ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 2000- 2018

معوقات التحقيق الجنائي في البيئة الافتراضية

Obstacles to criminal investigation in the virtual world

ط.د/ بوشارب هانية *
مخبر السياحة، الإقليم والمؤسسات.
كلية الحقوق والعلوم السياسية جامعة غرداية
bouchareb.hania@univ-ghardaia.dz

أ.د/ بن شهرة شول
مخبر السياحة، الإقليم والمؤسسات.
كلية الحقوق والعلوم السياسية جامعة غرداية
benchohra.choul@gmail.com

تاريخ إرسال المقال: 12/ 07/ 2023 تاريخ قبول المقال: 14/ 08/ 2023 تاريخ نشر المقال: 15/ 09/ 2023

الملخص:

تتسم الجرائم المعلوماتية وملاحقة مرتكبيها بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق الجنائي فيها، كونها تتصف بالجريمة المخفية وغير مرئية في العديد من حالاتها، قد لا يلاحظها المجني عليه أو يدرك حتى بوقوعها لذلك تتميز بصعوبة إثباتها، ولنقص التدريب الكافي لجهات التحقيق في التعامل مع الأدلة التي قد يتركها المجرم المعلوماتي وما قد يستخدمه من تدابير الحماية الفنية التي تحول دون كشف أمره مما يعيق الوصول إلى الدليل الذي يدينه.

الكلمات المفتاحية: الجريمة المعلوماتية، معوقات التحقيق الجنائي، المجرم المعلوماتي، الدليل الرقمي، البيئة الإفتراضية.

Abstract:

Due to the fact that information crimes often involve a hidden crime that is not always obvious, prosecuting their perpetrators presents a number of challenges that might impede the criminal investigation process. Evidence that the criminal may leave behind and the technological safeguards he may employ to keep his case from being made public and obstruct access to evidence that could be used against him.

Keywords:: information crime, obstacles to the criminal investigation, virtual criminal, digital evidence, virtual world.

* المؤلف المرسل

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 7404-2661
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 2000- 2018

مقدمة:

ظهور شبكة الأنترنت والتطور التكنولوجي الحاصل في عصرنا الحالي، أدى إلى إنتشار ما يسمى بالجرائم المعلوماتية التي يتمحور نشاطها في البيئة الإفتراضية، حيث أصبحت القواعد الإجرائية التقليدية غير قادرة على إثبات هذا النوع من الجرائم وقاصرة إزاء ملاحقة مقترفيها لكونها ترتكب بالخفاء وعن بعد، يصعب كشفها وإثباتها وتحديد هوية المساهمين فيها، كما يصعب الوصول إلى الأثر المادي للجريمة والحصول على الدليل الجنائي الرقمي الذي تخلفه، مما شكل ذلك عائقا أمام السلطة القضائية في مواجهتها والتصدي لها، بالتالي أدت هاته العوائق إلى صعوبة تكوين إقتناع الشخصي للقاضي الجزائي، الأمر الذي إستلزم بضرورة إيجاد وسائل حديثة وجديدة تختلف عن الطرق التقليدية لمكافحتها، وبناء على ما سبق لنا ذكره نطرح الإشكالية التالية:

فيما تتمثل المعوقات التي تعترض جهات التحقيق في مكافحة الجرائم المعلوماتية؟

ويهدف هذا المقال إلى تحقيق الأهداف التالية:

- التطرق إلى أهم المعوقات الفنية التي تعترض الجهات التي تتولى التحقيق في الجرائم المعلوماتية؛
- الوقوف على أهم الأسباب التي تحول دون المجني عليه عن الابلاغ عن وقوع الجرائم المعلوماتية؛
- تسليط الضوء على أهم الأساليب والتدابير الأمنية التي من الممكن أن يستخدمها المجرم المعلوماتي لإعاقة الوصول إليه؛
- المعوقات المرتبطة بالجهات التي تتولى التحقيق في الجرائم المعلوماتية؛
- كما يعد مرجعا ثريا في مجال العلوم القانونية من أجل الاستفادة أكثر في الموضوع.

وإرتأينا أن يكون مقالنا هذا وفق المنهج الوصفي التحليلي، والذي من خلاله سنقوم بوصف وتحليل أهم المعوقات التي تعترض جهات التحقيق في إستخلاص الدليل الرقمي.

للإجابة على الإشكالية المطروحة ارتأينا تقسيم دراستنا إلى مبحثين؛ نتطرق إلى المعوقات المرتبطة بالجهات التي تتولى التحقيق في الجرائم المعلوماتية ضمن (المبحث الأول)؛ الذي سوف نتطرق فيه إلى المعوقات التي مصدرها نقص خبرة سلطات الاستدلال والتحقيق في (المطلب الأول)؛ بينما سنتطرق للمعوقات المتعلقة بضخامة كم البيانات المعلوماتية في (المطلب الثاني)؛ وإلى ارتفاع تكاليف الحصول على الدليل الرقمي في (المطلب الثالث)؛ أما (المبحث الثاني) فقد خصصناه إلى المعوقات التي تعترض الوصول إلى الدليل الرقمي، بحيث سنتطرق إلى المعوقات المرتبطة بالمجني عليه "الإحجام عن الإبلاغ" في (المطلب الأول)؛ بينما إلى المعوقات المتصلة بالجاني "المجرم المعلوماتي" في (المطلب الثاني).

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 7404-2661
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 2000- 2018

المبحث الأول: المعوقات المرتبطة بالجهات التي تتولى التحقيق في الجرائم المعلوماتية

من الأسباب الجوهرية التي تحول دون إثبات الجريمة المعلوماتية، نقص الخبرة والمعرفة الفنية لدى سلطات الإستدلال والتحقيق في أساليب التصدي لهذه الجريمة (المطلب الأول)، ناهيك عن ضخامة كم البيانات المعلوماتية التي يجب فحصها في ظرف وجيز من طرف سلطات الإستدلال والتحقيق (المطلب الثاني)، بالإضافة إلى إرتفاع تكاليف الحصول على الدليل الرقمي المستخلص منها (المطلب الثالث).

