تاريخ الإرسال: 2018/09/18 تاريخ القبول:2018/10/09

إشكالية الإثبات في الجرائم الالكترونية

The issus of proof in cybercri

الطيبي البركه
طالب دكتواره
tayebi.elbarka@univ-adrar.dz
مخبر القانون والتنمية المحلية
جامعة أدرار
د. حاج سودي محمد
hadjs_01@yahoo.fr
جامعة أدرار

ملخص البحث

يتناول هذا المقال بالدراسة موضوع إشكالية الإثبات في الجرائم الالكترونية، حيث تطرق إلى أهم المعوقات التي تواجه سلطات التحقيق و التحري في إثبات الجرائم الإلكترونية، لا سيما المتعلقة منها بخصوصية الدليل الإلكتروني و خصوصية التحقيق، و المتمثلة في عدم ظهور الدليل الإلكتروني و سهولة محوه أو تدميره، و صعوبة التحري عنه في كشف غموض الجريمة والوصول إليه، وكذا ضعف التعاون الدولي في مكافحة هذا النوع من الجرائم ، باعتبارها غير مرئية ومتشعبة وعابرة للحدود الوطنية وتتطلب استخدام طرق تحقيق خاصة.

الكلمات المفتاحية: الدليل الإلكتروني؛ الجرائم الإلكترونية؛ الجرائم المعلوماتية؛ التحقيق؛ المعوقات؛ القانون رقم 04/09 للوقاية من جرائم تكنولوجيات الإعلام والاتصال و مكافحتها.

Abstract

This article discusses the problem of proof of cybercrime. It deals with the most important obstacles facing investigative authorities and the investigation of electronic crimes, especially

the privacy of the electronic evidence and the privacy of the investigation. To investigate crime detection and access, as well as to weaken international cooperation in the fight against this type of crime, as invisible, cross-border and transnational, requiring the use of special investigative methods
Keywords: electronic evidence; cybercrime; information crimes; investigation; constraints; law No. 09/04 on the prevention and control of ICT crime.

مقدمة

الإثبات هو إقامة الدليل على وقوع الجريمة ونسبتها إلى المتهم وذلك وفق طرق مشروعة ومحددة قانونا، والإثبات في مجال الجرائم الإلكترونية ينطبق عليه المفهوم العام للإثبات، وتبعا لذلك فهو يواجه العديد من الإشكاليات بغية استخلاصه نظرا للخصوصيات المتعلقة بطبيعة الجريمة باعتبارها غير مرئية ويسهل محو آثارها ويصعب الوصول إلى أدلة إدانتها، والسمات المتعلقة بخصوصية التحقيق في هذه الجرائم نظرا لصعوبة التحري في كشف غموضها وضعف التعاون الدولي في مكافحتها.

كما أن الطرق التقليدية في إستخلاص الأدلة يصاحبها الكثير من المشكلات العملية، ويكشف التحليل العميق لهذه الطرق أن هناك بعض الخطوات يمكن إلغاؤها باستخدام نظام يقوم على تكنولوجيا المعلومات والإتصالات، بحيث أصبحت عاجزة وقاصرة في مواجهة العديد من الأفعال التي تهدد مصالح إجتماعية وإقتصادية إرتبطت بظهور وانتشار جهاز الحاسب الآلي وشبكة الانترنت، والتي نتج عنها ظهور تسمية جديدة للدليل تعرف بالدليل الرقمي أو الإلكتروني.

وعليه وجب تحديث الأساليب الإجرائية المتبعة لجمع الأدلة في الجرائم الإلكترونية أو تبني وسائل جديدة للبحث و التحري تمكن من الحصول على الدليل الإلكتروني، دون أن تعرض حقوق الأفراد الآخرين وحرياتهم للخطر عند الإثبات في الجرائم الإلكترونية.

وهو ما قام به المشرع الجزائري على غرار باقي التشريعات المقارنة بتبني وسائل جديدة للبحث والتحري إضافة إلى الوسائل التقليدية في الجرائم الإلكترونية، بموجب

القانون 09-04 المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال و مكافحتها.

كما أن إستخدام هذه الوسائل في استخلاص الأدلة الإلكترونية تعترضه عدة عقبات منها ما يتعلق بخصوصية الدليل الإلكتروني ومنها ما يتعلق بخصوصية التحقيق، وعليه يمكن طرح الإشكالية التالية: أين تكمن معوقات الإثبات في الجرائم الإلكترونية؟

وللإجابة على هذه الإشكالية اعتمدت الخطة التالية: حيث قسم موضوع الدراسة إلى مطلبين تناول المطلب الأول المعوقات المتعلقة بخصوصية الدليل الإلكتروني، وتناول المطلب الثاني المعوقات المتعلقة بخصوصيات التحقيق.

المطلب الأول: المعوقات المتعلقة بخصوصية الدليل الإلكتروني

إن الإثبات الجنائي عملية متكاملة تستهدف البحث عن الأدلة الجنائية التي تثبت حدوث الواقعة الجنائية المرتكبة وظروف إرتكابها وأسبابها وتنسيقها إلى مقترفيها وذلك لتقديمهم للعدالة[1]، بحيث تواجه الجرائم الإلكترونية في هذا المجال عدة صعوبات عند إثباتها والتي انعكست بدورها على الأدلة المتحصل عليها من هذه الجرائم.

