مجلة الحقوق والحريات
المجلد 13، العدد 2
السنة 2025 ، ص531-ص550

أثر خصوصية إجراءات التحقيق في الجرائم المعلوماتية على حجية الدليل الرقمي في الإثبات

The impact of the privacy of investigation procedures in cybercrimes on the validity of digital evidence proof

د بوقصة إيمان [1] د بدايرية يحي [2]

[1] أستاذ محاضر ب بكلية الحقوق جامعة جيجل (الجزائر)
البريد الالكتروني imene.bouguessa@univ-jijel.dz
[2] أستاذ محاضر أ بكلية الحقوق جامعة تبسة (الجزائر)
البريد الالكتروني yahia.bedairia@univ-tebessa.dz

تاريخ الإرسال:	تاريخ القبول:	تاريخ النشر:
2025/04/29	2025/08/27	2025/10/31

الملخص:

تعتبر سرعة التنفيذ والاعتماد على البيانات الرقمية من أهم مميزات الجرائم المعلوماتية المستحدثة، وعليه وتماشيا مع الطابع الخاص لهذا النوع من الجرائم، ولمواكبة المستجدات والتطورات الدولية المقررة لمكافحة الإجرام المعلوماتي حرص المشرع الجزائري على تكييف منظومته القانونية بما يتماشى ومقتضيات خصوصية الجريمة المعلوماتية خاصة تلك المتعلقة بإجراءات البحث والتحري والتحقيق الخاصة بها ومتابعة مرتكبيها، إلا أن التسليم بفكرة إجراء تحقيق خاص يخالف الإجراء التقليدي يقودنا بالضرورة إلى بعض الإشكالات خاصة تلك المتعلقة بضرورة الموازنة بين الخصوصية وفعالية التحقيق الإلكتروني، ومدى حجية الدليل الإلكتروني المتحصل عليه أمام القضاء.

الكلمات المفتاحية: الجريمة المعلوماتية، التحقيق، الإثبات، الدليل الإلكتروني، التفتيش الإلكتروني.

Abstract:

The speed of execution and reliance on digital data are among the most important features of emerging cybercrimes, Accordingly, in keeping with the unique nature of this type of crime and keeping pace with international developments and trends in combating cybercrime,

المؤلف المرسل : د بوقصة إيمان

the Algerian legislature has been keen to adapt its legal system to the specific requirements of cybercrime, particularly those related to search, investigation, and prosecution procedures. However, accepting the idea of conducting a special investigation that departs from traditional procedures inevitably leads to some problems, particularly those related to the need to balance privacy and the effectiveness of electronic investigations, and the extent of the conclusiveness of electronic evidence obtained before the courts.
Keywords: cybercrime, investigation, proof, electronic evidence, electronic inspection.

مقدمة:

تعد الجريمة المعلوماتية أحد التحديات التي تواجه المجتمع الدولي في عصر التكنولوجيا الحديثة، ومع تزايد الاعتماد على الأجهزة الإلكترونية والشبكات الرقمية في مختلف جوانب الحياة، ظهرت أنواع جديدة من الجرائم التي تستهدف المعلومات وتهدد الأمن الرقمي، إذ تشمل هذه الجرائم مجموعة من الأنشطة غير القانونية مثل القرصنة الإلكترونية، سرقة البيانات، التلاعب بالمعلومات، الاحتيال عبر شبكة الأنترنت، والاعتداءات على الخصوصية، وهو ما دفع مختلف التشريعات الدولية إلى مكافحة هذا النوع من الإجرام الذي لا يزال إلى يومنا هذا يطرح العديد من الإشكالات في الواقع العملي خاصة تلك المتعلقة بالتحقيق وأدلة الإثبات، حيث أن التحقيق في الجرائم المعلوماتية يتطلب أدوات وتقنيات خاصة نظرًا للطبيعة الرقمية للجريمة، مما يجعلها تتطلب مهارات وتقنيات متقدمة، كما أن الإجراءات القانونية لتوثيق الجريمة المعلوماتية وتحقيق الأدلة تتطلب معرفة بالأنظمة الإلكترونية المعقدة وأساليب التتبع الرقمية، بما في ذلك تحليل سجلات الأجهزة والشبكات، واستخدام أدوات تحليل البيانات الرقمية، وهو ما يجعل إثبات الجريمة المعلوماتية أمرا معقدا لأنه يعتمد على جمع أدلة رقمية يمكن أن تكون عرضة للتعديل أو التلف، لذلك يعتبر الحفاظ على سلسلة الأدلة الرقمية من العناصر الأساسية في تحقيقات الجريمة المعلوماتية، و يشمل هذا استخدام تقنيات الحفظ السليم للأدلة الرقمية، وتوثيق جميع مراحل التحقيق، وضمان تقديم الأدلة بطريقة مقبولة في المحاكم.

وفي هذا الصدد أدخل المشرع الجزائري مجموعة من التعديلات على كل من قانون العقوبات وقانون الإجراءات الجزائية، كما استحدث القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، إضافة إلى القانون 18-04 المتعلق بالقواعد العامة للبريد والاتصالات الالكترونية[2]، والقانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.[3]

وتكمن أهمية الدراسة من خلال إبراز أهم الخصوصيات المدرجة لمواجهة هذا النوع من الإجرام، من حيث التطرق لأهم عناصر وأساليب التحقيق في الجرائم المعلوماتية وأهم الآليات الإجرائية في مجال التحقيق في هذه الجرائم، ومدى انعكاسها على إثبات هذا النوع من الجرائم أمام القاضي الجزائي من خلال تسليط الضوء على طبيعة وحجية الدليل الإلكتروني المتحصل من عمليات التحقيق ومدى ارتباطه بها، ومن هنا نجد أنفسنا أمام الإشكالية التالية: **فيما تتمثل خصوصية إجراءات التحقيق في الجرائم المعلوماتية؟ ومدى تأثير هذه الخصوصية على حجية الدليل الرقمي المتحصل عليه في الإثبات ؟**