المطلب الأول: المعوقات التي مصدرها نقص خبرة سلطات الاستدلال والتحقيق

تعد عملية البحث والتحقيق في الجرائم المعلوماتية في غاية الأهمية والتعقيد مما تفرض على القائمين بهذه العملية أن يكونوا على درجة كبيرة من العلم والمعرفة بخبايا المعلوماتية ويتحكمون جيداً في تقنياتها[1]، فهذه التقنية دائمة التطور وبشكل سريع، حيث إن مرتكبي هذه الجرائم يتابعون كل جديد ويعملون على تطوير سبل إخفاء أدلة جرائمهم، ومن هنا يتوجب على المحقق أن يكون على دراية تامة ومواكباً للتطور فيما يتعلق بجرائم الحاسوب والإنترنت[2].

ذلك أن حداثة الجرائم وتقنياتها العالية تتطلب من القائمين على البحث الجنائي والتحقيق الإلمام الكافي بها، فلا يكفي أن يكون لهم الخلفية القانونية أو أركان العمل الشرطي فقط، ولكن لابد من الإلمام بخبرة فنية في مجال الجريمة المرتكبة عبر الإنترنت[3]، ولذلك غالباً ما تواجه عملية إستخلاص الدليل الرقمي نقص في الخبرة الفنية والتقنية لدى جهات التحقيق، فهذا الأمر يشكل عائقاً في الكشف عن الجرائم المعلوماتية وينعكس سلباً على التحكم في فنيات إجراء الإستدلالات والتحقيقات[4]، مما يزيد من صعوبة وصولهم إلى الدليل الرقمي وكيفية ضبطه والمحافظة عليه[5]، لأن التكوين القانوني أو الأمني في مجال

---

[1]– عميمر عبدالقادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان– الجزائر–، 2021، ص 124.

[2]– خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 225.

[3]– صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013، ص 121.

[4] – عميمر عبدالقادر، المرجع السابق، ص 124.

[5]– بلجراف سامية، سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي، مجلة الدراسات القانونية المقارنة، مخبر القانون الخاص المقارن، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، شلف –الجزائر–، المجلد 07، العدد 01، 2021، ص 685.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 2000- 2018

الجريمة لا يعد كافياً بالنسبة للأشخاص المؤهلين للبحث والتحري في مجال الجرائم المعلوماتية[6]، ذلك أن كشف هذه الجرائم يقتضي أن تكون الأجهزة المعنية على دراية كافية بأساسيات التعامل مع هذه الجرائم وكيفية تقصيها وضبطها وصولاً إلى مرتكبيها[7].

فنقص الخبرة لدى هؤلاء قد يفضي إلى تدمير الدليل وإتلافه، على إعتبار أن جهلهم بأساليب ارتكاب الجرائم المعلوماتية يجعلهم في كثير من الأحيان يقعون في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها[8]، كما في حالة إغفال المحقق الدقة الواجبة في فحص وحصر ووصف الأدلة التي خلفها المتهم في مسرح الجريمة، أو إغفال ملاحظة ما وعدم تسجيلها إعتقاداً منه أنها غير ذات قيمة، ولكنها في الواقع قد تكون ذات ثقل في إستظهار الحقيقة[9]، وقد يدمر الدليل بسبب خطأ منه أو إهمال، أو بالتعامل مع الأقراص المرنة بلا خبرة أو حيطة ما يترتب عليه تلف الدليل ومحوه[10].

ولذلك يتطلب البحث والتحري عن هذا النوع من الجرائم تكويناً متخصصاً في مجال تقنيات تكنولوجيا الإعلام والإتصال وأنظمة المعالجة الآلية للمعطيات، وكل ماله علاقة بالبيئة الرقمية[11]، ومن هنا تأتي الدعوى إلى ضرورة تأهيل جهات البحث والتحقيق الجنائي في شأن التعامل مع هذه الجرائم وإستخلاص الدليل الإلكتروني منها، بما يواكب التطور الحاصل في هذا الجانب ومواكبة المتغيرات التكنولوجية في مجال الحوسبة والمعلوماتية[12].

ويتطلب إضافة إلى ذلك استقطاب خبراء الأدلة الجنائية الرقمية المتخصصين في الجرائم المعلوماتية من خلال التشجيع المادي برفع أجورهم ومنحهم مكافآت محفزة، وتوفير المعدات المتطورة في هذا المجال مثل ما قامت به بعض الدول[13] الرائدة في هذا الميدان[14].

---

[6] – عميمر عبدالقادر، المرجع السابق، ص 124.

[7] – بلجراف سامية، المرجع السابق، ص 685.

[8] – براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري– تيزي وزو، 2018، ص 210.

[9] – رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الاثبات الجنائي دراسة مقارنة، الطبعة الأولى، منشورات زين الحقوقية، بيروت–لبنان–، 2019، ص 188.

[10] – نفس المرجع، ص 189.

[11] – عميمر عبدالقادر، المرجع السابق، ص 124.

[12] – رفاه خضير جياد العارضي، المرجع السابق، ص 189.

[13] – لقد إهتمت أجهزة الأمن في الكثير من دول العالم لمواجهة جرائم الحاسوب والإنترنت والتحقيق فيها، ففي الولايات المتحدة الأمريكية، تمثل أعلى نسبة من المستخدمين لنظم المعلومات في العالم وتعاني بشكل كبير من جرائم الحاسوب والإنترنت، مما دعاها

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2023 المجلد: السابع العدد: الثاني ص.ص: 2000- 2018

المطلب الثاني: المعوقات المتعلقة بضخامة كم البيانات المعلوماتية

إن ضخامة كم البيانات والمعلومات على الشبكة المعلوماتية هي من أكبر العقبات التي تواجه رجال الضبط وسلطات التحقيق الجنائي في الجريمة المعلوماتية، فكمية المعلومات الضخمة هذه تحتاج إلى فحص ودراسة لإستخلاص الدليل العلمي لهذه الجريمة[15]، إذا كانت سلطات التحقيق في الجرائم التقليدية أمام مسرح جريمة واضح محدد المعالم يمكنهم التحقيق فيه، فإنهم في حالة الجريمة المعلوماتية سيكونون أمام عالم إفتراضي لا متناهي متباعد الأطراف متصل ببعضه البعض، من حيث المعلومات والأجهزة وحتى الكم الهائل والضخم والرهيب من البيانات والمعطيات الواردة فيه[16]، وإمكانية خروجها عن نطاق إقليم الدولة والبعد الجغرافي بين مرتكب الجريمة والضحية.