وتقف وسائل الإثبات الجنائي التقليدية عاجزة عن مواجهة الجرائم الإلكترونية التي تنصب على المعلومات والبيانات المخزنة في نظم المعلومات والبرامج مما أدى إلى بروز ظاهرة جديدة وهي الظاهرة الرقمية ذات الطبيعة التقنية الناجمة عن الحاسوب والانترنت نتج عنها ما يسمى بالدليل الإلكتروني أو الدليل الرقمي لإثبات وقوع الجرائم الإلكترونية ونسبتها لمرتكبيها.

والدليل الإلكتروني هو طريقة خاصة لإظهار الحقيقة والذي يتم فيه اللجوء إلى إحدى الوسائل الرقمية المتنوعة التي تدرس المحتويات داخل ذاكرة القرص الصلب والرسائل الإلكترونية المخزنة أو المنقولة رقميا[2]، وإن هذا الدليل ينبغي أن يخضع في قبوله لجملة من الشروط وهي أن يكون مشروعا ويقينيا وأن تتم مناقشته في جلسة الحكم، كما أن حجيته في الإثبات الجنائي تختلف بحسب نظام الإثبات

الجنائي الذي تعتمده الدولة، والذي هو في الجزائر نظام الإثبات الحر، بحيث لا يطرح إشكالا كبيرا من حيث اعتباره حجة، خاصة إذا تم استخلاصه وفق ضمانات قانونية وفنية تضمن صحته وسلامته[3]

إلا أن هذا الدليل الإلكتروني تعترضه عدة عقبات في استخلاصه من طرف سلطات التحقيق والتحري وهي عدم ظهور الدليل الإلكتروني(الفرع الأول) وسهولة محوه أو تدميره (الفرع الثاني) وصعوبة الوصول إلى هذا الدليل الإلكتروني (الفرع الثالث).

الفرع الأول: عدم ظهور الدليل الإلكتروني

إن الدليل الإلكتروني المراد استخلاصه من بيئة إلكترونية يستمد طبيعته من ذات العمليات الإلكترونية ولا يمكن كشفه بالطرق التقليدية وإنما قد يحتاج إلى استخدام تقنيات علمية متطورة يجب إتباعها للوصول إليه، لكونه دليل غير مادي(ملموس) وغير مرئي وغير مقروء، بحيث تتجلى هذه الخصوصية من خلال ما يلي:

أولا: إنها أدلة غير مرئية

حيث أن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التي تقع عليها أو بواسطتها ما هي إلا بيانات غير مرئية لا تفصح عن شخصية معينة، وهذه البيانات مسجلة إلكترونيا بكثافة بالغة وبصورة مرمزة غالبا على دعائم أو وسائل للتخزين ضوئية كانت أو ممغنطة لا يمكن للإنسان قراءتها وإن كانت قابلة للقراءة من قبل الأدلة نفسها ولا يترك التعديل أو التلاعب فيها إي اثر مما يقطع إي صلة بين المجرم وجريمته ويحول دون كشف شخصيته وكشف وتجميع أدلة بهذا الشكل لإثبات وقوع الجريمة ونسبتها إلى مرتكبيها هو أحد أهم المشاكل التي يمكن أن تواجه جهات التحري و الملاحقة[4].

ثانيا: أن أغلب الآثار المتخلفة عن هذه الجرائم هي آثار إلكترونية

و هذه الآثار بدورها إنما هي عبارة عن نبضات إلكترونية غير مرئية بالعين المجردة فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة بحيث أنه لا يمكن رؤيتها إلا من خلال الإستعانة بأجهزة ووسائل تقنية تظهرها للعيان،

إضافة إلى أن ضخامة حجم وكم البيانات والملفات الإلكترونية المجرمة من بين ذلك الكم الهائل لفصلها عن تلك البريئة منها وتؤدي في الغالب إلى إصطدام مهمة الإكتشاف بحق الأفراد في الخصوصية الشخصية[5].

ثالثا: أن الجرائم التقليدية يكون فيها الدليل مادي ومرئي ومقروء

بحيث إن كل الوقائع المتعلقة بهاته الجرائم خاضعة لسيطرة أجهزة العدالة وتخلف آثار مادية كالسكين والسلاح وبقع الدم في جريمة السرقة مثلا، عكس الجرائم الإلكترونية التي تكون فيها البيانات والمعلومات عبارة عن نبضات إلكترونية وتتم دون مشاهدة أو رؤية دليل الإدانة وسهولة محوه أو تدميره في مدة قصيرة وفي حالة قصور أجهزة عدالة غير متخصصة، والتي غالبا ما تنتفي قدراتهم على أن يتولوا بطريقة مباشرة فحص واختبار البيانات المشتبه فيها وتزداد جسامة هذه المشكلة بوجه خاص في حالة التلاعب في برامج الحاسب نظرا لتطلب الفحص الكامل للبرنامج وإكتشاف التعليمات غير المشروعة المخفية داخله قدرا كبيرا من الوقت والعمل وغالبا ما لا يكون له من حيث التكلفة الاقتصادية مبررا[6].