سوف نحاول الإجابة عن هذه الإشكالية من خلال هذه الدراسة معتمدين على المنهج الوصفي والمنهج التحليلي من خلال عرض وتحليل النصوص القانونية ذات الصلة بالموضوع وفقا للعناصر التالية:

المبحث الأول: خصوصية إجراءات التحقيق في الجرائم المعلوماتية

المبحث الثاني: الإثبات في الجرائم المعلوماتية

المبحث الأول: خصوصية إجراءات التحقيق في الجرائم المعلوماتية

تعتبر مرحلة جمع المعلومات والمعطيات من أهم مراحل الدعوى الجزائية التي تسبق المحاكمة فمن خلالها، يتم التعرف على من ارتكب الفعل وهو ما يعرف بالتحقيق، وعليه يمكن تعريف التحقيق بأنه مجموعة الإجراءات التي تستهدف البحث والكشف عن أدلة

[1] _ القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، جريدة رسمية عدد 47، الصادرة في 06 أوت 2009.

[2] _ القانون رقم 04/18 المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، جريدة رسمية عدد27، الصادرة في 13 ماي 2018.

[3] _ القانون رقم 07/18 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد34، الصادرة في 10 جوان 2018.

ارتكاب الجريمة ثم مدى كفايتها لإحالة المتهم للمحاكمة[1]، ويسند التحقيق في الجرائم لقاضي التحقيق حسب نص المادة 68 من قانون الإجراءات الجزائية، وعلى اعتبار أن الجرائم المعلوماتية من الجرائم المميزة استناد لطبيعتها الخاصة، فقد كرس المشرع الجزائري العديد من الإجراءات والآليات الخاصة بالكشف عن ملابسات هذا النوع من الجرائم وكشف مرتكبيها، ومن هذه الآليات ماهو تقليدي، ومنها ما تم استحداثه خصيصا للجرائم الإلكترونية، وهو ما سيتم توضيحه من خلال ما يلي:

المطلب الأول: التحقيق في الجرائم المعلوماتية عن طريق إجراءات التحقيق التقليدي:

تتمثل إجراءات التحقيق التقليدية في المعاينة والتفتيش والخبرة، ورغم أنها من الإجراءات المعتمدة في الجرائم العادية إلا أن المشرع اعتمدها من خلال إسقاطها على المجال الإلكتروني.

1_ المعاينة في الجريمة المعلوماتية:

المعاينة لغة بمعنى النظر، وعاين الشيء رآه بعينه، ودلالتها في اللغة تشير بمعناها الواسع إلى الرؤية والمشاهدة، ودلالتها القانونية في المجال الجنائي تعتمد على حاسة البصر، وتبعا لذلك تعني المعاينة رؤية أماكن ارتكاب الوقائع الجنائية، كما تنصرف إلى فحص جسم المجني عليه والمتهم وإثبات ما يوجد بها من آثار، وعرفها جانب من الفقه بأنها مشاهدة وإثبات الحالة في مكان ارتكاب الجريمة.[2]

وفي محاولة لتجاوز جوهر المعاينة لمجرد الرؤية والمشاهدة، وعدم اعتمادها على حاسة النظر، عرف بعض الفقه المعاينة بأنها "إثبات مباشر ومادي لحالة الأشخاص والأماكن ذات الصلة بالحادث، عن طريق رؤيتها أو فحصها فحصا حسيا مباشرا، وتنقسم المعاينة في مسرح الجريمة الرقمي إلى قسمين الأول، هو معاينة المكونات المادية للأجهزة التي تم بها ارتكاب الواقعة، ومن أمثلة هذه المكونات الحاسب بمكوناته المختلفة والأقراص والكابلات المتصل بها الحاسب وشاشات العرض ... إلخ، وكل ذلك مما يعتبر من المكونات المادية والتي

[1] فلاح عبد القادر، آيت عبد الله نادية، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، 2019، ص1695.

[2] _ أنظر_ محمد علي أحمد الكواري، مسرح الجريمة ودوره في كشف غموض الجريمة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 44.

لها ذات الطابع المادي المحسوس للأدلة المادية وتنطبق عليها القواعد نفسها المتعارف عليها للمعاينة التقليدية للأدلة المادية، والقسم الثاني هو معاينة مسرح الجريمة بعد وقوع الجريمة، وتختلف المكونات المعنية بهذه المعاينة باختلاف نوع الجريمة، ويرى الفقه الجنائي عدة ضوابط يتعين وضعها في الاعتبار عند معاينة مسرح الجريمة المعلوماتية وتخلص هذه الضوابط في الآتي:[1]

_ تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة، وتحديد مواقعها في أسرع فرصة ممكنة وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملف، وذلك لتعطيل الاتصالات لمنع تخريب الأدلة الموجودة أو محوها.

_ استعداد فريق التحقيق الذي يتولى إجراء المعاينة من الناحية الفنية والعملية، ولابد من قصر المعاينة على ذوي الخبرة في المجال المعلوماتي.

_ إعداد خطة عمل للمعاينة وكيفية إجرائها.

_ تأمين جميع الأجهزة الإلكترونية بما في ذلك الشخصية والمحمولة وإبعاد أي شخص لا علاقة له بمهمة التحقيق.

_ تصوير الحاسب الآلي والأجهزة المتصلة به، مع تسجيل وقت ومكان التقاط كل صورة، مع التركيز بصفة خاصة على الأجزاء الخلفية للحاسب الآلي وملحقاته، ومراعاة وقت وتاريخ ومكان التقاط كل صورة.[2]

_ دقة ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، ليتمكن المحقق من المقارنة والتحليل فيما بعد عند عرض الأمر على المحكمة.

