جامعة سعيدة، الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

عنوان المذكرة

حجية الدليل الرقمي في إثبات الجريمة الإلكترونية في التشريع الجزائري

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص: **إدارة الكترونية**

من إعداد الطالبان:

بومعراف نصر الدين

بغـداد رمـاس

تحت إشراف الأستاذة:

د. ناديـة حـزاب

أعضاء لجنة المناقشة

الدكتورة عيدة بلعابد	أستاذة محاضرة –ب–	جامعة سعيدة	رئيسا
الدكتورة نادية حزاب	أستاذة محاضرة –ب–	جامعة سعيدة	مشرفا ومقررا
الدكتور كمال فليح	أستاذ محاضر –أ–	جامعة سعيدة	عضوا

السنة الجامعية: 2024–2025

جامعة سعيدة، الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

عنوان المذكرة

حجية الدليل الرقمي في إثبات الجريمة الإلكترونية في التشريع الجزائري

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص: **إدارة الكترونية**

من إعداد الطالبان:

بومعراف نصر الدين

بغـداد رمـاس

تحت إشراف الأستاذة:

د. حـزاب نادية

أعضاء لجنة المناقشة

الدكتورة عيدة بلعابد	أستاذة محاضرة –ب–	جامعة سعيدة	رئيسا
الدكتورة نادية حزاب	أستاذة محاضرة –ب–	جامعة سعيدة	مشرفا ومقررا
الدكتور كمال فليح	أستاذ محاضر –أ–	جامعة سعيدة	عضوا

السنة الجامعية: 2024–2025

بسم الله الرحمن الرحيم

{ يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ}

صدق الله العظيم

بسم الله الرحمن الرحيم

الحمد لله ان هدانا لهذا وما كنا لنهتدي لولا أن هدانا الله

إلى الغالية "**أمي**"، أعز من رأت عيني،

من كانت في هذه الدنيا السَّند، التي تعلمت منها الصَّبر، الجد والكد،

اللهم اجعل قبرها روضة من رياض الجنة وأرزقها الفردوس الأعلى.

إلى العزيز "**أبي**" صاحب القلب الكبير والحلم الوفير،

اللهم مده بالصحة، أطل عمره وارزقه من فضلك.

إلى **أخواتي** الكريمات **وإخواني** الأعزاء، حاملي ذكرياتي الغالية.

إلى **عائلتي، زوجتي وأبنائي**، ثمرة دعائي ثم اجتهادي،

الذين أعطوني الدعم المعنوي لمواصلة الدرب،

أسأل الله الكريم أن يجعلني نبراسا لهم، ويجعلهم ذُخراً لي.

إلى زميلي، صديقي وأخي **بغداد رماس** الذي لم يدخر جهدا في هذا البحث،

كان خير سند في رحلتي الجامعية، فنعم الصاحب والصديق.

الى معلمتي الفاضلة **مليكة غرور**، أول من غرست فيَ حب العلم والعمل،

الى **كل معلم وأستاذ** استسقيت من علمه وأدبه،

الى **أساتذة جامعة سعيدة وإطاراتها** لرحابة صدورهم، ودعمهم المتواصل لنا،

الى **جميع** من كان سببا في إنارة دربي،

أهدي هذا العمل المتواضع، وأسأل الله الكريم أن يجعله صدقة جارية.

نصر الدين بومعراف

الإهداء

بسم الله الرحمن الرحيم

الحمد لله رب العالمين، والصلاة والسلام على سيدنا محمدٍ الصادق الوعد الأمين.

اللهم لا علم لنا إلا ما علَّمتنا إنك أنت العليم الحكيم،

اللهم علِّمنا ما ينفعنا وانفعنا بما علَّمتنا وزِدنا علماً

إلى الشمس التي نستظل بظلها، وتمنحنا الدفء بكل هدوء.

إلى القمر الذي ينير لنا عتمة الليل، ويخالجنا في كل شعور...

إليهما معا الإجلال والبر والحب والتقدير (**والدي الكريمين**)

إلى رفيقة العمر، ومن كان خير معين. إلى روح البراءة والأمل (**زوجتي، وابني إسلام**)

إلى الفخر والافتخار، رفقاء الدرب وسند العمر (**إخوتي وأخواتي**)

إلى رفيق الدرب، شريك السهر والاجتهاد، وزميل المحاضرات والامتحانات، من عرفت معه معنى التعاون والإخلاص (**صديقي نصر الدين بومعراف**)

إلى كل عزيز وصديق، من زرعوا فينا حب الخير والعطاء أهديكم جميعا رسالتي هذه ...

بغداد رماس

شكر وتقدير

الحمد لله رب العالمين والصلاة والسلام على أشرف المرسلين وعلى آله وصحبه أجمعين، أما بعد:

قال تعالى "وَقَالَ رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَىٰ وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ(19) ". سورة النمل.

الحمد لله والشكر لله كما ينبغي لجلال وجهه ولعظيم سلطانه، الحمد لله الذي بعزته وجلاله تتم الصالحات، أن وفقنا لإتمام هذا العمل المتواضع ونسأل الله أن يتقبله ويجعله صدقة جارية.

بكل فخر وامتنان، يسرنا ويسعدنا أن نتوجه بخالص كلمات الشكر وعظيم التقدير إلى أستاذتنا الفاضلة، الدكتورة نادية حزاب، الأستاذة بكلية الحقوق والعلوم السياسية – جامعة سعيدة، على إشرافها الكريم لهذا البحث، فقد كانت لتوجيهاتها العلمية السديدة ومتابعتها الدقيقة والمستمرة، ونصائحها القيمة، ودعمها المتواصل، الأثر البالغ في إخراج هذا العمل إلى النور، على النحو الذي نرجو أن يكون في مستوى تطلعاتها وتقديرها.

لقد كنتم، يا أستاذتنا، مثالا يحتذى به في العلم، والعطاء، والصبر، وكنتم دوما النور الذي أنار دربنا في لحظات التحدي والتردد.

إن بصمتكم العلمية والفكرية ستظل محفورة في صفحات هذا العمل، كما ستبقى كلماتكم المشجعة ودعمكم المتواصل مصدر إلهام لنا في مسيرتنا الأكاديمية.

فلكم منا أصدق عبارات الشكر والعرفان، على وقتكم الثمين، وجهودكم النبيلة، وإيمانكم المستمر بقدرتنا على الإنجاز.

كما نتوجه بجزيل الشكر والامتنان إلى السادة أعضاء لجنة المناقشة الأفاضل، الذين تفضلوا بقبول مناقشة هذا البحث، وبتخصيص جزء من وقتهم الثمين لتقييمه وإثرائه بملاحظاتهم العلمية الهادفة، التي نعدها مكسبا حقيقيا في مسيرتنا الأكاديمية.

وختاما، لا يسعنا إلا أن نرفع أكف الدعاء لكم أساتذتنا الكرام ولكل من ساهم في دعمنا وتوجيهنا خلال هذا المشوار، راجين من الله عز وجل أن يجعل هذا العمل خطوة متواضعة في طريق العلم وخدمة وطننا. مع خالص التقدير والاحترام من الطالبان **نصرالدين بومعراف وبغداد رماس.**

قائمة المختصرات

1. ج: الجزء
2. د.ج: دينار جزائري
3. ف: الفقرة
4. ق.إ.ج.ج: قانون الإجراءات الجزائية الجزائري
5. ق.ع.ج: قانون العقوبات الجزائري
6. ط: الطبعة
7. ص: الصفحة
8. P : Page

مقدمة

تعد الجريمة ظاهرة لصيقة بالمجتمع الإنساني منذ القدم، إذ إن تضارب المصالح وتعدد الأهداف بين الأفراد داخل الجماعة يؤدي بطبيعته إلى نشوء نزاعات اجتماعية قد تؤول إلى ارتكاب أفعال مجرمة قانونا. وقد عرفت الجريمة تطورا متوازيا مع تطور أنماط الحياة، وتنوعت أشكالها باختلاف المراحل التاريخية والاجتماعية التي مرت بها المجتمعات، وهو ما جعلها تمتد إلى مختلف مناحي الحياة الإنسانية، متأثرة بالزمان والمكان، وبالمتغيرات السوسيو–اقتصادية والثقافية التي تحيط بالفرد.

ومع تسارع وتيرة التقدم التكنولوجي والتقني، وبروز الفضاء الرقمي ووسائل الاتصال الحديثة كالفاكس، والإنترنت، وتقنيات الاتصال عبر الأقمار الصناعية، وجد المجرمون في هذه الوسائل بيئة خصبة لتنفيذ مخططاتهم الإجرامية. وقد أفرز هذا التطور صنفا جديدا من الجرائم، بات يعرف بالجرائم الإلكترونية، وهي جرائم مستحدثة لا تنحصر في نطاق إقليمي معين، بل تتجاوز الحدود الجغرافية للدول، مما يمنحها طابعا عابرا للحدود. وتعد هذه الجرائم نمطا من أنماط الذكاء الإجرامي الذي يصعب تصنيفه ضمن الأوصاف الجنائية التقليدية المعروفة في التشريعات الوطنية والدولية [1].

ونظرا لخصوصية الجريمة المعلوماتية من حيث البيئة التقنية التي ترتكب فيها، بات من الضروري اعتماد آليات قانونية وإجرائية جديدة تتجاوز الأساليب التقليدية المعتمدة في مكافحة الجرائم الكلاسيكية. فالمسرح الإجرامي في هذا النوع من الجرائم قد انتقل من الفضاء الواقعي المادي إلى الفضاء الافتراضي غير الملموس، وهو ما أدى إلى تحول في طبيعة وسائل الإثبات، حيث لم تعد الأدلة المادية التقليدية كافية، بل أصبح الاعتماد متزايدا على الأدلة الرقمية والإلكترونية التي تتناسب مع طبيعة الوسط الذي ارتكبت فيه الجريمة [2]. غير أن استخدام الدليل الرقمي في مجال إثبات الجرائم الالكترونية يطرح عدة إشكالات قانونية وعملية، تتعلق بكيفية جمعه وتحليله، ومدى مشروعيته، وكذا حجيته أمام القضاء، خاصة في ظل غياب إطار قانوني واضح أو تقنيات إجرائية موحدة تضمن توازنا بين حماية الحقوق والحريات من جهة، وفعالية العدالة الجنائية من جهة أخرى.

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر،2009، ص159.

[2] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجيستير، جامعة الحاج لخضر–باتنة–، كلية الحقوق والعلوم السياسية، 2013، ص 1.

إن دراسة موضوع حجية الدليل الرقمي في إثبات الجريمة الالكترونية في التشريع الجزائري له أهمية بالغة، حيث تظهر هذه الأهمية من خلال أنه يعالج نوعا جديدا من الأدلة الجنائية خاصة من الناحية القانونية، كما تبرز قيمة هذا الموضوع من خلال أن لديه صلة وثيقة بطائفة جديدة من الجرائم والتي ظهرت مع التطور التكنولوجي والمتمثلة في الجرائم الإلكترونية، حيث ظهرت بهدف التصدي لهذا النوع من الجرائم، وعليه وجد القضاء نفسه في مواجهة هذا الدليل المستحدث، والذي فرض تحديات جديدة للقضاة.

وتكمن أيضا أهمية الدراسة في أن هذا الموضوع تناول أحد الوسائل العلمية الأكثر انتشارا في قضايا إثبات الجرائم الالكترونية، وهي تلك الوسائل التي جاءت لتتلاءم والفكر الإجرامي الذي كان من الضروري على المشرع الجزائري أن يستحدث من التشريعات ما يتلاءم معه.

تهدف هذه الدراسة إلى تسليط الضوء على أهمية الدليل الرقمي بصفة خاصة من حيث الإثبات والحجية أمام القضاء في الجريمة الالكترونية، حيث إن تقدير الدليل الرقمي يتوقف على مسألتين تتمثل الأولى في أن يكون هذا الدليل معترف به، وأن القانون يجيز للقاضي الاستناد إليه لتكوين عقيدته، أما الثانية فتتمثل في وجوب توفره على مجموعة من الشروط التي تضفي عليه المشروعية.

كما أن الهدف من هذا البحث هو معرفة مدى مواكبة القانون الجزائري للتطور التكنولوجي وكيفية تعامله مع الدليل الرقمي، ولفت الانتباه إلى أهمية هذا الدليل للإثبات في الجرائم الإلكترونية، كما تجدر الإشارة إلى الفراغ التشريعي في مختلف القوانين فيما يتعلق بالدليل الرقمي، بما فيها التشريع الجزائري والذي لم ينص على الدليل الرقمي صراحة.

يعود سبب اختيار موضوع حجية الدليل الرقمي في إثبات الجريمة الالكترونية في التشريع الجزائري الى الاهتمام الشخصي بالتكنولوجيا والقانون والرغبة في تعميق معرفة هذا المجال لتعزيز المسيرة العملية والأكاديمية، وكذا إلى الرغبة في إثراء الدراسات الجامعية النظرية، وعلة ذلك نقص الدراسات والأبحاث التي تتعلق بتحديد مفهوم الدليل الرقمي وحجيته أمام القضاء، حيث أن هذا النوع من الأدلة

لم يتم دراستها بشكل علمي وقانوني معمق في الجزائر، إنما تم التطرق إليها في مؤلفات عامة دون أن يتم الإحاطة بها، بمعنى آخر تم التطرق إليها بشكل مقتضب.

في عصرنا الحالي ومع التطور التقني لأساليب ارتكاب الجريمة، أصبحت العديد من النظم القانونية في الإثبات تأخذ بالدليل الرقمي كأداة إثبات لها قيمة قانونية وحجية في الإثبات، وتساويه في الإثبات بالدليل التقليدي، والدليل الرقمي يتميز بطبيعة خاصة فهذا النوع من الأدلة يطرح معه إشكالات عدة نظرا لقابليته للتغيير في أية لحظة، وخلال ثواني يمكن محوها وإلغاؤها أو التلاعب في معطياتها، كما أنها أدلة لا غنى عنها في الجرائم الالكترونية، إلا أن الاستدلال بها مقيد من خلال احترام الخصوصية المعلوماتية كأصل عام.

وعليه فالإشكال الذي سيتم معالجته من خلال هذه الدراسة هو: الى اي حد يمكن الاعتراف بالدليل الرقمي كوسيلة اثبات في الجرائم الالكترونية؟

وتندرج تحت هذا التساؤل أسئلة فرعية وهي:

1. ما مفهوم الجريمة الإلكترونية والدليل الرقمي، وما هي خصائصهما؟

2. ما هي إجراءات جمع الدليل الرقمي وصعوبات استخلاصه؟

3. ما حدود سلطة القاضي الجنائي في قبول الدليل الرقمي والاقتناع به؟

تم الاستعانة في هذه الدراسة بالمنهج الوصفي، وذلك من خلال تعريف الدليل الرقمي وإبراز مختلف خصائصه وكذلك إجراءات الحصول عليه، بالإضافة إلى المنهج التحليلي، وذلك من خلال مناقشة ما يحتاجه الدليل الرقمي لجمع الحقائق والبيانات والاجراءات الخاصة بإحرازه، وكذا محاولة تحليل بعض النصوص القانونية وموقف القضاء من الدليل الرقمي وطرحها بشكل مفصل لأهميتها.

الإطار الزماني لدراسة الموضوع وقتنا الحالي، أما الإطار المكاني فهو الجزائر، وذلك من خلال التشريع الجزائري.

لمعالجة هذا الموضوع والإجابة عن الإشكالية والتساؤلات المطروحة تم تقسيم البحث إلى فصلين، الأول بعنوان الاطار المفاهيمي للجريمة الإلكترونية والدليل الرقمي، وقد تم تناول في المبحث الأول مفهوم الجريمة الالكترونية، وفي المبحث الثاني تم التطرق إلى مفهوم الدليل الرقمي، وأما الفصل الثاني

فقد كان بعنوان الطبيعة القانونية للدليل الرقمي في التشريع الجزائري، بحيث تم تناول في المبحث الأول إجراءات جمع الدليل الرقمي، وفي المبحث الثاني فعنون بقبول الدليل الرقمي أمام القضاء الجزائي وضوابط اقتناع القاضي به، وختاما خلصت إلى توضيح النتائج والتوصيات التي تم التوصل إليها.

مما لا شك فيه هناك بعض الصعوبات ويرجع ذلك إلى عدة أسباب:

1. حداثة الموضوع وتطوره السريع: التطور التكنولوجي السريع يجعل النصوص القانونية عاجزة عن مواكبة كل المستجدات، مما يصعب على الباحثين العثور على مراجع محدثة؛

2. ندرة الدراسات الأكاديمية المتخصصة: معظم البحوث القانونية في الجزائر تركز على مواضيع تقليدية، بينما تظل الدراسات حول الأدلة الرقمية قليلة وغير شاملة. وغياب مراجع عربية متعمقة في هذا المجال، التي قد لا تتوافق تماما مع السياق الجزائري؛

3. ضيق الوقت الذي يُصعب الحصول على الجدة والجودة في البحوث العلمية؛

4. ضعف البنية التشريعية والاجتهاد القضائي، فالتشريع الجزائري لا يزال في مرحلة التأسيس فيما يخص الأدلة الرقمية، مما يعني أن الاجتهادات القضائية محدودة وغير موثقة بشكل كاف.

الفصل الأول

الإطار المفاهيمي للجريمة الإلكترونية والدليل الرقمي

يشهد العصر الرقمي تطورا متسارعا في مجال التكنولوجيا والاتصالات، مما أدى إلى ظهور أشكال جديدة من الجرائم التي تستهدف الأنظمة المعلوماتية والبيانات الرقمية، والمعروفة بـ "الجريمة الإلكترونية". وتفرض هذه الجرائم تحديات كبيرة على الأنظمة القانونية والقضائية، خاصة فيما يتعلق بإثباتها عبر الدليل الرقمي، الذي يتميز بخصائص فريدة تختلف عن الأدلة التقليدية.

يتناول هذا الفصل الإطار المفاهيمي للجريمة الإلكترونية والدليل الرقمي من خلال مبحثين رئيسيين:

المبحث الأول: مفهوم الجريمة الالكترونية، والذي يتضمن تعريف الجريمة الإلكترونية، وأبرز الخصائص التي تميزها، بالإضافة إلى أنواعها.

المبحث الثاني: مفهوم الدليل الرقمي، حيث نستعرض تعريف الدليل الرقمي وأنواع وأشكال الدليل الرقمي.