رابعا: إن إستخلاص الأدلة يعد تحديا لرجال الأمن

لذلك يرى المختصين في جرائم الحاسب الآلي أن هذا الجهاز وما يقع عليه من جرائم معلوماتية يعد تحديا هائلا لرجال الأمن ذلك أن رجل الأمن غير المتخصص و الذي انحصرت معلوماته في جرائم قانون العقوبات بصورة تقليدية من قتل وضرب وسرقة لن يكون قادرا على التعامل مع الجريمة المعلوماتية التي تقع بطريقة تقنية عالية ولذلك فغالبية الجرائم الإلكترونية تكشف مصادفة وليس بطريق الإبلاغ عنها[7].

كما يرى جانب من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسؤولياتها نحو إكتشاف الجرائم وضبط المجرمين ومحاكمتهم وهذا يتطلب توفير الإمكانيات التقنية اللازمة لتحقيق الجرائم المعلوماتية وبمعنى آخر يتعين استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال للإستعانة بها في تحقيق هذه الجرائم ويتعين عدم التذرع بالميزانيات المالية كسبب يحول دون قيام الدولة بواجباتها نحو تحقيق العدالة الجنائية وحتى يتم ذلك يرى هذا

الجانب ضرورة الاستعانة بالنبضة المتخصصة في الحاسب الآلي حال تحقيق الجرائم المعلوماتية وذلك لضبط هذه الجرائم وإكتشافها وتقديم أدلة الإدانة فيها[8].

وتجدر الإشارة بهذا الخصوص إلى أن المشرع الجزائري تبنى وسائل تقنية جديدة لاستخلاص الدليل الإلكتروني، بموجب المواد 4،5،6،11[9] من القانون 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها، والمتمثلة في مراقبة الاتصالات الإلكترونية، تفتيش المنظومات المعلوماتية، حجز المعطيات المعلوماتية، حفظ المعطيات المتعلقة بحركة السير من طرف مقدمو الخدمات.

ومنه، يمكن القول أن الدليل المادي يمكن رؤيته وملامسته بأحد الحواس من طرف سلطات التحقيق والاستدلال عكس الدليل الإلكتروني الذي تكون المعلومات والبيانات فيه عبارة عن نبضات إلكترونية غير مرئية تنساب النظام المعلوماتي، مما يجعل أمر طمس هذا الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة.

الفرع الثاني: سهولة محوه أو تدميره

من المعوقات التي يمكن أن تعترض عمليات الإثبات في الجرائم الإلكترونية سهولة محو وتدمير أدلة الإدانة في فترة زمنية يسيرة، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها قي زمن قصير جدا بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده وبالتالي تنصله من مسؤولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسبة الإلكترونية أو الشبكة أو في الأجهزة ومن أمثلة ذلك قيام أحد مهربي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسبة الإلكترونية الذي يستخدمه في تخزين عناوين عملائه و المتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذه الحاسبة من خلال لوحة مفاتيحه محو وتدمير كافة البيانات كاملة[10].

ومع أن تعديل برمجة نظام تشغيل الحاسب كان قد أجري خصيصا بواسطة الفاعل للحيلولة دون نجاح أجهزة الملاحقة في إجراءات المتوقعة للبحث عن الأدلة

وضبطها إلا أنه لم يفلح في تحقيق هذا الهدف نتيجة لتوقع المتخصصين لمعالجة البيانات بالجهاز المركزي لمكافحة الغش المعلوماتي بالنمسا بأن شيء ما في نظام تشغيل حاسب الفاعل قد جرى تغييره و قيامهم بناء على ذلك باستنساخ الأقراص الممغنطة المضبوطة عن طريق أنظمة حاسبتهم[11].

ومن أمثلة ذلك قيام شخص مشغل للحاسبة الإلكترونية في دولة الإمارات العربية المتحدة بتهديد المؤسسة التي يعمل لها من أجل تحقيق بعض المطالب بمحو كافة البيانات المخزنة في الجهاز الرئيسي للشركة وعندما رفضت الشركة الاستجابة لمطالبه أقدم على الانتحار مسببا لها حرجا كبيرا في استرجاع البيانات التي كان قد حذفها[12].

وفي حالة مماثلة شهدتها ألمانيا الاتحادية سابقا أدخل الجناة في نظام الحاسب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها ومن شأنها محو هذه البيانات بالكامل بواسطة مجال كهربائي وذلك إذا ما تم اختراقه من قبل شخص غير مرخص له[13].

وتجدر الإشارة إلى أن الجاني دائما ما يحرص على محو الآثار التي تدل على إرتكابه لجريمته من خلال إعتماده على بعض التقنيات التي تساعده على محو وتعديل البيانات الإلكترونية في أقل مدة ممكنة.

كما أن الدليل الإلكتروني غالبا ما يترك آثارا في حالة محوه و تعديله، والخبراء المتخصصون فقط من يستطيعون كشف هذه التلاعبات التي يحدثها الجناة في النظم المعلوماتية لمحو آثار جرائمهم.