_ مراعاة عدم نقل أية مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوة مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة على الوسائل المعلوماتية.

_ التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة أو أوراق مستعملة، والأقراص الممغنطة، وفحصها ورفع البصمات ذات الصلة بالجريمة، كذلك التحفظ على

[1] _أنظر_ خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، 2012، ص 64.

[2] أنظر حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، طبعة01، دار النهضة العربية، القاهرة، 2017، ص 59.

مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، ولابد أن تتم الإجراءات وفقا لمبدأ المشروعية وفي إطار ما تنص عليه القوانين الجزائية.

_ تحريز الأدلة الإلكترونية المتحصلة من مسرح الجريمة من خلال ضبط وتحريز الدعائم الأصلية للبيانات وعدم الاكتفاء بضبط النسخ، مراعاة ظروف الحرارة والرطوبة لتخزينها والالتزام بالقواعد الفنية المتعلقة بنقلها، مع تأمين البرامج المضبوطة قبل تشغيلها فنيا وعمل نسخ احتياطية سليمة وكاملة، وتمييز كل دليل إلكتروني عن غيره بوضع علامة مادية خاصة به.[1]

2_التفتيش الإلكتروني:

يمكن تعريف التفتيش بأنه إجراء من إجراءات التحقيق يقوم به موظف مختص طبقا للإجراءات المقررة قانونا في محل يتمتع بالحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم، هذا بالنسبة للجرائم التقليدية[2]، أما بالنسبة للتفتيش في الجرائم الإلكترونية فيقصد به التنقيب في وعاء السر بقصد ضبط ما يفيد في كشف الحقيقة، فغاية التفتيش هو كشف ما تحتويه نظم الحاسوب من خفايا ونوايا إجرامية[3]، وبعد الانتهاء من التفتيش يتم ضبط الأدلة وهو الخلاصة النهائية للتفتيش يتم ضبط كل الأدلة المتعلقة بالجريمة، من أقراص صلبة، الأشرطة ، بطاقات الائتمان، وقد تبنى المشرع الجزائري في القانون04/09 المتعلق بالقواعد الخاصة بالوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، في المواد 06، 07،08، إجراءات خاصة بضبط البيانات المعلوماتية تحت عنوان حجز المعطيات المعلوماتية[4]، إذ قد يترتب عن التفتيش حجز المنظومة المعلوماتية في حالة اكتشاف

---

[1] أنظر خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، طبعة01، دار الفكر الجامعي، مصر، 2009، ص77.

[2] أنظر صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير، جامعة مولود معمري، تيزي وزو، 2013، ص 76.

[3] أنظر عادل عزام سقف الحيط، جرائم الذم والقدح المرتكبة عبر الوسائط الإلكترونية، الطبعة01، دار الثقافة، الأردن، 2011، ص 233.

[4] انظر المواد:06،07،08، من القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، المصدر السابق.

السلطة التي تباشر إجراء التفتيش عن وجود معطيات مخزنة تفيد في الكشف عن الجريمة مرتكبيها، ففي هذه الحالة من الممكن أن تحجز المنظومة برمتها، كما يمكن أن يحجز جزء منها فقط، ذلك باعتماد مجموعة من الإجراءات حسب ما يفهم من نص المادة 06[1]، وتتمثل في:

_ نسخ المعطيات على دعامة تخزين الكترونية تكون قابلة للحجز سواء المعطيات محل البحث أو المعطيات اللازمة لفهم المعطيات محل البحث.

_ إمكانية استعمال وسائل تقنية لتشكيل أو إعادة تشكيل المعطيات لتكون قابلة للاستغلال لإجراء التحقيق بشرط عدم المساس بمحتوى المعطيات.

وتجدر الإشارة أنه في حالة تعذر إجراء الحجز لأسباب تقنية، يتعين على السلطة التي تباشر إجراء التفتيش أن تستخدم تقنيات مناسبة لمنع نسخ أو الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال المنظومة، والهدف من هذا الإجراء الاحترازي هو الحفاظ على الأدلة في محيطها الالكتروني، لمنع أي محاولة لطمسها أو إخفاء معالمها، مما يساهم في نجاح إجراء التفتيش والحجز باعتباره أثر للتفتيش.[2]

ولقد حرصت القوانين الإجرائية على إحاطة إجراء التفتيش بشروط وضمانات أساسية نظرا لما يمكن أن يحدثه من مساس بحق الإنسان في حريته الشخصية، وهدف ذلك هو تحقيق الموازنة بين مصلحة المجتمع في عقاب المجرم وبين حقوق الأفراد وحرياتهم، ومن الشروط والضمانات التي يجب توافرها منها ما هو موضوعي ومنها ما هو شكلي:

أ_ الشروط الشكلية للتفتيش في البيئة الرقمية :[3]من أبرز هذه الشروط ما يلي:

_ **إجراء التفتيش يكون بحضور أشخاص معينين بالقانون:** إن المشرع الجزائري أوجب ضرورة حصول إجراء التفتيش المتعلق بالمساكن وملحقاتها بحضور المشتبه به عندما يتم تفتيش مسكنه من طرف الضبطية وإن تعذر ذلك يتم هذا الإجراء بحضور شاهدين، إلا أنه وبموجب التعديل الذي ألحقه على ق إ ج 06-22 استثنى تطبيق هذه الشروط عندما يتعلق الأمر بالجرائم المعلوماتية.

---

[1] أنظر المادة 06 من القانون 09-04.

[2] أنظر المادة 07 من القانون 09-04.

[3] أنظر صغير يوسف، مرجع سابق، ص 76.

