المشاكل التي تواجهها الملكية الفكرية في البيئة الرقمية
– بين صعوبة الاكتشاف والإثبات –

The problems by intellectual property between the difficulty of discovery and proof

زواني نادية: أستاذة محاضرة "أ"
كلية الحقوق جامعة الجزائر -1-

تاريخ إرسال المقال: 2018/11/12 **تاريخ قبول المقال:**22/06/2019

ملخص

لقد صادف تطور تقنيات الحاسب الآلي وانتشارها في العالم نحو سياسة السوق والعولمة، الشيء الذي جعل المعلوماتية عنصرا من عناصر السوق التي يمكن أن تكون في متناول الجميع، فإذا كان استخدام الانترنيت قد جلب للبشرية منافع لا حصر لها، وحقق لها من الخيرات والرفاهية ما لم تكن تحلم به من قبل، فإنه بلا شك قد فتح أمام الأشرار من بني البشر نوافذ قد تسبب أضرارا ومخاطر أمنية غير محدودة، وبالتالي يكون قد قدم للمجرمين خدمات في التخطيط للجريمة والإعداد لها وتنفيذها والتخلص من آثارها وبالتالي تسبب ذلك في أضرار لحقت بصاحب حقوق الملكية الفكرية نظرا لصعوبة حماية حقه في البيئة الرقمية.

الكلمات المفتاحية: الجريمة المعلوماتية – المجرم المعلوماتي – الإثبات في جرائم الانترنت – الدليل الالكتروني - التدابير الأمنية.

المؤلف المرسل: زواني نادية، zouaninadia1@gmail.com

Abstract

Internet crime is any crime or illegal on line activity committed on the internet, through the internet or using the internet.

On one hand, no doubt the internet can be an extremely useful tool for people and brought various benefits to the humanity all over the world.

On the other hand, the wisp read of internet crimes is increasing rapidly as more and people around the world are accessing the internet, besides, it have brought illimited threats and dangers for human security by the criminals, who organize the crimes.

These ones are defined by a category of transnational, national, or local group of highly centralized enterprises run by criminal who intend to engage in illegal activity.

All this brought damages to the owner of intellectual property rights, because they wouldn't be able to protect their own law in the numerical environment**.**

Key words: Crimes information - criminal information – internet crime proof – electronic proof – evidence.

مقدمة

لقد ساهمت التقنيات الحديثة في البيئة الرقمية في سهولة اقتناء المعلومات واختراقها بالطرق المختلفة، وأصبح من اليسير تسويقها، وقد ترتب على ذلك نتائج أثرت على الحقوق إيجابا وسلبا، فمن الناحية الإيجابية أدى ذلك إلى سهولة نشر المصنفات وانخفاض التكلفة، كما أتاحت الشبكة إمكانية توصيل العمل إلى الجمهور وتوزيعه بسرعة مما أدى إلى إمكانية تسويقها بسعر رخيص يقل بكثير عن السعر الذي تباع به المصنفات التقليدية.

أما من الناحية السلبية، فقد تسبب نشر المصنفات عبر الإنترنيت في صعوبات واجهت المؤلف في حماية حقه، فإذا كان استخدام تقنيات الحاسب الآلي قد جلب للبشرية منافع لا حصر لها، وحقق لها من الرفاهية ما لم تكن تحلم به، فإنه بلا شك قد تسبب في أضرار بليغة ومخاطر أمنية غير محدودة لكون أن جرائم الإنترنيت تختلف كثيرا في خصوصيتها مقارنة بالجرائم العادية، لكونها تتميز بطبيعة خاصة، وهذه الطبيعة تثير بعض المشكلات عند ضبط وتحقيق وإثبات الجريمة المعلوماتية.

فما هي الجريمة المعلوماتية ؟ وإلى أي مدى يمكن اكتشافها وإثباتها؟

وللإجابة على هذه الإشكالية، نقسم هذا البحث إلى ثلاثة محاور أساسية:

المحور الأول: مفهوم الجريمة المعلوماتية.

المحور الثاني: صعوبة اكتشاف الجريمة المرتكبة عبر الإنترنيت.

المحور الثالث: صعوبة إثبات الجريمة المعلوماتية.

