القدرة على التنقل إلكترونياً من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارّات مختلفة، الأمر الذي يسفر عنه وقوع الإرهاب عبر الفضاء الإلكتروني في عدة دول وتحكمها عدة قوانين وقواعد معنية بذلك، الأمر الذي يشكل تحدياً أمام الجهات القضائية في تطبيق القانون ويزيد من صعوبة التحقيق فيها [٨٧] .

المطلب الثاني
الصعوبات المتعلقة بالحصول على الدليل والجوانب الفنية والإرهاب عبر الفضاء الإلكتروني

- **أولاً : صعوبات تتعلق بالحصول على الدليل :**

إذا كانت الإدانة في الحكم الجنائي تبني على الجزم واليقين ، فإن الحصول على أدلة رقمية تكون لها حجيتها أمام القضاء أمر تكتنفه الكثير من الصعوبات . و من أهم هذه الصعوبات :

١ إخفاء الأدلة :

إذا كانت الرقابة على الإنترنت ضعيفة ، فإن مرتكبي جرائم الإرهاب عبر الفضاء الإلكتروني من التسلل والعبث في النبضات والذبذبات الإلكترونية التي تسجل عن طريقها المعلومات والبيانات بغرض إحداث تغيرات في البيانات والمعلومات والتلاعب في منظومة الحاسب الآلي ومحتوياته ، كما يمكن للإرهابيين القيام بدس برامج خاصة ضمن برنامجه فلا يشعر بها القائمون بالتشغيل ، الأمر الذي يمكن معه الإرهابيين أن ينجحوا في إخفاء ما قاموا به أو محو الدليل عليه ، مما يتعذر معه إعادة عرض أعمال التسلل والدخول ، وهكذا يستطيع الجناة في جرائم الإرهاب عبر الفضاء الإلكتروني إخفاء جرائمهم وطمس آثارها في وقت قصير ، وقبل وصول سلطة التحقيق ، الأمر الذي يؤدي إلى صعوبات تعيق إجراءات التحقيق الرامية إلى الوصول إلى دليل .

- **ومن صور إخفاء الدليل :**

١ـ إخفاء أدلة الإرهاب عبر الفضاء الإلكتروني في "قرص صلب خارجي " يتم إخفائه بعيداً مكان إقامة الجناة [٨٨] .

---

٨٧ بخصوص ارتكاب الجريمة الإلكترونية عبر عدة دول ؛ أنظر : سكولمان ، كريستنيا الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية، بحث مقدم ضمن أعمال الندوة الإقليمية حول "الجرائم المتصلة بالكمبيوتر"، ١٩ ٢٠ نيسان/يونيو٢٠٠٧،المملكة المغربية، ص ١١٩.

٨٨ جدير بالذكر أن شبكة الإنترنت أصبحت غنية بالمواقع التي تشكل جامعات للإرهابيين ؛ فمن خلالها يتم إعطاء دروس لهم تساعدهم على إخفاء جرائمهم بل وطمس كل دليل يتصل بجرائمهم الإرهابية التي يرتكبونها عبر الفضاء الإلكتروني . ففي أحد هذه المواقع نجد عدة نصائح تعوق عمل رجال الشرطة والنيابة ؛ إذ يقول هذا الموقع : هذه وسائل وأفكار مُقترحة ، أتطفل فيها على أهل الاختصاص ، وأهديها لكم يا أسود الإعلام =

٢- تشفير جهاز الحاسب الآلي أو تشفير القرص الصلب الخارجي [٨٩] ، أو تشفير المعلومات الموجودة على القرص الصلب الخارجي .

٣- عدم وجود أي بيانات تدل على صاحب أو مستخدم القرص الصلب الخارجي [٩٠] .

٤- عند دخول الإرهابي لمواقع إرهابية يمكنه بخطوات تضليلية إخفاء هذا الدخول أو إظهاره بصورة مغايرة للحقيقة [٩١] .

= الجهادي ، وأشُهد الله أني أحبكم ، وأحبُ من يُحبكم ، ولو كنت أستطيع ، لتناقشت معكم فيها ، ولرددت على كل من يُشارك منكم، ولكن عزائي أن جُل وقتي على الإنترنت بينكم ، ولكن تصعُب علي والله المُشاركة... الوسائل المُقترحة كالتالي :

{١}حفظ الأرشيف الجهادي كاملاً – المقصود بطبيعة الحال الأرشيف الإرهابي في "قرص صلب خارجي " ليسهل تشفيره أولاً ، وإخفائه ثانياً ، علماً أنه يوجد الآن في ألأسواق الالكترونية ،أقراص صلبة ذات سعات مُتعددة ، وفيها خاصّية التشفير بطول ٢٥٦ بت ، مثل القرص الصلب من شركة WD والمسمى My Passport Essentialحيث يأتي مُدمج في القرص الصلب برنامج WD Smart Ware وهو برنامج فيه الكثير من المُميزات ، ولكن الذي يُهمنا منها خاصّية وضع كلمة سر على القرص الصلب ، وفي حالة نسيانك لكلمة السر ستفقد جميع بياناتك في الداخل فتنبه!، ويأتي في نفس القرص شرح لمميزاته بلغات عدة من بينها اللغة العربية ....