_ **الميعاد الزمني لإجراء التفتيش في البيئة الرقمية:** حصر المشرع الجزائري تفتيش المساكن في أوقات معينة وحدد ميقات تنفيذ هذا الإجراء من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا وفي نطاق التفتيش في الجرائم المعلوماتية فإن الاستثناء وارد في المادة 47 فقرة 03 من ق.إ.ج [1] والمتعلق بجواز إجراء ضابط الشرطة القضائية للتفتيش في كل ساعة من ساعات الليل والنهار عندما يتعلق التحقيق بنوع معين من الجرائم، وقد شمل هذا الاستثناء الجرائم المعلوماتية.

ب_ الشروط الموضوعية للتفتيش في البيئة الرقمية: يمكن تحديد القواعد الموضوعية لتفتيش البيئة الرقمية والتي تعد الضوابط اللازمة لإجراء التفتيش وهي:[2]

_ **وجود سبب للتفتيش:** إن سبب التفتيش في الجرائم المعلوماتية هو ضرورة وقوع جريمة من الجرائم المعلوماتية التي نص عليها المشرع في نصوص التجريم والعقاب طبقا لمبدأ شرعية الجرائم والعقوبات، كما قو الحاصل في التشريع الذي أدرج فصلا خاصا (الفصل السابع) في قانون العقوبات لجرائم الإعتداء على نظم المعالجة الآلية للمعطيات، إلا أنه وبالرجوع إلى المادة 05 من قانون 04/09 [3] نجد أن المشرع الجزائري قد أجاز إمكانية اللجوء إلى إجراء التفتيش في نظام معلوماتي إما للوقاية من حدوث جرائم أو في حالة توفر معلومات على احتمال وقوع جرائم معينة،

_ **بطلان إجراء التفتيش:** يبطل إجراء التفتيش إذا كان متعلقا بالنظام العام غالبا في الشروط الموضوعية يؤدي إلى بطلان مطلق، ويمكن للقاضي أن يثيره من تلقاء نفسه، أما إذا كان متعلقا بالشروط الشكلية فغالبا البطلان نسبي يجوز لصاحب المصلحة التمسك به أو التنازل عن حقه في التمسك به، ويترتب على البطلان في معظم التشريعات استبعاد

---

[1] المادة 47 من قانون الإجراءات الجزائية الجزائري.

[2] أنظر سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر، باتنة، 2013، ص 154.

[3] المادة 05 من القانون رقم 04/09.

الدليل الناجم عن هذا التفتيش، وجميع الآثار المترتبة على إقرار البطلان في التفتيش في الجرائم العادية تترتب على بطلان التفتيش في الجرائم المعلوماتية .[1]

3_ الخبرة في الجرائم المعلوماتية

تعد الخبرة القضائية وسيلة من التي قد يلجأ إليها القاضي لتحديد المراكز القانونية للأطراف ويمكن تعريفها على أنها عبارة عن تدبير تحقيقي يهدف إلى الحصول على معلومات ضرورية بواسطة أصحاب الخبرة أو الاختصاص، من أجل البت في مسائل فنية أو تقنية ذات طبيعة محددة تكون محل نزاع، ويشترط في الخبير أن يتمتع بمؤهلات علمية وقدرة على التحكم في مجال الإعلام الآلي وهو ما تضمنته الفقرة الأخيرة من المادة 5 من القانون 04-09 المتضمن القواعد الخاصة بالوقاية من جرائم تكنولوجيا الإعلام والاتصال، ويتم اختيار الخبير من جدول الخبراء مع أداء اليمين القانونية، مع التزامه بأداء مهامه بنفسه بالاعتماد على وسائل علمية متطورة في أداء الخبرة، وجدير بالذكر أن المحكمة لا تلجأ إلى إجراء الخبرة إلا عند عدم إدراكها للمسألة المعروضة، أو عندما تكون الأدلة المعروضة في الدعوى غير كافية لتوضيحها، وهي تقتصر من حيث المبدأ على المسائل الفنية أو التقنية دون المسائل القانونية التي تبقى حصرا من اختصاص القاضي، وهكذا نجد أن الخبرة هي تحقيق قضائي اختياري طارئ في مسائل فنية تعتبر من الوقائع في موضوع نزاع معروض على القضاء للبت فيه.[2]

وتعد الخبرة الرقمية أحد أنواع الخبرة المستحدثة، فهي نتاج الثورة العلمية الجديدة في مجال استخدام الحاسب الآلي وشبكة الانترنيت، حيث يباشر الخبير في الوقائع الرقمية تطبيق القواعد العلمية لعلم الحاسب الآلي بهدف استرجاع البيانات التي تعد دليلا على إرتكاب الواقعة الرقمية، فالمحققون في جرائم الحاسب الآلي مثل عالم الآثار الذي يقوم بالتنقيب على الآثار، فمن الممكن أن تكون البيانات موجودة على الحاسب ويسهل الوصول إليها، وعلى الجانب الآخر قد تكون هذه البيانات يصعب الوصول إليها أو قد تكون هذه البيانات مشفرة وكذلك الشيء نفسه بالنسبة لفحص الشبكات فيجري العمل على البحث من مكان البيانات على الشبكة ومن أي جزء من الشبكة تم الدخول للبيانات أو أي فتحة

[1] أنظر هميسي رضا، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، عدد05، جامعة الوادي، الجزائر، جوان 2012، ص 174.

[2] محمد واصل، حسين بن علي الهلالي، الخبرة الفنية أمام القضاء، المكتب الفني، عمان، 2004، ص 22.

دخول استخدمت لإرتكاب الجريمة، ومن خلال هذا العلم يمكن التعرف على هوية الشخص الذي يقوم بالدخول إلى الشبكة.[1]

كما تستوجب طبيعة هذه الجرائم توافر شروط خاصة في الخبير الذي ينتدب لبحث مسائل فنية وعلمية بالنسبة لها وهي:

_ الإلمام بتركيب الحاسب وصناعته وطرازه ونظام تشغيله الرئيسية الفرعية والأجهزة الطرفية الملحقة بها، وكلمات المرور أو السر أو أكواد التشفير.