المحور الأول: مفهوم الجريمة المعلوماتية

يلاحظ أن شبكة المعلومات الدولية (الإنترنيت) تمثل أحدث تكنولوجيا العصر التي تم استخدامها في مختف جوانب الحياة، ولكن المعلومات تبين أن هناك أنماطا من الجريمة تتم عبر الإنترنيت، إلا أن هذا الوجه الإيجابي لهذه المخترعات يقابله وجه سلبي في ذات الوقت تمثل في استخدامها في سرقة المعلومات واختلاس الملفات والبرامج ودس الأمراض والحشرات التي تهاجم الحسابات وتصيبها بالتلف[1].

أولا: تعريف الجريمة المعلوماتية

لابد من الإشارة إلى صعوبة إعطاء مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فمنهم من يطبق عليها جريمة "الغش المعلوماتي" والبعض يطلق عليها "الاختلاس المعلوماتي"، والبعض الآخر يفضل تسميتها بالجريمة المعلوماتية[2].

ولقد تباينت التعاريف للجريمة المعلوماتية، فهناك من يعرفها بأنها كافة أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي[3].

ويرى الأستاذ "Tredman" أن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات[4]، وعرفها الأستاذ "Rosblat" على أنها كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والتي تحول طريقه[5].

كما تعرف بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية ويكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[6].

غير أن التعريف الأنسب هو أن الجريمة المعلوماتية هي سلوك إجرامي إيجابي أو سلبي من شأنه الاعتداء بأي صورة من الصور على المعلومات أو البيانات المخزنة داخل الحاسب أو داخل وسائط أخرى يتم تخزين المعلومات فيها من خلاله على نحو يلحق ضررا فعليا أو مفترضا بالجهة التي تم تخزين المعلومات لمصلحتها[7].

ولقد عبر خبراء المنظمة الأوربية للتعاون الاقتصادي عن الجريمة المعلوماتية بأنها كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها[8].

ولقد تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا لجرائم الحاسب الآلي وشبكاته، بحيث عرف الجريمة المعلوماتية بأنها: "أي

جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[9]. ويمكن استخلاص أن جرائم الإنترنيت هي نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسب الآلي وشبكة الإنترنيت) بطريقة مباشرة أو غير مباشرة لتنفيذ الفعل الإجرامي المستهدف، ولعل الهدف من وراء ارتكاب الجريمة المعلوماتية هو قهر نظام الحاسب الآلي وتخطي حواجز الحماية المقامة حوله أو بدافع الانتقام من رب العمل أو أحد الزملاء[10].

أما بالنسبة للمشرع الجزائري فإنه لم يعط تعريفا للجريمة الإلكترونية وإنما تبنى للدلالة على هذه الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات استنادا إلى قانون العقوبات رقم 04/15 المؤرخ في 2004/11/10.

ثانيا: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بعدة خصائص منها ما هو متعلق بطبيعة الجريمة في حد ذاتها ومنها ما هو متعلق بشخصية المجرم.

1) طبيعة الجريمة في حد ذاتها

تتميز الجريمة المعلوماتية بطبيعة خاصة وذلك لكونها:

- جريمة هادئة لا عنف فيها، بحيث يرتكب الجاني جريمته في غرفته خلف الحاسوب.
- جريمة فنية بحيث لا تترك آثارا، بحيث يقوم الجاني بجريمته في وقت قصير، دون أن يترك أي أثر.
- جريمة تعتمد على تغيير الأرقام والبيانات أو محوها من ذاكرة الحاسوب، وبالتالي يصعب القبض على الجاني في حالة تلبس.
- سرعة التنفيذ بحيث لا يتطلب تنفيذ الجريمة الوقت الكبير، فبضغطة واحدة على لوحة المفاتيح يمكن أن تنقل ملايين الدولارات من مكان إلى آخر.
- أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.
- أنها تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها لأنها تعتمد على قمة الذكاء في ارتكابها.
- هذا الفرع من الجرائم لا تقع إلا من أشخاص لهم خبر فنية كبيرة في مجال الحاسب الآلي، ويتسمون بالذكاء الشديد.

2) المجرم المعلوماتي

يقسم مجرمو المعلوماتية إلى مجموعة من الطوائف وهي[11]:

- الطائفة الأولى (Pranksters):

وهم الأشخاص الذين يرتكبون الجرائم والمعلوماتية بغرض التسلية والمزاح دون أن تكون لديهم نية الإضرار بالغير.

