

صعوبة عملية استخلاص الدليل الإلكتروني Difficulty extraction electronic evidence

بن شهرة شول

جامعة الاخوة منتوري قسنطينة 1

benchohra.choul@gmail.com

بوشارب هانية *

جامعة غرداية

bouchareb.hania@univ-ghardaia.dz



- تاريخ النشر: 2023/01/05

- تاريخ القبول: 2022/12/31

- تاريخ الإرسال: 2022/10/13

ملخص:

يعد الدليل الإلكتروني من أهم الوسائل في مجال إثبات الجرائم المعلوماتية، فالبينة الافتراضية التي يتواجد بها جعلته يتفرد بإمميزات وخصائص ميزته عن باقي الأدلة الجنائية التقليدية، إلا أن استخلاص هذا النوع من الأدلة يحيط به الكثير من الصعوبات، سواء ماتعلق بطبيعته التكوينية أو ماتعلق بإجراءات الحصول عليه. الكلمات المفتاحية الدليل الإلكتروني، الجريمة المعلوماتية، البينة الافتراضية، الصعوبات، الجرم المعلوماتي.

ABSTRACT:

Electronic evidence is considered as the most essential element in the fight against cyber crimes, The virtual environment in which it is located (the electronic evidence) makes it unique in the privileges and characteristics that distinguish it from the rest of the traditional evidence, However, the extraction of this type of evidence is surrounded by many difficulties, whether its related to the formative nature of this evidence or related to the procedures obtained.

key words. Electronic evidence, cybercrimes, The virtual environment, Difficultie , cyber criminal .

مقدمة:

نتيجة التطور العلمي وطغيان استخدام التقنيات الحديثة في شتى مجالات الحياة انعكس أثره وأسفر عنه ظهور نمط جديد من الإجرام المتمثل في الجرائم المعلوماتية، فهي جرائم تنشأ في وسط افتراضي ترتكب بأساليب متطورة وحديثة دون أن يترك أثرا ماديا لها، مما أدى إلى عدم قدرة الأدلة التقليدية على إثبات هذا النوع من الجرائم المستحدثة، الأمر الذي استلزم ضرورة إيجاد وسائل حديثة وجديدة تختلف عن الطرق التقليدية في الحصول على

* - المؤلف المرسل:

الدليل الجنائي الإلكتروني، بإعتباره الوسيلة الوحيدة لإثبات هذا النوع من الجرائم إلا أنه عند إستخلاصه تعترض جهات التحري والتحقيق عدة صعوبات وهذا راجع إلى الطبيعة التقنية الرقمية التي يتكون منها، والوسط المتواجد فيه. تبرز أهمية هذا المقال في كونه يسعى إلى التطرق إلى الطبيعة التكوينية للدليل الإلكتروني وإلى أهم الأساليب والتدابير الأمنية التي من الممكن أن يستخدمها الجناة لإعاقة الوصول إليهم؛ كما يتم تسليط الضوء على بعض من الوقائع العملية التي تؤيد دراستنا، كما يعد مرجعا ثريا يحتاجه الباحث في مجال العلوم القانونية من أجل الاستفادة أكثر في الموضوع.

بناء على ما سبق لنا ذكره نطرح الإشكالية التالية:

فيما تتمثل أهم الصعوبات التي تعترض عملية إستخلاص الدليل الإلكتروني؟

وإرتأينا أن يكون مقالنا هذا وفق المنهج الوصفي التحليلي، والذي من خلاله سنقوم بوصف الطبيعة التكوينية للدليل الإلكتروني وتحليل أهم الأسباب التي تؤدي إلى عرقلة إستخلاصه. وللإجابة على الإشكالية المطروحة ارتأينا تقسيم دراستنا إلى مبحثين؛ نتطرق إلى الصعوبات الناتجة عن الطبيعة التكوينية للدليل الإلكتروني في (المبحث الأول)؛ الذي سوف نتطرق فيه إلى الطبيعة غير المرئية للدليل الإلكتروني في (المطلب الأول)؛ بينما سنتطرق للطبيعة الديناميكية للدليل الإلكتروني في (المطلب الثاني)؛ أما (المبحث الثاني) فقد خصصناه إلى صعوبات التعقب الناتج عن طبيعة تقنية في ضبط الدليل الإلكتروني، بحيث سنتطرق إلى سهولة محو آثار الدليل الإلكتروني أو تعديله أو تدميره في (المطلب الأول)؛ بينما إلى إعاقة الوصول إلى الدليل الإلكتروني في (المطلب الثاني).