ويهدف هذا الفصل إلى توضيح الإطار المفاهيمي للجريمة الإلكترونية والدليل الرقمي، تمهيدا للتطرق للإطار القانوني للدليل الرقمي في الفصل الثاني.

المبحث الأول

مفهوم الجريمة الالكترونية

يعد ظهور الجريمة الإلكترونية نتيجة حتمية للتطور التكنولوجي، شأنها في ذلك شأن مفاهيم حديثة أخرى كالإدارة الإلكترونية والتجارة الإلكترونية. وكما أسهم التقدم الرقمي في تحسين حياة المجتمعات المعاصرة، من خلال دمج التقنيات الرقمية في مختلف القطاعات بهدف تقديم الخدمات بصورة أكثر كفاءة وسرعة وبأقل تكلفة، فقد أدى التسارع في تطور تكنولوجيا المعلومات، لاسيما مع بروز شبكة الإنترنت، إلى بروز آثار سلبية موازية، تجلت في الاستعمال غير المشروع لهذه الوسائل من قبل بعض الأفراد، خاصة في ارتكاب أفعال إجرامية.

ولغرض الإحاطة بهذا النمط المستحدث من الجرائم، نقسم هذا المبحث إلى مطلبين، يتناول أولهما تعريف الجريمة الإلكترونية وبيان خصائصها، في حين يخصص المطلب الثاني لعرض أنواع هذه الجريمة.

المطلب الأول

تعريف الجريمة الإلكترونية وخصائصها

لا يوجد اجماع على تعريف ثابت وشرعي للجريمة الإلكترونية لما يثيره المصطلح من تعقيدات مفاهيمية [1]، كما لا يختلف اثنان على أن الجريمة بمفهومها الواسع تعني كل مخالفة لأي قاعدة من القواعد التي تنظم سلوك الإنسان داخل الجماعة، أو يمكن تعريفها على أنها سلوك إجرامي يتمثل في ارتكاب فعل يعاقب عليه القانون، أو الامتناع عن تنفيذ أمر قضائي ملزم. وبوجه عام، تعرف الجريمة بأنها السلوك المضاد لمصلحة المجتمع والذي يلحق الضرر بصالحه العام. وعندما يرتكب هذا السلوك باستخدام الوسائل التكنولوجية الحديثة، لا سيما الحاسوب وشبكات الاتصال الإلكترونية عبر وسائل تقنية متطورة، يطلق عليه مصطلح "الجريمة الإلكترونية."

[1] عادل عزام سقف الحيط، جرائم الذم والتحقير المرتكبة عبر الوسائط الإلكترونية، دار الثقافة للنشر والتوزيع، 2019، ص 37.

وقد شهد مفهوم الجريمة الإلكترونية تطورا كبيرا، وامتدت الدراسة القانونية لها لتشمل مجموعة من الخصائص المميزة التي تفرزها عن باقي أنواع الجرائم التقليدية، حيث يتم التطرق الى تعريف الجريمة الالكترونية (الفرع الأول)، والى خصائصها (الفرع الثاني).

الفرع الأول

تعريف الجريمة الإلكترونية

للوقوف على مفهوم الجريمة الإلكترونية يقتضي الحال التعرض إلى التعريف الفقهي لهذه الجريمة (أولا)، ومن ثم تبيان التعريف التشريعي (ثانيا).

أولا: التعريف الفقهي للجريمة الإلكترونية: لم يتم التوصل في الفقه القانوني إلى تعريف جامع ومانع للجريمة الإلكترونية، مما أدى إلى تعدد التعريفات واختلافها تبعا للمنظور الذي يتبناه كل فقيه. وفي هذا السياق، يشير الفقيه **فان دير هلست وونيف** إلى وجود نقص في تعريف عام موحد وإطار نظري متكامل في مجال الجريمة الإلكترونية، حيث غالبا ما تستخدم مصطلحات متعددة مثل الافتراضية، والحاسوبية، والإلكترونية، والرقمية، والتي تعكس وجود فجوات جوهرية في التعريفات المطروحة [1].

ويعزى تباين التعريفات المتعلقة بالجريمة الإلكترونية إلى اختلاف الزاوية التي يتبناها الفقيه في تعريفها، إذ يرى بعض الفقه تعريفها بناء على الوسيلة التي ترتكب بها، أو موضوعها، أو بحسب مدى توافر المعرفة بتقنية المعلومات لدى مرتكبها، أو اعتمادا على معايير أخرى تختلف باختلاف القائلين بها [2]، كما يعتمد في تعريفها على معايير العناصر المتصلة بآليات ارتكابها أو بيئة ارتكابها أو صفات مرتكبيها، ذلك ما يبين في الآتي:

أ. معيار موضوع الجريمة أو نمط السلوك محل التجريم: في هذا السياق، تعرف الجريمة الإلكترونية على أنها نشاط غير مشروع يمارس بغية نسخ، أو تعديل، أو حذف، أو الوصول غير المصرح به

[1] محمد حجازي، جرائم الحاسبات والانترنت (الجرائم المعلوماتية)، المركز المصري للملكية الفكرية، القاهرة، مصر، 2005، ص 08.

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، مصر، الطبعة الأولى، 2008، ص 13.

إلى المعلومات المخزنة داخل الحاسوب، أو تلك التي تنقل من خلاله. وتضيف الباحثة **هدى قشقوش** إلى التعريف السابق، مؤيدة بذلك موقف أبرز فقهاء هذا الاتجاه مثل الفقيه **روزنبلات**، الذي أكد على الطابع غير المشروع للسلوك في الجريمة الإلكترونية، حيث عرفها بأنها: "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات" [1]. كما تعرف الجريمة الإلكترونية بأنها نمط من الجرائم التي ينص عليها قانون العقوبات، شرط ارتباطها باستخدام تقنية المعلومات في ارتكابها [2]. ويمكن تعريف الجريمة الإلكترونية أيضا بأنها الجريمة الناجمة عن إدخال بيانات مزورة إلى الأنظمة، أو إساءة استخدام المخرجات الناتجة عنها، إلى جانب أفعال أخرى تمثل جرائم أكثر تعقيدا من الناحية التقنية، مثل التلاعب بالأجهزة الحاسوبية [3].

ب. **معيار وسيلة ارتكاب الجريمة:** بناء على هذا التصور، تتحقق الجريمة الإلكترونية باستخدام الحاسوب كأداة رئيسية في ارتكابها. ففي هذا الصدد، يعرف الأستاذ جون فورستر الجريمة الإلكترونية بأنها فعل إجرامي يستخدم فيه الحاسوب كأداة للارتكاب. ويتفق مع هذا التعريف الفقيه **تايديمان** الذي يشير إلى أن الجريمة الإلكترونية تشمل كل أشكال السلوك غير المشروع التي ترتكب باستخدام الحاسوب. أما مكتب تقييم التقنية في الولايات المتحدة الأمريكية، فيصف هذه الجريمة بأنها " الجريمة التي تلعب فيها البيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا [4]".

أما منظمة التعاون الاقتصادي والتنمية فقد عرفت الجريمة الإلكترونية بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، ويكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية."

[1] هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، الطبعة الاولى،1992، ص22.

[2] محروس نصار غايب، الجريمة المعلوماتية، بحث منشور في مجلة التقني، المجموعة 24، الإصدار 9، العراق، 2011، ص 11.

[3] نفس المرجع، ص 12.

[4] نفس المرجع، ص 13

ويرجح اعتماد هذا التعريف نظرا لاتساعه وشموله لمختلف التصورات والاحتمالات المرتبطة بالجريمة الإلكترونية، فضلا عن كونه لا يغفل الطابع الفني والتقني المميز لها، وهو ما يمنحه مرونة أكبر في مواكبة ما قد تنتجه التطورات التكنولوجية والعلمية مستقبلا في هذا المجال.

ت. **معيار محل الجريمة ووسيلة ارتكابه (الحاسوب)**: وفي هذه الحالة يعد جهاز الحاسوب الضحية والوسيلة، ولتفصيل ذلك نورد التعريفات التالية: وفق هذا المنظور يعرف الفقيه **سميدينغ هوف** الجريمة الإلكترونية بأنها: "أي ضرب من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسوب".

وفي ذات الاتجاه ذهب كل من الفقيهان **روبرت ج لينكيست** و**جاك بولونيا**، فيعرفانها بأنها "الجريمة التي يستخدم فيها الحاسوب كوسيلة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الحاسوب نفسه ضحيتها." أما الفقيه **ماس** فيضيف إلى ذلك الهدف من اقتراف الجريمة الالكترونية وهو الحصول على الربح، فيعرفها بأنها تلك الاعتداءات التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح[1]".

ثانيا: التعريف التشريعي للجريمة الإلكترونية: من الثابت أن المشرع الجزائري قد أغفل إلى وقت غير بعيد، تنظيم الجريمة الإلكترونية ضمن الإطار القانوني الوطني، غير أنه سرعان ما تدارك هذا الفراغ التشريعي من خلال إصدار نصوص قانونية خاصة لمواجهة هذا النمط المستحدث من الجرائم. وقد تجسد ذلك في القانون رقم 04-15، الذي تضمن تعديلا لقانون العقوبات الجزائري، حيث أدرجت ضمنه أحكام جديدة في القسم السابع مكرر، تناولت الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات. وتبع ذلك صدور القانون رقم 09-04، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ومما ينبغي التنبيه إليه أن مصطلح "نظام المعالجة الآلية للمعطيات" يعد تعبيرا ذا طابع فني وتقني دقيق، يصعب على غير المتخصصين في المجال المعلوماتي، وخاصة من القانونيين، إدراك دلالته ومغزاه بشكل مباشر. ويضاف إلى ذلك أن هذا المصطلح يتميز بطابعه الديناميكي، إذ يخضع لتطورات سريعة

[1] محروس نصار غايب، الجريمة المعلوماتية، بحث منشور في مجلة التقني، المجموعة 24، الإصدار 9، العراق، 2011، ص 13.

ومتلاحقة في ميدان تقنيات الحوسبة ونظم المعلومات، الأمر الذي يضفي عليه صفة عدم الثبات ويعقد من مهمة تأطيره قانونيا بصورة دقيقة وشاملة [1].

وانطلاقا من الطبيعة التقنية المعقدة لمصطلح "نظام المعالجة الآلية للمعطيات"، فإن المشرع الجزائري، شأنه شأن العديد من التشريعات المقارنة، لم يقدم تعريفا قانونيا دقيقا لهذا النظام، وإنما أوكل مهمة تفسيره وتحديد معناه إلى كل من الفقه والقضاء.

ولمزيد من الإيضاح، سيتم التطرق إلى كيفية تناول هذا المصطلح في كل من القانون رقم 04-15 المتضمن تعديل قانون العقوبات، والقانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك على التوالي:

أ. **تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 04-15**: بالرجوع إلى قواعد القانون 04-15 من المادة 394 مكرر إلى المادة 394 مكرر 2 نجد أنه حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات، حيث حددها في المادة 394 مكرر بالآتي:

1. الدخول والبقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك؛
2. لا حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

أما المادة 394 مكرر 1 فقد أشارت إلى ما يلي[2]:

-إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

وبالنسبة للمادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات من الآتي:

---

[1] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، منشأة المعارف، الإسكندرية، مصر، 1999، ص120.

[2] المادة 394 مكرر 1، القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر 66-156 المؤرخ في 08 يونيو 1966 المتضمن ق.ع.ج الجريدة الرسمية، العدد 71، 2004.

-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

ب. تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 09-04: حددت المادة 2 منه [1] الجريمة الإلكترونية بقولها: " يقصد في مفهوم هذا القانون بما يأتي: الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في ق.ع.ج وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

الفرع الثاني

خصائص الجريمة الإلكترونية ومرتكبيها

تتسم الجرائم الإلكترونية بجملة من الخصائص التي تميزها عن الجرائم التقليدية، سواء من حيث طبيعتها أو وسائل ارتكابها أو الآثار المترتبة عنها. كما أن مرتكبي هذا النوع من الجرائم يتمتعون بصفات خاصة تميزهم عن الجناة في الجرائم العادية، لا سيما من حيث المؤهلات التقنية والدوافع السلوكية. وفيما يلي بيان لأهم هذه الخصائص:

أولا: خصائص الجريمة الإلكترونية: تتسم الجريمة الإلكترونية بجملة من الصفات أو الخصائص نبينها في الآتي:

أ. صعبة الاكتشاف: تتصف الجرائم الإلكترونية بطابعها الخفي والمستتر في غالب الأحيان، إذ كثيرا ما ترتكب دون أن ينتبه الضحية إلى وقوعها، حتى وإن حدثت أثناء تواجده الفعلي على الشبكة. ويعزى هذا الطابع إلى ما يتمتع به الجاني من مهارات تقنية عالية وقدرات فنية متقدمة، تمكنه من تنفيذ أفعاله الإجرامية بدقة وفعالية، سواء من خلال إرسال الفيروسات، أو سرقة الأموال والبيانات

[1] المادة 2، القانون 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47 لسنة 2009.

الشخصية، أو إتلاف المعلومات، أو التجسس، أو اعتراض وسرقة المكالمات، وغيرها من الأفعال التي تدخل ضمن نطاق الجريمة الإلكترونية [1].

وبناء على ما سبق، فإن الجرائم الإلكترونية غالبا ما لا تخلف آثارا مادية واضحة بعد ارتكابها، وإن وجدت آثار، فإن الاحتفاظ بها فنيا يعد أمرا بالغ الصعوبة. وتعقد هذه الخصائص من مهام جهات التحقيق التقليدية، إذ ترتكب هذه الجرائم باستخدام وسائل تقنية متطورة تعتمد على التمويه والتضليل، مما يعيق عملية التعرف على هوية مرتكبيها. وفي جميع الأحوال، فإن التصدي لهذا النوع من الجرائم يقتضي توفر خبرة فنية عالية ومتخصصة، قادرة على تتبع الآثار الرقمية وإثبات الركن المادي للجريمة.

ب. صعبة الإثبات: يعد إثبات الجريمة الإلكترونية من أصعب جوانب مكافحتها، نظرا لصعوبة تتبعها واكتشافها، حيث إنها في جوهرها مجرد بيانات وأرقام لا تترك آثارا مادية تقليدية يمكن تتبعها مثل البصمات. وغالبا ما يتم اكتشاف هذه الجرائم صدفة، وبعد مرور فترة زمنية طويلة على ارتكابها.

ومن جهة أخرى، فإن تعقب مرتكبي الجرائم الإلكترونية يتطلب مهارات فنية متخصصة لا تتوفر غالبا لدى المحققين التقليديين. كما أن الجناة يستخدمون وسائل التمويه والتضليل والتحايل لتعقيد عملية التعرف عليهم وضبطهم، مما يزيد من تحديات الإثبات والملاحقة القضائية.

ت. عابرة للحدود: المقصود بذلك أن هذا النوع من الجرائم لا يعتد بالحدود الجغرافية للدول ولا بين القارات، فمع انتشار شبكة الاتصالات بين دول العالم وأقاليمه أمكن ربط أعداد لا حصر لها من أجهزة الحاسوب عبر مختلف دول العالم بهذه الشبكة حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر، وهكذا فالجرائم الالكترونية تقع في أغلب الأحيان عبر حدود دولية كثيرة [2].

إن قدرة تقنيات المعلومات على تجاوز الحدود الجغرافية وتعزيز الترابط بين مختلف أرجاء العالم، جعل مسرح الجريمة الإلكترونية ذا طابع عالمي، وليس محليا. فالفاعل لا يكون بالضرورة حاضرا ماديا في مكان ارتكاب الجريمة، وإنما قد ينفذ فعله الإجرامي عن بعد، باستخدام جهاز حاسوب.

---

[1] محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، مصر، 2009، ص31.

[2] عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، ص 42.

ويترتب على ذلك غياب الوجود المادي للجاني في مكان وقوع الجريمة الإلكترونية، حيث تتباعد المسافات بين موقع تنفيذ الفعل الإجرامي (عن طريق جهاز الفاعل) والمعلومة أو النظام المعلوماتي محل الاعتداء. فقد يوجد الجاني في دولة ما، ويتمكن من اختراق نظام حاسوبي في دولة أخرى، ويلحق الضرر بشخص يقيم في دولة ثالثة، مما يبرز الطابع العابر للحدود الذي تتسم به هذه الجرائم [1].

ث. هادئة: في حين تتطلب الجرائم التقليدية جهدا عضليا ملموسا في ارتكابها، كما هو الحال في جرائم القتل والسرقة وغيرها، فإن الجرائم الإلكترونية تختلف في طبيعتها من حيث إنها لا تستلزم أي مجهود عضلي، بل تعتمد أساسا على التخطيط الذهني والدراسات العلمية الدقيقة المرتكزة على معرفة تقنية متخصصة في مجال الحاسوب [2].

ويعود ذلك إلى أن هذا النوع من الجرائم يرتبط مباشرة بالتلاعب بالمعطيات والبيانات، التي يتم تعديلها أو تغييرها أو محوها من السجلات المخزنة في ذاكرة الحاسوب.

ثانيا: خصائص مرتكبي الجريمة الإلكترونية: يتميز مرتكب الجريمة الإلكترونية بصفات خاصة تميزه عن غيره من مرتكبي الجرائم الأخرى، وذلك من حيث الآتي:

أ. الذكاء والتخصص: غالبا ما يتسم المجرم الإلكتروني بقدر كبير من الذكاء والمهارة التقنية، مما يؤهله لتعديل وتطوير الأنظمة الأمنية الإلكترونية. ويتمتع هذا المجرم بقدرة على التخطيط الدقيق لجريمته، بحيث يمنع إمكانية ملاحقته أو تتبع أفعاله عبر الشبكات أو داخل أجهزة الحاسوب. وعادة ما يقوم المجرم الإلكتروني بالتحضير المسبق لارتكاب جريمته من خلال دراسة دقيقة لجميع الظروف المحيطة بها، بهدف تفادي ما قد يؤدي إلى ضبط أفعاله والكشف عنه [3].

---

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2005، ص52.

[2] عبد الفتاح مراد شرح جرائم الكمبيوتر والإنترنت مشار إليه، ص 46.

[3] طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني لحماية المعلوماتي، دار الجامعة الجديدة، القاهرة، مصر، الطبعة 2009، ص177.