{ 4 }إخفاء القرص الصلب الخارجي المُشفر،الذي يحتوي على الأرشيف الجهادي ، في مكان بعيد عن مكان تواجدك الدائم . { 5 }عدم استخدام القرص الصلب الخارجي المُشفر ، إلا في حالة محدودة جداً كأخذ شيء منه ، أو إضافة شيء إليه ، وإرجاعه إلى مكانه الآمن .... .

راجع : الشبكة العربية الليبرالية

http://www.liberalls.org/vb/showthread.php?t=5668

٨٩ وهذا ما ينصح به أحد المواقع الإرهابية الإرهابيين بالآتي .... { 2 } الحرص على أن لا يوجد في داخل القرص الصلب الخارجي، أي شيء يدل على شخصيتك، كوجود أسمك، أو ملفات تدل عليك . { 3 }الحرص على عدم كتابة كلمة السر في مُفكرة على جهازك ، أو في ورقة بجانب جهازك ، أو غيرها ، بل في مكان واحد فقط ، في وسط رأسك.....

راجع ، الشبكة العربية الليبرالية :

http://www.liberalls.org/vb/showthread.php?t=5668

٩٠ ولذا ينصح أحد المواقع الإرهابية الإرهابيين بالآتي : .... { 2 }الحرص على أن لا يوجد في داخل القرص الصلب الخارجي، أي شيء يدل على شخصيتك، كوجود اسمك، أو ملفات تدل عليك ..... { 7 }احرص على أن لا يوجد في جهازك الشخصي الذي تستخدمه ، أي مواد جهادية ، و لا تنسى إزالة المواقع الجهادية من مُفضلتك. .

راجع : الشبكة العربية الليبرالية

http://www.liberalls.org/vb/showthread.php?t=5668

٩١ ولذا ينصح أحد المواقع الإرهابية الإرهابيين بالآتي .... { 10 } إذا كنت من رُواد المنتديات الجهادية ، ومن أصحاب المُشاركات فيها ، فلا تجعل في قرصك الخارجي الصلب ولا في أصبع الذاكرة "الجهادي" ما يدل على ذلك ويجب عليك حفظ اسمك في المنتدى ، وكلمة السر ، وبريدك الإلكتروني المُستخدم في المواقع الجهادية في رأسك فقط ، وأما مُشاركاتك التي أنزلتها في المنتدى الجهادي ، فقم بحفظها كصفحة HTML في ذاكرة الـ USB "الجهادية" ، بعد أن تُسجل خُروج من المنتدى ، حتى تظهر المشاركة كمقالة أُعجبت بها لأحد =

٥ـ كما يمكن أن يتمثل أخفاء الدليل في الاستعانة بفلاش ميموري أصابع ذاكرة يتم نقل كل نشاط الإرهابي فيها ، مما يسهل معه أن يتخلص منها وقت الضرورة ، فيفلت من التعقب أو التتبع أو سيف القانون والعدالة [٩٢] .

- **محو دليل الاغتيال عبر الفضاء الإلكتروني :**

ويمكننا أن نضرب مثالا على قدرة الإرهابيين على طمس الأدلة في إحدى الجرائم الإرهابية التي ارتكبت عبر الفضاء الإلكتروني وتم طمس الأدلة فيها ، ما حدث من تمت محاولة اغتيال أحد الأشخاص بإطلاق الرصاص عليه ، غير أنه نجا من هذه المحاولة ، وفي نفس الليلة حال تواجده بالمستشفي، قام الجناة باختراق الحاسب الآلي للمستشفي ، حيث غيروا الدواء له وحرروا له حقنة مميتة، وبالفعل مات بعد ساعات قليلة اخترقوا مرة أخرى الحاسب الآلي للمستشفي ، ثم غيروا نظام الدواء مرة أخرى إلى شكله الصحيح، الأمر الذي يجعل الممرضة هي المتهمة بالقتل [٩٣] .

= الكتاب "المجهولين" في المنتدى الجهادي ، ومن ثم انقلها إلى أرشيفك الجهادي ، وأحرص على عدم الاحتفاظ بالملفات الأصلية لمشاركاتك الجهادية في المنتديات ، من ملفات التصاميم المفتوحة ، أو مُسودات المقالات النصية ، وغير ذلك من الأمور التي قد تكشف عن شخصيتك ، في حال الوصول إليها ، و تُستخدم كدليل ضدك ،دون الحاجة لسماعاعترافاتك !! ، واجعل مكان صياغة أعمالك في أصبع الذاكرة "الجهادي" فقط ، وقم بحذفها مباشرة بعد أن تنتهي منها ، لزوال الفائدة منها ، و أما الذاكرة "الجهادية" فستقوم بإتلافها "مادياً" وشراء أخرى جديدة، كل فترة زمنية أن تجددها ، ولا تحتفظ بشيء من الملفات الأصلية لمشاركاتك على القرص الخارجي المشفر ولو مؤقتاً، اللهم إلا ما أشرت إليه من حفظها كنسخة HTML ، بعد إنزالها في المنتدى الجهادي ، وبهذه الطريقة ستُخفي جميع آثار أعمالك ومشاركاتك الجهادية السابقة ، عند إتلافك لذاكرة الـ USBالجهادية .