وإذا كان المحققون في الجرائم التقليدية يواجهون صعوبة في التدقيق ببعض السجلات والبيانات المكتوبة الممسوكة في شركة أو مُؤسسة، فماذا سيكون الوضع عليه في الحالات التي يتطلب التّحقيق في جريمة ما الإطلاع على آلاف من السجلات والبياناتِ الرّقميّةِ من نُصوص وَصُورٍ فوتوغرافيةٍ ومَقاطِعَ فديو، والبحث عنها بين عدد من آلاف الصفحات، كما أن الإطلاع عليها وتحليلها يستوجب الكثير من الوقت[17]، والتي يلزم فرزها من قبل الجهات المختصة وتصنيفها إلى بيانات مجرمة وأخرى غير مجرمة مما قد يتبين من الفحص أن عددا كبيرا من البيانات ربما يكون غير ذي فائدة، ونتيجة لعدم إمكانية وجود فرز في إطار التخزين الرقمي في العالم الرقمي، فإن فحص هذه البيانات يحتاج إلى وقت وجهد ونفقات

إلى إنشاء وحدة متخصصة للمكافحة والتحقيق في هذه الجرائم من ضمن مكتب التحقيقات الفيدرالي، ويكون تدريب عناصر هذه الوحدة مستمرا. ليواكب تطور جرائم الحاسوب والإنترنت. وفي المملكة الأردنية الهاشمية أنشأت مديرية الأمن العام قسما خاصا بجرائم الحاسوب والإنترنت منذ عام 1998، يتولى إجراءات المكافحة والاستدلال والتحقيق في الجرائم المرتكبة بواسطة الحاسوب هدفا أو بيئة لها، وتم رفد هذا القسم بمختصين في مجال علوم وهندسة الحاسوب، وزود بما يلزم من أجهزة ومعدات وبرمجيات تساعد في إجراءات التحقيق، وفي فحص الأجهزة المضبوطة في الجريمة والمحافظة على الأدلة، وللمزيد من التفصيل، ينظر: خالد عياد الحلبي، مرجع السابق، ص-ص، 225- 226.

[14]- عميمر عبدالقادر، المرجع السابق، ص 125.

[15] - حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت-لبنان-، 2014، ص 372.

[16] - بن بادة عبدالحليم، إجراءات البحث والتحري عن الجريمة المعلوماتية "الخصوصية والإشكالات"، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور الجلفة، المجلد الثاني، العدد 23، جوان 2015، ص 91.

[17] - عادل مشموشي، جرائم المعلوماتية (وتحديات أدواتها الإلكترونية، أساليبها التقنية، مسارحها الإفتراضية، مقتضياتها التشريعية)، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2019، ص407.

ضخمة فمثل هذه الأمور تشكل عقبة أمام سلطات البحث[18]، ويصبح الأمر أكثر تعقيداً فيما لو عَمَدَ المُجرِم إلى تَشتيت المعلومات والبيانات التي دَخَلَ إليها بهدَف تَضليل المحققين وإجهادهم، لكي يَكُفُّوا عن مُتابَعَةِ البَحثِ عن الأدلة الجُرميّة[19].

إضافةً إلى تَطَلُّبِ مُعاينَةِ الكثير من البيانات والمعلومات والإطلاع على مضامينها، والتّي يغلُبُ عليها طابع البيانات غير المرئية، والمحفوظة بلُغَةٍ رقميّةٍ يفهمها الحاسِبُ، وأنّ إستخراجها والإطلاع عليها يتطَلّبُ تَحويلها إلى لُغَةٍ يفهمها المُحقّق، كما يتطلب الأمرُ أيضاً عرَضَها على شَاشَة أو طباعتها؛ كُلٌّ ذلك يستوجِبُ مَعرفَة المُحقق بتقنيات الحاسوب، كذلك إن هذه الأمور تُشكّلُ حاجزاً أمام إثبات تلك الجرائم[20]. فإنه يكون من الملائم وجوب ندب خبراء فنيين فى مثل هذه الجرائم حتى يمكن فرز المعلومات التي يحتاجها التحقيق عن تلك التي لا حاجة لها، وإلا دخل رجل الضبط والمحقق في دائرة مغلقة من المعلومات لن يخرج منها، وهذا يتطلب أن يكون ندب هؤلاء الخبراء وجوبياً ومن ثم تعديل التشريعات الجنائية القائمة التي تجعل ندب خبير في الدعوى أمر جوازى للمحقق إن شاء أمر به أو رفضه، وذلك لأن طبيعة الجريمة تستلزم التعامل معها بطريقة حرفية أو فنية تفوق قدرات رجل الضبط أو المحقق إلا إذا كان مؤهلاً لذلك، فيمكنه الإعتماد على قدراته الشخصية فى ضبط وتحقيق هذه الجرائم شرط ألا يخرج عمله عن الأصول الفنية المتعارف عليها.[21]

المطلب الثالث: إرتفاع تكاليف الحصول على الدليل الرقمي

[18] – محمد صالح جاد المولى خليفة، الدليل الرقمي وحجيته في إثبات جرائم المعلومات دراسة مقارنة، بحث للحصول على درجة الدكتوراة، قسم القانون الجنائي، كلية الحقوق، جامعة طنطا، 2018، ص254.

[19] – عادل مشموشي، المرجع السابق، ص381.

[20] – نفس المرجع، ص407.

[21] – عبدالفتاح بيومي حجازي، الدليل الجنائي في جرائم الكمبيوتر والتزوير – دراسة معمقة في جرائم الحاسب الالي والأنترنت– ، دار الكتب القانونية، مصر، 2004، ، ص110.

إن أكثر عائق يواجه المحققين في جرائم الحاسوب هو عدم وجود دليل مرئي يمكن قراءته وإستيعابه، وذلك أن البرامج والبيانات التي تقع عليها الجريمة تكون غير قابلة للإدراك الحسي[22].