الفرع الثالث: صعوبة الوصول إلى الدليل الإلكتروني

أن النتائج العلمية الدقيقة للأجهزة المعملية لم تعد مجال تشكيك من محامي الدفاع بل طرق تجمعيها وحفظها و تقديم الأدلة العلمية للمحكمة هي التي أصبحت محل تشكيك من جانب المتهم[14]، والأصل أن الوصول إلى هذه الأدلة يتم عن طريق الشكاوى التي يقدمها المجني عليهم، إلا أن الأمر بالغ التعقيد في الجرائم الإلكترونية بالنسبة لجهات التحقيق التي لم تصل إلى تلك المعرفة والخبرة التي

تملكها اتجاه التحقيق في الجرائم التقليدية لأن الأمر يتطلب إحاطة كاملة بالتكنولوجيا الحديثة و معرفة واسعة بالعقبات التي تصعب من الوصول إلى الدليل الإلكتروني، و المتمثلة فيما يلي:

أولا: إحاطته بوسائل الحماية الفنية

يصعب الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقات المحاولات الرامية إلى الوصول إليها والإطلاع عليها أو استنساخها[15]، بحيث أن البيانات المخزنة إلكترونيا أو المنقولة عبر شبكات الإتصال تحاط بجدار من الحماية الفنية لإعاقة محاولة الوصول غير المشروعة إليها للإطلاع عليها واستنساخها، ..كذلك يمكن للمجرم المعلوماتي أن يزيد من صعوبة عملية التفتيش التي قد تباشر للحصول على الأدلة التي تدينه عن طريق مجموعة من التدابير الأمنية كاستخدام كلمة السر للوصول إليها أو دس تعليمات خفية بينها أو ترميزها لإعاقة أو منع الإطلاع عليها أو ضبطها، لذا فإن استخدام تقنيات التشفير لهذا الغرض يعد أحد العقبات الكبرى التي تعوق رقابة البيانات المخزنة أو المنقولة عبر حدود الدولة والتي تقلل من قدرة جهات التحري والتحقيق والملاحقة على الإطلاع عليها الأمر الذي يجعل حماية حرمة البيانات الشخصية المخزنة في مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية والإلكترونية أو بتدابير الأمن والدفاع أمر بالغ الصعوبة[16].

ثانيا: سلوكات الجاني

يعمد الجاني إلى تشفير تلك الملفات أو البيانات الإلكترونية التي تتضمن محتوى غير مشروع بغية منع الغير من الإطلاع عليها وإكتشافها كما هو الحال في حالة نقل البيانات المتعلقة بجرائم غسيل الأموال عبر الإنترنت بعد تشفيرها، ويحرص بعد ارتكابه لجريمته على محو آثارها التي تدل على وقوعها و ذلك من خلال التوسل بتقنيات معدة لهذا الغرض مع الأخذ بعين الاعتبار سهولة وسرعة إمكانية محو وتعديل البيانات الإلكترونية التي يمكن القيام بها في أزمان قياسية

متناهية القصر تقاس باللحظات والثواني[17]، لذلك تشكل عملية تشفير البيانات المخزنة إلكترونيا أو المنقولة عبر شبكات المعلوماتية عقبة كبيرة أمام إثبات الأدلة الرقمية.

ثالثا: الإمتناع عن التبليغ

أن المجني عليه أيضا يعوق من الوصول إلى الدليل الإلكتروني بحيث يمتنع في الغالب عن التبليغ عن الجرائم الإلكترونية وقد يسعى إلى التعتيم على المحققين وتضليلهم حتى لا يكتشفوا [18]هذه الجرائم لهذا لا نعجب إذا وجدنا أن أكثر تلك الجرائم لم تكتشف إلا بمحض الصدفة وهناك ما يشير إلى أن هذه الجرائم لم يكتشف منها إلا ما بنسبة واحد فقط و ما تم الإبلاغ عنه إلى السلطات المختصة لم يتعدى 15% من النسبة السابقة و حتى ما طرح أمام القضاء من هذه الجرائم فأن أدلة الإدانة فيه لم تكن كافية إلا في حدود الخمس 5/1[19].

وقد يكون المجني عليه مؤسسة مالية كبيرة كالبنوك التي تفضل في كثيرا من الأحيان عدم التبليغ عن الإصابة بفيروس حتى لا تهتز ثقة المتعاملين معها ويترتب على ذلك سحب ودائعهم واستثماراتهم فيها وكذلك تدخل هذه المؤسسات في اعتباراتها أن الإبلاغ عن الجرائم الإلكترونية التي وقعت ضدها ربما يؤدي إلى إحاطة المجرمين علما بنقاط الضعف في أنظمتها[20]، و ترفض في أحيان أخرى عدم التعاون مع الجهات الأمنية خشية معرفة العامة بوقوع الجريمة ويسعون بدلا من ذلك إلى محاولة تجاوز آثارها حتى و لو كانت الوسيلة هي مكافأة المجرم و نذكر على سبيل المثال بنك marchant bankcity في انجلترا لنقل 8 مليون جنيه إسترليني من إحدى أرصدته إلى رقم حساب في سويسرا و قد تم القبض على الفاعل إثناء محاولته سحب المبلغ المذكور ولكن بدلا من أن يقوم البنك بتحريك الدعوى الجنائية ضده فقد قام بدفع مبلغ 1 مليون جنيه إسترليني له بشرط عدم إعلام الأخريين عن جريمته وإخطار البنك بالآلية التي نجح من خلالها باختراق نظام الأمن الخاص بحاسب البنك الرئيسي[21].