- الطائفة الثانية (hackers):

وهم الأشخاص الذين يستهدفون من الدخول إلى أنظمة الحاسوب الغير مصرح لهم بالدخول إليها كسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة وبدافع الفضول، أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

- الطائفة الثالثة (Malicious hackers):

وهم أشخاص هدفهم إلحاق خسائر بالغير دون هدف الحصول على مكاسب مالية، ويندرج تحت هذه الطائفة مخترعي فيروسات الحاسب الآلي.

- الطائفة الرابعة (Personal problem solvers):

وهم الطائفة الأكثر شيوعا من مجرمي المعلوماتية، فهم يقومون بارتكاب جرائم معلوماتية يترتب عليها خسائر كبيرة تلحق بالمجني عليه ويكون الباعث في هذه الجريمة إيجاد حلول لمشاكل مادية تواجه الجاني.

- الطائفة الخامسة (Career problem solvers):

وهم مجرمي المعلوماتية الذين يهدفون من وراء نشاطهم الإجرامي تحقيق ربح مادي بطريق غير مشروع.

والجاني في الجريمة المعلوماتية قد يكون شخصا طبيعيا يعمل لحسابه ويهدف إلى تحقيق مصلحة خاصة به أو لحساب أحد الأشخاص المعنوية كشركة عامة أو خاصة تعمل في مجال المعلومات أو في مجال آخر.

ويتميز المجرم المعلوماتي:

- بالمهارة والمعرفة بالأنظمة المعلوماتية، وغالبا ما يكتسبها عن طريق الدراسات المتخصصة في المجال، أو عن طريق الخبرة المكتسبة في المجال التكنولوجي.
- السلطة، ويقصد بها الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات، وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الآلي وإجراء المعاملات.

المحور الثاني: صعوبة اكتشاف الجريمة المرتكبة عبر الإنترنيت

تتسم الجرائم التي ترتكب في نطاق شبكة الإنترنيت بكون محلها معلومات أو برامج معالجة آلية عير الحاسوب، أو جرائم تتعلق بالأشخاص عبر عالم افتراضي غير مرئي وغير محدود، مما يعطيها طابعا خاصا في طريقة ارتكابها، وهذا كله يجعلها صعبة الاكتشاف.

ولعل من أهم الصعوبات المحاطة بعملية اكتشاف هذا عمل غير القانوني، نذكر منها:

أولا: عدم وجود دليل مادي (مرئي)

إن من أبرز خصائص الجريمة المعلوماتية هو وقوعها في بيئة إلكترونية، وهذه الخاصية تترتب عليها حملة من النتائج التي تصعب من مهمة اكتشاف هذه الجرائم وإمكانية التحقيق فيها، وهذا عكس الجريمة التقليدية التي تخضع لسيطرة أجهزة العدالة، بخلاف الجريمة المعلوماتية التي تتم دون رؤية دليل الإدانة، وحتى في حالة وجود هذا الأخير، فيمكن للجاني طمسه أو محوه وفي حضور أجهزة العدالة غير المتخصصة[12].

فالجريمة التقليدية الدليل فيها يكون مرئيا من ذلك، السلاح الأبيض أو الناري أو المادة السامة المستعملة في القتل بحيث يستطيع عضو الضبط القضائي أو سلطة التحقيق رؤية الدليل بالعين المجردة وملامسته، بينما في الجريمة المعلوماتية فالبيانات والمعلومات تكون عبارة عن نبضات إلكترونية غير مرئية، تنساب عبر النظام المعلوماتي مما تجعل أمر طمس الدليل سهلا[13].

فلكل جريمة طريقة لاقترافها وكيفية معينة يستخلص منها الدليل لإدانة المجرم. فمثلا، انتحال الشخصية في بطاقة الائتمان عن طريق معرفة كلمة السر وتدمير المعلومات أو العبث بها. فكل هذه الأفعال غير المشروعة الدليل فيها غير مرئي فقط لأن هؤلاء المجرمين يستخدمون أساليب وتقنيات عالية.

وقد وصلت بعض العصابات من محترفي خرق الشبكة إلى تصميم للمحو التلقائي لأي أثر تابع عن اختراقهم مما يؤدي بالضرورة إلى استحالة رؤية الدليل، وفي بعض الأحيان النادرة قد يرى الدليل ولكن لا تقوم معظم الشركات التجارية بالتبليغ، وهذا خوفا على سمعتها التجارية[14].