كما يتمتع المجرم الإلكتروني بمهارات تقنية متقدمة يستغلها في اختراق الشبكات وكسر كلمات المرور أو الشفرات الأمنية، بهدف الوصول إلى البيانات والمعلومات المخزنة في أجهزة الحاسوب أو المتداولة عبر الشبكات [1].

ب. الذوبان في المجتمع: يتميز المجرم الإلكتروني أيضا بكونه فردا اجتماعيا متوافقا مع المجتمع الذي يعيش فيه، إذ لا يضع نفسه عادة في حالة عداء مع محيطه الاجتماعي. ومع ذلك، قد يرتكب هذا النوع من الجرائم بدوافع متنوعة تتراوح بين التسلية واللهو، أو الرغبة في إثبات التفوق على الحاسوب أو البرامج التي يستخدمها، أو السعي لتحقيق مكاسب مالية، أو حتى تحقيق أهداف انتقامية.

المطلب الثاني

أنواع الجرائم الإلكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة التي اختلف الفقه في تصنيفها تحت مسميات متعددة، وغالبا ما أغفلت معظم هذه التصنيفات الخصائص الجوهرية للجرائم الإلكترونية وموضوعها المميز. وأهم ما يميز هذه الجرائم هو استهدافها للكيانات المعنوية المتعلقة بالحاسوب الآلي، حيث ترتكب باستخدام أجهزة إلكترونية. أما الجرائم التي تستهدف الكيانات المادية للحاسوب الآلي فتدرج ضمن الجرائم التقليدية.

يرجع اختلاف الفقه في تقسيم الجرائم الإلكترونية إلى ظهور أنواع جديدة من هذه الجرائم بشكل مستمر، حيث إن الجرائم الإلكترونية لا تحصى ولا يمكن حصرها في أصناف وأشكال محددة. فمع كل تطور في وسائل استخدام الحاسوب والإنترنت، تظهر جرائم جديدة مصاحبة لهذا التطور، مما يجعل طبيعة هذه الجرائم متغيرة ومتجددة باستمرار [2].

[1] محمد علي قطب الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، عمان، الأردن، ص 14.

[2] ابراهيم رمضان ابراهيم عطايا، الجريمة الالكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، مجلة كلية الشريعة والقانون بطنطا، مصر، المجلد 30، العدد 2، أفريل 2015، ص 373.

لم يستقر الفقه بعد على معيار موحد لتصنيف الجرائم الإلكترونية، ويعزى ذلك إلى تشعب هذا النوع من الجرائم وسرعة تطورها المستمرة. فهناك من يصنفها استنادا إلى وسيلة ارتكاب الجريمة، أو بناء على محل وقوعها، أو وفق معايير أخرى مختلفة. وبناء على هذه المعايير، يمكن تقسيم الجرائم الإلكترونية إلى[1] فرعين، الجرائم الواقعة بواسطة النظام المعلوماتي (الفرع الأول) والجرائم الواقعة على النظام المعلوماتي (الفرع الثاني).

الفرع الأول

الجرائم الواقعة بواسطة النظام المعلوماتي

يعتبر الحاسوب الآلي في هذا النوع من الجرائم أداة تسهل تحقيق النتيجة الإجرامية وتزيد من جسامتها، حيث يهدف الجاني من وراء ذلك إلى تحقيق مكاسب مالية غير مشروعة. وتعتمد هذه الجرائم على استخدام النظام المعلوماتي ذاته أو برامجه كوسيلة لتنفيذ الأفعال الإجرامية. وتنقسم هذه الجرائم بدورها إلى الفئات التالية:

أولا: الجرائم الواقعة على الأشخاص: تتمتع الحياة الشخصية بدرجة عالية من الخصوصية والحرمة التي لا يجوز لأي شخص انتهاكها أو اقتحامها. ومن أمثلة ذلك الاعتداء على المعلومات الإلكترونية الخاصة بالمحامين، أو الأطباء، أو المحاسبين، أو غيرهم من المهنيين، حيث قد تتم الجريمة عبر الاطلاع غير المشروع على بيانات ومعلومات شخصية، أو تسجيل المكالمات، أو الفيديوهات، أو مراقبة الأفراد دون رضاهم.

أما فيما يتعلق بجريمة نشر المواد الإباحية، فيتجلى الركن المادي لها في السلوك الذي يتخذه الفاعل من خلال تهيئة صفحات إلكترونية تحتوي على مواد مخالفة للآداب العامة، ومن ثم نشرها عبر شبكة الإنترنت. بينما يتحدد الركن المعنوي في الحالة النفسية للفاعل، بحيث يكون لديه القصد المباشر للنشر والعلم والإرادة في تنفيذ هذا الفعل.

[1] حفوظة الأمير عبد القادر وغرداين حسام، الجريمة الإلكترونية وآليات التصدي لها، الملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 93.

ثانيا: الجرائم الواقعة على الأموال: قد صاحب ظهور شبكة الإنترنت تطورات هائلة في مختلف المجالات، حيث أصبحت معظم المعاملات التجارية تنجز من خلالها، مثل عمليات البيع والشراء، مما أدى إلى تطور وسائل الدفع والوفاء التي أصبحت جزءا لا يتجزأ من هذه المعاملات. في ظل هذا التداول المالي الإلكتروني، استغل بعض المجرمين الفرصة لممارسة أعمال إجرامية عدة، منها السطو والسرقة، والتحويل الإلكتروني غير المشروع للأموال، وقرصنة أرقام البطاقات الممغنطة.

ومع التحول من المعاملات التجارية التقليدية إلى المعاملات الإلكترونية، وما رافقه من تطور في وسائل الدفع، أصبحت هذه المعاملات عرضة لمجموعة متنوعة من الجرائم، من بينها:

أ. السطو على أرقام بطاقات الائتمان والتحويل الإلكتروني الغير مشروع.

ب. القمار وغسيل الأموال عبر الأنترانت.

ت. جريمة السرقة والسطو على أموال البنوك.

ث. تجارة المخدرات عبر الأنترنيت."

ثالثا: الجرائم الواقعة على أمن الدولة: استغلت العديد من الجماعات المتطرفة الطابع الاتصالي لشبكة الإنترنت لبث معتقداتها وأفكارها، متجاوزة ذلك إلى ممارسات تهدد أمن الدول المستهدفة، لا سيما من خلال الجرائم الإرهابية والجريمة المنظمة التي اكتسبت أبعادا جديدة في سياق استخدام الإنترنت. فقد أتاح الإنترنت لهذه الجماعات ارتكاب جرائم تمس بالمجتمعات والدول، بل وأكثر من ذلك، سمح لعدد من الدول بممارسة التجسس على دول أخرى عبر الاطلاع على أسرارها العسكرية والاقتصادية، خصوصا في مناطق النزاعات.

ويظل المساس بالأمن الفكري من أخطر الجرائم المرتكبة عبر الإنترنت، حيث تتيح هذه الشبكة فرصا للتأثير في معتقدات وتقاليد المجتمعات بأكملها، مما يسهل إحداث حالة من الفوضى الاجتماعية والسياسية [1].

[1] ناصر محمد البقهي، أثر التحويل مجتمع معلوماتي على الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف بن عبد العزيز الدراسات الأمن الفكري بجامعة الملك سعود المملكة السعودية من 22 الى 25 جمادى الأولى 1430 هـ. ص 18.

الفرع الثاني

الجرائم الواقعة على النظام المعلوماتي

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية يمس النظام المعلوماتي ويستهدف إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي [1].

أولا: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي: يقصد بالمكونات المادية للنظام المعلوماتي تلك الأجهزة والمعدات الملموسة المستخدمة في تشغيله، مثل الأسطوانات والشرائط والكابلات وغيرها من الوسائط التقنية. ونظرا للطبيعة المادية لهذه العناصر، فإن الجرائم الواقعة عليها تعد من قبيل الجرائم التقليدية، مثل السرقة وخيانة الأمانة، والإتلاف العمدي، والحرق، أو العبث بمفاتيح التشغيل، مما قد يلحق خسائر مادية جسيمة.

وقد وقع بالفعل هذا النوع من الجرائم في فرنسا، حيث تم إتلاف معدات تابعة لمؤسسة كبيرة متخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية، وقدرت الخسائر الناجمة عن ذلك الحادث بحوالي خمسة ملايين فرنك فرنسي.

ثانيا: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي: تعد هذه الصورة من الجرائم، بلا شك، من أكثر الصور شيوعا وخطورة ضمن الجرائم الإلكترونية، حيث يقوم الجاني من خلال أساليب احتيالية بإدخال معطيات في نظم المعالجة الآلية للمعطيات، أو إتلاف تلك المعطيات، أو حذفها، أو تعديلها. ويؤدي هذا السلوك إلى الإخلال بوظيفة النظام المعلوماتي وإلحاق أضرار بالغة بسلامة البيانات ومصداقيتها [2].

وقد عالج المشرع الجزائري هذا النمط من الجرائم من خلال نص المادة 394 مكرر من ق.ع.ج، والتي تنص على أنه يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة مالية

---

[1] سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماستر في العلوم الجنائية وعلم الإجرام، كلية الحقوق جامعة أبوبكر بلقايد، تلمسان، الجزائر، 2010، ص12.

[2] سومية عكور، الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانوني والأمني، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، كلية العلوم الإستراتيجية، الأردن، 02-04/09/2014، ص 12.

من 5000.00 دج إلى 20.000.00 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها، من خلال هذا النص ومن أجل معالجة عناصر هذه الجريمة يتوجب تحديد معنى الإتلاف ثم الوسائل التي يتحقق بها الإتلاف.

ويقصد كذلك بالإتلاف إفناء مادة الشيء أو هلاكه كليا وبالتالي توقف الشيء تماما على أن يؤدي منفعته ولو لم تفن مادته سواء كان هذا التوقف كليا أو جزئيا ويكون الشيء غير صالح للاستعمال بجعله لا يقوم بوظيفته المرصود لها على النحو الأكمل.

كما يقصد أيضا بإتلاف برامج الحاسوب الآلي ومعلوماته إتلاف أو محو تعليمات البرامج والبيانات ذاتها ويطلق عليها مصطلح تدمير نظم المعلومات وعادة لا يستهدف مرتكب هذا الاعتداء فائدة مالية لنفسه، بل لمجرد إعاقة نظام المعلومات.

ومن اجل الإشارة إلى مدلول الإتلاف استخدم المشرع الجزائري عدة تعابير حيث استخدم (أدخل، أزال وعدل) وإن كان لهذه التعابير مدلولات خاصة، إلا أنها تندرج تحت مدلول الإتلاف وهو ما ذهبت إليه بعض التشريعات المقارنة خاصة التشريع الفرنسي، وبالتالي يمكن القول كذلك أن المشرع الجزائري قد أورد هذه الصور التي يتحقق بها الإتلاف على سبيل المثال لا الحصر، وبمعنى أخر يمكن أن يتحقق الإتلاف بصور أخرى غير تلك التي أوردها المشرع الجزائري في ق.ع.ج.

إن المقصود بالإتلاف في هذا الإطار ذلك الذي يوجه إلى الجانب المنطقي والمعنوي في الحاسب الآلي، والذي بات يشكل قيمة اقتصادية عالية، فإتلاف برامج ومعلومات الحاسب الآلي فيه إفقاد لمنفعة هذه البرامج والمعلومات."

ثالثا: الجرائم الواقعة على البرامج الإلكترونية: تنقسم الجرائم المعلوماتية ضد البرمجيات إلى جرائم تمس البرامج التطبيقية، كقيام مبرمج في بنك أمريكي بتعديل برنامج لإضافة دولار على كل حساب يتجاوز عشرة دولارات وتحويلها إلى حساب خاص باسم "zzwick"[1]، وجرائم تمس برامج التشغيل، كتصميم

[1] سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماستر في العلوم الجنائية وعلم الإجرام، كلية الحقوق جامعة أبوبكر بلقايد، تلمسان، الجزائر، 2010، ص42.

شركة تأمين في لوس أنجلوس برنامجا وهميا لإصدار 46,000 وثيقة تأمين مزيفة بهدف تحصيل عمولات غير مشروعة [1].

المبحث الثاني

مفهوم الدليل الرقمي

إن تقييم أي أمر يعتمد بشكل أساسي على فهمه، لذا فإن تقييم الدليل الرقمي واعتباره وسيلة للإثبات يتطلب أولا تكوين تصور واضح عنه، وتحديد معالمه الأساسية، وفهم طبيعته من خلال تعريفه، ودراسة خصائصه، وأنواعه، وأشكاله المختلفة.

المطلب الأول

تعريف، أنواع وأشكال الدليل الرقمي

يعد الدليل الرقمي من المستحدثات البارزة في نطاق الإثبات، نظرا للتحديات القانونية والفنية التي يثيرها. وسنستعرض هذا من خلال فرعين: تعريف الدليل الرقمي (الفرع الأول)، وخصائص الدليل الرقمي (الفرع الثاني).

الفرع الأول

تعريف الدليل الرقمي

إن الدور الذي سيلعبه الدليل الرقمي في الإثبات الجزائي يجعل بيان تعريفه وخصائصه من الأهمية بمكان، لأن معرفة ذلك يسهم في تحديد ما يصلح أن يكون دليلا، ومدى توفر شروط مشروعيته وتقدير قيمته في الإثبات، لذا نتطرق للتعريف اللغوي والفقهي للدليل الرقمي (أولا)، ثم للتعريف التشريعي (ثانيا).

[1] سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماستر في العلوم الجنائية وعلم الإجرام، كلية الحقوق جامعة أبوبكر بلقايد، تلمسان، الجزائر، 2010، ص42.

أولا: التعريف اللغوي للدليل الرقمي: ان مصطلح الدليل الرقمي من المصطلحات المركبة لذا سنتعرف على الدليل الرقمي من خلال التعرف على المقصود بالدليل وكذا المقصود بالرقمي، ومن ثم التعريف بها كمصطلح مركب.

أ. **تعريف الدليل:** لتعريف الدليل نتطرق لتعريفه لغة واصطلاحا.

1. **الدليل لغة:** يراد به عدة معان، منها المرشد أو ما يستدل به [1]. ومنها ما يتوصل به إلى معرفة الشيء[2]، من ذلك قوله تعالى (فَلَمَّا قَضَيْنَا عَلَيْهِ الْمَوْتَ مَا دَلَّهُمْ عَلَى مَوْتِهِ إِلَّا دَابَّةُ الْأَرْضِ تَأْكُلُ مِنْسَأَتَهُ فَلَمَّا خَرَّ تَبَيَّنَتِ الْجِنُّ أَنْ لَوْ كَانُوا يَعْلَمُونَ الْغَيْبَ مَا لَبِثُوا فِي الْعَذَابِ الْمُهِينِ)[3]. ومنها ما يراد به الحجة والبرهان[4]، ومن ذلك قوله تعالى (وَقَالُوا لَن يَدْخُلَ الْجَنَّةَ إِلَّا مَن كَانَ هُودًا أَوْ نَصَارَىٰ ۗ تِلْكَ أَمَانِيُّهُمْ ۗ قُلْ هَاتُوا بُرْهَانَكُمْ إِن كُنتُمْ صَادِقِينَ)[5]. والدليل بمعناه الأخير هو الذي يتعلق بهذا البحث.
2. **الدليل اصطلاحا:** في الاصطلاح الشرعي هو ما يلزم من العلم به العلم بشيء آخر[6]. وأما الدليل في الاصطلاح القانوني، فقد وردت عدة تعريفات له، ومن أهمها ما جاء من أن الدليل يعرف بأنه "ما يثبت به الحق المدعى به، أو هو الوسائل التي يستنتج منها القضاة صحة الدعوى "[7].

ب.تعريف الرقمي: لتعريف الرقمي نتطرق لتعريفه لغة واصطلاحا

1. **الرقمي لغة:** مشتق من اللفظ "رقم ". وقد جاء تعريف الرقمية لغة بأنها " اللغة التي تعد خصيصا طبقا لقواعد معينة لتستخدم في الحاسبات الالكترونية كوسيلة للعمل بها "[8].

---

[1] المعجم الوسيط في اللغة العربية لمجموعة من علماء اللغة العربية، ج1، مطبعة مصر شركة مساهمة مصرية، 1960.

[2] نواف مزيد السريحي، الاستدلال والدليل في القران الكريم، مجلة الدراسات العربية، جامعة المنيا، كلية العلوم، العدد 25، 2012، ص 1052.

[3] سورة سبأ، الآية 14.

[4] ابن منظور، لسان العرب، (2/282). مشار إليه لدى نواف مزيد السريحي، مرجع سابق.

[5] سورة البقرة، الآية 111.

[6] احمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2015، ص 6.

[7] أحمد فتحي زغلول، شرح القانون المدني، المطبعة الأميرية، مصر، 1913، ص 385.

[8] أحمد مختار عمر، معجم اللغة العربية المعاصرة، عالم الكتب، المجلد الأول، ط 2008، ص 930.

2.**الرقمي اصطلاحا:** عرف قاموس أكسفورد مصطلح "رقمي" بأنه طريقة لنقل وتخزين المعلومات الصوتية والكتابات والفيديو في الشبكة الالكترونية وجهاز الحاسوب، إذ أن أجهزة المعالجة الرقمية تقوم بتحويل المعلومات إلى أرقام وتخزينها في ذاكرة الحاسوب مما يساعد على معالجة البيانات في الشبكة العنكبوتية[1].

وهكذا فإن الرقمية ما هي إلا طريقة لنقل وتخزين المعلومات الصوتية والكتابات والفيديو في الشبكة الالكترونية أو جهاز الحاسوب من خلال أرقام يمكن للأجهزة أن تقوم بتخزينها بطريقة معينة ثم عند طلبها يقوم الحاسب أو الآلة بإعادة قراءة هذه الأرقام ليخرج النصوص بشكلها العادي سواء كان صورة، أو فيديو، أو مستند، أو غيره [2].

ثانيا: التعريف الفقهي للدليل الرقمي: الدليل القانوني اصطلاحا وسيلة يستعين بها القاضي، ويستدل بها على حقيقة الواقعة موضوع النزاع المطروح أمامه، بهدف كشف الحقيقة التي ينشدها.

وقد عرف بعض الفقهاء الدليل الرقمي بأنه: " الدليل الذي يجد له أساسا في العالم الافتراضي إلى الجريمة"، ويرى آخر أن الدليل الرقمي هو: الدليل المأخوذ من أجهزة الحاسوب الآلي، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيات، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة، كالنصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم، وذلك من أجل اعتماده أمام أجهزة تنفيذ وتطبيق القانون .