والدليل فيها يتميز بأنه دليل غير مرئي فهو عبارة عن نبضات إلكترونية متواصلة الإيقاع مكونة من سلسلة طويلة من الأرقام الثنائية (0،1)، والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكون منه[23] فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة[24]، مما يستحيل معه الإطلاع عليها بوسائل غير تقنية تعالج هذه الذبذبات في صورة مفهومة للبشر[25]، وبالتالي أن أغلب البيانات المخزنة التي تتداول عبر الحاسبات الآلية تكون على هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحاسبات الآلية[26]، لذا يتطلب الإستعانة بأجهزة وأدوات التقنية وإستخدام برامج حاسوبية ملائمة للإطلاع عليه أو إستخراجه في هيئة ملموسة أو مادية وهي تعد أساليب علمية[27].

ولهذا يقتضي توافر الإمكانيات المادية والبشرية وإستقطاب أجهزة الكفاءة المهنية المتخصصة في هذا المجال لكي يتم الإستعانة بها في كشف هذا النوع من الجرائم وضبط الأدلة[28]، مما تتطلب محققين وقضاة يتمتعون بحد أدنى من المعرفة بتقنية المعلومات، وبكيفية عمل الحاسوب وشبكة الإنترنت، والكثير من البرامج المشغلة لها، الأمر الذي يتطلب صرف أموال باهظة على أجهزة إنفاذ القانون المكلفين بالتصدّي لهذه الظاهرة ومُكافحتها، من خلال إخضاع عناصرها لتدريبات ودورات تعليمية تقنية مُتخصصة ومكثفة[29]، وماتحتاجه من تكلفة مالية في إعداد الدورات والتدريب فإعداد الطابعات والماسحات

---

[22]–عبد القادر درقاوي، جريمة السرقة في عصر المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الخاص، كلية العلوم القانونية والعلوم الإدارية، جامعة أبي بكر بلقايد، تلمسان، 2005/2004، ص 183.

[23]– بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري تيزي وزو، 2019، ص– ص 42–43.

[24]–الطيبي البركه، إشكالية الإثبات في الجرائم الإلكترونية، مجلة آفاق علمية، المركز الجامعي تمنراست –الجزائر– ، المجلد 11، العدد 01، 2019، ص 269.

[25]–حنان ريحان مبارك المضحكي، المرجع السابق، ص 356.

[26]– بلجراف سامية، المرجع السابق، ص 684.

[27]– مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية –أبحاث المؤتمر السنوي الدولي الخامس9 –الكويت–، الجزء الثاني، العدد 3، أكتوبر 2018، ص– ص 197–198.

[28] – بن فردية محمد، الاثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر (1)، 2014/ 2015، ص 215.

[29] – عادل مشموشي، المرجع السابق، ص 403.

الضوئية والشاشات وأجهزة التخزين والبرامج الحديث يحتاج إلى مئات آلاف من الدولارات، بالإضافة إلى النفقات الأخرى المرتبطة بإنشاء وحدات لجرائم الحاسوب والمختبرات الخاصة، فهذه النفقات تعد أعباء على الميزانيات بوصفها متكررة بمعنى لازم من توفيرها في كل ميزانية إذ أن مواكبة التطور المستمر للأنظمة والأجهزة يحتاج لرصد ميزانيات سنوية لها[30]، هذا بالإضافة إلى التكلفة التي تتطلبها عملية الإستعانة بالخبراء خلال البحث عن الأدلة ومعاينة بعض البرامج وتوضيح كيفية عملها[31].

وهذه الخبرة في المقابل تشكل عبئا بسبب حجم وضخامة المصاريف التي يتم إنفاقها في سبيل الحصول على الدليل الإلكتروني، فالإشكال الأساسي هنا يتعلق بطبيعة الدليل الإلكتروني وما يتطلب إثباته من تكاليف باهظة، خاصة أمام غياب مؤسسات متخصصة في هذا الشأن خصوصا في الدول العربية، التي تضطر للجوء إلى مؤسسات أجنبية، مما يجعل التكاليف خاضعة للسعر العالمي المقرر في اللوائح المالية لتلك المؤسسات[32].

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 إستقطاب 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 وحتي يتم ذلك يرى هذا الجانب ضرورة الإستعانة بالنبضة المتخصصة في الحاسب الآلي حال تحقيق الجرائم المعلوماتية وذلك لضبط هذه الجرائم واكتشافها وتقديم أدلة الإدانة فيها[33].

لذلك نقترح إنشاء مخابر معتمدة تابعة للأجهزة العدالة الجنائية، تكون مجهزة بأحدث وسائل التقنية، مع ضرورة تبادل المعلومات مع المراكز والمؤسسات الأجنبية حكومية كانت أم خاصة حتى تستفيد من خبراتها في المجال التقني لاسيما تجربة الولايات المتحدة الأمريكية بإعتبارها من الدول السباقة في هذا المجال، وذلك عن طريق الندوات والمؤتمرات، فضلاً عن دورات تدريبية وذلك في إطار التعاون الدولي الذي يستهدف تقريب وجهات النظر وتوحيد المفاهيم بين الدول المختلفة، والتعرف على أحدث التطورات

[30] – محمد صالح جاد المولى خليفة، المرجع السابق، ص 263.

[31]– عادل مشموشي، المرجع السابق، ص 403.

[32] – أسامة حسين محي الدين عبد العال، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية "دراسة مقارنة"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة –مصر–، المجلد11، العدد 2، يونيو 2021، ص 710.

[33] – الطيبي البركه، المرجع السابق، ص–ص، 270 –271.

من خلال تبادل الخبرات لاسيما أمام الفجوة الرقمية التي يعيشها سكان العالم خاصة بين الدول المتقدمة والدول النامية، في إطار إستخدام نظم تكنولوجيا المعلومات ومدى إمكانية إستيعاب السرعة في التطوير سواء من حيث القطع الصلبة أو البرمجيات[34].

المبحث الثاني: المعوقات التي تعترض الوصول إلى الدليل الرقمي

تتصف الجريمة المعلوماتية بالجريمة المخفية وغير مرئية في العديد من حالاتها غالبا يتم إكتشاف وقوعها عن طريق الصدفة وإذا ما تصادف وإكتشفها المجني عليه فإنه يعمد في أغلب الأحيان إلى الإحجام عن التبليغ بوقوعها (المطلب الأول)، ولا يترك مرتكبها أثراً مادياً يدل على إقترافه للسلوك الإجرامي مما يحول بدوره دون إكتشاف هذا النوع المستحدث من الجرائم (المطلب الثاني).