المبحث الأول: الصعوبات الناتجة عن الطبيعة التكوينية للدليل الإلكتروني

يقصد بالطبيعة التكوينية للدليل الرقمي هي الخصائص الفيزيائية التي يتميز بها، سواء ماتعلق بالطبيعة غير المرئية له (المطلب الأول)، أو ماتعلق بطبيعته الديناميكية (المطلب الثاني).

المطلب الأول: الطبيعة غير المرئية للدليل الإلكتروني

إن أكثر عائق يواجه المحققين في جرائم الحاسوب هو عدم وجود دليل مرئي يمكن قراءته واستيعابه، وذلك أن البرامج والبيانات التي تقع عليها الجريمة تكون غير قابلة للإدراك الحسي¹، بحيث لا تخلف آثارا مادية تدل على مرتكبيها كما هو الحال في الجرائم التقليدية، فلا وجود للكسر ولا للدم ولا أيا من الآثار التقليدية للجريمة، فالجريمة المعلوماتية يتمحور نشاطها في بيئة رقمية.

¹ -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، 2004/2005، ص 183.

الدليل فيها يتميز بأنه دليل غير مرئي فهو عبارة عن نبضات إلكترونية مكونة من سلسلة طويلة من الأرقام الثنائية (0,1)¹، والتي تتميز بعدم تشابها فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكون منه، فالكثافة مثلا في العالم الرقمي ليس لها وجود مادي في شكل ورقي وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فأى شيء في العالم الافتراضي يتكون من الصفر والواحد وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة وأما تكوين معطياته فإنها تختلف من حيث الحجم والموضوع².

فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة³، مما يستحيل معه الإطلاع عليها بوسائل غير تقنية تعالج هذه الذبذبات في صورة مفهومة للبشر⁴، 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 الآلية⁵، لذا يتطلب الاستعانة بأجهزة وأدوات التقنية واستخدام برامج حاسوبية ملائمة للإطلاع عليه أو إستخراجه في هيئة ملموسة أو مادية وهي تعد أساليب علمية⁶، إلا أن ترجمته وإخراجه في شكل مادي ملموس لا يعني أن هذا التجميع المادي هو الدليل بل أن هذه العملية ليست سوى عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الإستدلال بها على معلومة معينة⁷.

وتأتي من هنا مشكلة ضبط هذه المعطيات وإحرازها في شكل إلكتروني وحجزها ووضعها في خاتم قانوني لإستغلالها في البحث، وإذا كانت بعض التجهيزات والتقنيات تسمح للباحثين بالوصول إلى هذه المعطيات التي تبقى في ذاكرة الحاسوب المستعمل، إلا أنها تتطلب خبرة عالية وإمكانات قد لا تتوفر عادة لدى مصالح الشرطة القضائية المكلفة بالبحث⁸.

¹- بن فردية محمد، الدليل الجنائي الرقمي وحجته أمام القضاء الجزائري (دراسة مقارنة)، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة بجاية - الجزائر، المجلد 09، عدد 01، 2014، ص 214.

²- 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.

³- الطيبي البركة، إشكالية الإثبات في الجرائم الإلكترونية، مجلة آفاق علمية، المركز الجامعي تلمسان - الجزائر، المجلد 11، العدد 01، 2019، ص 269.

⁴- حنان ربحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية بيروت - لبنان، الطبعة الأولى 2014، ص 356.

⁵- بلجراف سامية، سلطة القاضي الجزائري 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، ص 684.