راجع : الشبكة العربية الليبرالية http://www.liberalls.org/vb/showthread.php?t=5668

٩٢ وهذا الأمر ينصح به الإرهابيين بعضهم البعض الآخر ؛ حيث تقول أحد المواقع الإرهابية : ..... { 4 }اقتناء أصبعي ذاكرة USB ، من أي حجم تريد، حيث يُستخدم أحَدها للاستخدامات الشخصية فقط، ولا يُستخدم أبداً في حفظ مواد جهادية ولو مؤقتاً ، وجعل الآخر كوسيلة نقل للمواد الجهادية بين جهازك الشخصي وبين القرص الخارجي المُشفر الذي يحتوي على الأرشيف الجهادي ، فمثلاً عند نزول فيلم جهادي جديد ، أو مجلة جهادية أو غير ذلك من المواد الجهادية ، قم بإدخال أصبع الذاكرة "الجهادي" في جهازك ، ثم قم بتحميل الفيلم الجهادي أو المجلة الجهادية وحفظها مباشرة إلى أصبع الذاكرة " الجهادي" ، وبعد أن يمتلئ أصبع الذاكرة "الجهادي" بالمواد الجهادية ، يأتي الآن فقط دور القرص الصلب الخارجي المُشفر ، فتقوم بجلبه ، وتفريغ المواد الجهادية الموجودة في أصبع الذاكرة فيه ، وتُرجع القرص الصلب الخارجي المُشفر فوراً ، إلى مكانه الآمن، وذلك يعني بالطبع ، عدم حاجتك الفعلية إلى استخدام القرص الخارجي الصلب إلا في فترات زمنية متباعدة ، حسب حجم أصبع الذاكرة لديك.....
راجع : الشبكة العربية الليبرالية http://www.liberalls.org/vb/showthread.php?t=5668

٩٣ أنظر أمثلة من الإرهابي الإلكتروني لدى :
Examples of Cyber terrorism , from student paper by Jimmy Sproles and Will Byars for Computer Ethics Class 1998.http://csciwww.etsu.edu/gotterbarn/stdntppr/cases.htm

زيارة ٤ يناير ٢٠١٥

٢ غياب الدليل ضد متهم معين:

وقد يتوصل المحقق لوجود جريمة إرهابية ارتكبت عبر الفضاء الإلكتروني ، فقد يفشل في الوصول لمرتكب هذه الجريمة ، رغم وصول المحقق لأدلة على اقتراف الجريمة ، فقد لا تفصح عن صلة شخص معين بالجريمة المرتكبة ، نظرا لأن معظم نظم الحاسب الآلي لا تسمح للمراجعين والفنيين بالتتابع العكسي لمسار مخرجاتها ، علاوة على صعوبة تتبع الآثار الإلكترونية ومراجعة وفحص الكم الهائل من البيانات والمعلومات المدرجة بالأنظمة ، وتعمد الجناة إلى إخفاء هويتهم .

٣ إعاقة الوصول إلى الدليل :

قد يلجأ الجناة في جرائم الإرهاب عبر الفضاء الإلكتروني إلى وسائل تضليلية تعرقل الوصول إلى الدليل ، كما هو الحال بالنسبة لاستخدام تقنيات التشفير [٩٤] ، أو كلمة السر، وذلك بهدف حجب المعلومة عن التداول العام ، ومنع الغير بما فيه أجهزة الرقابة من الوصول غير المشروع إلى البيانات والمعلومات المخزنة أو التلاعب فيها [٩٥] .

وهنا يكون أمام المحقق صعوبات تعرقل وصوله للحقيقة أو حصوله على دليل . فهل يجوز له إجبار المتهم على ذكر الباسوورد كلمة المرور أو فك التشفير ؟

وفقاً للقواعد التقليدية لا يجوز إجبار شخص على تقديم دليل ضد نفسه ، ولذا لا يكون أمام المحقق إلا أن يلجأ إلى فك التشفير أو الولوج إلى جهاز الحاسب الآلي أو الموقع الإلكتروني بوسائل أخرى فنية مثل برامج فك الشفرات أو معرفة الكود نمبر الرقم السري [٩٦] .

---

٩٤ مصطلح التشفير Cryptography هو عملية يتم فيها إخفاء المعلومات عن طريق مفتاح سري وخوارزمية،حيث إن الشخص الذي يعلم المفتاح ويعلم خوارزمية التشفير يمكنه فك الشفرة أي استعادة المعلومات الأصلية ، يمكن أيضا أن يقوم شخص لا يعرف خوارزمية التشفير ومفتاح التشفير بفك الشفرة ولكن تسمى العملية هنا عملية غير مخوله . راجع :

http://www.ejabah.info/ar/%D9%85%D8%A7_%D9%87%D9%88_%D8%A7%D9%84%D8%AA%D8%B4%D9%81%D9%8A%D8%B1 Cryptographic _%D8%9F