المطلب الأول: المعوقات المرتبطة بالمجني عليه (الإحجام عن الإبلاغ)

من الصعوبات التي تواجه أجهزة الأمن والمحققين أن هذه الجرائم لا تصل إلى علم السلطات والمحققين وذلك راجع إما لصعوبة إكتشافها من طرف الأشخاص العاديين أو حتى من قبل الشركات التي وقعت ضحية لها وكذا الإحجام عن الإبلاغ خوفاً من إهتزاز ثقة عملائها خاصة على مستوى المؤسسات التجارية والبنوك[35].

فذاتية الجريمة المعلومية من حيث كونها مجهولة ومستترة تتم في بيئة تقنية لا تترك وراءها أي أثر خارجي تحول دون إكتشافها من طرف المجني عليه[36]، وإذا ما تصادف وإكتشفها فإنه يعمد في أغلب الأحيان إلى التستر عليها[37] والصمت بدل إبلاغ الشرطة للتحقيق بشأنها ومعرفة مرتكبها[38]، وففي بعض

---

[34]– عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي قي القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، 2010، ص–ص، 255– 256.

[35] – بن فردية محمد، المرجع السابق، ص 223.

[36]– سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر باتنة، 2013/2012، ص191.

[37] – ففي دراسة للمعهد الوطني للعدالة التابع لوزارة العدل الأمريكية شملت (127) من العاملين في مجال التحقيق في جرائم الحاسبة الالكترونية والانترنت يمثلون (11) وكالة رسمية، كان غالبية المشاركين في الدراسة يعتقدون أن معظم جرائم الحاسبة الالكترونية والانترنت التي يتم اكتشافها لا يبلغ عنها للشرطة، كما توصلت دراسة أخرى أجراها معهد أمن الحاسبة الالكترونية (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، وللمزيد من التفصيل، ينظر: الطيبي البركه، المرجع السابق، ص 275.

[38] – سعيداني نعيم، المرجع السابق، ص 191.

الأحيان عدم علمه بوقوعه ضحية جريمة المعلوماتية وبالإضافة على ذلك قد يرجع إلى عدم إدراكه بأن مثل هذه الأفعال والهجمات تدخل ضمن الأفعال المعاقب عليها قانوناً، وهو ما يزيد في صعوبة كشف هذا النوع من الجرائم والوصول إلى أدلة وإثبات صلتها بفاعليها[39].

وقد أثبتت التجارب أن معظم الجهات المجني عليها، لاسيما والتي غالبا ما تكون مصرفاً أو مؤسسة مالية، شركة أو مشروعاً صناعياً ضخماً [40]، قد تمتنع عن الكشف حتى بين موظفيها عما تعرضت لها من إعتداءات إلكترونية، وتكتفي فقط بإتخاذ إجراءات إدارية وأمنية داخلية دون أن تبلغ السلطات المختصة عنها[41]، وذلك حتى فى الدول المتقدمة من الناحية التقنية والتي ترتفع فيها معدلات هذا النوع من الجرائم[42].

وذلك بسبب حرص هذه المؤسسات على عدم المساس بسمعتها وفقدان زبائنها والمتعاملين معها الثقة في كفاءتها وقدرتها على حماية مصالحهم[43]، مما قد يترك إنطباعاً بعدم إتخاذها للإحتياطات الأمنية اللازمة لحماية معلوماتها، أو لنتيجة إهمالها أو قلة خبرتها أو عدم وعيها الأمني، مما قد ينعكس سلباً على أرباحها وقيمة أسهمها، خاصة أصحاب المؤسسات التي تشكل فيها سمعة المؤسسة عاملاً أساسياً في مجال المنافسة، لأن التبليغ عن حدوث الإعتداء ومايتبعه من إجراءات يمكن أن يؤثر سلباً على ثقة العملاء في المؤسسة، وهو ما يجعل أصحاب هذه المؤسسات يحجمون عن ذلك، لهذا فإنهم يسعون إلى إصلاح الخلل الذي أصاب الأنظمة الخاصة بمؤسساتهم، أو البحث عن تسويات ودية مع مرتكبي هذه الجرائم[44].

ولا يقفون عن حد عدم الإبلاغ عن الجريمة بل إنهم يرفضون التعاون مع الجهات الأمنية خشية معرفة العامة بوقوع الجريمة[45]، ويسعون بدلاً من ذلك إلى محاولة تجاوز آثارها حتى ولو كانت الوسيلة هي مكافأة المجرم[46]، تجنباً للأضرار بسمعتها أو خوفاً من أن الكشف عن أسلوب إرتكاب الجريمة قد

---

[39]– بن فردية محمد، المرجع السابق، ص 222.

[40] –صغير يوسف، المرجع السابق، ص 119.

[41]– براهيمي جمال، مرجع السابق، ص199.

[42]– علي عدنان فيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة)، دار الكتب والوثائق القومية، الإسكندرية، 2012، ص 82.

[43]– براهيمي جمال، المرجع السابق، ص 199.

[44]–عميمر عبدالقادر، المرجع السابق، ص–ص، 123 – 124.

[45]– نفس المرجع، ص 123.

[46] – بن فردية محمد، المرجع السابق، ص 222.

يؤدي إلى تكرار وقوعها بتقليدها من طرف الآخرين[47]، وقد تكون الخشية بسبب أن التبليغ قد يكون فرصة ذهبية أمام المجرم المعلوماتي لمعرفة ثغرات النظام المعلوماتي للمؤسسة، ومختلف نقاط الضعف فيها[48].