وفي دراسة للمعهد الوطني للعدالة التابع لوزارة العدل الأمريكية شملت (127) من العاملين في مجال التحقيق في جرائم الحاسبة الإلكترونية والإنترنت يمثلون (11) وكالة رسمية كان غالبية المشاركين في الدراسة يعتقدون أن معظم جرائم الحاسبة الإلكترونية والإنترنت التي يتم اكتشافها لا يبلغ عنها للشرطة، كما توصلت دراسة أخرى أجراها معهد أمن الحاسبة الإلكترونية (CSI) بالاشتراك مع مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية إلى أن حوالي (70%) من الجرائم التي يتم اكتشافها لا يتم البلاغ عنها لسلطات إنفاذ العدالة[22].

كما أنه بالرغم من حرية القاضي الجنائي في الإثبات إلا أنه لا يستطيع أن يقبل دليلا متحصل من إجراء غير مشروع، ليس فقط لأن ذلك يتعارض مع قيم العدالة وأخلاقيتها و إنما لأنه كذلك يمس بحق المتهم في الدفاع[23].

وعليه يمكن القول أن كافة السلوكات التي يقوم بها المجرم المعلوماتي والمجني عليه أو الضحية في الجرائم الإلكترونية تصعب من الوصول إلى الدليل الإلكتروني، لذلك عمد المشرع الجزائري إلى وضع طرق إثبات أخرى في مواجهة الأدلة الرقمية وألزم مقدمي خدمات الإنترنت بتقديم المساعدة للسلطات القضائية من أجل تسهيل عملية الوصول إلى أدلة الإدانة في هذه الجرائم.

المطلب الثاني: المعوقات المتعلقة بخصوصية التحقيق

إن التحقيق في الجرائم الإلكترونية أو ما يعرف بالتحقيق الرقمي هو عبارة عن مجموعة من الأساليب المتبعة من أجل معرفة وتقديم معطيات الإعلام مخزنة (الدليل الرقمي) في وسيلة إلكترونية ممغنطة أمام جهة قضائية[24]، ويتسم بعدة معوقات يمكن أن تعرقل عملية التحقيق وتؤدي إلى نتائج سلبية يمكن أن تنعكس على نفسية المحقق في حد ذاته بفقدانه الثقة في نفسه وفي أدائه، وعلى المجتمع بفقدانه الثقة في أجهزة العدالة الغير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وعلى المجرم نفسه بزيادة الثقة لديه بحيث يستطيع الإفلات من الجهات الأمنية الغير قادرة على اكتشاف أمره، بسبب صعوبة التحري في كشف غموض الجريمة (الفرع الأول) وضعف التعاون الدولي في مكافحة الجرائم الإلكترونية

(الفرع الثاني)

الفرع الأول: صعوبة التحري في كشف غموض الجريمة

إن التحري في كشف غموض الجريمة الإلكترونية تعترضه عدة عقبات،و تتمثل في ما يلي:

أولا: الكم الهائل للبيانات

يشكل الكم الهائل للبيانات التي يتم تداولها من خلال الأنظمة المعلوماتية أحد مصادر الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بواسطتها والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات والتي قد لا تثبت كلها تقريبا شيئا على الإطلاق[25].

ثانيا: مميزات الجرائم الإلكترونية

أن الجرائم الإلكترونية تتميز بحداثة أساليب إرتكابها وسرعة تنفيذها وسهولة إخفائها و دقة و سرعة محو آثارها وهي تعتمد في الأساس على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها وتحتاج لخبرة فنية يصعب على الخبير التقليدي التعامل معها[26].

ومن تم يقتضي أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسبة الإلكترونية وطريقة تشغيلها وأساليب ارتكاب الجرائم عليها أو بواسطتها مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها وضبط الأدوات التي استخدمت في ارتكابها، لذلك فقد وجدت صعوبات جمة في كشف غموضها و إجراء التفتيش والضبط اللازمين أو التحقيق فيها على نحو استدعى إعداد برامج تدريب وتأهيل لهذه الموارد من الناحية الفنية على نحو تمكينها من تحقيق المهمة المطلوبة وبكفاءة عالية.

ففي الفترة الأولى لظهور هذا النوع من الجرائم وقعت الشرطة في أخطاء جسيمة أدت إلى الأضرار بالأجهزة أو الملفات أو الأدلة الرقمية الخاصة بإثبات الجريمة، ونعطي مثالا لهذا الخطأ من عمل الشرطة بالولايات المتحدة الأمريكية فقد

حدث أن طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي للتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة و قد حدث نتيجة ذلك أن تسببت دائرة الشرطة بدون قصد في إتلاف ما كان قد سلم من الملفات والبرامج[27].