والذي يلاحظ على هذا التعريف أنه يقصر مفهوم الدليل الرقمي على ذلك الذي يتم استخراجه من الحاسب الآلي، ولاشك أن في ذلك تضييق لدائرة الأدلة الرقمية، فهي كما تستمد من الحاسوب الآلي، من الممكن أن يتحصل عليها من أية آلة إلكترونية أخرى، كالهاتف و آلات التصوير والفاكس، تعتمد التقنية الرقمية في تشغيلها، وتكون مصدرا للدليل الرقمي، كما أن هذا التعريف يخلط بين الدليل الرقمي ومسألة استخلاصه، إذ عزفه بأنه الدليل المأخوذ من الحاسب الآلي، وهذا يعني أن الدليل الرقمي

[1] دعاء محمد نجم، ماهية المجتمع الرقمي، كلية الخدمة الاجتماعية، جامعة حلوان، ص 47.

[2] حكيمة جاب الله، فريدة بن عمروش، التكنولوجيا الرقمية، قراءة في المفاهيم وبعض الأبعاد النظرية، المجلة العلمية للتكنولوجيا وعلوم الإعاقة، المجلد 3، العدد 1، 2021، ص 122.

لا تثبت له هذه الصفة إلا إذا تم أخذه واستخلاصه من مصدره، وهذا برأينا ليس صحيحا، إذ من شأن التسليم بهذا المعنى القول إن المجالات المغناطيسية أو الكهربائية، قبل فصلها عن مصدرها بالدليل الرقمي ما يعني أن مخرجات الآلة الرقمية لا تكون لها قيمة إثباتيه مادامت في الوسط الافتراضي الذي نشأت فيه أو بواسطته، وهذا غير دقيق، وهو ما يصم هذا التعريف بالقصور لكونه لا يعطى تعريفا جامعا للدليل الرقمي. ويعرف آخر الدليل الرقمي بأنه: "الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، وأجهزة ومعدات أدوات الحاسوب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال وأصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها "[1].

وبناء على ما سبق نعرف الدليل الرقمي بأنه: مجموعة مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية أو غيرها، لتقديمها إلى القضاء بغرض إثبات الوقائع الجرمية، أو لتقرير إدانة أو براءة المتهمين بارتكابها، وفي نطاق الجرائم الإلكترونية تعد الأدلة الرقمية مرحلة متقدمة من الأدلة المادية الملموسة، تستخلص بالاستعانة بما ابتكره العلم الحديث من وسائل التقنية العالية، التي هي محور الأدلة الرقمية وجوهرها، فالأدلة الرقمية نوع متميز من وسائل الإثبات، له من الخصائص العلمية والمواصفات القانونية ما يؤهله ليكون نوعا جديدا من الأدلة [2].

ثالثا: التعريف التشريعي للدليل الرقمي: نجد أن العديد من القوانين الجزائية الخاصة بمكافحة الجرائم المعلوماتية أو الإلكترونية، وإن لم تشر صراحة إلى الدليل الرقمي، إلا أنها عرفت البيانات الإلكترونية أو البرامج المعلوماتية على انها البيانات الرقمية المخزنة في الأجهزة الحاسوبية أو المنظومات المعلوماتية، أو المنقولة بواسطتها، والتي يمكن استخدامها في إثبات جريمة معلوماتية أو نفيها.

[1] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري: الإثبات الجزائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجزائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض 2-1428/11/04هـ، ص 13.

[2] محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، سنة 2004م، ص234.

وبالرجوع للمشرع الجزائري نجد أنه لم يعرف الدليل الرقمي سواء في القانون 09-04 السالف الذكر أو حتى في المرسوم 15- 261 [1] المتعلق بتنظيم الهيئة الوطنية للوقاية من جرائم تكنولوجيات والإعلام والاتصال.

الفرع الثاني

خصائص الدليل الرقمي

للدليل الرقمي جملة من الخصائص التي تميزه عن الأدلة التقليدية، سواء من حيث طبيعته غير المادية، أو من حيث طريقة جمعه وتحليله والحفاظ عليه. هذه الخصائص تفرض تحديات قانونية وتقنية في آن واحد، وتستلزم اعتماد معايير دقيقة لضمان حجيته وقبوله أمام الجهات القضائية، ولفهم طبيعته الخاصة ودوره المتزايد في مجال الإثبات يمكن حصر خصائصه في ثلاث:

أولا: غير ملموس: فالدليل الرقمي يفتقر إلى الطبيعة المادية التي تميز الأدلة التقليدية، كالسلاح الذي عليه بصمات القاتل المستعمل في جريمة القتل، أو المال المسروق والذي ضبط في حيازة السارق[2]، أما في الجرائم المعلوماتية فإن الآلة التقنية لا تفرز سوى نبضات إلكترونية أو كهربائية أو مغناطيسية أو ضوئية في شكل رموز أو أصوات أو صور أو أية إشارة تقل فيها، إن لم تنعدم الآثار المادية الملموسة، وهي ذات دلاله تعبيرية واضحة ومفهومة أيا كانت الدعامة التي تستعمل في إنشائها أو الوسيط الذي تنتقل عبره، ولا يغير من هذه الخصيصة القيام بتجميع تلك النبضات، وترجمتها وإخراجها في شكل دليل ملموس، لأن هذا التجميع لا يعد هو الدليل، بل إن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الاستدلال بها على معلومة معينة.

ثانيا: تقني علمي: الدليل الرقمي ذو طبيعة تقنية، إذ إنه ينشأ في عالم تقني افتراضي (هو بيئة تقنية المعلومات)، ولا يسهل إدراكه إلا من الخبير الفني، ويمثل الواقعة التي تنبئ بوقوع جريمة أو فعل غير مشروع، وهي واقعة علمية بناها العلماء والتقنيون[3]. وفهم مضمون الدليل الرقمي يعتمد على استخدام

[1] مرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] طارق عبد الرؤوف الخن، الجريمة المعلوماتية، منشورات الجامعة الافتراضية السورية، 2010-2011، ص 130.

[3] جميل عبد الباقي الصغير، أدلة الإثبات الجزائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، د.ت، 2002، ص 96.

أجهزة خاصة بتجميع وتحليل فحواه، ليكون دليل إثباته، ولما كانت التقنية ابنة العلم فكذلك يعد جميع ما ينشأ عن التقنية سببا في تقرير أن الأدلة الجزائية الرقمية هي أدلة علمية يرجع إلى أنها تستمد مما يصنعه أهل العلوم التقنية من آراء واستنتاجات علمية يتم الوصول إليها بواسطة أجهزة وبرامج تقنية[1]، ويخرج من نطاق الأدلة الرقمية كل ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة، لعدم إمكانية الاستدلال به على معلومة معينة، ما يعدم قيمته كدليل في الإثبات الجزائي[2]، ومن ثم فإن إطلاق الصفة الرقمية على أي دليل يستلزم وجود توافق بين هذا الدليل والبيئة التي يعيش فيها، وهي العالم الافتراضي الكامن في الأقراص والحواسيب والخوادم والشبكات التي يتم تداول الحركة عبرها[3]، وأن تكون الوسيلة العلمية المولدة للدليل قد استقر العمل بها علميا، وأجمع العلماء على صحة ودقة نتائجها، وأن استعمالها تم عن طريق الخبراء المختصين[4].

ثالثا: صعب التخلص منه: يتسم الدليل الرقمي بأنه يرصد جميع تحركات الفرد وسلوكياته ويسجلها، وهذه السمة من أهم خصائص الدليل الرقمي، وهو بذلك يشبه الدليل العلمي المتعلق بالحمض النووي، لجهة صعوبة التخلص منه[5].

وبهذه الخاصية تتميز الأدلة الرقمية عن الأدلة التقليدية، التي تجعل أجهزة العدالة تعاني من مسألة قيام الجاني أو غيره من ذوي المصلحة بالتخلص منها، كالتخلص من بصمات الأصابع بمسحها من موضعها، ويمكن التخلص من الأوراق التي تحمل إقرارات معينة بتمزيقها وحرقها. أما في حالة الأدلة الرقمية فالأمر مختلف تماما، فمع أن الدليل الرقمي يتميز بسرعة زواله وإمكانية إتلافه بسهولة، وأنه

---

[1] ميسون الحمداني، ميسون خلف حمد الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي، مجلة كلية القانون، جامعة النهرين، 2016، ص200.

[2] طارق الجملي، الدليل الرقمي في مجال الإثبات الجزائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة من 28 الى 2009/10/29، الذي نظمته أكاديمية الدراسات العليا، طرابلس، ص 04.

[3] جميل عبد الباقي الصغير، أدلة الإثبات الجزائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، د.ت، 2002، ص 96.

[4] محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة، دار الجامعة الجديدة 2018، ص 365

[5] طارق عبد الرؤوف الخن، الجريمة المعلوماتية، منشورات الجامعة الافتراضية السورية، 2010-2011، ص 130.

متقلب[1]، إلا أنه يمكن إعادته للحياة مرة أخرى، فكل محاولة للتخلص من البيانات الإلكترونية بحذفها أو إلغائها، أو بإعادة التهيئة أو التشكيل للقرص الصلب باستخدام الأمر (Format)، فإن هذه المحاولات لا تشكل عائقا يحول غير إمكانية استرجاع تلك البيانات، بصورة كلية أو جزئية، وذلك بفضل البرامج الحاسوبية التي تقوم بوظيفة استعادة البيانات والمعلومات والبرامج التي تم حذفها، كاستخدام أداة استرداد الملفات المحذوف [2]، وهذا يعني أنه يصعب على الجاني إخفاء جريمته أو أدلتها، لأنه يمكن استخراج نسخة مطابقة للدليل من خلال النسخ المحفوظة في النظام.

رابعا: إمكانية النسخ: يمتاز الدليل الرقمي بسهولة استنساخه بوقت قصير من غير المساس بالأصل، إذ يمكن استخراج ما تريد من النسخ المطابقة لأصله تماما، لها القيمة العلمية والحجية الدليلية في الإثبات ذاتها التي النسخة الأصلية، فالنسخ تكرار للأصل وليس نسخة منه [3]، وهذه النسخ تمكن الجهات المختصة من إجراء الفحص المعلوماتي عليها، ومن ثم نحفظ الدليل من الفقدان كلية أو التلف أثناء عملية الفحص، أو التغيير أو العبث في مضمونه [4]. وهذه الميزة يفتقر لها الدليل التقليدي الذي لا يمكن نسخه، ومن ثم يكون من السهل جدا التخلص منه، كالتخلص من الأوراق المكتوبة بتمزيقها أو حرقها، والتخلص من بصمات الأصابع بمسحها من موضعها على أداة الجريمة أو من مكان ارتكابها.

خامسا: إمكانية كشف التعديل: قد يقول قائل إنه من السهولة – سواء على الجاني أم على غيره من المحققين أو الخبراء المعلوماتيين أثناء عملية جمع الدليل – التلاعب بالأدلة الرقمية أو إتلافها أو إدراج بيانات رقمية أخرى فيها وبسرعة متناهية، لكن هذا القول يرد عليه بأن هذه السهولة يقابلها إمكانية كبيرة لكشف ومعرفة هذا التعديل أو الإتلاف، عن طريق برامج وتطبيقات تقنية خاصة ترصد

---

[1] Myriam Quéméner, Magistrat, Les spécificités juridiques de la preuve numérique (1) AJ Pénal 2014, p. 63.

2 عمر محمد بن يونس، الدليل الرقمي، دار النشر الطبعة الأولى، مصر، د.ن، 2007 م، ص 47.

3 يوسف مومني، طرق إثبات الجريمة المعلوماتية، استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر، ص8، http://www.lawjo.net، تاريخ الدخول 2017/07/27.

4 عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري: الإثبات الجزائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجزائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض 2-1428/11/04هـ، ص 15.

كل المعلومات (حركات الشخص)، حيث أنه إذا كانت البيانات مخزنة في حاسوب أو آلة مشابهة، فأي مخرجات مطبوعة منها أو مخرجات يمكن قراءتها بالنظر إليها، وتعكس دقتها، تعد بيانات أصلية، فالبيانات أو المعلومات المتحصلة من الإنترنت، والتي تم استخراجها بوسيلة ما تعد دليلا أصليا كاملا. الأمر الذي يكشف ما إذا تم العبث بالدليل، وإمكانية المقارنة بين النسخة المعدلة وأصلها، إن وجد.

المطلب الثاني

أنواع وأشكال الدليل الرقمي

أدى الاستخدام الواسع للحاسوب والانتشار السريع لوسائل الاتصال الإلكترونية إلى ازدياد تداول المعلومات والبيانات الإلكترونية في الوسط الافتراضي، والتي يمكن تحميلها أو حفظها أو توثيقها بأوعية متعددة، كالأقراص المغناطيسية، أو الضوئية، أو أقراص الفيديو الرقمية، أو غيرها من الأوعية الإلكترونية، لذلك يتحتم علينا تحديد هذه الأنواع (أولا) وبيان أشكال الدليل الرقمي (ثانيا).

الفرع الأول

أنواع الدليل الرقمي

يظهر الدليل الرقمي في صور وأشكال مختلفة تنبثق عنها أنواع عديدة من الأدلة الرقمية، تختلف باختلاف الزاوية التي ننظر منها إلى الأدلة، وهل هي الغاية منها، أو كيفية تكوينها أو مصدرها.

أولا: الأدلة الرقمية من حيث الغاية: إذا نظرنا إلى الأدلة الرقمية على اعتبار الغاية منها، كنا أمام نوعين من الأدلة الرقمية، أدلة أعدت لتكون وسيلة إثبات، وأدلة لم تعد لهذه الغاية[1]:

أ. **الأدلة المعدة للإثبات:** هذا النوع من الأدلة الرقمية يمكن إجماله في طائفتين، الأولى هي:

1. السجلات التي تم إنشاؤها بواسطة الآلة بشكل تلقائي، وتعد هذه السجلات من مخرجات الآلة التي لم يسهم الإنسان في إنشائها كسجلات الهاتف وفواتير أجهزة السحب الآلي ATM.

[1] طارق الجملي، الدليل الرقمي في مجال الإثبات الجزائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة من 28 الى 2009/10/29، الذي نظمته أكاديمية الدراسات العليا، طرابلس. ص 5 وما يليها.

2. السجلات التي حفظ جزء منها بالإدخال بواسطة الإنسان وجزء آخر تم إنشاؤه بواسطة الآلة ومن الأمثلة على ذلك البيانات التي يتم إدخالها إلى الآلة وتمت معالجتها من خلال برنامج خاص، ومن الأمثلة على ذلك إجراء العمليات الحسابية على بيانات محفوظة بسجلات داخل نظام إلكتروني معين [1].

ب. الأدلة غير المعدة للإثبات: وهذا النوع من الأدلة الرقمية ينشأ من غير إرادة الشخص، أي إنه أثر يتركه الجاني من غير أن يكون راغبا في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، ويمكن تسميته أيضا بالآثار المعلوماتية الرقمية، وهي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها، وكافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية.

والواقع أن هذا النوع من الأدلة لم يعد أساسا للحفظ من جهة من صدر عنه، غير الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة، ولو بعد فترة زمنية من أن نشوئها، فالاتصالات التي تجرى عبر الإنترنت والمراسلات الصادرة عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك. وتبدو أهمية التمييز بين هذين النوعين فيما يأتي:

ت. الأدلة الرقمية التي لم تعد لتكون دليل إثبات: هي الأكثر أهمية من الأدلة التي أعدت لتكون كذلك، لكون هذه الأدلة لم تعد أصلا لتكون أثرا لمن صدرت عنه، ولذا فهي في العادة ستتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها.

يتميز النوع الأول من الأدلة الرقمية بسهولة الحصول عليه، كونه قد أعد أصلا لأن يكون دليلا على الوقائع التي يتضمنها في حين للحصول على الآخر تتبع تقنية خاصة لا تخلو من الصعوبة والتعقيد.

[1] سهى عريقات، الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي، جامعة القدس، كلية الحقوق، دون تاريخ، ص 20 وما يليها.

النوع الأول وكونه أعد للإثبات، عادة ما يعمد إلى حفظه للاحتجاج به لاحقا، وهو ما يقلل من إمكانية فقدانه على عكس النوع الثاني الذي لم يعد ليحفظ، ما يجعله عرضة للفقدان لأسباب عدة منها فصل التيار الكهربائي عن الجهاز مثلا.

ثانيا: أنواع الأدلة الرقمية بالنظر إلى كيفية تكوينها ومصدرها: إذا نظرنا إلى كيفية إنتاج الدليل ومصدره، فإننا نكون أمام نوعين من الأدلة الرقمية هما: نوع ينتجه الحاسوب تحديدا، ونوع آخر يكون الفرد مسؤولا عن تكوينه، حيث تعيش الأدلة في بيئتها الرقمية، وهو ما يطلق عليه الدليل المخزن رقميا، إذ تفيد دلالة البحث في محتوى هذا الدليل أن الفرد هو الذي قام بتكوينه في بيئة تكنولوجيا المعلومات[1].

أ. **الأدلة التي ينتجها الحاسوب:** في هذا النوع يقوم الحاسوب تحديدا بتكوين محتوى الدليل رقميا من غير تدخل الفرد في هذا التكوين، فالدليل هنا يعد من مخرجات حركة البرامج التي يسيطر عليها الحاسوب ذاته حين استقباله للبرمجيات التي تعمل على تشغيله وتفاعله، وليس مستخدم الحاسوب أو مرتكب الجريمة، وفي مجال الإنترنت فإن المسيطر هو مزود خدمات الإنترنت (ISP) تحديدا الذي سمح بدخول الأشخاص إلى الإنترنت والتمتع بخدماته فما تقوم به مخرجات حركة البرامج في جرائم الإنترنت في إطار تكوين الدليل الرقمي أنها تجعل إمكانية قيامه ليست بالمستحيل، ويبقى الأمر بعد ذلك متعلقا بمدى إمكانية قبول الدليل في القانون أو أمام القضاء حسب الأحوال.