٩٥ لذا نجد أن الإرهابيين ينصحون بعضهم البعض الآخر بالآتي : ..... { 8 }يجب أن تضع كلمة سر على جميع ملفاتك المهمة "جداً" وذلك بجمعها في ملف واحد ثم ضغطها باستخدام برنامج الـ Win RAR،ولأن الهدف من استخدام برنامج الضغط هو وضع كلمة سر على ملفاتنا المُهمة ، فلسنا في حاجة إذاً إلى إنقاص حجم الملفات فقم باختيار نوع الضغط Store من قائمة Compression method ومن مجموعة Advanced قم بوضع كلمة سر معقّدة بضغطك على Set password ومن ثم إدخال كلمة السر المعقّدة التي تحتوي على أحرف صغيرة وكبيرة ، وأرقام ، ورموز، وأجعلها لا تقل عن 10 خانات ، وبعدها فعّل خيار الـ Encrypt file names لتشفير أسماء الملفات، وعدم إظهارها إلا في حالة إدخالك لكلمة السر.... .راجع : الشبكة العربية الليبرالية :

http://www.liberalls.org/vb/showthread.php?t=5668

٩٦ أنظر أمثلة لفك الشفرات لدى في إحدى القضايا التي حدثت في ألمانيا : داود ، حسن طاهر ، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، ٢٠٠٠م ، ص ٢٣٣_٢٣٤ .

٤ الكتابة على المساحة الفارغة للقرص الصلب وتضليل المحقق :

قد يلجأ الجناة في جرائم الإرهاب عبر الفضاء الإلكتروني إلى استغلال المساحة الفارغة على القرص الصلب في تخزين أدلة ارتكابهم هذه الجرائم ، مما يعرقل عمل المحقق [٩٧] .

٩٧ راجع : الشبكة العربية الليبرالية :

http://www.liberalls.org/vb/showthread.php?t=5668

حيث يوضح هذا الموقع نصائح للإرهابيين من بينها النصيحة رقم ٩ التي توجه كلامها لكل إرهابي كالآتي : {9} قم باستخدام البرامج التي تقوم بالكتابة على المساحة الفارغة MFT في القرص الصلب الخاص بجهازك الشخصي ، كل فترة زمنية أنت تحددها ، كمرة واحدة في الشهر مثلاً ، و من البرامج المقترحة برنامج Cleaner حيث يُوجد فيه خاصّية الكتابة على المساحة الفارغة MFT حتى ٣٥ مرة ،و قد يستغرق ذلك ساعات طويلة ، حسب المساحة الفارغة في قرصك الصلب وحسب مواصفات جهازك ، حيث أن كل ما تقوم بحذفه من جهازك ، يذهب مباشرة للمساحة الفارغة MFT ويسهُل على الهواة استرجاع الملفات المحذوفة ، فضلاً عن الأجهزة الأمنية ، فأحرص أخي على الكتابة عليها بشكل دوري .

الخاتمة

- **عدم صلاحية الأدوات التقليدية لمكافحة الإرهاب الرقمي :**

جلي مما تقدم أن الإرهاب عبر الفضاء الإلكتروني هو ظاهرة جديدة في عالم الجريمة ، ولا يصح منطقاً ولا عقلاً ولا عدالة أن نستخدم ذات الأدوات التقليدية لمكافحة هذا الإرهاب . ومن ثم لا يصلح دفاعاً عن تقليدية أدوات المكافحة أن نتمسك بضرورة احترام الحريات الفردية والشرعية الجنائية التقليدية ، لعدة أسباب :

أولاً : لأن أية حرية ليست مطلقة ، بل هي حرية دائما وأبدا نسبية ، فأنت حر ما لم تضر.

وثانياً : الشرعية الجنائية التقليدية تحكم القواعد التقليدية .

وعليه فنحن لا نطالب بالتحرر المطلق من الشرعية الجنائية ، بل نطالب بأن تكون الشرعية الجنائية أكثر مرونة من القواعد العادية التي تواجه الإجرام العادي . لأننا نتحدث عن جرائم إرهابية ترتكب عبر الفضاء الإلكتروني، تهدد كيان المجتمع ووحدته وسلامته ، فالشرعية الجنائية العادية – بأفكارها التقليدية – لا تصلح لمواجهة خطر العصر ، ألا وهو الإرهاب ، فلابد أن نقر بوجود شرعية جنائية غير عادية لمواجهة الخطر الجديد على الحياة وعلى الإنسانية وعلى الدول . فالإرهاب الذي نوجهه هو إرهاب عدمي ، أي يريد أن يرتد بالمجتمعات إلى مرحلة العدم ، أي مرحلة المربع رقم الصفر ، فهو يريد هدم كافة الأنظمة القائمة في أي مجتمع أي نظام القضاء – ونظام الجيش – ونظام الحكم ، ليبدأ بعد ذلك ببناء أنظمة أخرى استمدت أفكارها من كتب صفراء ، وآراء متطرفة ، تم تلقينها للجماعات الإرهابية عبر كهوف مظلمة من خلال تنظيماتهم السرية .

ولذا فإن مواجهة هذا الفكر المتطرف والإرهابي لا يجب أن يخضع للشرعية الجنائية العادية ، بل لشرعية جنائية غير عادية ، تستمد مبادئها وأحكامها من منطلق أن التهاون مع الأفكار المتطرفة أو الإرهابية معناه انهيار مؤسسة القانون ذاتها ، والعودة بالمجتمعات إلى عصر ما قبل الدولة ، وليس أدل على ذلك من أن الدول التي دهسها قطار الإرهاب ، انزلقت لمستنقع التفكك والتشرذم ، ودفعت هذه الدول فواتير غالية من دماء الأبرياء ، ومن انهيار لكثير من مؤسساتها ، بل انتكست هذه الدول عبر كافة الأصعدة ، فعادت إلى عصر الفوضى والهمجية واللادولة .