ثالثا: أساليب التحري التقليدية

أن أساليب التحري أو التحقيق التقليدية لا تصلح لكشف غموض هذه الجرائم وضبط مرتكبيها والتحفظ على أدلتها، لذلك عمدت العديد من التشريعات إلى وضع أساليب أخرى للتحري عن هذه الجرائم، ومن بينها المشرع الجزائري الذي قام بوضع أساليب تتوافق مع الطبيعة التقنية للتحري عن هذه الجرائم بموجب القانون 09-04 المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وأهمها المراقبة الإلكترونية والتي تحوي أسلوبي الوقاية و المكافحة وإجراءات التفتيش في النظم المعلوماتية وحجز الأدلة الرقمية (حجز المعطيات) وحفظ معطيات السير من طرف مقدمي الخدمات

ويبدو أن المشرع الجزائري وبغية تسهيل عمل المحققين في وضع الترتيبات التقنية المشار لها تجاوز كل الحدود ولم يراع حرمة الحياة الخاصة، وقد يكون الدافع إلى ذلك هو طابع الخطورة التي تكتسيه الجريمة إذ أنه ومع سرية المراسلات مضمونة دستوريا وفي المواثيق الدولية كما ورد في المادة 12 من الإعلان العالمي لحقوق الإنسان[28]، وهذه الضمانة الدستورية نص عليها المشرع الجزائري في الفقرة الأولى من المادة 46 من الدستور الحالي، المعدل بموجب القانون رقم 16-01 مؤرخ في 26 جمادى الاولى عام 1437 الموافق 6 مارس 2016، المتضمن التعديل الدستوري[29].

كما يمكن للمجني عليه في هذه الجرائم أن يقدم خدمات كبيرة لرجال الشرطة أو لسلطة التحقيق بتقديمه معلومات تحقق فائدة كبيرة في معرفة طبيعة الجريمة التي وقعت وأساليب ارتكابها و الأدوات المستخدمة في ارتكابها والأشخاص المشتبه فيهم وبواعث الجريمة وما إذا كان هناك شهود أم لا[30].

إضافة إلى أن إثبات الجرائم التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية سيتأثر بطبيعة هذه الجرائم و بالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم إكتشاف العديد من الجرائم في زمن إرتكابها، أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم، أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرر بالأفراد وبالمجتمع[31].

وعليه يمكن القول أن التحري في كشف غموض الجريمة من طرف سلطات التحقيق يتطلب تدريبهم وتأهيلهم وإلمامهم بالتقنيات الأساسية لتكنولوجيات الإعلام والاتصال ومواكبتهم للتطور السريع الحاصل في هذا المجال والإستعانة بالخبراء في الأمور التقنية المعقدة على نحو يمكنهم من استخلاص الأدلة الإلكترونية من بيئة افتراضية والتحقق من سلامتها وتقديمها كأدلة موثوقة للقضاء.

الفرع الثاني: ضعف التعاون الدولي في مكافحة الجرائم الإلكترونية

إن التعاون والتنسيق بين الأفراد والشركات يلعب دورا رئيسيا في إثبات الجريمة الإلكترونية، وعلى العكس من ذلك فإن غياب سياسة التعاون الدولي والتنسيق بين الدول في مقاومة الجريمة الإلكترونية يقابله في ذات الوقت تعاون واضح بين محترفي الإجرام المعلوماتي فضلا عن البرامج إلي يستعين بها القراصنة في أنشطتهم الإجرامية فإنهم يتعاونوا فيما بينهم ويتبادلون النصائح والخبرات فيما يتعلق بأنشطتهم، مما يزيد فاعلية وخطورة هجومهم و خصوصا في ظل قصور وعدم فاعلية سياسة الدفاع الخاصة والمنصوص ضد هذه الجريمة[32].

لذلك تنشأ ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات على وجه الخصوص من سهولة حركة المعلومات في أنظمة تقنية المعلومات حيث يرجع لهذه السهولة في حركة المعلومات بأنه بالإمكان إرتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة بينما يتحقق نجاح هذا النشاط الإجرامي في دولة أخرى [33].

كما أنه ورغم المناداة بضرورة التعاون الدولي في مكافحة هذه الجريمة إلا أن هناك عوائق تحول دون ذاك وتجعل هذا التعاون صعبا، وأهمها:

1-عدم وجود نموذج موحد للنشاط الإجرامي: فالأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية لا يوجد فيها اتفاق عام مشترك حول نماذج إساءة إستخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحا في بعض الأنظمة يكون محرما في أنظمة أخرى، ويرجع ذلك إلى عدة عوامل كإختلاف العادات والتقاليد والديانات والثقافات من مجتمع لآخر.

2-اختلاف النظم القانونية الإجرائية: بسبب تنوع واختلاف النظم القانونية الإجرائية نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى.

3-عدم وجود معاهدات ثنائية أو جماعية بين الدول: وحتى في حالة وجودها فإنها تكون قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الإنترنت.