_ طبيعة البيئة التي يعمل في ظلها الحاسب من حيث التنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية، وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

_ قدرة الخبير على إتقان ما أمر به دون أن يترتب على ذلك تدمير الأدلة المتحصلة من الوسائل الإلكترونية.

_ التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعامتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على الحاسب أو النظام أو الشبكة.

ويتعين كذلك على الخبير في الجرائم المرتكبة عبر الوسائط الإلكترونية التنسيق مع المحقق الجنائي قبل محاكمة الجاني في هذه الجريمة، على أن يشمل اللقاء كافة الخبراء الذين ساهموا مع سلطات الضبط أو التحقيق في تلقي البلاغ أو إجراءات الضبط والتفتيش أو فحص البرامج وجمع الأدلة الجنائية، على أن يتم في هذا الوقت حصر الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل، كما يجب على المحقق الجنائي أن يشرح لهؤلاء الخبراء الجوانب القانونية لطبيعة عملهم مع التأكيد على ربط الأدلة والخبرة العلمية لعناصر وأركان الجريمة المقام عنها الدعوى الجنائية ضد المتهم.

وتجدر الإشارة إلى أنه وإن كان المقرر أن المحكمة تملك سلطة تقديرية بالنسبة لقرير الخبير الذي يرد إليها، إلا أن ذلك لا يمتد إلى المسائل الفنية فلا يجوز لها تفنيدها إلا بأسانيد فنية تخضع للتقدير المطلق لمحكمة الموضوع ومن ثم فلا تستطيع المحكمة

[1] خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات في الجرائم المتعلقة بشبكة المعلومات الدولية، دار الصفوة، مصر، 2004، ص 154.

أن تفندها وترد عليها إلا بأسانيد فنية قد يصعب عليها أن تشق طريقها فيها إلا عن طريق خبرة فنية أخرى.[1]

المطلب الثاني: التحقيق في الجرائم المعلوماتية عن طريق إجراءات التحقيق المستحدثة:

إن الطبيعة الخاصة للجريمة المعلوماتية والمجرم المعلوماتي، جعلت من إجراءات التحقيق التقليدية قاصرة نوعا ما في كشف هذا النوع من الجرائم، وعليه استحدث المشرع الجزائري بموجب قوانين خاصة آليات تحقيق خاصة، مثلما هو موضح ادناه:

1_التسرب الإلكتروني:

نظم المشرع الجزائري هذا الإجراء من خلال المواد 65 مكرر11 إلى غاية 65 مكرر 18 من قانون الإجراءات الجزائية حيث تناول مفهومه وشروطه، وتتمثل عملية التسرب في نطاق الجريمة الإلكترونية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي، عن طريق اختراق

مواقع معينة، أو الاشتراك في محادثات غرف الدردشة و الظهور بمظهر كما لو كان فاعلا مثلهم مستخدما أسماء أو صفات وهمية لإيقاع الجاني.[2]

2_المراقبة الإلكترونية:

وردت المراقبة الإلكترونية كإجراء في قانون 09-04 والذي أقر اللجوء إلى استعمال تقنية مراقبة الإتصالات الالكترونية بشأن الكشف عن الحقيقة في الجرائم الماسة والمتصلة بتكنولوجيات الإعلام والإتصال عن طريق إجراءات وقواعد خاصة نظمها هذا القانون فيها خصوصية تميزها عن إجراءات التدابير التقنية الواردة في الأحكام العامة ق.إ.ج. ولتبيين خصوصية شروط وإجراءات المراقبة الإلكترونية التي تنفرد بها.[3]

---

[1] أنظر صغير يوسف، مرجع سابق، ص 91.

[2] فلاح عبد القادر، آيت عبد الله نادية، المقال السابق، ص 1698.

[3] لتوضيح فإن المراقبة الإلكترونية تخضع لنفس الشروط العامة للتدابير التقنية إلا أن هناك خصوصية تنفرد بها إضافة لتلك الشروط العامة كذلك أن الإذن المتعلق بالمراقبة الإلكترونية المنصب على نوع معين من الاتصالات متمثلة في الاتصالات الإلكترونية، على عكس التدابير التقنية المنصبة على جميع أنواع الاتصالات سواء السلكية أو اللاسلكية أو غيرها.

أ_الشروط الموضوعية لإجراء مراقبة الاتصالات الإلكترونية: يمكن إجمال الضوابط الموضوعية التي أقرها القانون لمراقبة الاتصالات الالكترونية في مجموعة من الضمانات التي انفراد بيه القانون 09-04 تحديدا في المادة الثالثة منه:[1]

_ لتحقيق الغرض من عملية اللجوء إلى مراقبة الإتصالات الالكترونية أقر المشرع الجزائري إجراء اللجوء إلى مراقبة الاتصالات في حالات استثنائية فقط لما لها من اعتداء على حق الإنسان في سرية حياته الخاصة واتصالاته الشخصية لغرض معين وهو الوصول إلى حقيقة الجريمة والكشف عن مرتكبيها خلال مرحليتي جمع الاستدلالات والتحقيق الابتدائي وإذا لم يتم التوصل إلى ذلك عن طريق اللجوء إلى إجراءات التقليدية.