ثانيا: فرض الجاني لتدابير أمنية

يقدم الحاسب الآلي خدمات جليلة للإنسان في حياته اليومية وبالقدر ذاته يمكن أن يقدم للمجرم خدمات في التخطيط للجريمة والإعداد لها وتنفيذها والتخلص من آثارها[15].

يتمتع المجرمون عبر الإنترنيت بمهارات فائقة ويتجلى ذلك في طريقة إخفاء معالم جرائمهم مع إزالة آثارها عن طريق التلاعب بقواعد البيانات والقوائم في جهاز الكمبيوتر والبرامج دون ترك أثر، كل هذا يجعل إقامة الدليل من الصعب على الجريمة المرتكبة عبر الإنترنيت وإثباتها[16].

فالمجرمون الذين يرتكبون جرائمهم بالوسائل الإلكترونية الحديثة من فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم غير المشروعة قبل ارتكابها لكي لا يقعوا تحت طائلة العقاب. فهم يزيدون من صعوبة إجراءات التفتيش التي يتوقع حدوثها للبحث عن الأدلة التي تدينهم باستخدام كلمة السر التي لا يمكن لغيرهم من الوصول إلى البيانات المخزنة إلكترونيا أو المنقولة عبر شبكات الاتصال، وقد يلجأ هؤلاء المجرمون أيضا إلى دس تعليمات خفية بين هذه البيانات أو استخدام الرمز أو التشفير بالنسبة لها ؛ بحيث يستحيل على غيرهم الإطلاع عليها ويتعذر على الجهات التحري والضبط الوصول إلى كشف لأفعالهم غير المشروعة[17].

ثالثا: الامتناع عن الإبلاغ

نظرا لكون معظم الجهات المجني عليها التي غالبا ما تكون مصرفا أو مؤسسة مالية، شركة أو مشروعا صناعيا ضخما تعمل على انتهاج سياسة التكتم وعدم التصريح بحدوث هذه الجرائم خوفا من فقدان سمعتها التجارية مما يؤدي إلى صعوبة اكتشاف الجريمة المرتكبة عبر الإنترنيت[18].

ولا يتم، في الغالب الأعم الإبلاغ عن جرائم الإنترنيت لعدم اكتشاف الضحية لها وإما خشية من التشهير، لذا نجد أن معظم جرائم الإنترنيت تم اكتشافها بالصدفة، بل وبعد وقت طويل من ارتكابها. زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها ؛ فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة والعدد الذي تم اكتشافه هو رقم خطير، وبعبارة أخرى، الفجوة بين هذه الجرائم الحقيقية وما تم اكتشافه فجوة كبيرة[19].

تتفشى هذه الظاهرة على نمو أكثر حدة في المؤسسات المالية كالبنوك والمؤسسات الادخارية حين تخشى مجالس إدارتها عادة من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها وانصرافهم عنها[20].

رابعا: عدم التحلي بالحيطة والحذر

إن الكثير من ضحايا الجرائم المعلوماتية لا يتخذون الحيطة والحذر لاكتشاف مثل هذه الجرائم في حال وقوعها لكون أغلبهم لا يستخدمون برامج وتقنيات للحماية

ضد الاختراق والتجسس والوقاية من الفيروسات، ما يترتب على ذلك عدم إمكان اكتشافهم للجريمة الواقعة لحظة وقوعها، وهذا الأمر يشمل حتى المؤسسات والشركات المالية والتجارية بحيث أنها لا تقوم بمراجعة حساباتها المالية والتجارية يوميا ولا حتى شهريا لتكتشف مثل هذه الجرائم في أوانها[21].

المحور الثالث: صعوبة إثبات الجريمة المرتكبة عبر الانترنت

الإثبات هو إقامة الدليل على وقوع الجريمة ونسبتها إلى المتهم، وذلك وفق الطرق التي حددها القانون.

والإثبات في مجال الجرائم المعلوماتية ينطبق عليه المفهوم العام للإثبات وبذلك، يواجه صعوبات كثيرة تتعلق كما رأينا في صعوبة الحصول على الدليل. وإذا تم الحصول على هذا الدليل نجد أن هناك عقبات أخرى تقف وراء الاستفادة من هذا الدليل.

وترجع صعوبة الإثبات في هذه الجريمة إلى أنها جريمة يصعب فنيا الاحتفاظ بآثارها، بالإضافة إلى غموض حدودها الإجرامية، كما أنها جريمة بيضاء تعتمد على قمة الذكاء في ارتكابها[22].