- **توصيات البحث :**

– **ونخلص من هذه الدراسة إلى التوصيات التالية :**

– لا مراء في أن المشرع البحريني كان موفقاً تماماً حينما نص في قانون جرائم تقنية المعلومات البحريني ـ سالف البيان – على العديد من إجراءات التحقيق المتعلقة بالجرائم الإلكترونية على النحو السالف بيانه ، وهو ما يسري بطبيعة الحال على الإرهاب الرقمي ، فهذه الإجراءات كافية في حد ذاتها لمواجهة الجرائم الإلكترونية ومنها جرائم الإرهاب عبر الفضاء الإلكتروني .

١ـ ضرورة تدريب القائمين على البحث والتحقيق الجنائي على تقنية وعلوم الحاسب الآلي لمواكبة كل جديد في هذا المضمار .

٢ـ التحرر من القيود التقليدية فيما يتعلق بإجراءات الضبط والتفتيش والإجراءات الاحتياطية تجاه المتهمين بارتكاب جرائم إرهابية عبر الفضاء الإلكتروني ، ومنح السلطات القائمة على البحث والتحقيق الجنائي سلطات أوسع مما هو مقرر في الجرائم التقليدية .

٣ـ ضرورة الموازنة بين المصلحة العامة للمجتمع التي تفرض ضرورة مواجهة إجرائية حاسمة فالإرهاب عبر الفضاء الإلكتروني ، وبين المصلحة الخاصة للمتهمين أو المشتبه في أنهم يقترفون هذا الإرهاب ، ولاسيما فيما يتعلق بالحق في الخصوصية ، وحرية التعبير ، وعند التعارض بينهما تفضل المصلحة الأولى على الثانية .

٤ـ إدخال مقرر دراسي جديد ضمن برامج الدراسة في كليات الحقوق والشرطة تتكفل ببيان كيفية البحث والتحقيق الجنائي وطرق الإثبات في جرائم الإرهاب عبر الفضاء الإلكتروني .

٥ـ نهيب بالمشرعين والمقنين بالدول العربية والإسلامية بأن يحذو حذو المملكة العربية السعودية ودولة الإمارات العربية المتحدة بشأن سن القوانين لمواجهة الجرائم المعلوماتية بوجه عام ، والإرهاب عبر الفضاء الإلكتروني بصفة خاصة .

٦ـ نأمل أن تسن القوانين اللازمة للوقاية من خطر الإرهاب عبر الفضاء الإلكتروني ، بحيث تسمح لرجال الشرطة المختصين بمراقبة الإنترنت وغيره من وسائل التواصل الاجتماعي لوقاية المجتمع من خطر الإرهاب الإلكتروني .

٧ـ نأمل أن تنضم كافة الدول العربية للاتفاقيات الدولية التي تسمح بالتعاون القضائي مع الدول الأخرى خاصة فيما يتعلق بالتصدي للإرهاب المرتكب عبر الفضاء الإلكتروني، سواء في ذلك فيما يتعلق بالوقاية منه بالسماح باختراق بعض المواقع أو حجبها إلخ ، وسواء فيما يتعلق بتسهيل الحصول على الأدلة الرقمية التي يمكن الحصول عليها لإدانة الجناة ، وكل ما يساهم في مكافحة هذا الإرهاب.

قائمة المراجع[٩٨]

أولاً : باللغة العربية :

(أ) الكتب والمؤلفات العامة والمتخصصة :

١- د. أحمد ، هلالي عبد اللاه ، تفتيش نظم الحاسب الآلي ، ط١ ، دار النهضة العربية ، القاهرة ١٩٩٧ .

٢- د. أحمد ، هلالي عبد اللاه، حجية المخرجات الكمبيوترية في المواد الجنائية، ١٩٩٩.

٣- د. الهيتي ، محمد حماد مرهج ، الموسوعة الجنائية في البحث والتحقيق الجنائي – أصول البحث والتحقيق الجنائي – موضوعه ، أشخاصه ، والقواعد التي تحكمه – دار الكتب القانونية ، دار شتات للنشر والبرمجيات – مصر – ٢٠٠٨م .

٤- د. حسني ، محمود نجيب ـ شرح قانون الإجراءات الجنائية، ط ٣، ١٩٩٨ .

٥- د. داود ، حسن طاهر، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، ٢٠٠٠ ف .

٦- د. رستم ، هشام ـ الجوانب الإجرائية للجرائم المعلوماتية ، أسيوط ، مصر ، ١٩٩٤ .

٧- د.العادلي ، محمود صالح – موسوعة القانون الجنائي للإرهاب – الجزء الأول : المواجهة الجنائية للإرهاب – دار الفكر الجامعي بالإسكندرية – مصر – ٢٠٠٢م .

٨- د.حسن المرصفاوى ـ شرح قانون الإجراءات والمحاكمات الجزائية الكويتية ، ط ١٩٧٠ . د. ن.

٩- د. عبد المطلب ، ممدوح عبد الحميد ـ البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت – دار الكتب القانونية – مصر – ٢٠٠٦م .

١٠- د. عقيدة ، محمد أبو العلا ـ شرح قانون الإجراءات الجنائية، ط ٢٠٠١– دار النهضة العربية بالقاهرة – ج ٢.