ب. **الأدلة التي ينتجها الفرد:** فمن حيث التخزين الإلكتروني فإنه تعبير يحمل على مفهوم تدخل الفرد في تكوين الملف أو مجموعة الملفات التي يتم تخزينها في الحاسوب، لكونه يشكل بنيتها، ذلك أن تخزين البيانات في الحاسوب يأخذ أحد شكلين، إما بيانات يتم استخدامها في شكل معلومات محددة، وإما بيانات يتم تخزينها من غير أن تستخدم، وفي هذه الحالة لا نكون بصدد مساحة مادية في القرص الصلب، وإنما مجرد مجموعة من الأرقام فقط، والمعيار المميز لهذه الملفات عن مخرجات حركة الحاسوب هو التدخل الإنساني، وبشكل مباشر، في تكوينها.

1 عمر محمد بن يونس، الدليل الرقمي، دار النشر، الطبعة الأولى، مصر، 2007، ص 05.

ويلاحظ أن هذا التقسيم ليس مطلقا، وإنما مقيد بعدم وجود تداخل بين منطق عمل مخرجات حركة البرامج وبين التخزين الإلكتروني أو الرقمي، فإذا وجد مثل هذا التداخل، فإن الأمر لا يعدو سوى مزجا ظاهريا من حيث تكوين الدليل الرقمي، ومثال ذلك أن يعطي شخص أمرا لبريده الإلكتروني باستمرار بث رسالة معينة تتضمن تشهيرا يمس إحدى الشخصيات، ففي هذه الحالة نكون بصدد بث لتخزين قائم مسبقا بطريقة نظام مخرجات حركة البرامج، إلا أنه يجب ألا ننسى أن مضمون الرسالة كتبها الشخص المذكور[1].

من مخرجات حركة البرامج التي يسيطر عليها الحاسوب ذاته حين استقباله للبرمجيات التي تعمل على تشغيله وتفاعله، وليس مستخدم الحاسوب أو مرتكب الجريمة، وفي مجال الإنترنت فإن المسيطر هو مزود خدمات الإنترنت تحديدا الذي سمح بدخول الأشخاص إلى الإنترنت والتمتع بخدماته فما تقوم به مخرجات حركة البرامج في جرائم الإنترنت في إطار تكوين الدليل الرقمي أنها تجعل إمكانية قيامه ليست بالمستحيل، ويبقى الأمر بعد ذلك متعلقا بمدى إمكانية قبول الدليل في القانون أو أمام القضاء حسب الأحوال.

ويأخذ المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب الصادر في عام 2002 بالتقسيم السابق لنوعي الأدلة الرقمية، إذ يميز بين نوعين من السجلات، نوع مخزن في الحاسوب، ويتمثل في الوثائق الإلكترونية التي تحتوي على كتابات عائدة لشخص ما، كرسائل البريد الإلكتروني، وملفات الوورد، ورسائل غرف الدردشة على الإنترنت، ونوع يؤخذ من الحاسوب، وهي نتائج برامج الحاسوب التي لا تمسها الأيدي البشرية، كسجلات الدخول إلى الإنترنت، وسجلات الهاتف، وإيصالات الصراف الآلي وغيرها، هذه السجلات هي نتائج البرامج الحاسوبية، وهذا النوع من السجلات يمكن للمحاكم أن تأخذ به، إذا كان برنامج الحاسوب يؤدي عمله على نحو جيد وسليم[2].

1 عمر محمد بن يونس، الدليل الرقمي، دار النشر، الطبعة الأولى، مصر، 2007، ص06.

2 طارق عبد الرؤوف الخن، الجريمة المعلوماتية، منشورات الجامعة الافتراضية السورية، 2010-2011، ص 133.

الفرع الثاني

أشكال الدليل الرقمي

إن الدليل الرقمي المستمد من الحاسوب أو الإنترنت قد يظهر في أشكال وهيئات عديدة، منها الصور الرقمية، المحررات الإلكترونية، والتسجيلات الصوتية.

أولا: الصور الرقمية: وهي تتجسد في الحقائق المرئية حول الجريمة، وفى العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية، وإذا كانت الصورة الرقمية تمثل تقنية بديلة للصورة الفوتوغرافية التقليدية، وقد تبدو أكثر تطورا، إذا ما قورنت بها، لكنها ليست بالضرورة أفضل منها [1].

وتتجه العديد من الدول ولا سيما الغربية منها، إلى استخدام المراقبة الإلكترونية، في الشوارع العامة والأسواق الكبيرة، وأجهزة الصراف الآلي، والمطارات، وذلك عن طريق وضع كاميرات فيديو رقمية توظف في كشف الجرائم وإثباتها، والذي أصبح أمرا ملحا، إذ بالإضافة إلى كون الصور المسجلة في كاميرات المراقبة أداة وقاية من حوادث السرقة والسطو والتحرش وغيرها من الجرائم، فإنها تعد أداة ضبط ودليل إثبات ضد مرتكبي هذه الجرائم.

ثانيا: المحررات الإلكترونية: وهي النصوص التي يتم تحريرها بواسطة الآلة الرقمية، كرسائل البريد الإلكتروني والهاتف المحمول، والبيانات المسجلة بأجهزة الحاسوب، والأوعية الإلكترونية المتضمنة للمعلومات كالأقراص الممغنطة [2]، ومنها – أيضا – المخرجات الورقية المتضمنة المعلومات الموجودة على الحاسوب، ويستخدم في ذلك الطابعات، ومنها عرض المعلومات والبيانات المعالجة آليا، والمتعلقة بالدليل الرقمي عن طريق شاشة الحاسوب.

وقد استخدم الحاسوب في مجال تخزين المعلومات الجزائية بهدف استرجاعها، أو تحليلها مستقبلا وعند الحاجة كالمعلومات المتعلقة بأوصاف المشتبه بهم الذين يجري البحث عنهم، ونبذة شخصية عن تخصصاتهم الإجرامية، وفي أثناء التحقيق أو المحاكمة يتم البحث في هذه المعلومات المخزنة، للحصول على نتائج تتعلق بتحديد الهوية القضائية، وطباعة صورة الشخص المشكوك في أوصافه عن طريق الطابعة الملحقة بالحاسوب

1 عمر محمد بن يونس، الدليل الرقمي، دار النشر، الطبعة الأولى، مصر، 2007، ص 6.

2 احمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد العاشر، العدد الأول، ص 486-487.

واستعراضها في صورة محرر إلكتروني يظهر على الشاشة [1]، وبذلك تعد المحررات الإلكترونية شكلا من أشكال الأدلة الرقمية، والتي يمكن أن تقود إلى برهان صحة الواقعة أو الوقائع موضوع التحقيق أو الحكم.

وفي دول العالم المتقدم جرى العمل على الاستعانة بالشهادات الإلكترونية، والتي تتم عبر وسائل إلكترونية من خلال شبكة الإنترنت مثلا، عندما يتعذر على الضحية أو الشاهد، ولا سيما إذا كان طفلا، الإدلاء بشهادته في المكان الذي يوجد فيه المتهم، وهو مكان انعقاد المحكمة، وهو ما يحصل أيضا في جرائم الاعتداء الجنسي على الأطفال، وهناك كذلك الاعتراف الإلكتروني، سواء أكان مخزنا في ذاكرة الحاسوب الرئيسة أم متداولا عبر شبكات الحاسوب، والذي يتم إرساله عبر البريد الإلكتروني إلى شخص آخر أو إلى السلطات القضائية عبر الشات عند استجوابه عن بعد، أو عبر البريد الإلكتروني.

ثالثا: التسجيلات الصوتية: وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الإنترنت والهاتف وغيرهما[2].

[1] جميل عبد الباقي الصغير، أدلة الإثبات الجزائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، دون طبعة، 2002، ص 96.

[2] جميل عبد الباقي الصغير، المرجع السابق، ص 96.

الفصل الثاني

الطبيعة القانونية للدليل الرقمي

في التشريع الجزائري

أصبح من الضروري مواكبة التطور التكنولوجي من خلال تكييف الإطار القانوني ليستوعب خصوصيات الدليل الرقمي وما يطرحه من إشكاليات تتعلق بإجراءات جمعه، مشروعيته، حجيته، ومدى قبوله والاقتناع به.

يناقش من خلال هذا الفصل الطبيعة القانونية للدليل الرقمي في التشريع الجزائري، بالتركيز على إجراءات الحصول عليه، مدى قبول هذا النوع من الأدلة في الإجراءات الجزائية، وموقف المشرع من مشروعية الحصول عليه، بالإضافة إلى الاستثناءات التي تطرأ على قاعدة حرية الإثبات وما يترتب عن مخالفة هذه القواعد من جزاءات إجرائية. كما يعالج الفصل الضوابط التي يجب أن تحكم قناعة القاضي عند الأخذ بالدليل الرقمي، من حيث ضرورة مناقشته علنا، وتحقيق اليقين القضائي بشأنه، ووجوب تسبيب الحكم استنادا إليه.

تناول هذا الفصل الطبيعة القانونية للدليل الرقمي في التشريع الجزائري من خلال مبحثين رئيسيين:

المبحث الأول: إجراءات جمع الدليل الرقمي، والذي يتضمن الإجراءات العامة والخاصة لجمع الدليل الرقمي، بالإضافة إلى صعوبات استخلاصه.

المبحث الثاني: قبول الدليل الرقمي أمام القضاء الجزائي وضوابط اقتناع القاضي به، حيث يتم التطرق فيه قبول الدليل الرقمي أمام القضاء الجزائي، وكذا ضوابط اقتناع القاضي الجزائي بالدليل الرقمي.

وهذا بهدف تقديم تصور متكامل حول الوضع القانوني للدليل الرقمي في الجزائر، وإبراز مدى تكامل المبادئ العامة للإثبات مع الطبيعة التقنية الخاصة لهذا النوع من الأدلة، وذلك بغية تحقيق التوازن بين مصلحة العدالة الجنائية واحترام الحقوق والحريات الأساسية للأفراد.

المبحث الأول

إجراءات جمع الدليل الرقمي

يشكل التطور السريع في أنواع وأساليب ووسائل ارتكاب الجرائم الإلكترونية تحديا مستمرا للجهات المكلفة بمكافحتها، مما يضعها في سباق دائم مع الزمن لمواكبة هذه المستجدات. كما يستوجب ذلك

من السلطات القضائية إعادة النظر في آليات التعامل مع هذه الجرائم، إذ أن الإجراءات التقليدية غالبا ما تفتقر إلى الفاعلية في مواجهتها، نظرا للطبيعة غير المادية لهذه الجرائم وصعوبة استحضار الأدلة المادية التقليدية.

وعليه سنتناول مبحث إجراءات جمع الدليل الرقمي من خلال التطرق إلى الإجراءات العامة لجمع الدليل الرقمي (المطلب الأول)، ثم إلى الإجراءات الخاصة لجمع الدليل الرقمي وصعوبات استخلاصه (المطلب الثاني).

المطلب الأول

الإجراءات العامة لجمع الدليل الرقمي

تسمى هذه الاجراءات بالإجراءات العامة نظرا لأهميتها وضرورتها في كشف الجرائم التقليدية وجمع الادلة المرتبطة بها، كما تظل ذات الاهمية نفسها في مجال الجرائم الالكترونية. وقد نظم المشرع الجزائري طرق استنباط هذه الاجراءات تحقيقا لهذه الغاية، ومن أبرزها التي نص عليها القانون المعاينة، التفتيش، الضبط، سماع الشهود، وندب الخبراء[1]، يرى بعض الفقه أن لهذه الاجراءات دورا محدودا في بيئة تكنولوجيا المعلومات كما سيتضح لاحقا، إذ أن الشهادة مثلا لا يمكن تصورها كدليل مباشر على السلوك المكون للجريمة الالكترونية نظرا لطبيعة هذه الجرائم التي تعتمد على التلاعب

1 عائشة بن قارة، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن دار الجامعة الجديدة، الإسكندرية، مصر، 2010، ص 78.

بالبيانات والانظمة والبرامج، والتي لا يمكن للغير ملاحظتها أو إدراكها بشكل مباشر ليشهدوا بها امام القضاء. كما أن مجرد الاعتراف الذي يتم الحصول عليه عبر الاستجواب لا يكفي في مثل هذه الجرائم التقنية ما لم يكن مدعوما بأدلة اخرى. بالإضافة الى ذلك، تتطلب هذه الجرائم خبرة تقنية عالية يجب ان يمتلكها الخبير المكلف بتقديم الرأي الفني.

الفرع الأول

المعاينة في البيئة الإلكترونية.

المعاينة هي إجراء ينتقل بمقتضاه القائم بالتحقيق إلى مسرح الجريمة ليطلع بنفسه على الملابسات ويجمع الآثار الناتجة عن الجريمة وطريقة وقوعها، بالإضافة إلى جمع الأشياء الأخرى التي قد تفيد في كشف الحقيقة وإثبات الجريمة [1].

وتكمن أهمية المعاينة في فاعليتها في التحقيق، كما أن المعاينة تتم لمسرح الجريمة بما يحتويه من آثار مادية، وتهدف كإجراء، إلى التحفظ على الأدلة تمهيدا لفحصها من قبل جهات التحقيق لاستخلاص الدلائل والقرائن لإثبات ارتكاب الجاني لجريمته.

يقصد بمعاينة مسرح الجريمة الإلكترونية معاينة الآثار التي يتركها مستخدم الإنترنت، والتي تشمل الرسائل المرسلة أو المستقبلة، وجميع الاتصالات التي تمت عبر الحاسوب وشبكة الإنترنت. ويلاحظ أن الآثار الرقمية المستخلصة من أجهزة الحاسوب قد تكون ذات فائدة كبيرة لما تحويه من معلومات دقيقة تساعد في كشف الحقيقة.

وبالتالي، فإن صفحات المواقع الإلكترونية، والبريد الإلكتروني، والفيديو الرقمي، وغرف الدردشة والمحادثة، والملفات المخزنة في الحاسوب الشخصي، جميعها تشكل وسائط يمكن أن تحتوي على أدلة مهمة تسهم بشكل كبير في كشف الحقيقة بشأن الجريمة محل التحقيق.

1 مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، دار النهضة العربية، القاهرة، مصر، بدون طبعة، سنة 2003، ص 639.

الفرع الثاني

التفتيش

بصفة عامة التفتيش هو إجراء من إجراءات التحقيق يهدف إلى الكشف عن الحقيقة من خلال البحث عن الأدلة المتعلقة بجريمة وقعت فعلا ويجري التحقيق بشأنها. ولا يعد التفتيش من إجراءات البحث والتحري عن الجرائم التي لم يتم التأكد من وقوعها. ويقصد به دخول المساكن والأماكن التابعة لأشخاص يشتبه

في مساهمتهم في الجريمة أو حيازتهم لأوراق أو أشياء ذات صلة بالأفعال المجرمة، ويتم ذلك من قبل الضبطية القضائية أو القضاة، إما برضا أصحابها أو قسرا، وذلك وفقا لما نصت عليه المادة 44 من ق.إ.ج.ج.

يعد التفتيش من إجراءات التحقيق ذات الخطورة الخاصة، نظرا لأنه يمس حق الإنسان في الخصوصية. وبناء على ذلك، أحاط المشرع هذا الإجراء بمجموعة من الضمانات لحماية حقوق المتهم، ويترتب على عدم احترام هذه الضمانات بطلان إجراءات التفتيش.

عاقب المشرع الجزائري على الاعتداءات التي تمس بسلامة المعالجة الآلية للمعطيات، حيث جرم العديد من الأفعال التي تشكل بمختلف صورها الجريمة الالكترونية، وذلك بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، والذي تم من خلاله استحداث القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

ومسايرة للتطورات، أصدر المشرع الجزائري القانون رقم 09-04 المؤرخ في 08 اوت 2009، والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال مكافحتها، حيث نص في المادة 5 منه على جواز تفتيش منظومة معلوماتية او جزء منها، وكذلك المعطيات المعلوماتية المخزنة فيها [1].

[1] قانون 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 05 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، الصادرة بتاريخ 16 أوت 2009.

الفرع الثالث

الضبط

إن الغاية من التفتيش هي ضبط الادلة المادية التي تفيد في كشف الحقيقة، ولذلك فإن ضبط الاشياء المتعلقة بالجريمة يعد الأثر المباشر للتفتيش. وبناء على ذلك، فإن غالبية التشريعات تجمع بين احكام الضبط والتفتيش في موضوع واحد، غير أن ذلك لا يعني أن الضبط لا يتم إلا نتيجة للتفتيش، إذ يمكن أن يكون الضبط ناتجا عن إجراء آخر مثل المعاينة.

والضبط في نطاق قانون الإجراءات الجزائية يقصد به الحصول على أشياء لها صلة بجريمة وقعت وتفيد في كشف حقيقتها ونسبتها إلى المتهمين. غير أن الضبط في الجريمة الإلكترونية يختلف عن الضبط في الجرائم التقليدية من حيث المحل، إذ إن الأول يرد على أشياء ذات طبيعة معنوية مثل البيانات، المراسلات، والاتصالات الإلكترونية، في حين أن الثاني يرد على أشياء مادية سواء كانت منقولة أو عقارات. وقد أثارت هذه الطبيعة المعنوية للبيانات جدلا فقهيا واختلافا تشريعيا حول مدى إمكانية ضبطها، خاصة إذا كانت مجردة من أي دعامة مادية مثبتة عليها، ويرجع ذلك إلى أن الضبط بحسب الأصل لا يرد إلا على الأشياء المادية [1].

الفرع الرابع

الشهادة

الشهادة هي الأقوال التي يدلي بها أشخاص من غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء تعلقت بإثبات الجريمة وظروف ارتكابها أو بإسنادها إلى متهم أو نفيها عنه. وتكتسي الشهادة في مجال الإجراءات أهمية كبيرة، ذلك أن الجريمة ليست تصرفا قانونيا علنيا، بل هي عمل غير مشروع يسعى الجاني عادة إلى إخفائه والتكتم عليه، مما يجعل العثور على شاهد عيان يمثل مكسبا مهما للعدالة.

[1] عائشة بن قارة، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن دار الجامعة الجديدة، الإسكندرية، مصر، 2010، ص 144.

ولا تقل الشهادة اهمية في الجريمة الالكترونية عن باقي الاجراءات في الحصول على الدليل الرقمي، اذ تقضي القاعدة العامة بأن يلتزم الشاهد بالإدلاء بكل ما يعلمه من معلومات تتعلق بواقعة الجريمة والاشخاص المتورطين فيها، وكذا تقديم اي وقائع اخرى من شأنها ان تفيد في كشف الحقيقة [1].