ولعل أهم الصعوبات التي تعتري عملية الإثبات ما يلي:

أولا: الطابع العالمي للجريمة المعلوماتية

إن الجريمة المعلوماتية تتميز باتساع النطاق أو البعد الجغرافي لها، وهذا البعد العالمي يخلق مشاكل عديدة مثل تتبع الاتصالات الإلكترونية عن طريق سلطات التحقيق لأجل إقامة الدليل على الجرائم التي ترتكب في مجال الإنترنيت[23].

كما أن اختلاف التشريعات فيما بينها، في ما يتعلق بشروط قبولها للأدلة وتنفيذ بعض الإجراءات محل التفتيش والمعاينة عبر الحدود يثير مشاكل تعيق اتخاذ الإجراءات اللازمة لضبط هذا النوع من الجرائم العابرة للحدود، فقد يتم الإبلاغ عن الجريمة في مكان معين، بينما توجد الأدلة المادية في دولة أخرى مما يتطلب إخضاع إجراءات التحقيق لقوانين أو تشريعات جنائية في هذه الدولة.

ثانيا: نقص المعرفة الفنية لدى سلطات التحقيق

إن صعوبة اكتشاف الجريمة بالدرجة الأولى مرده إلى نقص خبرة المحققين، أي رجال الضبط القضائي أو أجهزة الأمن، مما يضعنا أمام معادلة غير متكافئة، أطرافها أجهزة التحقيق ينقصها الخبرة في مجال الكمبيوتر والإنترنيت، والطرف الآخر قراصنة يمتازون بمهارات عالية ويواكبون كل جديد في عالم المعلوماتية[24].

وهنا تظهر أهمية الأجهزة الأمنية في رصد حركة مرتكبي جرائم الحاسب الآلي واكتشاف الجرائم المرتكبة عن طريق الرصد الميداني لحركة المعاملات التجارية ومراقبة المشبوهين داخل المؤسسات المالية[25].

وتلعب الشرطة على رأس أجهزة العدالة دورا رئيسا في تطبيق القانون، وفي التحري عن الجرائم، غير أن الأمر يصعب عندما يتعلق الأمر بنظام المعالجة الآلية؛ فنقص الخبرة لدى رجال الضبطية القضائية، لكون أن التحقيق في جرائم الحاسب الآلي هي مسألة فنية وصعبة خاصة بالنظر إلى اعتبارات التكوين العلمي والتدريبي لرجال الضبط القضائي وسلطات التحقيق الجنائي، لأن الجريمة المعلوماتية تتطلب إلماما بتقنياتها[26] ؛ فالدليل الفني قد يكون مضمونه مسائل فنية لا يقوى على فهمها إلا الخبير المتخصص في تقنيات الإعلام الآلي، لأن الجريمة المرتكبة عبر الإنترنيت ترتكب خارج إطار الواقع المادي الملموس، وتقوم أركانها في بيئة الحاسب والإنترنيت، مما يعقد الأمر لدى سلطات الأمن وأجهزة التحقيق على أساس أن المعلومات في بيئة الإنترنيت تكون عبارة عن نبضات إلكترونية غير مرئية.

فلقد عانى المحققون ورجال الشرطة كثيرا في التصدي للجريمة المعلوماتية بسب قصور التشريعات العقابية التي تجرم الأفعال التي يمكن أن تكون لها علاقة بسوء استعمال الحاسب، ويرجع ذلك لحداثة هذه الجريمة وسرعة التطورات التي اتسمت بها تقنية الحاسب الآلي مقابل بطء حركة التشريعات العقابية[27].

ثالثا: صعوبة الحصول على الدليل الإلكتروني

إن إجراءات البحث عن الجرائم الإلكترونية وضبطها مازالت تتم في إطار النصوص الإجرائية التقليدية، الأمر الذي سيترتب عنه مشاكل بالنسبة لضبط هذه الجرائم الحديثة ذات الكيان المعنوي، والتي قد تتعدد أماكن ارتكابها داخل الدولة الواحدة أو يمتد نطاقها ليشمل عدة دول عبر شبكة الانترنت، فيتعذر معه اتخاذ إجراءات جمع الأدلة[28].