١١- د. ممدوح ، خالد ـ فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي – مصر ـ ٢٠٠٩ .

---

٩٨ يراعى أننا أكتفينا هنا بالإشارة إلى المراجع الأساسية في هذه القائمة ؛ أما المراجع الثانوية والأحكام والقوانين التي اعتمدت هذه الدراسة ، فاكتفينا بالإشارة إليها في موضوعها .

(ب) الرسائل العلمية والأبحاث والمقالات العلمية :

١ـ إبراهيم ، حسين – التحقيق الجنائي في مواجهة التقنيات والمتغيرات المدنية – مجلة كلية الدراسات العليا – أكاديمية مبارك للأمن – مصر – العدد الثامن – يناير ٢٠٠٣م ـ ص ٢١٨ .

٢ـ د. ارحومة ، موسى مسعود – الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية – بحث مقدم إلى المؤتمر المغاربي الأول حول : المعلوماتية والقانون – الذي نظمته أكاديمية الدراسات العليا – طرابلس – ليبيا – خلال الفترة ٢٨ـ ٢٩ /١٠/ ٢٠٠٩ .

٣ـ بوحويش ، عطية عثمان محمد ، حجية الدليل الرقمي في إثبات جرائم المعلوماتية ، رسالة التخصص العالي الماجستير ، مقدمة إلى أكاديمية الدراسات العليا/فرع بنغازي ، للعام الجامعي ٢٠٠٩ .

٤ـ د. عقيدة ، محمد أبو العلا – التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية ـ بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية – أكاديمية شرطة دبي ، مركز البحوث والدراسات تاريخ الانعقاد: ٢٦ـ ٢٨ إبريل /نيسان ٢٠٠٣ـ دبي ـ الإمارات العربية المتحدة .

٥ـ سندالي ، عبد الرزاق ، التشريع المغربي في مجال الجرائم المعلوماتية، ضمن أعمال الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر»، ٢٠ ـ ١٩ نيسان/ يونيو، ٢٠٠٧، المملكة المغربية.

٦ـ سكولمان ، كريستنيا ـالإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية، بحث مقدم ضمن أعمال الندوة الإقليمية حول "الجرائم المتصلة بالكمبيوتر"، ٢٠ـ١٩ نيسان/يونيو٢٠٠٧،المملكة المغربية، ص ١١٩.

(ج) كتب لغات ومعجم وكتب مترجمة :

١ـ سيدر برج بيتر . سي أساطير إرهابية – بين الوهم والمغالاة والواقع – ترجمة معروف ، عفاف – ١٩٩٢ـ القاهرة .

٢ـ مجمع اللغة العربية – المعجم الوجيز – القاهرة ـ ٢٠٠٠م .

٣ـ منعم ، لينا ، و بو عقل ، سامية ، و كلداني ، تمارا وآخرون – مفردات اللغة القانونية – فرنسي ، عربي، إنكليزي – مترجم من أصل فرنسي – الناشر دالوز وهاشيت أنطوان – بيروت – ٢٠١٠ م .

٤- نخلة ، موريس ، و البعبلكي ، روحي ، و مطر ، صلاح – القاموس القانوني الثلاثي - قاموس قانوني موسوعي شامل ومفصل – عربي / فرنسي / إنجليزي – منشورات الحلبي الحقوقية – بيروت - الطبعة الأولى – ٢٠٠٢م .

ثانياً : المراجع الأجنبية :

(أ) باللغة الانجليزية :

1. Criminal Profiling: An Introduction to Behavioral Evidence Analysis,by Brent E. Turvey, Diana Tamlyn, Jerry Chisum , 1 edition , Academic Press Limited 1999.
2. Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age ,by Tom Douglas Brian Loader , Thomas Douglas,1st edition, Routledge, 2000.
3. Cyber Crime: How to Protect Yourself from Computer Criminals by Laura E. Quarantiello, Tiare Publications, 1996.
4. Digital Evidence and Computer Crime, by Eoghan Casey, 1st edition Academic Pr. 2000.
5. Fighting Computer Crime: A New Framework for Protecting Information, by Donn B. Parker, 1 edition, John Wiley & Sons 1998.
6. Information Warfare Principles and Operations, by Edward Waltz 1998.
7. Mohrenschlager M : computer crimes and others crimes aganiste information technology in the Germany. Rev. Int. dr. pen. 1993 , p. 319,. Spec. p. 349.
8. Taylor R. : Computer crime, "in criminal investigation edited" by Charles Swanson, n. chamelin and L. Territto, Hill, inc. 5edition 1992, p.450 .
9. Yamaguchi Atsushi : “Computer crimes and others crimes against information Technology in Japan، Rev. int. de dr. pén. 1993. P. 448.

(ب) باللغة الفرنسية :

1- Sicber U. : Les crimes informatiques et d' autres crimes dans le dommaine de la technologie informatique, Rev. int. dr. péèçàân. 1993, p.291,spec.p.307 et s.

2- Meunier C. : La loi du 28 Nov. 2000 relative a la criminalite informatique. Rev. Dr. pen. Crim. 2002 , p. 611 et s.