4-مشكلة الاختصاص في جرائم الإنترنت: وتثار هذه المشكلة بالنسبة للاختصاص على المستوى الدولي وذلك لاختلاف التشريعات والنظم القانونية من دولة لأخرى حيث ينجم عنها تنازع الاختصاص بين هذه الدول بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود، فيحدث أن ترتكب داخل إقليم دولة معينة إلا أنها تمتد إلى خارج إقليم دول أخرى مما يعني خضوعها لأكثر من قانون جنائي.

5-عدم وجود قنوات اتصال: أن من أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين هي الحصول على المعلومات والبيانات المتعلقة بهم ولتحقيق هذا الهدف كان لازما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أمنية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العلمية التي غالبا ما تكون مفيدة في التحري لجرائم معينة ولمجرمين معينين وبالتالي تنعدم الفائدة من هذا التعاون[34].

لذاك أصبح أمر التعاون الدولي ومكافحة الجرائم الإلكترونية أمرا حتميا يستلزم ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة هذه الجرائم،

والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، ويجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، سبل المكافحة، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دول أخرى، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو إبرام الاتفاقيات الدولية[35].

وفي مجال الإجراءات فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاما من أجل التسيير دون عقبة لطلب المساعدة القانونية الوطنية [36]، ويسهل من عملية القبض على مرتكبي هذه الجرائم، و ذلك دون مساس هذه الإجراءات بسيادة الدول الأخرى و أمنها ونظامها العام أو أي مصلحة أخرى من مصالحها الأساسية.

كما تجدر الإشارة إلى أن المشرع الجزائري نص في الفصل السادس من القانون 09-04 المؤرخ في 2009/08/05، السالف الذكر، على قواعد تتعلق بالإختصاص القضائي والمساعدة القضائية الدولية المتبادلة وتبادل المعلومات واتخاذ الإجراءات التحفظية ووضع قيود على طلبات المساعدة القضائية الدولية التي من شأنها المساس بالسيادة الوطنية أو النظام العام.

خاتمة

تثير مسألة الإثبات صعوبات في مواجهة الجرائم الإلكترونية، التي تقع على العمليات الإلكترونية بالوسائل الإلكترونية، نظرا لكون هده الجرائم تقنية تنشأ في الخفاء ببيئة إلكترونية، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية للنيل من الحق في المعلومات، ينتج عنها ما يعرف بالأدلة الإلكترونية التي تعتبر إحدى الآثار المهمة في الكشف عن هذه الجريمة و الربط بينها و بين مرتكبيها.

وأن الدليل الإلكتروني عند استخلاصه تعترضه عدة عقبات منها ما يتعلق بخصوصية الدليل الإلكتروني في حد ذاته بسبب عدم ظهوره وسهولة محوه أو تدميره وصعوبة الوصول إليه، ومنها ما يتعلق بخصوصية التحقيق بسبب صعوبة التحري في كشف غموض الجريمة وضعف التعاون الدولي في مكافحة الجرائم الإلكترونية.

كما أنه لتسهيل عملية جمع الأدلة الإلكترونية تم تحديث الأساليب الإجرائية المتبعة لإثبات وقوع الجريمة الإلكترونية من طرف المشرع الجزائري وبعض

التشريعات المقارنة على نحو يكشف غموض هذه الجريمة ونسبتها لمرتكبيها ودون أن يعرض حقوق الأفراد الآخرين وحرياتهم للخطر.

ومما سبق تقترح عدة حلول لمواجهة المعوقات المتعلقة بخصوصية الدليل الإلكتروني في حد ذاته و المعوقات المتعلقة بخصوصية التحقيق.

بالنسبة لخصوصية الدليل الإلكتروني، نقترح ما يلي:

1-حث المجني عليهم بالتبليغ عن الجرائم الإلكترونية فور معاينتها بوضع رقم هاتفي خاص تحت تصرفهم .

2-إعطاء صلاحيات واسعة لجهات التحقيق في إستخلاص الأدلة إثناء استخدام الأساليب التقنية الحديثة التي تفيد في إثبات الجريمة وكشف مرتكبيها على نحو يكفل عدم المساس بحقوق الأفراد الآخرين و حرياتهم.

3-جمع الآثار المعلوماتية الرقمية بطريقة صحيحة وسلمية تضمن عدم تغييرها والتأكد من أنها لم يتم العبث بها أو تعديل محتواها.

4-ضرورة إجراء الاختبارات التكنولوجية والعلمية على الدليل الإلكتروني المستخلص والتحقق من أصالته ومصدره كدليل موثوق يمكن تقديمه إلى القضاء.

أما بالنسبة لخصوصية التحقيق، نقترح ما يلي:

1-ضرورة زيادة التأهيل التقني والفني لجهات التحقيق من خلال إلمامهم بالتقنيات الأساسية لتكنولوجيات الإعلام والإتصال، والإستعانة بالخبراء في الأمور التقنية لمواكبة الطبيعة الفنية والعلمية المعقدة للجرائم الإلكترونية، واستخلاص الدليل الرقمي من الأجهزة الرقمية.