كما يوجد عامل آخر يجعل أصحاب المؤسسات يحجمون عن التبليغ يتمثل في الخوف من أن تؤدي أعمال التحقيق إلى الكشف عن محتويات منظوماتهم المعلوماتية أو الخوف من لجوء سلطات البحث والتحري إلى إحتجاز منظوماتهم المعلوماتية أو تعطيل شبكاتها لفترة طويلة بسبب إجراءات التحقيق، وهو ما يؤثر على وتيرة سير أعمالهم[49]، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق، عطفاً على ما قد تسببت الجريمة خسارتها أصلاً [50]، وأيضا تشكيكها في قدرة وكفاءة سلطات الأمن على التصدي لهذا النمط الإجرامي الجديد[51]، إعتقاد بعض الضحايا بعدم قدرة الأجهزة الأمنية على التوصل لمرتكبي الجرائم بسبب نقص خبرتهم وعدم توفر الإمكانيات اللازمة للتوصل إلى المجرمين[52].

ففي هذا الشأن أجريت دراسة في فرنسا أسفرت على نتائج مخيبه تدل على صعوبة إكتشاف الجرائم المعلوماتية ومن ثمة صعوبة التصدي لها، حيث أثبتت هذه الدراسة أن نسبة الجرائم التي تم التبليغ عليها تمثل 15 %.

أما الجرائم التي يتم إكتشافها فقدرت ب 01 %، فيما قدرت نسبة الجرائم التي تم الوصول فيها إلى أدلة تدين مرتكبيها فلم تتعد 03 % كما أكدت دراسة أمريكية أن الرقم الأسود لجرائم الحاسب في إرتفاع مستمر[53].

لأجل ذلك فقد طرحت العديد من الإقتراحات لحمل المجني عليهم في الجريمة المعلوماتية على التبليغ والتعاون مع السلطات بأن تفرض النصوص القانونية المتعلقة بجرائم المعلوماتية إلتزاما على عاتق

---

47 – سعيداني نعيم، المرجع السابق، ص 191.

48– أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث ل.م.د، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، 2020-2021، ص 35.

49 – عميمر عبدالقادر، المرجع السابق، ص 124.

50– علي عدنان فيل، المرجع السابق، ص 83.

51– براهيمي جمال، المرجع السابق، ص 199.

52 – أومدور رجاء، المرجع السابق، ص 36.

53– بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر 01 – بن يوسف بن خدة–، 2018/2017، ص 234.

موظفي الجهات المجني عليها بالإبلاغ عما يصلهم من أخبار عن وقوع تلك الجرائم مع تقدير الجزاء عن الإخلال بهذا الإلتزام[54].

وبعد أن تم عرض الإقتراح على لجنة الخبراء في المجلس الأوربي، تم رفضه وبرروا الرفض بالقول أنه من غير المقبول تحويل المجني عليه إلى جاني وإحلاله محله وهو ضحيته[55]، ولذلك وردت إقتراحات بديلة قد تكون مقبولة منها الإلتزام بإبلاغ جهة خاصة، أو إبلاغ سلطات إشرافية، وتشكيل أجهزة خاصة لتبادل المعلومات وكذلك إصدار شهادة أمن خاصة تمنح بعد عمل مراجعة وتدقيق من قبل هيئة خاصة من المراجعين ويتعين على هذه الهيئة إبلاغ الشرطة بما تكتشفه من جرائم.[56]

وقد أوصى المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات والذي عقد في ريو دي جانيرو بالبرازيل في الفترة من 4-9 سبتمبر 1994 بضرورة تشجيع المجني عليهم على الإبلاغ عن هذا النوع من الجرائم فور وقوعها، وهو ما أوصى به المجلس الأوربي وهذا بهدف تخفيض الرقم الأسود للجرائم المعلوماتية[57].

المطلب الثاني: المعوقات المرتبطة بالجاني (المجرم المعلوماتي)

لا تقف صعوبة إثبات الجرائم الإلكترونية عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها، وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة[58]، بالإضافة على ذلك تمتد إلى الجناة أنفسهم لأن مرتكبي هذا النوع من الجرائم قد يستخدمون الوسائل الإلكترونية المختلفة لإعاقة الوصول إليهم[59].

فالمجرم المعلوماتي هو الذي لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها وإسترجاعها بإستخدام الحاسوب الإلكتروني الرقمي وملحقاته ووسائل الإتصال الرقمية، وذلك بأداء فعل أو الإمتناع

---

[54] – سعيداني نعيم، المرجع السابق، ص 193.

[55]– زراري نسرين، بوقرة إسماعيل، الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات، مجلة الحقوق والعلوم السياسية ، جامعة خنشلة، المجلد 09، العدد01، السنة 2022، ص 113.

[56]– عبد الفتاح بيومي حجازي، المرجع السابق، ص-ص، 75-76.

[57] – بن فردية محمد، المرجع السابق، ص 223.

[58]–خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2009، ص 75.

[59] – بلجراف سامية، مرجع السابق، ص 684.

عنه مما يحدث إضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محليا أو دوليا.[60]

ويستخدم مقدرته العقلية ولا يلجأ إلى إستخدام العنف أو الإتلاف المادي بل يحاول أن يحقق أهدافه بهدوء[61]، دون إحداث أي نوع من الصخب أو اللجوء إلى العنف، فعن طريق إستخدام طرق علمية مبتكرة يمكنه تجاوز الحواجز الإلكترونية، ولهذا يوصف الإجرام المعلوماتي بإجرام الأذكياء[62].

وما 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 إلكترونياً بكثافة بالغة وبصورة مرمزة غالباً على دعائم أو وسائط للتخزين لا يمكن للإنسان قراءتها، وإن كانت قابلة للقراءة من قبل الآلة نفسها، ما يقطع أي صلة بين المجرم وجريمته ويعوق أو يحول دون كشف شخصيته[63]، وكشف وتجميع أدلة بهذا الشكل لإثبات وقوع الجريمة ونسبتها إلى مرتكبيها هو أحد أهم المشاكل التي يمكن أن تواجه جهات التحري والملاحقة[64].

فالمجرم المعلوماتي غالبا ما يضرب سياجا أمنيا على أفعاله غير المشروعة قبل إرتكابه لها، فيزيد بذلك من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقنية التي تدينه[65].

ويحرص بعد إرتكابه لجريمته على محو آثارها التي تدل على وقوعها وذلك من خلال استعمال تقنيات معدة لهذا الغرض مع الأخذ بعين الإعتبار سهولة وسرعة إمكانية محو وتعديل البيانات الإلكترونية التي يمكن القيام بها في أزمان قياسية[66]، وبالتالي تنصله من مسؤولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسب الآلي أو الشبكة أو في الأجهزة بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم إستطاعة هذه السلطات إقامة الدليل ضده، بحيث لا تتمكن السلطات من كشف الجريمة إذا علمت بها[67].