⁶- مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية - أبحاث المؤتمر السنوي الدولي الخامس 9 - الكويت، الجزء الثاني، العدد 3، أكتوبر 2018، ص - ص 197-198.

⁷- عمير عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد تلمسان - الجزائر، 2021، ص 106.

⁸- 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 118.

فهي كما أسلفنا ترتكب في بيئة رقمية غالبا يتم إكتشاف وقوع الجريمة بطريق الصدفة، ولا يترك مرتكبها أثرا ماديا يدل عليه كما هو الحال في الجرائم التقليدية¹، فالجرائم التي ترتكب على العمليات الإلكترونية والتي تعتمد في موضوعها على التشفير والأكواد السرية والنبضات، يصعب أن تخلف وراءها آثارا مرئية قد تكشف عنها، أو يستدل من خلالها على الجناة² وبذلك يشكل هذا الدليل عائقا أمام رجال التحري والتحقيق خاصة أنهم اعتادوا على الإثبات المادي للجرائم³.

المطلب الثاني: الطبيعة الديناميكية للدليل الإلكتروني

يعد الطابع عبر الوطني أهم السمات التي تميز الجريمة الإلكترونية عن غيرها من الجرائم التقليدية، ويقصد به أن آثار هذه الجرائم قد تتجاوز الحدود الوطنية للدولة إلى غيرها من الدول، لإرتباطها بالشبكة العالمية للمعلومات- الأنترنت- وما طرأ عليها من تطورات هائلة في الآونة الأخيرة، تلاشت أمامها كل الحواجز والحدود الجغرافية للدول⁴، بحيث لا يتطلب من المجرم المعلوماتي الانتقال إلى مسرح الجريمة وقطع المسافات، والمروء على الحواجز الأمنية وتسلق الأسوار، وإنما يمكن إرتكاب الفعل المجرم وهو خلف مكتبه ولا يغادر مكانه⁵، وهو ما يعني عدم التواجد المادي المادي للمجرم المعلوماتي في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين النتيجة أي المعطيات محل الإعتداء⁶، والتي لا تتوقف عند حدود الدولة بل يمكن أن تمتد إلى النطاق الإقليمي لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها⁷، فمثلا يستطيع شخص موجود في الجزائر أن يرتكب يرتكب جريمة معلوماتية مستعينا بالحاسب الآلي المتصل بشبكة الأنترنت، ويكون المجني عليه شخص طبيعي أو معنوي موجود في الولايات المتحدة الأمريكية.

وإضافة على ماسبق أصبحوا يلجؤون إلى تخزين معلوماتهم في شبكة الإتصالات البعيدة التي تتواجد خارج النطاق الإقليمي الذي يتواجدون به⁸، مما يترتب على ذلك صعوبة تعقب الأدلة الرقمية وضبطها، لأنه يستلزم القيام

¹ - عبد الإله النوايسة، جرائم تكنولوجيا المعلومات شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمان الأردن، الطبعة الأولى 2017، ص 80.

² - 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-، المجلد 11 العدد 2، يونيو 2021، ص 707.

³ - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة الإسكندرية، 2010، ص 252.

⁴ - إبراهيم 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 186.

⁵ - عمير عبد القادر، المرجع السابق، ص 121.

⁶ - خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى 2009، ص 77.

⁷ - عمير عبد القادر، المرجع السابق، ص 121.

⁸ - نفس المرجع، ص 122.

بأعمال إجرائية خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها¹، كتفتيش نظم الحاسوب أو معاينة مواقع الإنترنت المخالفة، وهذا كله يصطدم مع مشكل الحدود والولايات القضائية، وهذا راجع إلى أن هذه الإجراءات فيها مساسا بسيادة الدولة المقصودة، وهو ما ترفضه الغالبية من الدول، لذلك أبرمت العديد من الإتفاقيات والمعاهدات الدولية في مجال التعاون الدولي، الذي يهدف إلى التقريب بين القوانين الجنائية، من أجل جمع هذا النوع من الأدلة العابرة للحدود خاصة في إطار مكافحة الجرائم العالمية ومنها الجرائم الإلكترونية².