الفرع الخامس

الخبرة

إذا كان التحقيق يهدف إلى الوصول إلى الحقيقة، فإن هذا الهدف قد تعترضه مسائل فنية لا يملك المحقق الكفاءة اللازمة للفصل فيها أو التعامل معها، نظرا لأنها تتطلب مهارات وقدرات خاصة قد لا تكون متوفرة لديه. ولهذا السبب، تبرز الحاجة إلى الاستعانة بخبير أو أكثر من أهل الاختصاص لبيان مسألة معينة أو أكثر قد تطرأ أثناء سير التحقيق، تعد الخبرة إحدى وسائل الإثبات في المواد الجزائية، وقد ازدادت أهميتها في ظل التطور العلمي المتسارع، إلى درجة أن بعض الآراء تعتبر أن الخبير أصبح بمثابة القاضي الفعلي، نظرا لدوره الحاسم في تحليل القضايا المعقدة التي تتطلب معرفة فنية أو علمية دقيقة. ولم يعد من الممكن تجاهل النتائج التي يقدمها العلم، والتي غالبا ما تكون فاصلة في النزاعات المطروحة أمام القضاء.

فالخبير، وإن كان عالما أو متخصصا في مجال معرفي معين، إلا أن ما يميز عمله هو تطبيقه لهذه المعرفة على واقعة محددة مرتبطة بالقضية، وليس مجرد استعراض للنظريات العامة. وعليه أن يقدم أجوبة واضحة ومحددة حول المسائل التي يطلب منه النظر فيها، وأن يتخذ موقفا يستند إلى خبرته العلمية. لذلك، لا يكفي أن يقدم تقريرا فنيا يحتوي على معلومات نظرية فقط، بل يجب أن يتضمن تحليلا موضوعيا ورأيا صريحا يساعد الجهة القضائية في الوصول إلى الحقيقة.

فالخبرة بوجه عام تعد علما متطورا يتماشى مع التقدم العلمي والتكنولوجي في مختلف الميادين، وهو ما يفرض الاستعانة بذوي الاختصاص لفهم الجوانب الفنية المعقدة التي قد تعترض التحقيق. كما أن الخبرة تمثل فنا يقوم على المزج بين ما هو تقني وعلمي وما هو قانوني، وهو عمل

[1] عائشة بن قارة، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن دار الجامعة الجديدة، الإسكندرية، مصر، 2010، ص 126.

لا يمكن لأي شخص القيام به، بل يتطلب توفر الخبير على معرفة عميقة بالمجالين معا، حتى يتمكن من إعداد تقرير متكامل ومنسجم يساهم بفعالية في كشف الحقيقة.

يقصد بها إبداء رأي فني من شخص مختص في شأن واقعة ذات أهمية في الدعوى الجزائية. وبقدر تنوع مجالات الحياة وتداخلها، يزداد تنوع مجالات الخبرة، وبقدر اختلاف القضايا المعروضة أمام المحاكم، تتنوع المهام المسندة للخبراء.

تعد الخبرة التقنية من أهم أدوات التفاعل القانوني القضائي مع ظاهرة الحوسبة والرقمية، حيث تلعب دورا أساسيا في تعويض نقص المعرفة القضائية الشخصية بظاهرة الإنترنت. هذا يعني أن القضاء يتعامل مع الواقع سواء في صورته التقليدية أو المتطورة، كما أن الظواهر الجديدة، رغم تدخل القانون لوضع حلول لها، يبقى للدور القضائي في تفسير النصوص القانونية أهمية كبيرة. ولأداء هذا الدور بفعالية، يجب أن يتوافق القضاء مع طبيعة التقنية بعيدا عن الافتراضات، مما يجعل الخبرة التقنية في مجال الإنترنت أداة رئيسية في تكوين الحكم الجنائي [1].

هذا النوع المتخصص من الخبرة بدأ يأخذ مكانة بارزة في إثبات الجرائم الإلكترونية، حيث يعرف في الفقه المقارن بمصطلح المعلوماتية الشرعية. وتعني المعلوماتية الشرعية استخدام الأساليب العلمية لجمع وتحليل وتسيير الأدلة الرقمية المأخوذة من مصادر رقمية، بالإضافة إلى الاحتفاظ بها وتوثيقها بشكل يسهل إعادة بناء وقائع القضية وكشف الجريمة. وتعد المعلوماتية الشرعية عملية بحث يقوم بها الخبير المعلوماتي بهدف الحصول على الأدلة الرقمية اللازمة لتوضيح مجريات القضية أمام المحكمة [2].

لا شك أن الخبرة تعد من أهم العوامل المساعدة لسلطات التحقيق في التعامل مع الوقائع الإجرامية، وذلك للحفاظ على الأدلة ومنع إتلافها. ولا تختلف الخبرة المطلوبة في الجرائم التقليدية عن تلك اللازمة في الجرائم المعلوماتية، سواء من حيث القواعد المنظمة لها أو نوعية الخبير المنتدب. ينبغي أن يكون الخبير على دراية بنظم الحاسوب، فالقاضي عند الاستعانة بالخبرة في مسألة تخص القضية المعروضة أمامه، يسعى لاختيار الخبير وفق تخصصه، ويخضع مجال التخصص لقاعدة طبيعية تعتمد

[1] عمر محمد بن يونس، الدليل الرقمي، دار النشر، الطبعة الأولى، مصر، 2007، ص 110

[2] طارق عبد الرؤوف الخن، الجريمة المعلوماتية، منشورات الجامعة الافتراضية السورية، 2010-2011، ص 331

على التحصيل العلمي المنهجي، كما هو الحال في دراسة الطب أو الهندسة أو العلوم الفنية المتصلة بالجريمة مثل علم البصمات وعلوم الصيدلة.

المطلب الثاني

الإجراءات الخاصة لجمع الدليل الرقمي

لم تسلم طرق الإثبات من تأثيرات ثورة المعلومات وتكنولوجيا الاتصالات، فالتناغم المطلوب تحقيقه دائما بين طبيعة الدليل وطبيعة الجريمة التي يولد منها ويصلح لإثباتها، أفرز إلى حيز الوجود طرقا إجرائية تتناسب والطبيعة التقنية للجريمة المعلوماتية وللدليل الرقمي، ولاستخلاصه يتم الاعتماد على إجراءات خاصة تستند إلى توظيف تقنية المعلومات في جمع هذا النوع من الأدلة. وفي هذا السياق، كرس المشرع الجزائري عدة آليات تشريعية لمكافحة الجريمة المعلوماتية، من أبرزها ما تضمنه القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-155 المتضمن ق.إ.ج.ج، حيث استحدث إجراءي التسرب واعتراض المراسلات. كما أضاف القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إجراءين آخرين هما مراقبة الاتصالات الإلكترونية، وتسجيل الأصوات والتقاط الصور.

الفرع الأول

مراقبة الاتصالات الإلكترونية

نص المشرع الجزائري على هذا الإجراء في ق.إ.ج.ج في صورة الترصد الإلكتروني في المواد من 65 مكرر إلى 65 مكرر 10 متمثل في الأعمال التالية:[1]

اعتراض المراسلات وتسجيل الأصوات والتقاط الصور حيث يلجأ لهذا الإجراء متى اقتضت ضرورات التحري والتحقيق في الجرائم الخطيرة منها الجريمة الالكترونية وذلك مع ضرورة مراعاة مجموعة من الشروط القانونية، من أهمها الحصول على إذن كتابي مسبق من وكيل الجمهورية أو قاضي التحقيق، حسب الجهة المختصة. كما يشترط

[1] المادة 65 مكرر 10، قانون 06- 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر 66-155 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 84، الصادرة بتاريخ 24 ديسمبر 2006، ص 04.

أن تتم هذه العمليات تحت رقابة السلطة القضائية المختصة، مع اتخاذ الترتيبات التقنية اللازمة لتسجيل الكلام والتقاط الصور، وذلك لمدة لا تتجاوز أربعة (04) أشهر، قابلة للتجديد وفقا لمقتضيات التحقيق [1].

أولا: تعريف مراقبة الاتصالات الإلكترونية: تعرف على أنها هي العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع المعطيات والمعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته، مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر، يشبه لحد بعيد ما تضمنته المواد السالفة الذكر في ق.إ.ج.ج.

المقصود بالاتصالات الالكترونية: يقصد بها إرسال، أو استقبال علامات، أو إشارات، أو كتابات أو صور أو معلومات مختلفة بواسطة أي وسيلة الكترونية (المادة 2 من القانون 09-04).

ثانيا: حالات اللجوء للمراقبة الالكترونية وضوابطها: لا يكمن اللجوء لإجراء المراقبة الإلكترونية إلا إذا توفرت حالاتها.

أ. **حالات اللجوء للمراقبة الإلكترونية:** نصت المادة 4 من القانون رقم 09-04 على حالات خاصة تبرر اللجوء إلى بعض الإجراءات الاستثنائية، وتتمثل هذه الحالات في الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب، أو تلك التي تمس بأمن الدولة. ويلاحظ أن المشرع الجزائري قد فعل في هذا الإطار أحد مستويات السياسة الجنائية، وهو المستوى الوقائي، إلى جانب المستويين التجريمي والعقابي [2].

وتتخذ هذه الإجراءات الاستباقية عندما تتوافر معلومات تفيد باحتمال وقوع اعتداء يستهدف المنظومة المعلوماتية على نحو من شأنه تهديد النظام العام، أو الدفاع الوطني، أو مؤسسات الدولة، أو الاقتصاد الوطني، أو عندما تقتضي ذلك التحريات أو التحقيقات القضائية، أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

---

[1] حاحة عبد العالي، الآليات القانونية لمكافحة الفساد الإداري في الجزائر، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة بسكرة، 2013/2012، ص268.

[2] المادة 4، قانون 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 05 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، الصادرة بتاريخ 16 أوت 2009، ص 05.

ب. **ضوابط المراقبة الإلكترونية من خلال القانون رقم 09-04:** تتمثل الإجراءات المنصوص عليها في هذا السياق في ضرورة الحصول على إذن مسبق من النائب العام لدى مجلس قضاء الجزائر، ويتم ذلك بناء على تقرير مفصل يتضمن طبيعة الترتيبات التقنية المستخدمة والأغراض الموجهة لها.

كما يشترط أن تسند عملية تنفيذ المراقبة فقط لضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، دون أن يسمح لأي جهة أخرى بالقيام بها، تأكيدا على الطابع المتخصص والدقيق لهذا النوع من الإجراءات.

وبالنسبة للمدة تم تحديدها بستة (6) أشهر قابلة للتجديد وهذا عندما يتعلق الأمر بالحالة الأولى المتمثلة في الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

وعليه، تجدر الإشارة إلى أن التصدي للجرائم الإلكترونية يستوجب تفعيل مبادئ سريان القانون الجزائي من خلال تعزيز التعاون الدولي، إذ لا يمكن للدول، لا سيما النامية منها، مجابهة هذا النوع من الجرائم بمفردها. وقد كرس المشرع الجزائري هذا التوجه في القانون رقم 09-04، حيث نص في مادته 16 على إمكانية اللجوء إلى المساعدة القضائية الدولية المتبادلة، والتي يمكن أن تتم، في الحالات المستعجلة، عبر وسائل الاتصال السريع كالفاكس أو البريد الإلكتروني. غير أن هذه المساعدة تخضع لجملة من القيود نصت عليها المادة 18 من ذات القانون، منها: احترام السيادة الوطنية، الحفاظ على سرية المعلومات المتبادلة، وعدم استعمالها إلا في نطاق ما ورد في الطلب. وتظهر مظاهر التعاون الدولي في عدة صور منها: تبادل المعلومات وهذا حسب المادة 17، بتقديم الوثائق والبيانات اللازمة، نقل الإجراءات الجزائية من دولة إلى أخرى بموجب اتفاقيات دولية [1]، والإنابة القضائية وفق المواد من 721 إلى 725 من ق.إ.ج.ج، بالإضافة إلى تسليم المجرمين، في ظل تحول المجرم الإلكتروني إلى مجرم دولي[2].

[1] المواد 16، 17 و18، قانون 09-04 مؤرخ في 14 شعبان 1430 الموافق 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، الصادرة بتاريخ 16 أوت 2009، ص05.

[2] المواد 721 -725 الأمر رقم 66-155 مؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 يتضمن قانون الإجراءات الجزائية.

الفرع الثاني

اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

سعى المشرع الجزائري إلى تعزيز آليات مكافحة الجرائم الخطيرة، لا سيما تلك المرتكبة من طرف الشبكات الإجرامية المنظمة التي تعتمد على تقنيات حديثة تتسم بالسرعة والفعالية. وفي هذا الإطار، عمل على إدراج الوسائل التقنية ضمن وسائل البحث والتحري في التحقيقات الجنائية الخاصة بهذا النوع من الجرائم.

وقد تم تنظيم هذه الوسائل والإجراءات في قانون الإجراءات الجزائية، تحديدا في المواد من 65 مكرر 5 إلى 65 مكرر 10 [1]، حيث أجاز المشرع لضباط الشرطة القضائية وأعوانهم، إذا اقتضت الضرورة، اللجوء إلى هذه الوسائل التقنية في الجرائم المتلبس بها، إضافة إلى بعض الجرائم الأخرى، وذلك بموجب إذن مسبق من وكيل الجمهورية أو قاضي التحقيق، كل حسب اختصاصه.

أولا: اعتراض المراسلات: اعتراض المراسلات هو إجراء من إجراءات التحقيق يتم بصفة سرية ويمس بسرية الأحاديث والاتصالات الخاصة، تأمر به السلطة القضائية وفق الشروط والإجراءات التي يحددها القانون، ويهدف إلى الحصول على دليل غير مادي يتعلق بجريمة ثبت وقوعها. ويتضمن هذا الإجراء استراق السمع لمحتوى المراسلات أو المحادثات، وتسجيلها على وسائط مخصصة لذلك، باستعمال أجهزة تقنية معدة لهذا الغرض.

وهنا يفرق الفقه بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، الأول يكون دون رضا المعني والثاني بطلب أو رضا صاحب الشأن ويخضع لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك.

حدد المشرع الجزائري في الفقرة الثانية من المادة 65 مكرر 05 من ق.إ.ج.ج نوع المراسلات التي يجوز اعتراضها، وهي تلك التي تتم عبر وسائل الاتصال السلكية واللاسلكية. وقد نص القانون رقم 09-04

[1] المواد 65 مكرر 5 – 65 مكرر 10، قانون 06- 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر 66-155 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 84، الصادرة بتاريخ 24 ديسمبر 2006، ص 04.

صراحة على جواز اعتراض هذا النوع من المراسلات، وأجاز أيضا اتخاذ الترتيبات التقنية اللازمة لمراقبة الاتصالات الإلكترونية، بالإضافة إلى التفتيش والحجز داخل المنظومة المعلوماتية، وذلك في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" [1].

ثانيا: تسجيل الأصوات والتقاط الصور: لم يعرف المشرع الجزائري تسجيل الأصوات وبالرجوع إلى نص المادة 65 مكرر 05 ق.إ.ج.ج، نستشف أن المقصود من تسجيل الأصوات هو وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به، بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عامة.

أما بالنسبة لالتقاط الصور كذلك لم يعرف المشرع الجزائري هذه العملية صراحة، إلا أنه أشار إليها بلفظ "**الالتقاط**" وتعرف على أنها تلك العملية التقنية التي تتم دون موافقة المعنيين من أجل التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

وتجدر الإشارة أن المشرع عندما جمع بين اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في عنوان واحد، بحكم أن هذه التقنيات تؤدي إلى نفس الغرض متى توافرت الضمانات المنصوص عليها في المواد من 65 مكرر 5 إلى غاية 65 مكرر10 ق إ ج.[2]

ثالثا: إجراءات وشروط اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: إن المشرع الجزائري ولضرورة التحقيق في بعض الجرائم الحساسة سمح بالقيام بمثل هذه العمليات، إذ فضل مصلحة التحقيق وكشف المجرمين عن حرمة المساس بالحياة الخاصة، وفقا لأحكام المواد من 65 مكرر 5 الى غاية 65 مكرر 10 ق إ ج، كما أتاح للضبطية القضائية حق استعمال الأساليب والوسائل التقنية في إطار البحث والتحري في الجرائم المستحدثة وفقا للشروط والإجراءات التالية:

[1] قانون 09-04 مؤرخ في 14 شعبان 1430 الموافق 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، الصادرة بتاريخ 16 أوت 2009، ص 05.

[2] المواد 65 مكرر 5- 65 مكرر 10، قانون 06- 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر 66-155 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 84، الصادرة بتاريخ 24 ديسمبر 2006، ص 04.

أ. **طبيعة الجريمة:** نصت المادة 65 مكرر 5 ق إ ج على إجراءات التحري والتحقيق الخاصة بحالة التلبس أو التحقيق الابتدائي في جرائم المخدرات، والجريمة المنظمة العابرة للحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية، وجرائم تبييض الأموال، وجرائم الإرهاب، وجرائم الصرف وجرائم الفساد إذا اكتشفت أثناء التحريات الخاصة جرائم أخرى غير مذكورة في الإذن فهذا لا يكون سببا لبطلان الإجراءات العارضة وفقا للأحكام المادة 65 مكرر 6 ف2 ق.إ.ج.ج [1].

ب. **أن يكون الإذن صادر من وكيل الجمهورية أو قاضي التحقيق:** وهو شرط أساسي لمباشرة عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ويشترط لصحته أن يكون مكتوبا ويتضمن جميع المعلومات المكونة للجريمة، مع تحديد المدة الزمنية للعملية بأربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري، حيث "يتعين على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم وأن يبادروا بغير تمهل الى اخطار وكيل الجمهورية بالجنايات أو الجنح التي تصل الى علمهم"، وهذا حسب المادة 18 ف 1 من ق.إ.ج.ج.

ت. **الرقابة القضائية:** يجب خضوع هذه العمليات المسموح بها قانونا إلى رقابة وكيل الجمهورية المختص، وفي حالة فتح تحقيق قضائي فإن هذه العمليات يكون قاضي التحقيق صاحب السلطة لإصدار الإذن وتحت رقابته.