_ مقتضيات التحريات والتحقيقات القضائية: وهو ما أخذ به المشرع الجزائري في نص المادة الثالثة من قانون 09-04 بأن يتم اللجوء إلى هذا الإجراء متى تطلبت مستلزمات التحريات أو التحقيقات القضائية الجارية، والملاحظ أن المشرع الجزائري لم ينص على إمكانية اللجوء إلى المراقبة بعد ارتكاب الجريمة والبحث عن الحقيقة للوصول إلى مرتكبيها فقط بل أقر أيضا اللجوء إلى استعمال هذه التدابير كوسيلة وقائية للحماية من وقوع جرائم معينة، وهو ما نصت عليه المادة 4 في فقرتها الأولى والثانية، [2] وعليه عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية يتم اللجوء إلى المراقبة الالكترونية والملاحظ أن اللجوء إلى المراقبة يكون بعد ارتكاب الجريمة وأثناء مرحلة جمع الاستدلالات أو التحقيق القضائي الغرض منه هو التوصل إلى معرفة مرتكبي الجريمة وذلك في حالة عدم جدوى الإجراءات التقليدية في الوصول للحقيقة، وهو ما نصت عليه المادة4 من القانون 09-04.[3]

---

[1] والتي تنص مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات يمكن لمقتضيات النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية.

[2] والتي تنص على أن "ا- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، ب_ في حالة توفر معلومات عن احتمال اعتداء على المنظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني".

[3] تنص الفقرة 3 على أن "لمقتضيات التحريات أو التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية".

_ في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة: ويتعلق الأمر هنا بالجرائم التي ترتكب خارج الإقليم الجزائري أن تفيد الدولة المعنية بنتائج تتعلق بمعاينة هذه الجرائم الماسة بتكنولوجيات الإعلام والاتصال وكشف مرتكبها بشرط أن يتم ذلك في إطار تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة أي أن يكون ذلك في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل.

ب_ الشروط الشكلية لإجراء مراقبة الاتصالات الإلكترونية: تأخذ مراقبة الاتصالات الإلكترونية نفس خطورة التدابير التقنية الثلاث المنصوص عليها قي ق.إ.ج.ج في المادة 65 مكرر5 والمتعلقة باعتراض المراسلات تسجيل الأصوات السابق التعرض لهم المنصبة على الاتصالات الشخصية لكونها تمس أيضا الحياة الخاصة للأفراد ومن أجل ذلك ينبغي إحاطة إجراء المراقبة بضمانات تكفل استعمالها في نطاق الهدف الذي وجدت من أجله، ومن أهم الضمانات يعهد اتخاذ هذا الإجراء للسلطة المختصة سواء تعلق الأمر بمنح الإذن أو المختصة بطلبه وتنفيذه.

كما أن خصوصية الشكلية تتمثل في مدة الإذن بمراقبة الاتصالات الالكترونية والجهة المختصة بمنحه فبالرجوع إلى القانون 09-04 نجد أن المادة 4 منه في فقرتها الثالثة[1] حددت مدة الإذن الذي يمنحه النائب العام لدى مجلس قضاء الجزائر لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته.

3_اعتراض المراسلات:

يعد هذا الإجراء من بين الأساليب الخاصة للبحث والتحري في الجرائم الخطيرة وذات الطبيعة الخاصة، وبموجب المادة 65 مكرر5 ق.إ.ج.ج يجوز لقاضي التحقيق متى تطلبت مقتضيات التحقيق ذلك أن يرخص بموجب إذن مكتوب للضبطية القضائية باعتراض المراسلات السلكية واللاسلكية، ووضع الترتيبات التقنية اللازمة لالتقاط الأصوات والصور في أي مكان عام أو خاص، ويجوز لقاضي التحقيق أن يسخر لأجل إنجاح العملية كل عون

[1] والتي تنص على أن "عندما يتعلق المر بالحالة المنصوص عليها في الفقرة أ من هذه المادة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه إذن لمدة ستة أشهر (6) قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة في الأغراض الموجهة لها".

مؤهل لدى كل هيئة أو وحدة أو مصلحة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية طبقا لنص المادة 65 مكرر8 ق.إ.ج.ج كما أنه هو المختص بالرقابة على العملية وبتمديد مدة الأربعة أشهر في حالة انقضائها وعند انتهاء العملية يسلم له ضابط الشرطة القضائية الملف الخاص بها ويحرر محضرا يضمنه كل ما قام به والنتائج المتواصل إليها طبقا للمادة 65 مكرر 10 من قانون الإجراءات الجزائية.[1]

4_ الحفظ والإفشاء العاجلان للمعطيات الإلكترونية:

يعتبر هذا الإجراء من الإجراءات الجديدة حيث تضمنت المادة 10 من القانون 09_ 04 الخاص بالوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال عددا من الالتزامات على مزودي خدمة الأنترنت بتقديم المساعدة في التحقيق، مثل حفظ البيانات والمعلومات، وإفشاء أي معلومة مهمة لمساعدة رجال الضبطية القضائية، وفي حال عدم التزامهم تترتب عليهم المسؤولية الجزائية.[2]

المحور الثاني: الطابع الخاص للإثبات في الجرائم المعلوماتية:

يرتبط التحقيق بالإثبات ارتباطا وثيقا، إلا أن الإثبات في الجرائم المعلوماتية أمر معقد وصعب نظرا لاختلاف الدليل الإلكتروني عن الأدلة المادية التقليدية، حيث يعتبر دخيلا نوعا ما على القاضي الذي استأنس بالأدلة المادية، وهذا لا ينفي أن الدليل الإلكتروني وسيلة فعالة في إثبات وضبط الجرائم المعلوماتية.

المطلب الأول: الطبيعة القانونية للدليل الإلكتروني:

تبرز الطبيعة القانونية للإثبات من خلال ضبط مفهومه وإبراز خصائصه ومميزاته:

1_تعريف الدليل الإلكتروني:

يعرف الدليل الإلكتروني على أنه: " كل البيانات التي يمكن اعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من إنجاز شيء ما"[3]، ويعرف الدليل الرقمي أيضا بأنه الدليـل المعلوماتي المخزن على شكل أرقام إثني عشرية، وفق نظام الشيفرة الثنائية، التي تعرف

[1] انظر المواد65 مكرر وما بعدها من قانون الإجراءات الجزائية.