المبحث الثاني: صعوبات التعقب الناتج عن طبيعة تقنية في ضبط الدليل الإلكتروني

لا تقف مشكلة إستخلاص الدليل الإلكتروني عند طبيعته التكوينية فقط، بل تمتد لتشمل إجراءات الحصول عليه، سواء بسهولة محوه أو تعديله أو تدميره (المطلب الأول)، أو سواء بصعوبة الوصول إليه (المطلب الثاني).

المطلب الأول: سهولة محو آثار الدليل الإلكتروني أو تعديله أو تدميره

فإذا كان من السهل على جهات التحري أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع والمساعدة، فإنه قد يصعب عليها القيام بهذا التحري وبهذه الطرق بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية، فارتباط الجريمة المعلوماتية بالبيئة التقنية إنعكس على طبيعة الدليل المترتب عنها³، ففي هذه البيئة تكون البيانات والمعلومات فيها عبارة عن نبضات إلكترونية يمكن إستقبالها، أو إشعاعات كهرومغناطيسية يمكن إلتقاطها، سواء من كابلات الربط أو من خلال الأثير تمكن الجاني من فرض تدابير أمنية تمنع إكتشافه، ومن ثمة تمنع الحصول على دليل ضده⁴. يستعمل المجرم الإلكتروني عدة أساليب وتقنيات تسمح له بإخفاء كل آثار الجريمة والتستر عنها بسهولة كبيرة⁵، وذلك من خلال التوسل بتقنيات معدة لهذا الغرض مع الأخذ بعين الإعتبار سهولة وسرعة إمكانية محو وتعديل البيانات الإلكترونية التي يمكن القيام بها في أزمان قياسية متناهية القصر تقاس باللحظات والثواني⁶، فمن خلال إدخاله لبعض التعليمات في نظام الحاسوب يتم محو البيانات بالكامل، في لمح البصر كما يمكنه وبمجرد كبسة زر خاطفة على لوحة المفاتيح أن يقوم بإلغاء الأوامر الصادرة للجهاز⁷، على إعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما أن يحس الجاني بأن أمره سينكشف، حتى يبادر بإلغاء هذه الأوامر، الأمر الذي يجعل كشف الجريمة

¹ - عائشة بن قارة مصطفى، المرجع السابق، ص 253.

² - أسامة حسين محي الدين عبد العال، المرجع السابق، ص 708.

³ - 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، 2012/2013، ص 190.

⁴ - محمد حماد مرهج الهيتي، الجريمة المعلوماتية نماذج من تطبيقاتها - دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني -، دار الكتب القانونية - دار شتات للنشر والبرمجيات مصر - الإمارات، 2017، ص 103.

⁵ - براهيمي جمال، المرجع السابق، ص 198.

⁶ - الطيبي البركة، المرجع السابق، ص - ص 273-274.

⁷ - عمير عبد القادر، المرجع السابق، ص 119.

وتحديد مرتكبها أمرا في غاية الصعوبة¹، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده²، فضلا عن سهولة تنصله من مسؤولية هذا العمل بإرجاعه حسبما تشهد بذلك وقائع عديدة، على خطأ في نظام الحاسب أو الشبكة أو في الأجهزة³، وإلى جانب هذا الأسلوب يستعمل الجناة أسلوب التغليف والتضليل الذي يتم إما عن طريق طريق التلاعب بقواعد البيانات والبرامج أو إدخال بيانات مختلفة مزيفة أو محرفة في نظام معلومات الحاسب، أو تغيير مسار البيانات الصحيحة المدخلة دون أن يحس المجني عليه بذلك⁴، ويجتهد المهندسون في مجال تقنية المعلومات في ابتكار برامج معينة لهذا الغرض، وتكمن آلية عملها في أنه بمجرد محاولة شخص غير مصرح له ولوج النظام أو استخدام جهاز الحاسوب المزود بهذا البرنامج، فإن هذا الأخير يصدر أمرا للجهاز بحيث يتم إتلاف البيانات المخزنة به ومحوها بصورة تلقائية⁵.