---

[60] – خليلي سهام، خصوصية المجرم الالكتروني، مجلة المفكر، جامعة محمد خيضر بسكرة، العدد 15، جوان 2017، ص 405.

[61] – نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 77.

[62] – عميمر عبدالقادر، المرجع السابق، ص 43.

[63] – رفاه خضير جياد العارضي، المرجع السابق، ص 15.

[64]– الطيبي البركه، المرجع السابق، ص 269

[65]– سعيداني نعيم، المرجع السابق، ص 190.

[66]– الطيبي البركه، المرجع السابق، ص 273.

[67]– خالد عياد الحلبي، المرجع السابق، ص 223.

كما يمكن التنصل من مسؤولية الفعل فمن خلال إدخال الجاني لبعض التعليمات في نظام الحاسوب يتم محو البيانات بالكامل، كما يمكنه وبمجرد كبسة زر خاطفة على لوحة المفاتيح أن يقوم بإلغاء الأوامر الصادرة للجهاز إذا أحس أن أمره سينكشف لأن الجريمة المعلوماتية تتم في صورة أوامر تصدر إلى الجهاز، وهو ما يجعل إكتشاف الجريمة وتحديد مرتكبها أمراً في غاية الصعوبة[68].

فضلاً عما تقدم، فإن الوصول إلى الدليل الرقمي تعترضه عقبة أخرى تكمن في أن الجناة المتمرسين يجتهدون في إخفاء هوياتهم للحيلولة دون تعقبهم أو كشف أمرهم، بحيث تظل أنشطتهم مجهولة وبمنأى عن علم السلطات المعنية بمكافحة الجريمة[69]، حيث توجد الكثير من البرامج التي تمكن المستخدم من إخفاء شخصيته، سواء أثناء إرسال البريد أو تصفح المواقع، الأمر الذي يجعل عملية إستعادة الأدلة أو إعادة تشكيلها عملية معقدة وصعبة تحتاج إلى خبرة وجهد ووقت وأدوات دقيقة قد لا تكون في الكثير من الأحيان متاحة لسلطات البحث والتحري[70]، وهذا ما يجعل أمر ملاحقتهم أو تحديد هويتهم أشبه بالمستحيل سواء عند قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها لأن مرتكب الجريمة المعلوماتية غالباً ما يستعمل الأسماء المستعارة أو يتفادى الدخول إلى الشبكة من هاتفه الخاص[71].

كذلك يمكن للمجرم المعلوماتي أن يزيد من صعوبة عملية التفتيش التي قد تباشر للحصول على الأدلة التي تدينه عن طريق مجموعة من التدابير الأمنية كإستخدام كلمة السر للوصول إليها أو دس تعليمات خفية بينها أو ترميزها لإعاقة أو منع الإطلاع عليها أو ضبطها، لذا فإن إستخدام 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[72].

[68] – عميمر عبدالقادر، المرجع السابق، ص 119.
[69] – بلجراف سامية، المرجع السابق، ص 684.
[70] – عميمر عبد القادر، المرجع السابق، ص 121.
[71] – بلجراف سامية، المرجع السابق، ص 685.
[72] – الطيبي البركه، المرجع السابق، ص 273.

الأمر الذي يجعل عملية إستعادة الأدلة أو إعادة تشكيلها عملية معقدة وصعبة تحتاج إلى خبرة وجهد ووقت وأدوات دقيقة قد لا تكون في الكثير من الأحيان متاحة لسلطات البحث والتحري[73].

وعليه نجد أن القاضي يصعب عليه إدانة شخص دون أن يتأكد يقينيًا بأن هذا الشخص هو المذنب في إرتكاب الجريمة ويرى جانب من الفقه حول ضرورة تدخل المشرع بإضافة حالة ارتكاب الجرائم المعلوماتية كظرف استثنائي يسمح لرجال السلطة العامة القيام بضبط الأدلة عند وقوع الجريمة دون الحصول على إذن سابق من النيابة العامة لتفادي مثل هذه الدفوعات وللتأكد من أن الدليل لم يتم التغيير فيه[74].

الخاتمة:

وفي الأخير نستنتج أن التحقيق الجنائي في مجال الجرائم المعلوماتية يكتنفه الغموض وتحيط به العديد من المعوقات، إذ في بعض الأحيان يصعب الحصول على الأثر المادي المكون للجريمة، الأمر الذي إستلزم ضرورة ظهور نوع من التحدي لجهات التحقيق في تصدي لهذا النوع من الجرائم وإستخلاص الدليل الرقمي؛ ومن خلال ذلك توصلنا إلى جملة من النتائج نذكرها فيما يلي:

1. تتميّز الجرائم المعلوماتية بطابعها الفني، مما تتطلب التمتع جهات التحقيق بحد أدنى من المعرفة والمهارة الفنية والتقنية؛
2. عدم وجود آلية للفرز الذاتي لضخامة كم البيانات والمعلومات على الشبكة المعلوماتية، فكمية المعلومات الضخمة هذه تحتاج إلى فحص ودراسة لإستخلاص الدليل الرقمي، مما تتطلب إلى وقت وجهد ونفقات ضخمة مما تشكل عقبة أمام سلطات البحث؛
3. يحتاج الدليل الرقمي إلى موارد مادية وبشرية أحياناً تفوق إمكانيات الدولة بسبب حجم وضخامة المصاريف التي يتم إنفاقها في سبيل الحصول عليه؛
4. المجني عليه يلعب دوراً رئيسياً في صعوبة إكتشاف وقوع جريمة المعلوماتية، فهو نادراً ما يقوم بالإبلاغ عنها، وإذا ما تصادف و إكتشفها فإنه يعمد في أغلب الأحيان إلى التستر عليها والإحجام عن

[73]– عميمر عبد القادر، المرجع السابق، ص 121.

[74] – بن فردية محمد، المرجع السابق، ص–ص، 216 – 217.