ث. **وضع التقنية:** بعد الحصول على الإذن يسمح لضابط الشرطة القضائية بوضع الترتيبات التقنية في الأماكن الخاصة والعمومية وغيرها دون موافقة وعلم الأشخاص المعنيين، وهذا للمحافظة على سرية العملية، كما أجاز المشرع أن تكون هذه الترتيبات خارج المواعيد المحددة

[1] المادة 65 مكرر 6 ف2 قانون 06- 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر 66-155 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 84، الصادرة بتاريخ 24 ديسمبر 2006، ص 04.

في نص المادة 47 من ق.إ.ج.ج [1]، والتي تنص على ألا يجوز البدء في تفتيش المساكن قبل الساعة الخامسة (05) صباحا، ولا بعد الساعة الثامنة مساء، إلا في حالات استثنائية نذكر منها:

- إذا طلب صاحب المنزل ذلك.
- إذا وجهت نداءات من الداخل.
- أو في الأحوال الاستثنائية المقررة قانونا.

ج. **الإطار المكاني للأساليب التقنية في التحري عن الجرائم:** بالرجوع إلى المادة 65 مكرر 5 من ق.إ.ج.ج، حددت الأماكن التي يتم فيها استعمال الوسائل التقنية وهي الأماكن العمومية وهي التي تتم الدخول اليها والخروج منها بحراسة تامة كالأسواق، والأماكن الخاصة كالفنادق والعيادات، وكذا المحلات السكنية.

ح. **المحافظة على السر المهني:** يلزم على الضبطية القضائية أثناء أداء مهامهم أو وظيفتهم بكتمان السر المهني الذي اطلعوا عليه سواء كان عن طريق تسجيل الأصوات أو التقاط الصور خاصة إذا تعلق الأمر بأماكن يشغلها أشخاص ملزمون بكتمان السر المهني مثل مكاتب المحامين أو الموثقين أو إذا تعلق الأمر بأشخاص يحملون أسرار مهنية مثل القضاة والأطباء.

خ. **تسخير الأعوان المؤهلين والمكلفين بالمواصلات السلكية واللاسلكية:** أجاز المشرع لوكيل الجمهورية أو ضباط الشرطة القضائية الذي أذن له باستعمال الوسائل الخاصة في البحث والتحري ولقاضي التحقيق أو ضباط الشرطة القضائية الذي ينوبه أن يكلف عون مؤهل وصاحب خبرة وكفاءة في مجال المواصلات السلمية واللاسلكية بالتكفل بالجوانب التقنية لعمليات اعتراض المراسلات وتسجيل الصوات، وهذا ما جاء في نص المادة 65 مكرر 8 من ق.إ.ج.ج.

د. **تحرير محضر عن العملية:** كمبدأ عام يجب على ضباط الشرطة القضائية تحرير تقارير عن كل عملية تطبيقا لنص المادة 65 مكرر 09 من ق.إ.ج.ج، أنه "يجب تحرير محضر يذكر فيه جميع

[1] المادة 47، الأمر رقم 66-155 مؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 يتضمن قانون الإجراءات الجزائية.

التفاصيل العملية من بدايتها إلى نهايتها وكذلك يذكر فيه تاريخ وساعة بداية العملية وتاريخ الانتهاء منها" [1].

ذ. **ضبط التسجيلات ووضعها في أحراز:** بما أن التسجيلات أو الأشرطة المصورة تعتبر أدلة إثبات مادية أصلية تقتضي الشرعية الإجرائية حفظها بطريقة خاصة، وذلك بوضعها في أحراز مختمة يضمن عدم التلاعب بها أو العبث في الحديث المسجل سواء بالحذف أو الإضافة، وضمها إلى المحضر وهذا ما نستنتجه من خلال استقراء نصوص المواد 18 و45 ق.إ.ج.ج، وتجدر الإشارة هنا إلى أن المشرع الجزائري لم يشر إلى عرض هذه التسجيلات والصور على المشتبه فيهم في مرحلة جمع التسجيلات ويرجع ذلك الى الطابع السري الذي يتميز به هذه الجرائم الخطيرة على عكس ما نجده في المادة 42 من نفس القانون حيث أوجب عرض الأشياء المضبوطة على المشتبه فيهم لتميزها بطابع العلنية.

ثالثا: التسرب: لقد منحت التعديلات الجديدة لق.إ.ج.ج المتضمنة بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-155، لقاضي التحقيق صلاحيات جديدة لم يكن يتمتع بها من قبل، وذلك لمواجهة أنواع معينة من الجرائم نظرا لخطورتها ولطبيعتها الخاصة، وهذه الصلاحيات تتمثل في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وكذلك الإذن بإجراء عملية التسرب لأجل مراقبة الأشخاص بإيهامهم من طرف الشخص المتسرب بأنه فاعل معهم أو شريك لهم أو خاف لمتحصلات الجريمة، وذلك متى كانت الوقائع المحقق فيها متعلقة بجرائم المخدرات أو الجرائم الماسة بأنظمة المعالجة الآلية

[1] عبد الله أوهابية، شرح ق.إ.ج.ج، دار هومة للطباعة والنشر، الجزائر، 2011، ط 2، ص280.

للمعطيات أو الجريمة المنظمة أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالصرف، وكذا جرائم الفساد [1].

كما يعرف التسرب بأنه قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.

ويمكن تجسيد عملية التسرب في الجرائم الإلكترونية بإشراك ضابط أو عون الشرطة القضائية في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال أو كلام يقوم حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة ويظهر بمظهر طبيعي كما لو كان فاعل معهم، ويحاول الاستفادة من معرفتهم حول كيفية اقتحام الهاكر لموقع ما أو مباشرة الحديث في الموضوع الجنسي حتى يتمكنوا من اكتشاف وضبط الجرائم التي تتم من خلالها كالدعوة للدعارة مثلا.

المبحث الثاني

قبول الدليل الرقمي أمام القضاء الجزائي وضوابط اقتناع القاضي به

أخذ المشرع الجزائري بمبدأ حرية الإثبات، حيث أجاز إثبات الجرائم بكل الوسائل ما لم يرد نص بخلاف ذلك، مع مساواة الأدلة من حيث القيمة القانونية ما دامت جمعت وفق الإجراءات. وأكد على مبدأ الاقتناع الشخصي للقاضي الجزائي، الذي يمنح حرية تقدير الأدلة وتأثيرها في نفسه. رغم غياب نص صريح حول الدليل الرقمي، فإن قبوله يستند إلى هذا النظام المرن في الإثبات. لذا قسم هذا المبحث الى مطلبين، يتم التطرق الى قبول الدليل الرقمي أمام القضاء الجزائي (المطلب الأول)، والى ضوابط اقتناع القاضي الجزائي بالدليل الرقمي (المطلب الثاني).

[1] قانون 06- 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر 66-155 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 84، الصادرة بتاريخ 24 ديسمبر 2006، ص 04.

المطلب الأول

قبول الدليل الرقمي أمام القضاء الجزائي

أن قبول الدليل الرقمي أمام القضاء الجزائي يعتمد على مدى مشروعيته التي تظل محل جدل، خاصة فيما يتعلق بمدى التزامه بالضمانات الإجرائية والحقوق الدستورية، كحماية الخصوصية. وعند الإخلال بهذه الضمانات، تترتب جزاءات إجرائية قد تؤدي إلى استبعاد الدليل أو بطلانه، مما قد يؤثر على مسار العدالة الجنائية. قسم هذا المطلب الى فرعين، مشروعية الدليل الجزائي الرقمي واستثناءات قبوله (الفرع الأول)، والجزاء الإجرائي المترتب على عدم مشروعية الدليل الرقمي (الفرع الثاني).

الفرع الأول

مشروعية الدليل الجزائي الرقمي واستثناءات قبوله

ينقسم هذا الفرع إلى قسمين، الأول مشروعية الدليل الجزائي الرقمي، والثاني استثناءات قبول الدليل الرقمي.

أولا: مشروعية الدليل الجزائي الرقمي: يقصد بمشروعية الدليل الأساس القانوني الذي يرتكز عليه سواء في وجوده أو في إجراءات الحصول عليه، وتعد من الضمانات الأساسية لقبول هذا النوع من الأدلة في الإجراءات الجزائية.

أ. **مشروعية وجود الدليل الجزائي الرقمي:** تقتضي مشروعية وجود الدليل الرقمي أن يكون المشرع قد قبل هذا الدليل ضمن أدلة الإثبات الجنائي، والقوانين ذات الصياغة اللاتينية تشمل القانون الفرنسي والقوانين الأخرى التي تأثرت به كالقانون الإيطالي والإسباني، وقوانين أمريكا اللاتينية، وتشمل أيضا القانون الألماني والقوانين المشتقة منه، ذلك أن القانون الألماني وإن لم يكن لاتيني النزعة إلا أن صياغته تتشابه مع القانون الفرنسي، بالإضافة إلى القانون المصري وكذا الجزائري، تتشابه في الصياغة، فمصادر القانون فيها واحدة وأصولها العامة متحدة وتقسيماتها متماثلة والاصطلاحات القانونية فيها متشابهة، كما أن نظام الإثبات الحر هو السائد في هذه النوعية من القوانين [1]، فطبيعة النظام

[1] هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية دراسة مقارنة، دار النهضة العربية القاهرة، مصر، ط2، 2008، ص 29.

هو المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الإلكتروني[1].

ب. مشروعية الحصول على الدليل الجزائي الرقمي: من الضروري أن يتم رسم ضوابط وأطر معينة يجب أن تمارس في نطاقها عملية البحث عن الأدلة وتحصيلها والتحقيق فيها، بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع من ورائه، وهو الوصول إلى الحقيقة الفعلية في الدعوى وهي الهدف الأسمى لق.إ.ج.ج.

ويعني مبدأ مشروعية الحصول على الدليل الرقمي بما يتضمنه من مفاهيم إلكترونية، ضرورة اتفاق الإجراءات مع القواعد القانونية والأنظمة المتبعة في وحدات المجتمع المتحضر، أي أن قاعدة مشروعية الدليل الجزائي لا تقتصر فقط على مجرد المطابقة مع القواعد القانونية، بل يجب أن تراعي المبادئ السامية لحقوق الإنسان وقواعد النظام وحسن الآداب في المجتمع [2]، و يشترط في الدليل الجزائي عموما لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة، وذلك يقضي أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون في هذا الشأن، ونحن هنا نبحث عن مشروعية الدليل الرقمي فإننا نقتصر على ما يثير جمع هذا الدليل من إشكالات قانونية بالنظر إلى طبيعته الخاصة، ولذا يمكننا القول أن ما يثيره الدليل الرقمي من حيث مشروعية الحصول عليه يتركز بشكل أساسي في إجراءات التفتيش للبحث عن هذا الدليل، وذلك يتم بنقطتين رئيستين وهما الصفة القائمة بالتفتيش ومدى مشروعية التفتيش عن الدليل الرقمي وضبطه في الوسط الافتراضي.

ومن المقرر أن الإدانة في أي جريمة لا بد أن تكون مبنية على أدلة مشروعية في الحصول عليها وفق قواعد الأخلاق والنزاهة، و احترام القانون من طرف الجهة المتخصصة بجمع الدليل الرقمي بما يتضمنه من لأدلة مستخرجة من وسائل الكترونية، و لا يكون إلا إذا أجرى التفتيش عنه أو الحصول عليه أو كانت عملية

[1] رشيدة بوكر، الدليل الإلكتروني ومدى حجيته في الإثبات الجزائي في القانون الجزائري مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، سوريا، المجلد27، العدد 02، سنة 2011، ص 314.

[2] عبد الله محمد هلال، حجية مخرجات الكمبيوتر في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، مصر، 2008، ص 104.

تقديمه إلى القضاء و إقامته أمامه بالطرق التي رسمها القانون، فمتى ما تم الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد بقيمته مهما كانت دلالته الحقيقة وذلك لعدم مشروعيته، وعلى هذا الأساس فإن إجراءات جمع الأدلة الرقمية المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة، وبالتالي بطلان الدليل المستمد منها ولا تصلح أن تكون أدلة تبنى عليها الإدانة في المواد الجنائية.

ثانيا: استثناءات قبول الدليل الرقمي: إذا كان مبدأ حرية الإثبات يجيز للقاضي حرية الاستعانة بكافة وسائل الإثبات إلا أن هذا الإطلاق ليس بلا قيد وبلا حدود، لأن ذلك سيؤدي إلى التساهل في ارتكاب الجرائم تحت غطاء البحث عن الأدلة والتحقيق فيها. تنحصر هذه الاستثناءات في التقيد بأدلة معينة في إثبات جريمة الزنا، أما الثاني فيتعلق بطرق الإثبات الخاصة بالمواد غير الجنائية.

أ. الاستثناءات المستمدة من نصوص قانونية خاصة:

1.**إثبات جريمة الزنا:** وضعت المادة 212 من ق إ ج قاعدة عامة في إثبات الجرائم مفادها إجازة الإثبات بأي طريق من طرق الإثبات، وأوردت استثناء على بعض الجرائم أنها تثبت بطرق قانونية محددة على سبيل الحصر[1]، وجريمة الزنا هي من الجرائم المعنية بهذا الاستثناء، إذ جاء في المادة 341 من ق.ع.ج أن الدليل عن ارتكاب الجرائم المعاقب عليها في المادة 339 يقوم إما على محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة تلبس، وإما بإقرار وارد في رسائل أو مستندات صادرة من المتهم وإما بإقرار قضائي[2].

[1] المادة 212، الأمر رقم 66-155 مؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 يتضمن قانون الإجراءات الجزائية.

[2] المادة 341 الأمر رقم 66-156 مؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 يتضمن قانون العقوبات.

غاية المشرع من هذا التقييد هو منع الدعاوى الكيدية في موضوع يتصل بالسمعة، فيخشى المشرع من الادعاء على أشخاص أبرياء بالزنا كذبا وابتزازا [1].

ويلاحظ على النص أن دليلا واحدا من هذه الأدلة كافيا بذاته لإدانة المتهم، كما أنه لا فرق بين الزوج والزوجة والشريك في الإثبات، فالأدلة واحدة بالنسبة لهم جميعا.

2. **اثبات المسائل غير الجنائية:** من المسلم به أن إثبات المسائل غير الجنائية التي تطرح على القاضي الجزائي سواء كانت مدنية أو تجارية أو أحوال شخصية، وهو ما نصت عليه صراحة المادة 352 من ق.إ.ج.ج التي جاء فيها أن المحكمة الملزمة بالإجابة عن المذكرات المودعة على هذا الوجه إيداعا قانونيا يتعين عليها ضم المسائل الفرعية والدفوع المبداة أمامها للموضوع والفصل فيها بحكم واحد يبت فيه أولا في الدفع ثم بعد ذلك في الموضوع، ولا يجوز لها غير ذلك إلا في حالة الاستحالة المطلقة أو أيضا عندما يتطلب نص متعلق بالنظام العام إصدار قرار مباشر في مسألة فرعية أو دفع [2].

وتقييد القاضي الجنائي بوسائل الإثبات المقررة في القوانين غير الجنائية بالنسبة للمسائل الأولية مشروط بأن تكون هذه المسألة عنصر مفترض في الجريمة سابقة في وجودها على ارتكاب الفعل الإجرامي، بمعنى ألا تكون هذه المسألة هي ذاتها الفعل الإجرامي وإلا جاز إثباتها بكافة طرق الإثبات بما فيها الدليل الرقمي باعتبارها مسألة جنائية.

الفرع الثاني

الجزاء الإجرائي المترتب على عدم مشروعية الدليل الرقمي

الدعوى الجزائية هي مجموعة الأعمال الإجرائية التي تهدف إلى التحقق من وقوع الجريمة ونسبتها إلى فاعلها، وهي تشمل جميع الإجراءات التي تباشر منذ أول عمل من أعمال التحقيق

[1] محمود نجيب حسني شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الثاني، دار النهضة العربية، القاهرة 2013، ص 874.

[2] عفيفي كامل عفيفي وفتوح الشاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة "، منشورات الحلبي الحقوقية، 2003، سوريا، ص 302.

حتى صدور حكم بات، وقد اشترط المشرع في كل عمل إجرائي ضرورة توافر شروط معينة لا يصح إلا بها، وهذا يعني أن الإجراء يجب أن يتم بالطريقة التي حددها القانون ومن قبل السلطة التي أناط بها هذا القانون اتخاذ الإجراء [1].

أولا: بطلان التفتيش في البيئة الإلكترونية: لقد نظم المشرع الجزائري قواعد وإجراءات التفتيش والحجز والجزاءات المترتبة عن مخالفتها في المواد 44 إلى 49 والمادة 64 ومن المواد 79 إلى 85 من ق.إ.ج.ج وقد نصت المادة 48 [2]على أن عدم مراعاة الإجراءات التي استوجبتها المادتان 45 و47 من هذا القانون يترتب عنها البطلان، وبالتالي فإن أي تفتيش يقوم به ضابط الشرطة القضائية بالمخالفة لأحكام المواد 44، 45 و47 يقع باطلا، أي أن مخالفة القيود المتعلقة بالحضور ووقت التفتيش والإذن من السلطة القضائية المختصة يترتب عليها البطلان، وإن كان قيد احترام الوقت والقيد المتعلق بالحضور لا يطبق في حالة التحري حول الجرائم المنصوص عليها في المادة 47 من ق.إ.ج.ج ومن بينها الجرائم الإلكترونية.

وتجدر الإشارة إلى أن هذا البطلان هو بطلان نسبي متعلق بمصلحة الأطراف تطبق عليه جميع القواعد التي تطبق على البطلان النسبي وهو في نفس الوقت بطلان قانوني إذ نص عليه المشرع صراحة، ويترتب على كون مخالفة أو عدم مراعاة قواعد وإجراءات التفتيش والحجز المنصوص عليها في المادتين 45 و47 البطلان النسبي المتعلق بمصلحة الأطراف، أي أنه لا يجوز التمسك ببطلان التفتيش أو الحجز أو التنازل عنه إلا لمن قررت الأحكام لمصلحته، فهو بالتالي ليس بطلانا مطلقا لعدم تعلقه بالنظام العام وأن المصلحة التي يحميها هي مصلحة شخصية [3].

---

[1] محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي (دراسة مقارنة)، دار الثقافة، عمان، الأردن، بدون طبعة، 2011، ص67.

[2] تنص المادة 48 من قانون الإجراءات الجزائية الجزائري على ما يلي: " يجب مراعاة الإجراءات التي استجوبتها المادتان 45 و47 ويترتب على مخالفتها البطلان."