من الوقائع العملية التي تؤيد ذلك ما قامت به عصابة إيطالية محترفة إختراق أنظمة الحاسب الآلي، وذلك من خلال تصميمها جهاز يحو تلقائيا جميع آثار أي خطوات وتعاملات سابقة استخدمته في إختراق نظم لحاسبات آلية خاصة بشركات معينة، وفي جميع أنحاء العالم⁶، وأيضا ما حصل في ألمانيا أثناء محاكمة بعض المتورطين في قضايا الفساد طلبت السلطات الألمانية المساعدة من السلطات السويسرية في ضبط البيانات التي توجد في النظام المعلوماتي لإحدى الشركات التي تعامل معها المتهم والتي يوجد مقرها بسويسرا، إلا أنه أثناء سير الإجراءات تمكن أحد الجناة من محو البيانات التي كان من الممكن أن تستخدم كدليل، إلا أن هذا الفعل لم يعق سلطات التحقيق من الاستعانة بفنيين في مجال تقنية المعلومات الذين تمكنوا من إسترجاع هذه البيانات بعد حصولهم عليها مسجلة على أحد الأقراص الصلبة التي تم ضبطها⁷.

المطلب الثاني: إعاقة الوصول إلى الدليل الإلكتروني

لا تقف صعوبة إثبات الجرائم الإلكترونية عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها، وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة⁸، بالإضافة على ذلك تمتد إلى الجناة أنفسهم لأن مرتكبي هذا

¹ - بلجراف سامية، المرجع السابق، ص 684.

² - علي عدنان فيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، دار الكتب والوثائق القومية الإسكندرية، 2012، ص 80.

³ - صغير يوسف، المرجع السابق، ص 125.

⁴ - براهيم جمال، المرجع السابق، ص 198.

⁵ - بلجراف سامية، المرجع السابق، ص 684.

⁶ - محمد حماد مرهج الميقي، جرائم الحاسوب ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع عمان-الأردن، الطبعة الأولى 2006، ص 213.

⁷ - عمير عبد القادر، المرجع السابق، ص 199.

⁸ - خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي الاسكندرية، الطبعة الأولى 2009، ص 75.

النوع من الجرائم قد يستخدمون الوسائل الإلكترونية المختلفة لإعاقة الوصول إليهم¹، فالجرم المعلوماتي غالبا ما يضرب سباحا أمنيا على أفعاله غير المشروعة قبل إرتكابه لها، فيزيد بذلك من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقنية التي تدينه².

ومن التدابير الأمنية التي من الممكن أن يستخدمها الجناة لإعاقة الوصول إليهم وبالتالي نزع كل صلة بينهم وبين فعلهم الإجرامي، إخفاء هوية المستخدم³ باستخدام مختلف أدوات الإتصال أمرا متاحا، ومن بين الأدوات التي تستخدم لهذا الغرض برنامج (بسيفون pasiphon) وشبكة (تور Tor) والهدف من هذا الإجراء هو عرقلة تتبع عنوان بروتوكول الأنترنت (IP) لهذا المستخدم⁴، ويزداد الأمر صعوبة حينما تكون المعلومات المحملة في عناوين (IP) غير حقيقية أو زائفة وهذا ممكن حين استخدام الحزم المعلوماتية (Packet) عنوان IP زائف، بحيث يظهر أن المعلومات جاءت من نظام معالجة محدد بينما في الحقيقة جاءت من كومبيوتر آخر ومثال ذلك عندما يقوم برنامج خبيث بإدخال معلومات كاذبة أو غير حقيقية عن عنوان (IP) في حزم الإرسال وقبل الولوج في الشبكة المعلوماتية⁵ المعلوماتية⁵ أو نتيجة استخدام الجاني حاسبا آخر غير حاسبه الشخصي، كاستخدام الحواسيب الموجودة بالأمكان العامة، أو اللجوء إلى مقاهي الأنترنت، على اعتبار أن جل هذه المقاهي لا تقوم بتسجيل أسماء مرتاديها أو التحقق من هوياتهم⁶، أو نتيجة تردد عدد كبير من الأشخاص على المكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط بين زمن إرتكابها وبين حدوث النتيجة الإجرامية (كما هو الحال بالنسبة لمقاهي الأنترنت) مما يفسح المجال لحدوث تغيرات أو عبث في الآثار المادية للجريمة أو زوال بعضها، وهو ما يلقي ظلالا من الغموض على الدليل⁷، وهو ما أستغله مرتكبوا الجرائم المعلوماتية لطمس هوياتهم، وارتكاب جرائمهم دون إمكانية التعرف عليهم بسهولة، وهو ما جعل إخفاء الهوية من أهم العوائق التي تواجه العاملين في مجال البحث والتحري عن هذه الجرائم، بحيث يصعب