- **ثالثاً : الإنترنت :**

م	اسم المرجع	اللينك الخاص به :
١	الغضوري ، بدر محمد عقيد بالشرطة الكويتية ، ١٨ أكتوبر، ٢٠١٢ ، البحث الجنائي التحريات السرية	http://balghadouri.blogspot.com/2012/10/blog-post.html
٢	كساب ، محمد ـ مراقبة الشبكات الاجتماعية في دول العالم: التكنولوجيا تضيق على الحريات تقرير ، موقع جريدة المصري اليوم ، ٣يونيو ٢٠١٤ ، زيارة ٣٠ ديسمبر ٢٠١٤ .	http://www.almasryalyoum.com/news/details/457780#
٣	منظمة الخصوصية الدولية، اسكات قطر، ٢٠٠٣/٩/٢١	http://www.privacyinternational.org/article.shtml?cmd 347 =x-347-103775. زيارة ٢٠٠٦/٦/١
٤	موقع صحيفة عكاظ السعودية :	http://www.okaz.com.sa/new/mobile/20130810/Con20130810626858.htm
٥	الشهري ، منصور ـ الداخلية: لا نتابع مستخدمي مواقع التواصل بل نرصد من يهدد الوطن – خبر منشور بصحيفة عكاظ السعودية ـ العدد : ٤٤٣٧ – الصادر في ١٤٣٤/١٠/٠٣ هـ ـ الموافق ١٠ أغسطس ٢٠١٣ م – زيارة ٣١ ديسمبر ٢٠١٤ ، الموقع الإلكتروني للصحيفة .	http://www.okaz.com.sa/new/mobile/20130810/Con20130810626858.htm
٦	وكالة أنباء البحرين بنا	http://www.bna.bh/portal/mobile/news/574939
٧	عامر ، محمد حسن ـ دول العالم تراقب شبكات التواصل.. والمبرر: مواجهة الإرهاب.. بريطانيا: الملكة دافعت عن	http://www.elwatannews.com/news/details/496671

	قانون المراقبة لمواجهة التطرف.. والرقابة مكنت الصين والسعودية من كشف خلايا إرهابية ، ٣ يونيه ٢٠١٤ ، زيارة ٢٩ ديسمبر ٢٠١٤ ، الموقع الإلكتروني للجريدة الوطن المصرية .	
٨	بان العاني ، الكويت تشن حملة مراقبة على شبكات التواصل الاجتماعي بعد تغريدة زعيم داعش ، ٢٠١٤/٨/٦م ، موقع البوابة نيوز ، زيارة ٢٢ديسمبر٢٠١٤ :	http://www.albawabhnews.com/719988
٩	الزلاقي ، أيهاب ـ خصم عنيد الإنترنت والحكومات العربية ـ تقرير منشور بموقع المبادرة العربية لإنترنت حر – عن الدول العربية – تقرير قطر ، زيارة ٢٥ ديسمبر ٢٠١٤ .	http://old.openarab.net/ar/node/101
١٠	إجابة ـ موسوعة الأسئلة والإجابات الحرة ، د. ت ، ما هو التشفير Cryptographic ؟ ، زيارة ٢ ديسمبر ٢٠١٤ .	http://www.ejabah.info/ar/%D9%85%D8%A7_%D9%87%D9%88_%D8%A7%D9%84%D8%AA%D8%B4%D9%81%D9%8A%D8%B1 Cryptographic _%D8%9F
١١	الزلاقي ، أيهاب ـ خصم عنيد الإنترنت والحكومات العربية ـ تقرير منشور بموقع المبادرة العربية لإنترنت حر – عن الدول العربية – تقرير الكويت زيارة ٢٠٠٦/٦/٢ :	http://old.openarab.net/ar/node/102
١٢	بعض المواقع مثل تقوم بتوفير برمجيات تتيح للمستخدم الدخول للمواقع المختلفة دون أن يتم كشف الـ ip الخاصة بأجهزتهم وغيره الكثير جدا من البرامج التي تقوم بذات الوظيفة ، مثل :	www.anonymizer.com
١٣	جاسم ، محمد عبد القادر ، إذا ريشت	http://www.aljasem.org/default.asp?opt=2&art_id=88

	النملة..دنى زوالها! ، ٢٠٠٥/١٠/٩ ، زيارة ٢٢ سبتمبر ٢٠١٤ ، موقع المحامي محمد عبد القادر جاسم .	
١٤	المركز العربي للبحوث القانونية والقضائية التابع لجامعة الدول العربية ـ القانون العربي الاسترشادي للإجراءات الجزائية ، ٢٩ نوفمبر ٢٠٠٦ ، زيارة ٢٢ ديسمبر ٢٠١٤ .	http://www.carjj.org/node/1742
١٥	منظمة الخصوصية الدولية، إسكات قطر، ٢٠٠٣/٩/٢١، زيارة ٢٠٠٦/٦/١ .	http://www.privacyinternational.org/article.shtml?cmd 347 =x-347-103775
١٦	المبادرة العربية لإنترنت حر ، د. ت ، حامد خاجة، وكيل وزارة الاتصالات : تصريحات لوكالة اسوشيتد برس حول حجب الحكومة بعض المواقع التي تروج أفكارا متطرفة ، زيارة ٢٠٠٦/٦/٢	http://old.openarab.net/ar/node/102
١٧	قاموس عربي / عربي ، د .ت ، كلمة الصعوبة ، زيارة ٢٢ أكتوبر ٢٠١٤ :	http://www.arabdict.com-عربي/%D8%A7%D9%84%D8%B5%D8%B9%D9%88%D8%A8%D8%A9/عربي%
١٨	قاموس عربي / عربي ، د .ت ، كلمة تحديات ، زيارة ٢٢ أكتوبر ٢٠١٤ :	http://www.arabdict.com/%D8%B9%D8%B1%D8%A8%D9%8A-%D8%B9%D8%B1%D8%A8%D9%8A/%D8%AA%D8%AD%D8%AF%D9%8A%D8%A7%D8%AA
١٩	المبادرة العربية لإنترنت حر ، د. ت ، صحفيون بلا حدود، الانترنت تحت المراقبة، قطر، فيصل حسين، مواطن قطري : حديث لصحيفة الشرق للتعبير عن رضاه بخدمات الانترنت ، زيارة ٢٠٠٦/٦/٢ .	http://www.rsf.org/article.php3?id_article=10765
٢٠	موقع الرأي الحر، ٢٠٠٥/١٠/٢، تعليقا على قرار السلطات بإغلاق موقع	http://www.raihur.com/index.php?p=87