[2] انظر المادة 10 من القانون 09-04، المصدر السابق.

[3] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2010، ص53.

بالديجيتال، ويقسم الدليل الرقمي إلى دليلين هما، الدليل الرقمي الأصلي وهو البنود العينية أو الحسية، كذلك المستمسكات البيانية التي تتعلق بهذه البنود عند الإمساك بها وحجزها، والدليل الرقمي المكرر هو استنساخ رقمي لجميع المستمسكات البيانية التي يحتويها البند العيني الأصلي.[1]

2_ خصائص الدليل الإلكتروني: يتمتع الدليل الرقمي بجملة من الخصائص تميزه عن الأدلة الأخرى أهمها:

_ الدليل الإلكتروني دليل علمي يتشكل من معطيات رقمية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات[2] أي يرتبط ببيئة العالم الافتراضي، وهي بيئة علمية شديدة التعقيد، وتفيد هذه الخاصية في أنه لا يمكن الكشف عن الدليل الرقمي إلا باستخدام الأساليب العلمية، كذلك والطبيعة العلمية المعقدة لهذا الدليل توجب أن يفتش عنه ويحرز وينسخه تقنيون مختصون في الكشف الجنائي الرقمية، فالدليل العلمي ليس كالدليل العادي، فالتقنية الافتراضية لا تنتج سلاح أو سكين يتم به اكتشاف القاتل، وإنما تنتج نبضات رقمية تشكل قيمتها وجوهرها.

- الدليل الرقمي دليل متنوع ومتطور، فعلى الرغم من أن أساس الدليل الرقمي لغة الحوسبة الرقمية غير أنه يشمل كافة أشكال المعطيات التي يمكن تداولها رقميا بكافة أنواعها وهو يتخذ أشكال وهيئات عديدة، كأن يكون بيانات غير مقروءة، كما هو الحال في بيانات مراقبة الشبكات والخوادم، أو أن يكون على شكل مستند معد لمعالجة النصوص، أو بمعلومات أو برامج، كما يتميز الدليل الرقمي بأنه يترك آثار قد يصعب التخلص منها[3]، وقد وضعت مجموعة الثمانية الكبار، والتي تمثلها الهيئة الدولية لدليل الحاسب الآلي عدة ضوابط لتفتيش الدليل الرقمي.[4]

---

[1] أنظر_ عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، طبعة01، دار الثقافة، عمان، 2011، ص 233.

[2] فلاح عبد القادر، آيت عبد المالك نادية، المقال السابق ، ص 1702.

[3] أنظر محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، طبعة01، منشورات الحلبي الحقوقية، بيروت، 2011، ص342.

[4] وضعت مجموعة الثمانية مبادئ هي:

_ يجب تطبيق الإجراءات القضائية والأسس الإجرائية عند التعامل مع الدليل الرقمي.

_ عند مصادرة الدليل الرقمي يجب ألا تكون الإجراءات المتخذة لتحريره سببا في تغيير طبيعة هذا الدليل.

_ صعوبة التخلص من الدليل الإلكتروني، وهي أهم خاصية، حيث يمكن استرجاع الدليل يعد محوه وإصلاحه، وذلك باستخدام برمجيات ذات طبيعة رقمية متطورة.[1]

المطلب الثاني: حجية الدليل الرقمي في الإثبات الجنائي:

يقصد بحجية الدليل الإلكتروني قوته الاستدلالية في إبراز الحقيقة وصدق نسب الفعل الإجرامي إلى شخص معين أو إنكاره[2]، وقد استقر الفقه والقانون الوضعي على أن للقاضي سلطة واسعة في تقدير الأدلة واستنباط القرائن وما تحمله الوقائع من دلالات، شريطة أن يكون الدليل ثابت بيقين، مرتبطا بالوقائع الرئيسية ومنسجما مع التسلسل المنطقي للأحداث، من الطبيعي أن ينسحب هذا الرأي على الأدلة الجنائية الرقمية وباعتبارها أحد أقسام الأدلة المادية العلمية، بل أكثر منها حجية في الإثبات لأنها محكمة بقواعد علمية وحسابية قاطعة لا تقبل التأويل كما أنها في ذات الوقت معالجة بوسائل التقنية المعلوماتية التي أصبحت تستغل في الجرائم المستحدثة،[3] حيث ينبغي على المحقق السيطرة والتحكم بالأدلة ولابد من تمييز الأدلة وتوثيق كل ما يعثر عليه في مسرح الجريمة والاستمرار في التوثيق خلال فترة التحقيق كاملة[4]، وترتبط قيمة الدليل الإلكتروني وقوة حجيته بعنصرين أساسيين هما مشروعيته ومصداقيته:

1_ مشروعية الدليل الإلكتروني: يخضع قبول أو رفض الدليل الرقمي تبعا للمبادئ التي تقوم عليها أنظمة الإثبات السائدة، وفي هذا الصدد نجد المشرع الجزائري وكغيره من

_ عندما تقتضي الضرورة تعامل شخص ما مع الدليل الرقمي الأصلي يجب أن يكون هذا الشخص مراقبا في هذا المجال.

_ يجب أن تكون جميع الأنشطة المتعلقة بتحريز الوثائق الرقمية أو الدخول إليها تخزينها، نقلها، موثقا توثيقا كاملا، مع المحافظة عليها وتوفيرها للمراجعة.

_ متى وجد الدليل الرقمي في حوزة شخص ما، فعليه تحمل كامل المسؤولية حول أي نشاطات قد تتخذ هذا الدليل طوال فترة حيازته له.

[1] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1701.

[2] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1702.

[3] _أنظر_ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، طبعة 01، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص251.

[4] أنظر_ أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، دار النهضة العربية، القاهرة، 2015، ص 260.