¹ - بلجراف سامية، المرجع السابق، ص 684.

² - سعيداني نعيم، المرجع السابق، ص 190.

³ - وقد أشار في المؤتمر الدولي للجرائم الحاسوب المنعقد في أوسلو في الفترة ما بين 29-31/05/2000 موضوع عدم إمكانية البنية التحتية للأنترنت من التوصل إلى تحديد شخصية مرتكب الجريمة أو المصدر الحقيقي لها، وإن كانت توفر إمكانية التعرف على عنوان ورقم الحاسوب فقط المرتبط بالأنترنت والمستعمل كوسيلة لارتكاب الجريمة عن طريق عنوان IP الذي يشير إلى رقم يعين الحاسوب الموصول على الأنترنت. لكن في مقابل ذلك فإن هذا الرقم ليس موحدا على المستوى العالمي، بالإضافة إلى أن مصداقية الهوية عبر الأنترنت (IP) تنقلص كثيرا في بعض الدول إذا علمنا أن كل خط هوية على الأنترنت يصادفه عدد من الهويات التي يمكن أن تكون محلا للتغاير بين أعضاء الأنترنت المشتركين في مزود خدمة واحد، ذلك أن أي شخص يملك هوية رقمية محددة حقا حال وجوده على الأنترنت، إلا أنه إذا حدث وإنقطع الإرسال فإن الشخص نفسه إذا عاد من جديد إلى الأنترنت فإن الهوية السابقة لن تكون له وإنما لغيره ومن الممكن جدا أن يتواجد بحوية (IP) أخرى، وللمزيد من التفصيل، ينظر: سعيداني نعيم، المرجع السابق، ص- ص 193-194.

⁴ - عمير عبد القادر، المرجع السابق، ص- ص 122-123.

⁵ - سعيداني نعيم، المرجع السابق، ص 194.

⁶ - بلجراف سامية، المرجع السابق، ص 684.

⁷ - براهيم جمال، مرجع السابق، ص 198.

تحديد مرتكب الجريمة أو موقعه¹، وفي هذا الإطار نجد أن المشرع الفرنسي قد أوجب على جميع مزودي خدمات الإتصال للجمهور أن يحددوا على مواقعهم هوية ناشر مضمون الرسالة وبياناته وذلك بموجب المادة 43 من قانون 1986/09/30 وهذا الإجراء من شأنه أن يقدم الكثير من الشفافية بالنسبة للخدمات الموضوعة تحت تصرف الجمهور ويساعد على سهولة تحديد هوية الجاني، بالإضافة كذلك إلى ضرورة تحديد هوية المشتركين بشبكات المعلومات لتسهيل عمل الضبطية في حال وقوع أي مخالفة بحيث يجب على مؤدي الخدمة أن يكون قادرا على تقديم بيانات شخصية عن زبائنه في إطار التحقيقات عندما يطلب منه ذلك².