فمعاينة مسرح الجريمة المعلوماتية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة، وذلك راجع إلى أن كثيرا من الأشخاص يترددون إلى مسرح الجريمة خلال فترة من زمان وقوع الجريمة حتى اكتشافها ؛ الأمر الذي يعطي مجالا للجاني أن يغير أو يتلف الآثار المادية إن وجدت، وهذا ما يولد الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المرتكبة عبر الإنترنيت[29].

فالجاني الذي يستخدم الوسائل الإلكترونية يتميز بذكاء وإتقان فني للعمل، لذلك فهو يتمكن من إخفاء الفعل غير المشروع، بل أكثر من ذلك، فهو يستطيع محو

الدليل في زمن قصير، فالجاني يمكنه محو الأدلة التي تكون قائمة ضده بحيث لا تتمكن السلطات من كشف جريمته.

رابعا: سرعة محو الدليل وإخفاؤه

تعتبر سهولة إخفاء الدليل ومحوه وتدميره من بين الصعوبات التي يمكن أن تعترض العملية الإثباتية في مجال جرائم الإنترنيت، بحيث يقوم الجاني بمحو أو تدمير أدلة الإدانة بسهولة ومهارة، فضلا عن إمكانية تنصله من مسؤولية هذا العمل بإرجاعه إلى خطا في نظام الحاسوب أو في الأجهزة، مما يزيد من خطورة تبخر الدليل التقني الذي يمكن تعديله أو حذفه نهائيا في بضع ثواني[30].

وكمثال لذلك، نجد أن الجناة يستخدمون التشفير وكلمات السر التي تمكنهم من إخفاء الأدلة التي قد تكون قائمة ضدهم.

فالدليل يمكن محوه من شاشة الكمبيوتر في زمن قياسي، وفي لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبيها أمرا صعبا[31].

فالمعلومات المتداولة عبر الإنترنيت تكون على هيئة رموز مخزنة على وسائط تخزين ممغنطة لا تقرأ إلا بواسطة الحاسب الآلي والوقوف على الدليل الذي يمكن فهمه بالقراءة، والتوصل عن طريقه إلى الجاني يمكن فهمه بالقراءة، والتوصل عن طريقه إلى الجاني يبدو أمرا صعبا[32].

ونظرا للطبيعة الخاصة التي تتسم بها الجريمة أدى ببعض التشريعات إلى تبني الخبرة والمعاينة كأسلوبين للتحقيق والإثبات وكشف الجريمة.

فبالنسبة للخبرة، فيجب أن تكون من نوع خاص، فبعض الدول تعمل على إعادة تأهيل بعض القراصنة من أجل الاستفادة من خبراتهم في الاختراق، وفي هذا الصدد يجب أن يتحلى الخبير بمؤهلات وقدرات فنية عالية ودراية تامة بشبكة الإنترنيت وكيفية عزل النظام المعلوماتي والحفاظ على الأدلة، دون تلف[33].

وبالنسبة للمعاينة فلابد من تبليغ الجهة المؤهلة عالميا بتقنية خاصة من أجل التحفظ على الأدلة الموجودة، وحتى تكون معاينة محكمة فيجب توافر عدة تدابير منها ضمان عدم انقطاع التيار الكهربائي، والعمل ضمن فرق بحث[34].

خاتمة

لقد اصطدمت محاولات التصدي للجريمة المرتكبة عبر الإنترنيت بعدة صعوبات. فخصوصية الجريمة والسرعة في تطورها وانتشارها أدى بأغلب هذه المحاولات إلى الفشل، والدليل على ذلك ما نسمعه عبر وسائل الإعلام المختلفة عن الجرائم الكثيرة التي مازالت ترتكب عبر الشبكة العالمية للإنترنيت، حيث يعتبر اكتشاف وإثبات الجريمة المرتكبة عبر الإنترنيت من أكثر الصعوبات التي تواجهها السلطات في تطبيق القانون ففي الغالب، تكون هذه الجرائم مستترة، وكذلك الأمر بالنسبة لإثباتها في ظل الطابع اللامادي للجريمة. حيث تفتقر هذه الجرائم للدليل المادي مما يجعل أمر إثباتها غاية في الصعوبة والتعقيد.

إن تطوير ثقافة الحاسب الآلي وسط رجال الأمن يكفل للأجهزة الأمنية نجاحا في مواكبة ظاهرة الجرائم المعلوماتية لذلك لابد من:

- تلقين رجال الأمن مبادئ علوم الحاسب الآلي وكيفية التعامل مع هذا الجهاز.
- المشاركة في الدورات التدريبية التي تنظمها المعاهد الخاصة في مجال الحاسوب.
- الاهتمام بتدريب الخبراء المحققين والقضاة على التعامل مع الجرائم المعلوماتية ذات الطبيعة الفنية والعلمية المعقدة.