المشرعين أفرد نصوص تحفز القاضي على قبول أي دليل بما في ذلك الدليل التقني، كما أن حرية الإثبات في المسائل الجزائية من المبادئ المستقرة في نظرية الإثبات، مثلما هو مقرر في نص المادة 212 من قانون الإجراءات الجزائية، إذ يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكما تبعا لاقتناعه الشخصي، ومن بين مبررات الأخذ بمبدأ حرية الإثبات ظهور الأدلة العلمية الحديثة التي كشفت عنها التطورات العلمية الحديثة في إتيان الجريمة ونسبها غلى المتهم، كالبصمة الوراثية، ويتجلى الدور الإيجابي للقاضي الجزائري في الجرائم الإلكترونية في عنصرين هامين هما:

_ توفر الدليل من خلال البحث عن الدليل باستعمال السلطات المخولة له قانونا، حيث يستطيع أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إليه من خلال الإفصاح عن كلمات المرور والشفرات الخاصة بتشغيل البرامج.

_ سلطة الأمر بتفتيش نظم الحاسوب بجميع مكوناته بحثا عن الدليل الرقمي.

2_ مصداقية الدليل الرقمي: للخبرة التقنية أهمية في استخلاص مصداقية الدليل الرقمي من عدمها[1] وأخيرا يبقى للقاضي الجزائي السلطة التقديرية للأخذ بالأدلة الرقمية من عدمها، والتي تستمد من ضرورة الاقتناع بالأدلة الإلكترونية الصحيحة وضرورة مناقشته لها في الجلسة.

خاتمة:

من خلال ما تم عرضه يمكن القول أنه، ورغم مواكبة التطورات فيما يخص مكافحة الجريمة المعلوماتية من خلال استحداث قانون إجرائي متضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الاتصال وهو القانون 09-04، كما أورد المشرع في قانون الإجراءات الجزائية استثناءات وإجراءات خاصة فيما يخص البحث والتحري والتحقيق في الجرائم المعلوماتية، إلا أن الواقع العملي يطرح العديد من الإشكالات التي تواجه سلطات البحث والتحقيق منها تنوع الجرائم المعلوماتية وصعوبة حصرها والتعامل معها، كذلك يمكن أن يطرح اختلاف النظام الإجرائي بين الدول خاصة تلك المتعلقة بإجراءات التحقيق إشكالا يتعلق بمدى حجيته الدليل الإلكتروني على الوقائع المراد إثباتها من حيث مشروعية ومصداقية وسلامة الدليل المتحصل عليه.

[1] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1704.

التوصيات:

_ ضرورة إعادة النظر في المنظومة القانونية المقررة لمكافحة الجريمة الإلكترونية، من خلال إلتزام المشرع بإصدار قانون مستقل بمكافحة الجرائم المعلوماتية يواكب التطورات التكنولوجية.

_ ضرورة اعتماد المشرع الجزائري على نصوص خاصة بالأدلة الإلكترونية والنص عليها صراحة كأداة للإثبات الجنائي، مع فرض معايير وضوابط تساعد أجهزة العدالة الجنائية على اعتماد هذه الأدلة.

_ لا بد من تدعيم الأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية في كل مرة بتقنيات ووسائل وأساليب جديدة تضمن المواجهة الفعالة.

_ ضرورة عقد دورات تدريبية للجهات المختصة بالتحقيق تبين طرق استخدام تقنيات الحفظ السليم للأدلة الرقمية، وتوثيق جميع مراحل التحقيق لضمان تقديم الأدلة بطريقة مقبولة في المحاكم.

_ لا بد من الاستفادة من تجارب الدول المتطورة في مواجهة الجرائم المعلوماتية.

_ ضرورة التعاون الدولي لمكافحة الجرائم المعلوماتية، من خلال تفعيل التنسيق الأمني فيما يخص متابعة مرتكبي هذا النوع من الجرائم وإلقاء القبض عليهم.

قائمة المصادر والمراجع:

أ_ المصادر:

_ الأمر 66_156 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.

_ القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، جريدة رسمية عدد 47، الصادرة في 06 أوت 2009.

_ القانون رقم 04/18 المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، جريدة رسمية عدد27، الصادرة في 13 ماي 2018.

_ القانون رقم 07/18، المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد34، الصادرة في 10 جوان 2018.

ب_ الكتب:

_ أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، دار النهضة العربية، القاهرة، 2015.

_ محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، طبعة01، منشورات الحلبي الحقوقية، بيروت، 2011.

_ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، طبعة 01، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

_ محمد واصل، حسين بن علي الهلالي، الخبرة الفنية أمام القضاء، المكتب الفني، عمان، 2004.

_ خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات في الجرائم المتعلقة بشبكة المعلومات الدولية، دار الصفوة، مصر، 2004.

_عادل عزام سقف الحيط، جرائم الذم والقدح المرتكبة عبر الوسائط الإلكترونية، الطبعة01، دار الثقافة، الأردن، 2011.

_ محمد علي أحمد الكواري، مسرح الجريمة ودوره في كشف غموض الجريمة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.

_ خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، 2012.

_ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، طبعة01، دار الفكر الجامعي، مصر، 2009.

_ حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، طبعة01، دار النهضة العربية، القاهرة، 2017.

_ عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2010.

ج_ المقالات:

_هميسي رضا، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، عدد05، جامعة الوادي، الجزائر، جوان 2012.

-فلاح عبد القادر، آيت عبد الله نادية، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، 2019.

د_ مذكرات الماجستير:

_صغير يوسف، الجريمة المرتكبة عبر الأنترنت، (مذكرة ماجستير)، جامعة مولود معمري، تيزي وزو، 2013.

_ سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، (مذكرة ماجستير)، جامعة الحاج لخضر، باتنة، 2013.