الإبلاغ عنها، ولا يقف عن حد عدم الإبلاغ عن الجريمة بل أحيانا أنه يرفض أي التعاون مع الجهات الأمنية؛

5. القدرة العالية للمجرم المعلوماتي بالإحاطة بالأساليب الأمنية وتدابير الحماية الفنية التي تحول الوصول إلى هوياته الحقيقية وإكتشاف أفعاله غير المشروعة وكذا قدرته على محو وإخفاء كل آثار الجريمة والتستر عنها في فترة وجيزة.

وتجدر بنا الإشارة إلى أنه من خلال هذا البحث توصلنا إلى مجموعة من الإقتراحات نذكرها كما يلي:

1. ضرورة التأهيل التقني والفني لجهات البحث والتحقيق الجنائي في مجال التعامل في الجرائم المعلوماتية، وإخضاعهم لتدريبات ودورات تعليمية تقنية مُتخصصة ومكثفة وإمدادهم بأفضل وسائل التقنية الحديثة وتقنيات الحاسب الآلي ونظم المعلومات التي تمكنهم من الحصول عليها؛
2. نظرا لطبيعة الجريمة المعلوماتية يستلزم التعامل معها بطريقة فنية تفوق قدرات جهات البحث والتحقيق، فإنه يكون من الملائم وجوب ندب خبراء فنيين فى مثل هذه الجرائم، وحبذا تعديل قانون الاجراءات الجزائية بجعل ندب خبير في الدعوى العمومية أمر جوازي للمحقق إن أمر به أو رفضه في الجرائم محل الدراسة؛
3. يقتضي توافر الإمكانيات المادية والبشرية وإستقطاب أجهزة الكفاءة المهنية المتخصصة في هذا المجال لكي يتم الإستعانة بها في كشف هذا النوع من الجرائم وضبط الأدلة؛
4. تشجيع المجني عليهم بالإبلاغ عن أية جريمة معلوماتية فور ملاحظتها، وحبذا لو ينص المشرع الجزائري على إلتزام يقع على عاتق موظفي الجهات المجني عليها بحكم الوظيفة أو مهنة هذه الوظائف، بالإبلاغ عما يصلهم من أخبار عن وقوع تلك الجرائم والتعاون مع السلطات مع تقدير الجزاء عن الإخلال بهذا الإلتزام؛
5. ضرورة سن قانون مستقل خاص بالجرائم المعلوماتية وإقرار المزيد من الجزاءات الرادعة على هذا النوع المستحدث من السلوكيات الإجرامية، وتطوير المنظومة التشريعية في مجال الإثبات الإلكتروني؛

6. التركيز على الجانب الوقائي بنشر الوعي والثقافة القانونية بين أفراد المجتمع من أجل إدراكهم بخطورة هذه الجرائم وما تسببه من أضرار.

قائمة المصادر والمراجع:

أولا: الكتب

1. حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت–لبنان–، 2014؛
2. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان،2011؛
3. خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2009؛
4. رفاه خضير جياد العارضي، الدليل الإلكتروني وأثره في مجال نظرية الاثبات الجنائي دراسة مقارنة، الطبعة الاولى، منشورات زين الحقوقية، بيروت–لبنان، 2019؛
5. سعد عاطف عبد المطلب حسنين، الحماية الجنائية للمصنفات الرقمية دراسة مقارنة، دار الفكر الجامعي، الاسكندرية، 2018؛
6. عادل أحمد مشموشي، جرائم المعلوماتية وتحديات (أدواتها الالكترونية، أساليبها التقنية، مسارحها الافتراضية، مقتضياتها التشريعية)،الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2019؛
7. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، 2010؛
8. عبدالفتاح بيومي حجازي، الدليل الجنائي في جرائم الكمبيوتر والتزوير – دراسة معمقة في جرائم الحاسب الالي والأنترنت– ، دار الكتب القانونية، مصر، 2004؛
9. علي عدنان فيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة)، دار الكتب والوثائق القومية، الإسكندرية، 2012؛
10. عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان– الجزائر–، 2021؛
11. نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008.

ثانيا: الرسائل الجامعية

1. أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث ل.م.د، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، 2020-2021؛
2. براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري- تيزي وزو، 2018؛
3. بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري تيزي وزو، 2019؛
4. بن فردية محمد، الاثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر(1)، 2014/ 2015؛
5. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر باتنة، 2013/2012؛
6. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013؛
7. عبد القادر درقاوي، جريمة السرقة في عصر المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الخاص، كلية العلوم القانونية والعلوم الادارية، جامعة أبي بكر بلقايد، تلمسان، 2005/2004؛
8. فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر 01 – بن يوسف بن خدة-، 2018/2017؛
9. محمد صالح جاد المولى خليفة، الدليل الرقمي وحجيته في اثبات جرائم المعلومات دراسة مقارنة، بحث للحصول على درجة الدكتوراة، قسم القانون الجنائي، كلية الحقوق، جامعة طنطا، 2018.

رابعا: المقالات

1. أسامة حسين محي الدين عبد العال، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية "دراسة مقارنة"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة -مصر-، المجلد11، العدد 2، يونيو 2021؛

2. بلجراف سامية، سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي، مجلة الدراسات القانونية المقارنة، مخبر القانون الخاص المقارن بكلية الحقوق والعلوم السياسية بجامعة حسيبة بن بوعلي شلف –الجزائر–، المجلد 07، العدد 01، 2021؛
3. بن بادة عبدالحليم، إجراءات البحث والتحري عن الجريمة المعلوماتية " الخصوصية والإشكالات"، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور الجلفة، المجلد الثاني، العدد،23، جوان 2015؛
4. خليلي سهام، خصوصية المجرم الالكتروني، مجلة المفكر، جامعة محمد خيضر بسكرة، العدد 15، جوان 2017؛
5. زراري نسرين، بوقرة إسماعيل، الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد 09، العدد01، السنة 2022؛
6. الطيبي البركه، إشكالية الإثبات في الجرائم الإلكترونية، مجلة آفاق علمية، المركز الجامعي بتمنراست –الجزائر–، المجلد 11، العدد 01، 2019؛
7. مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية –أبحاث المؤتمر السنوي الدولي الخامس9– الكويت–، الجزء الثاني، العدد 3، أكتوبر 2018.