فأجهزة العدالة مدعوة لدراسة ظاهرة الجريمة المعلوماتية واتخاذ التدابير العلمية اللازمة للسيطرة عليها واكتشاف ما يقع منها وحماية المجتمع من أضرارها الاقتصادية والاجتماعية.

الهوامش

1- عادل عبد الجواد محمد، إجرام الإنترنيت، مجلة الأمن والحياة، العدد 221، شوال 1421، ص 70.

2 -نهلة عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 15.

3 -محمود عبد الرحيم الديب، الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والإنترنيت، دار الجامعة الجديدة للنشر، الإسكندرية، 2005، ص 41.

4 -محمد أمين الشوابكة، جرائم الحاسوب والإنترنيت، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، الطبعة (1)، 2004، ص 08.

5 -يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنيت، منشورات اتحاد المعارف العربية، ط1، 2013، ص 213..

6 -محمد محمد شنا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001، ص 74.

7- المرجع نفسه، ص 75.

8 -محمد الشوا، ثورة المعلومات وانعكاساتها عن قانون العقوبات، الطبعة 2، دار النهضة العربية، القاهرة، 1998، ص 7.

9 -محمد أمين أحمد الشوابكة، المرجع السابق، ص 10.

10 -أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربي، القاهرة، 2005، ص 41.

11 -عبد العال الديربي، الجريمة المعلوماتية، تعريفها، أسبابها، خصائصها، مقال منشور عبر الإنترنيت بتاريخ 2013/01/13 عبر الموقع المركز العربي لأبحاث الفضاء الإلكتروني. www.accronline.com.

12 -عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنيت، دار الكتب القانونية، مصر، 2002، ص 24.

13- نهلة عبد القادر المومني، الجرائم المعلوماتية، المرجع السابق، ص 56.

14 -عبد الفتاح البيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، طبعة 2006، ص 41.

15 -محمد الأمين البشري، أنواع جرائم الحاسب الآلي، وكيفية ضبطها، مجلة الشرطة، العدد 356، أوت 2000، ص 46.

16- فريد منعم جبور، حماية المستهلك عبر الإنترنيت ومكافحة الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، 2010، ص 269.

17-علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، ص 20، مقال متوفر على الموقع التالي: http://www.arablawinfo.com.

18 -محمود حماد مرهج الهيتي، جرائم الحاسوب - ماهيتها، موضوعها، أهم صورها والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع، الأردن، 2006، ص 217.

19 -محمد صالح العادلي، الجرائم المعلوماتية - ماهيتها وصورها، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، 02 – 04 أفريل 2006، ص 1، 14.

20 -هشام محمد فريد رستم، أصول التحقيق الجنائي واقتراح إنشاء آلية عربية موحدة للتدريس التخصصي، جامعة الإمارات العربية المتحدة، المجلد (2)، الطبعة 3، 2004.

21- عبد الفتاح البيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 41.

22 -محمد عبد الرحيم الديب، المرجع السابق، ص 57.

23 -علي محمود علي حمودة، المرجع السابق، ص 50.

24 -أسامة أبو الحجاج، دليلك الشخصي إلى الإنترنيت، دار النهضة، مصر، القاهرة، 1998، ص 20.

25 -محمد الأمين العشري، التحقيق في جرائم الحاسب الآلي والإنترنيت، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد 30، ص 350 – 351.

26 -عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 81.

27- محمد الأمين العشري، المرجع السابق، ص 321.

28 -علي محمود علي حمودة، المرجع السابق، ص 21.

29 -نهلة عبد القادر المومني، المرجع السابق، ص 56.

30- هشام محمد فريد رستم، المرجع السابق، ص 429.

31 -موسى مسعود أرحومة، الإشكالية الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطن، المؤتمر المغاربي الأول حول المعلوماتية والقانون أكاديمية الدراسات العليا، طرابلس، 2009، ص 3.

32 -محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنيت، دار النهضة العربية، القاهرة، دون سنة الشر، ص 3.

33 -أسامة أبو الحجاج، المرجع السابق، ص 20.

34 -فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/لبنان 24 – 2017/03/25، ص 115.