فضلا عما تقدم فإن الوصول إلى الدليل الرقمي يعترضه عقبة أخرى تكمن في أن قد يلجأ هؤلاء المجرمون أيضا إلى دس تعليمات خفية بين هذه البيانات أو استخدام الرمز أو التشفير³ وذلك بالعمل على ترميز أو تشفير⁴ المعلومات المخزنة إلكترونيا والمنقولة عبر شبكات الإتصال، بحيث يستحيل على غيره الإطلاع عليها⁵ إلا من قبل من يحمل المفتاح الثاني الذي يمكنه أن يحل به الشفرة، ويصبح بذلك الدليل الرقمي مشفرا أو مرمزا، ويشكل استخدام تقنيات التشفير لهذا الغرض أحد أكبر العقبات التي تعوق الرقابة على البيانات المخزنة أو المنقولة عبر حدود الدولة، والتي تحد من قدرة جهات التحري والتحقيق والملاحقة على قرائتها، الأمر الذي يجعل صون حرمة البيانات الشخصية المخزنة في مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية والإلكترونية أو بتدابير الأمن والدفاع أمرا بالغ الصعوبة⁶.

وهذا ما يجعل أمر ملاحقتهم أو تحديد هويتهم أشبه بالمستحيل سواء عند قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها⁷، بحيث تظل أنشطتهم مجهولة وبمناى عن علم السلطات المعنية بمكافحة الجريمة⁸ الأمر الذي يجعل عملية إستعادة الأدلة أو إعادة تشكيلها عملية معقدة وصعبة تحتاج إلى خبرة وجهد ووقت وأدوات دقيقة قد لا

¹ - عمير عبد القادر، المرجع السابق، ص 123.

² - سعيداني نعيم، المرجع السابق، ص- ص 194-195.

³ - خالد ممدوح ابراهيم، مرجع السابق، ص 75.

⁴ - يقصد بتشفير البيانات استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها البيانات أو المعلومات المراد تمريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات المخزنة في الحاسوب بدونها. مع العلم أن عملية التشفير تتم وفق معادلات رياضية معقدة تسمى الخوارزميات. وهنا أيضا يجد المحقق نفسه أمام خيارين لحل مشكلة التشفير وهما، إما أن يحصل على مفاتيح الشفرات من المتهم مشغل الحاسوب، وإما أن يحاول فك الشفرات بنفسه. إلا أن في الخيار الثاني يجب أن يكون المحقق ملم بعلم تحليل الشفرات أو ما يعرف بعلم استرجاع النص الواضح بعبارة معينة بدون معرفة المفاتيح، ويرتكز هذا العلم على الرياضيات التطبيقية وفروعها المختلفة مثل نظرية الاحتمالية ونظرية الإعداد والإحصاء والجبر، وهو الأمر المفقود لدى المحقق، وللمزيد من التفصيل، ينظر: براهيمي جمال، المرجع السابق، ص 207.

⁵ - سعيداني نعيم، المرجع السابق، ص 190.

⁶ - صغير يوسف، المرجع السابق، ص 127.

⁷ - بلجراف سامية، المرجع السابق، ص 685.

⁸ - نفس المرجع، ص 684.

تكون في الكثير من الأحيان متاحة لسلطات البحث والتحري¹ وعليه نجد أن القاضي يصعب عليه إدانة شخص دون أن يتأكد يقينياً بأن هذا الشخص هو المذنب في ارتكاب 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 فيه².

الخاتمة:

وفي الأخير نستنتج أن من بين الأسباب الأساسية التي تقف وراء صعوبة إكتشاف الجرائم المعلوماتية راجع إلى عدة اعتبارات منها ما هو متعلق بالطبيعة التكوينية للدليل الإلكتروني الذي يتخلف عنها والذي يعتبر إحدى الآثار المهمة في الربط بينها وبين مقتربها، فهو ينشأ في وسط افتراضي تكون البيانات والمعلومات فيه عبارة عن نبضات إلكترونية غير مرئية مما ينتج أثر غير مادي ولا يمكن إدراكه بالحواس على غرار الأدلة التقليدية، ومنها ما هو راجع إلى ما يستخدمه الجناة من الأساليب الأمنية وتدابير الحماية الفنية التي تحول دون كشف أمرهم ومن ثم تعيق مهمة أجهزة الإستدلال والتحقيق في الوصول إلى الدليل الذي يدينهم؛ ومن خلال ذلك توصلنا إلى جملة من النتائج نذكرها فيما يلي:

1. الطبيعة التكوينية للدليل الإلكتروني والوسط الذي ينشأ فيه جعلته دليلاً غير ملموس لا يدرك بالحواس العادية، بل يتطلب لإدراكه الإستعانة بمعدات وأجهزة وأدوات الحاسبات الآلية وإستخدام نظم برمجية حاسوبية فهو يحتاج إلى مجال تقني يتعامل معه؛
 2. يمتاز الدليل الإلكتروني بطبيعة ديناميكية نتيجة إمكانية تخزين البيانات بالخارج بواسطة شبكة الإتصالات البعيدة؛
 3. القدرة العالية للمجرم المعلوماتي على إخفاء ومحو كل آثار الجريمة والتستر عنها في فترة وجيزة؛
 4. إحاطة مرتكبي الجريمة المعلوماتية ببعض الإحتياطات الأمنية مما يحول دون الوصول إلى هوياتهم الحقيقية وإكتشاف أفعالهم غير المشروعة؛
 5. غير كفاية ونجاعة كل النصوص التقليدية لمعالجة سائر الجرائم المرتكبة في مجال الكمبيوتر والإنترنت؛
 6. نقص المهارة الفنية والتقنية المطلوبة للتحقيق في الجرائم المعلوماتية.
- وتجدر بنا الإشارة إلى أنه من خلال هذا البحث توصلنا إلى مجموعة من الإقتراحات نذكرها كما يلي:
1. 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؛

¹ - عمير عبد القادر، مرجع السابق، ص 121.

² - بن فردية محمد، المرجع السابق، ص 216.

2. الإهتمام أكثر بالتأهيل التقني والفني لجهات التحقيق في مجال التعامل مع الأدلة الإلكترونية، وإمدادهم بأفضل وسائل التقنية الحديثة وتقنيات الحاسب الآلي ونظم المعلومات التي تمكنهم من الحصول عليها؛
3. التركيز على نشر الوعي العام بين أفراد المجتمع من مخاطر هذه الجرائم المستحدثة وما تسببه من أضرار، وأهمية التبليغ عن مقترفيها حتى تسهل السيطرة عليها.

قائمة المصادر والمراجع:

أولا: الكتب

1. حنان ربحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية بيروت-لبنان، الطبعة الأولى 2014؛
2. خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، الطبعة الأولى 2009؛
3. خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي الإسكندرية، الطبعة الأولى 2009؛
4. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة الإسكندرية، 2010؛
5. عبد الإله النوايسة، جرائم تكنولوجيا المعلومات شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمان الأردن، الطبعة الأولى 2017؛
6. علي عدنان فيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، دار الكتب والوثائق القومية الإسكندرية، 2012؛
7. عميمر عبدالقادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد تلمسان- الجزائر، 2021؛
8. محمد حماد مرهج الهيتي، الجريمة المعلوماتية نماذج من تطبيقاتها دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونية - دار شتات للنشر والبرمجيات مصر- الإمارات، 2017؛
9. محمد حماد مرهج الهيتي، جرائم الحاسوب ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع، عمان-الأردن، الطبعة الأولى 2006.

ثانيا: الرسائل والمذكرات

1. 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؛
2. 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؛
3. 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، 2012/2013؛
4. 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؛
5. 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، 2004/2005.

رابعاً: 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-، المجلد 11 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 فردية محمد، الدليل الجنائي الرقمي وحجتيه أمام القضاء الجزائي (دراسة مقارنة)، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبدالرحمان ميرة بجاية -الجزائر-، المجلد 09، عدد 01، 2014؛
4. الطيبي البركة، إشكالية الإثبات في الجرائم الإلكترونية، مجلة آفاق علمية، المركز الجامعي بتمنراست -الجزائر-، المجلد 11، العدد 01، 2019؛
5. مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية -أبحاث المؤتمر السنوي الدولي الخامس 9- الكويت-، الجزء الثاني، العدد 3، أكتوبر 2018.