2-يجب نشر الوعي والثقافة القانونية بين المواطنين ومؤسسات المجتمع المختلفة من أجل إدراكهم بخطورة هذه الجرائم وصعوبة استخلاص الأدلة الإلكترونية وأهمية التبليغ عن مرتكبيها.

3- ضرورة إتباع القواعد الفنية اللازمة لحماية البيانات والمعلومات من مخاطر التعديل عليها أو تعريضها للإتلاف.

4-تعزيز التعاون والتنسيق بين مختلف الدول والمؤسسات الدولية المعنية بمكافحة الجريمة الإلكترونية وخصوص الإنتربول عن طريق عقد اتفاقيات ثنائية وجماعية ذات علاقة بالأدلة الإلكترونية والأنظمة المشتركة.

وعليه، يمكن القول في الأخير، أن تجاوز هذه الصعوبات من الناحية القانونية يكون من خلال تفعيل نصوص قانون الإجراءات الجزائية و
تماشيها مع هذه الاقتراحات، إضافة إلى مواكبتها كل المستجدات التي تعترض عملية الإثبات في الجرائم الإلكترونية.

الهوامش والمراجع المعتمدة

1 محمد محمد عنب، تكنولوجيا الإثبات الجنائي، مجلة الأمن والحياة، أكاديمية الشرطة والقاهرة، العدد 396، 2015، ص108.

2 أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون 09-04، (مذكرة لنيل شهادة الماجستير في القانون الجنائي، جامعة قاصدي مرباح ورقلة، 2013)، ص69.

3 إلهام شهرزاد روابح، مقال بعنوان الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية، مجلة البحوث والدراسات القانونية والسياسية، العدد العاشر، جامعة البليدة، 2016، ص196،195،194.

4 عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص327.

5 جاسم خريبط خلف، مقال بعنوان الدليل الجنائي في الجريمة المعلوماتية، مجلة القانون للدراسات والبحوث القانونية، جامعة ذقار، 2016، ص09.

6 عبد العال الديربي، محمد صادق إسماعيل ، المرجع السابق، ص327.

7 جاسم خلف خريبط، المرجع السابق، ص7.

8 علي عدنان الفيل، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية– دراسة مقارنة، ماجستير قانون، كلية الحقوق، جامعة الموصل، المكتب الجامعي الحديث، الأسكندرية، 2012، ص80.

9 المواد 4،5،6،11 من القانون 09–04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، 2009.

10 الديربي عبدالعال ، محمد صادق إسماعيل ، المرجع السابق، ص327.

11 المرجع نفسه، ص329.

12 علي عدنان الفيل، المرجع السابق، ص81.

13 الديربي عبدالعال ، محمد صادق إسماعيل ، المرجع السابق، ص329.

14 خيراني فوزي، الأدلة العلمية و دورها في الإثبات الجنائي، مذكرة لنيل درجة الماجستير في العلوم القانونية والإدارية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2012، ص142.

15علي عدنان الفيل، المرجع السابق، ص80.

16 الديربي عبدالعال ، محمد صادق إسماعيل ، المرجع السابق، ص330.

17 جاسم خريبط خلف، المرجع السابق، ص8.

18 مسرة خالد الحمد، الدليل الرقمي و معايير جودته، الطبعة الأولى، مركز الكتاب الأكاديمي، عمان، 2014، ص149.

19 محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2007، ص35.

20 جاسم خريبط خلف، المرجع السابق، ص10.

21 الديربي عبدالعال ، محمد صادق إسماعيل، المرجع السابق، ص339.

22 علي عدنان الفيل، المرجع السابق، ص82.

23 بن لاغة عقيلة، حجية أدلة الإثبات الحديثة، مذكرة لنيل شهادة الماجستير فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق بن عكنون، جامعة الجزائر1، 2012، ص116.

24 أحمد مسعود مريم، المرجع السابق، ص78.

25 الديربي عبدالعال ، محمد صادق إسماعيل ، المرجع السابق، ص340.

26 مسرة خالد الحمد ، المرجع السابق، ص101.

27 علي عدنان الفيل، المرجع السابق، ص،19.

28 زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى عين مليلة، الجزائر،2011، ص161.

29 الفقرة الأولى من المادة 46 من الدستور الجزائري تنص على ما يلي:" لا يجوز إنتهاك حرمة حياة المواطن الخاصة، و حرمة شرفه، و يحميها القانون.
سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"

30 علي عدنان الفيل، المرجع السابق، ص20.

31 جورج أسحق حنين، دراسة عن الجرائم المعلوماتية و الإلكترونية عبر شبكة الإنترنت وسبل مواجهتها، الإدارة العامة المركزية للمعلومات الإحصائية، 2015، ص16.

32 جاسم خريبط خلف، المرجع السابق، ص 24، 25.

33 الديربي عبدالعال ، محمد صادق إسماعيل ، المرجع السابق، ص345.

34 جاسم خريبط خلف ، المرجع السابق، ص25،26.

35 سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق و العلوم السياسية، جامعة أبوبكر بلقايد تلمسان، 2011، ص21.

36 الديربي عبدالعال ، محمد صادق إسماعيل ، المرجع السابق، ص346.