	"حامد العلى"، وقيل في أسباب حجب الموقع إنه يروج لفكر الإرهاب .	
٢١	**Examples of Cyber-terrorism** from student paper by Jimmy Sproles and Will Byars for Computer Ethics Class 1998 زيارة ٣ يناير ٢٠١٥	http://csciwww.etsu.edu/gotterbarn/stdntppr/cases.htm
٢٢	موقع المبادرة العربية لإنترنت حر ، د. ت ، محمد الغانم، مدير عام هيئة تنظيم الاتصالات تصريحات صحفية تعليقا على عدم وجود رقابة على الانترنت داخل المناطق الحرة ، زيارة ٣١ ديسمبر ٢٠١٤ :	http://old.openarab.net/ar/node/90
٢٣	موقع بوينج بوينج، Boing Boing ،banned in UAE, Qatar, elsewhere 27/2/2006، زيارة ٣ ديسمبر ٢٠١٤ .	http://boingboing.net/2006/02/27/boingboing-banned-in.html
٢٤	وكالة أنباء البحرين بنا ، ١٣/ ٨ / ٢٠١٤ ، زيارة ٣١ ديسمبر ٢٠١٤ .	http://www.bna.bh/portal/mobile/news/574939
٢٥	وزارة الداخلية المصرية ، إدارة مكافحة جرائم الحاسبات وشبكات المعلومات ، د. ت ، زيارة ٣ سبتمبر ٢٠١٤م ، موقع وزارة الداخلية المصرية .	http://citizenservice.moiegypt.gov.eg/crimes_web/main.htm
٢٦	Criminal intelligence , Wikipedia, the free encyclopedia ,5 November 2014 , Visit December 30, 2014 ,	http://en.wikipedia.org/wiki/Criminal_intelligence .
٢٧	ويكيبيديا، الموسوعة الحرة ، إرهاب إلكتروني ، ١٦ ديسمبر ٢٠١٤، زيارة ٢٥ ديسمبر ٢٠١٤ :	http://ar.wikipedia.org/wiki/%D8%A5%D8%B1%D9%87%D8%A7%D8%A8_%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A .
٢٨	ويكيبيديا، الموسوعة الحرة ، علوم	http://ar.wikipedia.org/wiki/%D8%B9%D9%84%D9%88%D9%85_%D8%AC%D

	جنائية رقمية ، ٣٠ أغسطس ٢٠١٤ ، زيارة ٣٠ ديسمبر ٢٠١٤ :	9%86%D8%A7%D8%A6%D9%8A%D8%A9_%D8%B1%D9%82%D9%85%D9%8A%D8%A9 .
٢٩	International Association of Chiefs of Police IACP Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing At the Local, State and Federal Levels 2002 . Retrieved from	http://www.ncirc.gov/documents/public/supplementaries/intel_sharing_report.pdf
٣٠	Department of Justice DOJ , National Criminal Intelligence Sharing Plan 2003 . Retrieved from	http://www.fas.org/irp/agency/doj/ncisp.pdf
٣١	^International Association of Chiefs of Police IACP National Law Enforcement Policy Center 2003 . Retrieved from	http://www.ojp.usdoj.gov/BJA/topics/CI_Paper_0703.pdf
٣٢	Field Manual FM 3-19.50 Police Intelligence Operations 2006 . Retrieved from	https://rdl.train.army.mil/soldierPortal/atia/adlsc/view/public/22739-1/FM/3-19.50/chap4.htm;jsessionid=2Dp2J7GTSyJPCJpXR821z1Mvh17s0z9VsGLgtBMJLwv2DTyngKbZ!99557122
٣٣	Elias Diana , Associated Press ,Kuwait blocks sites that incite violence. زيارة ٤ أغسطس ٢٠١٤	http://usatoday30.usatoday.com/tech/news/techpolicy/2005-02-08-kuwait-websites_x.htm
٣٤	Nirvana : خُلاصة المُحتوى العربي، على الإنترنت حول التحقيق الجنائي الرّقمي الشبكة العربية الليبرالية ، ٤إبريل ٢٠١١ ، زيارة ١ نوفمبر ٢٠١٤ :	http://www.liberalls.org/vb/showthread.php?t=5668