[3] د. فتحي والي، نظرية البطلان في قانون المرافعات رسالة دكتوراه جامعة القاهرة، مصر سنة 1988، ص 498 نقلا عن: أحمد الشافعي، البطلان في قانون الإجراءات الجزائية دراسة مقارنة دار هومه، الجزائر، ط5، 2005، ص 130.

ثانيا: بطلان الشهادة: أداء اليمين هو من أهم الضمانات التي تضفي الثقة على الشهادة ولكي تكون دليلا يعتد به وتجعل الشاهد يخضع لضميره في قول الحق، ويتجنب الكذب أو تحريف الشهادة، فالشاهد الذي يدلي بشهادته دون أداء اليمين تعتبر هذه الشهادة باطلة، فأداء اليمين هو إجراء من النظام العام وبدونه يبطل كل أثر يترتب عن الشهادة [1].

كما يمكن الدفع ببطلان الشهادة في الحالات التالية:

1. سماع القصر وأدائهم اليمين القانونية.
2. سماع أحد أقارب المتهم وأصهاره.
3. عدم أداء الشاهد لليمين القانونية وعدم إمضائه لمحضر الشهادة.
4. أداء الشهادة تحت تأثير الإكراه المادي والمعنوي [2].

ومن الحالات التي لا يجوز فيها سماع الشخص كشاهد حالة وجود شخص تقوم ضده دلائل قوية ومتماسكة على قيام إتهام في حقه، كأن يتبين أنه يشارك في الوقائع الملاحق بها الأشخاص المتهمين في نفس القضية، وهو ما نصت عليه الفقرة الأخيرة من المادة 89 من ق.إ.ج.ج، وكذلك إذا كان الشخص المراد السماع لشهادته قد وجهت ضده شكوى مصحوبة بادعاء، وقد رفض سماعه كشاهد عند تبليغ الشكوى إليه طبقا لأحكام المادة 73 من ق.إ.ج.ج، والحالة الأخيرة إذا كان ادعى الشخص مدنيا، فلا يجوز عندئذ سماعه كشاهد طبقا لنص المادة 243 من نفس القانون [3].

ومن الأسباب التي تؤدي إلى النقض والبطلان عدم ذكر مضمون شهادة الشاهد بالحكم القاضي بالإدانة، لأنه لا يفسح المجال لمحكمة النقض مراقبة تطبيق القانون تطبيقا صحيحا [4].

---

[1] إبراهيم بلعليات، أركان الجريمة وظروف إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، ط1، سنة 2007، ص 203.

[2] إبراهيم بلعليات، المرجع السابق، ص 206.

[3] محمد حزيط مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومه الجزائر، ط3، سنة 2008.، ص 114.

[4] إبراهيم بلعليات، المرجع السابق، ص 206.

ثالثا: بطلان الخبرة التقنية: تعد جميع الإجراءات التي نصت عليها المادة 144 وما بعدها من ق.إ.ج.ج وتقابلها المادة 157 وما بعدها من ق.إ.ج الفرنسي إجراءات جوهرية، حيث إنها تضمن قيمة الخيرة وأن القواعد التي نصت عليها هذه المواد الخاصة بتعيين الخبراء تعتبر من النظام العام.

وقد اعتبر القضاء أن تعيين خبير غير مسجل في قائمة الخبراء بأمر غير مسبب يترتب عنه البطلان، كما أن عدم مراعاة أحكام المادة 151 فقرة 3 [1] من ق.إ.ج.ج المتعلقة باستجواب المتهم يترتب عنه بطلان من نوع البطلان الذي يلحق مخالفة أحكام المادة 105 من ق.إ.ج.ج، حيث يمتد هذا البطلان إلى إجراءات التحقيق اللاحقة لهذا الاستجواب ويتعرض القرار الذي أشار واستند إلى خبرة مشوبة بالبطلان إلى البطلان ويجب نقضه سواء تعلق الأمر بقرار إحالة أمام جهة قضائية للحكم صادر عن غرفة الاتهام أو قرار إدانة، غير أنه يجب إثارة الوجه المتعلق ببطلان الخبرة والتمسك به في الوقت المناسب، ذلك أن طابع النظام العام للبطلان الذي يلحق الخبرة المرتبطة بإدارة العدالة ليس بالدرجة التي تسمح بإمكانية إثارة هذا البطلان لأول مرة أمام المحكمة العليا حتى ولو كان العيب الذي يلحق الخبرة هو إغفال أداء الخبير لليمين [2].

رابعا: بطلان التسرب: لقد سبقت الإشارة إلى أنه ضمانا من المشرع تحت طائلة البطلان أن يكون الأمر محدد المدة وأن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته، كما يحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (04) أشهر ويمكن أن تجدد هذه العملية حسب مقتضيات التحقيق وضمن نفس الشروط الشكلية والزمنية [3].

---

[1] المادة 151 فقرة 3، الأمر رقم 66-155 مؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 يتضمن قانون الإجراءات الجزائية، المعدل والمتمم.

[2] أحمد الشافعي، البطلان في قانون الإجراءات الجزائية دراسة مقارنة دار هومه، الجزائر، ط5، 2005، ص 144.

[3] المادة 65 مكرر 15، قانون 06- 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر 66-155 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 84، الصادرة بتاريخ 24 ديسمبر 2006.

المطلب الثاني

ضوابط اقتناع القاضي الجزائي بالدليل الرقمي

إن الرباط الموجود بين مبدأ حرية الإثبات ومبدأ الاقتناع الشخصي رباط لا يمكن تصور انفصامه، فكلاهما يكمل الآخر، بل إن المبدأ الثاني هو نتيجة طبيعية للأول، لذلك فليس من باب الصدفة أن يذكر المشرع في نفس النص القانوني هذين المبدأين [1].

فالقاضي الجزائي وإن كان يتمتع بسلطة واسعة في تقديره للأدلة بما في ذلك الدليل الرقمي، إلا أن هذه السلطة ليست مطلقة، بل وضع المشرع ضوابط وهي بمثابة صمام أمان إزاء انحراف القاضي عند ممارسته لها [2]. ولذا قسم هذا المطلب الى فرعين، يقينية الدليل الجزائي الرقمي ومناقشته في الفرع الأول، وفي الفرع الثاني صعوبات استخلاص الدليل الرقمي.

الفرع الأول

يقينية الدليل الجزائي الرقمي ومناقشته

منح المشرع للقاضي الجزائي سلطة واسعة في تقديره للأدلة المطروحة أمامه، بما في ذلك الدليل الرقمي، فله أن يبحث ويتحرى الحقيقة بكافة الأدلة، فهو غير ملزم بإصدار حكم الإدانة أو البراءة لوجود دليل معين طالما أنه لم يقتنع به، وذلك عملا بمبدأ الاقتناع الشخصي. لكن هاته السلطة ليست مطلقة، وإنما قيدها المشرع بضوابط [3]، تعمل على حسن سير عمل القاضي وتحقيق العدالة.

أولا: مبدأ يقينية الدليل الجزائي الرقمي: اليقين القضائي ليس هو اليقين بالمعنى الفلسفي كحالة نفسية وذهنية تلتصق فيها حقيقة الشيء في الذهن على نحو لا يثير شكا ولا يحتمل غلطا، بل هو يقين قائم

[1] محمد مروان نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ديوان المطبوعات الجامعية، الجزائر، بدون طبعة، 1999، ج 2، ص 478.

[2] عائشة بن قارة، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن دار الجامعة الجديدة، الإسكندرية، مصر، 2010، ص267

[3] عائشة بن قارة، المرجع السابق، ص 267.

على تسبيب وأدلة وضعية، ولذلك فهو يقين تقريبي يوصف في العلم بأنه اقتناع وهو حالة ذهنية يتوفر فيها لدى القاضي من الأدلة الوضعية ما يكفي لاقتناعه بالتسليم بثبوت الواقعة كما أثبتها في حكمه، ويكفي فقط أن يشك القاضي في ثبوت التهمة بالبراءة مادامت المحكمة قد ألمت بواقعة الدعوى وأدلتها وخلا حكمها من عيوب التسبيب ومن الخطأ في القانون [1].

ثانيا: مبدأ مناقشة الدليل الجزائي الرقمي: يعني مبدأ وجوب مناقشة الدليل الجزائي بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى.

ولا يختلف الأمر بالنسبة للأدلة الرقمية بوصفها أدلة إثبات، إذ ينبغي أن تطرح في الجلسة وأن يتم مناقشتها في مواجهة الأطراف، فظهور المعلوماتية بكل خصائصها لا يغير شيئا من مبدأ الاقتناع الذاتي، فالاقتناع يجب أن يكون بناءا على أثر الدليل المتولد في نفس القاضي، والذي لا يترك أي مجال للشك، وحيث أن القانون لم يقم في المجال الجنائي نموذجا خاصا للإثبات، فإن قاضي الموضوع تكون له حرية التقدير، وله الهيمنة في الواقع على القيمة الدامغة للعناصر الإثباتية التي يؤسس عليها اقتناعه، والتي يكون للأطراف حرية الاعتراض عليها ومناقشتها في كافة مراحل الدعوى.

وهذا يعني أن الأدلة الرقمية سواء كانت مطبوعات أم بيانات معروضة على شاشة الحاسب، أم كانت بيانات مدرجة في حاملات البيانات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية، كل ذلك سيكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة.

وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات، يجب أن يعرض في الجلسة، ليس من خلال ملف الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الوسائل الإلكترونية.

[1] ياسر الأمير فاروق مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، مصر، ط1، سنة 2009، ص 667.

وأرست هذا الضابط المادة 212 فقرة 2 من ق.إ.ج.ج التي تنص على ما يلي: "ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

كما يرى الدكتور **محمد مروان** أن علنية الجلسات تشكل إحدى أهم الضمانات الممنوحة للمتهم، من جهة فإن حضور الجمهور يضمن عدم إهدار حقوق الدفاع، ومن جهة أخرى فإن القاعدة تعتبر ذات أهمية كبيرة بالنسبة للقضاء نفسه إذ أنها تصون هيبته وسمعته، فبإمكان الجمهور حضور الجلسة إلى غاية النطق بالحكم طبقا لنصوص المواد 285 [1]، 342 [2]، 355 من ق.إ.ج.ج .

ثالثا: تسبيب الاحكام القضائية: من الضمانات القانونية التي أقرها المشرع لتقييد حرية القاضي في الاقتناع هي تسبيب الأحكام طبقا لنص المادة 349 من ق.إ.ج.ج التي تنص على ما يلي: "كل حكم يجب أن ينص على هوية الأطراف وحضورهم أو غيابهم في يوم النطق بالحكم، ويجب أن يشتمل على أسباب ومنطوق، وتكون الأسباب أساس الحكم "، فتسبيب الأحكام هو شرط موضوعية اقتناع القاضي، ويقصد بالأسباب الحجج الواقعية والقانونية التي ينبني عليها الحكم.

فالمتهم لابد أن يعرف بدقة لأي سبب أدين وصدر في حقه حكم قضائي، كما أن استيعاب الأسباب من طرف المتهم المدان قد يسهل بعد تنفيذ العقوبة وأثناء تنفيذها إعادة إدماجه، كما أن تسبيب الحكم هو عمل عقلاني يسمح للقاضي بتفحص وسائل الإثبات بكل تمعن، وهو العملية الأساسية التي تسمح في إطار التدرج القضائي ممارسة الرقابة وكذا الطعون" [3].

[1] المادة 285، الأمر 66-155 مؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 يتضمن قانون الإجراءات الجزائية.

[2] المادة 342، الأمر 66-155، مصدر سابق.

[3] محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ديوان المطبوعات الجامعية، الجزائر، بدون طبعة، 1999، ج 2، ص 498.

الفرع الثاني

صعوبات استخلاص الدليل الرقمي

بالرغم من الجهود المبذولة في مكافحة الجريمة الالكترونية إضافة إلى الدور البارز الذي يلعبه الدليل الرقمي في إثبات مختلف الجرائم المعلوماتية، إلا أن الواقع العملي والقانوني كشف عن الكثير من الصعوبات التي تثيرها عملية الإثبات بتلك الأدلة الرقمية الحديثة، أهمها:

أولا: صعوبات تتعلق بالدليل الرقمي: واجه الأدلة الرقمية عدة صعوبات، أبرزها إمكانية التلاعب بها أو حذفها بسهولة، مما يثير الشكوك حول مصداقيتها. كما أن استخراجها وتحليلها يتطلب تقنيات متقدمة وخبرات متخصصة لضمان قبولها قانونيا.

أ. **صعوبة رؤية الدليل الرقمي:** 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 الحسي، 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].

ب. **سهولة محو الدليل الرقمي:** يستعمل المحرم الإلكتروني عدة أساليب وتقنيات تسمح له بإخفاء كل آثار الجريمة والتستر عنها بسهولة كبيرة، وذلك من خلال تقنيات معدة لهذا الغرض مع الأخذ بعين الاعتبار سهولة وسرعة إمكانية محو وتعديل البيانات الإلكترونية التي يمكن القيام بها في أزمان قياسية متناهية القصر تقاس باللحظات والثواني، 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 للجهاز [2].

[1] 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، ص 183.

[2] عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد تلمسان، الجزائر، 2021، ص 119.

ت. **إعاقة الوصول إلى الدليل الرقمي:** لا تقف صعوبة إثبات الجرائم الإلكترونية عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها، وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة، بالإضافة على ذلك تمتد إلى الجناة أنفسهم لأن مرتكبي هذا النوع من الجرائم قد يستخدمون الوسائل الإلكترونية المختلفة لإعاقة الوصول إليهم، فالمحرم المعلوماتي غالبا ما يضرب سياجا أمنيا على أفعاله غير المشروعة قبل ارتكابه لها، فيزيد بذلك من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقنية التي تدينه [1].

ثانيا: صعوبات تتعلق بالتشريع: المشرع الجزائري واقتداء بأغلب دول العالم وأمام قصور القواعد القانونية التقليدية في مواجهة الجريمة المستحدثة، وجد نفسه امام حتمية استحداث قوانين تنسجم وحداثة الجريمة، مما ادى الى تعديل القانون الجنائي بشقيه الموضوعي والإجرائي من خلال التحلي بنصوص امرة مستحدثة، لتجريم الظاهرة وتحديد سبل واليات مكافحتها وذلك باستصدار قوانين خاصة تتلاءم والطبيعة الخاصة للجريمة الإلكترونية، كما تضمنت التعديلات المختلفة لقانون الإجراءات الجزائية الجزائري عدة قواعد اجرائية مستحدثة تتماشى وحداثة الجريمة الالكترونية [2].

[1] 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.

[2] سميرة عبد الدايم الجرائم المستحدثة بين الموضوع والوسيلة، المجلة النقدية للقانون والعلوم السياسة، المجلد 16 العدد 2 تيزي وزو، السنة 2021.ص 516.

خـــــاتمة

يتجلى لنا من خلال دراستنا هذه أن الجريمة الالكترونية هي من أكثر الجرائم التي عرفها العالم الحديث خطورة فهي آفة أنتجتها الثورة التكنولوجية والمعلوماتية، وذلك نظرا لما تتسم به من اختلاف عن الجرائم المعروفة في العالم التقليدي ويكمن تمايزها عن الجريمة الكلاسيكية بدءا بتسميتها وتعريفها وصولا إلى الأركان التي تقوم عليها. فمنهم من عرفها على أنها أساس وسيلة لارتكاب الجريمة، و الأخر جمع بين هذه التعاريف، حيث لا يلجا الى العنف كما هو الحال في المجرم التقليدي، وإن مجرد الحصول على الدليل الالكتروني للإثبات الجزائي وإقامة الحجة أمام القضاء لا يكفي لاعتماده دليلا للإدانة، وبالنظر إلى مدى حجية الدليل الالكتروني في نطاق الإثبات الجنائي ومدى اعتماد القانون هذه الحجية، فالدليل الالكتروني يخضع في عملية تقييمه لنفس القواعد المقررة لباقي الأدلة سواء كانت هذه القواعد تتعلق بسلطة القاضي في قبول الدليل أو تتعلق بسلطته في تقدير هذا النوع من الأدلة.

ومما سبق ذكره استخلصنا من هذه الدراسة مجموعة من النتائج والتوصيات يمكن إجمالها فيما يلي:

نتائج الدراسة:

– يعتبر الدليل الرقمي أداة فعالة في إثبات الجرائم الإلكترونية بسبب طبيعته الفنية والتقنية، رغم كونه غير مادي.

– يواجه الدليل الرقمي تحديات مثل سهولة التعديل أو الإتلاف، لكن التطور التقني يتيح استرجاعه حتى بعد محوه.

– تتطلب عمليات جمع الأدلة الرقمية إجراءات خاصة مثل التفتيش الإلكتروني ومراقبة الاتصالات.

– يواجه المحققون صعوبات تقنية وقانونية في جمع الأدلة الرقمية، مثل تحديد هوية الجناة وحماية الخصوصية.

– يشترط لقبول الدليل الرقمي أن يكون مشروعا، أي تم الحصول عليه وفق الإجراءات القانونية، مع احترام حقوق الدفاع.

– يخضع الدليل الرقمي لمبدأ الاقتناع الشخصي للقاضي، لكنه مقيد بضوابط مثل المناقشة العلنية وتسبيب الأحكام.

– القصور التشريعي في تنظيم طرق جمع الأدلة الرقمية.

– نقص الخبرات التقنية لدى المحققين والقضاة في التعامل مع الأدلة الرقمية.

– صعوبة التنسيق الدولي في حالات الجرائم العابرة للحدود.

– لم ينص المشرع الجزائري صراحة على الدليل الرقمي، لكنه يقبله ضمن نظام الإثبات الحر المنصوص عليه في قانون الإجراءات الجزائية المادتين 212 و307.

– استحدث المشرع نصوصًا قانونية لمكافحة الجرائم الإلكترونية، مثل القانونين رقم 04-15 ورقم 09-04، لكنه لم يحدد إجراءات مفصلة لجمع الأدلة الرقمية.

توصيات الدراسة:

– إصدار نصوص صريحة تنظم الدليل الرقمي وإجراءات جمعه.

– تحديث التشريعات لمواكبة التطورات التكنولوجية.

– تدريب القضاة والمحققين على التعامل مع الأدلة الرقمية.

– تعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية.

قائمة المصادر والمراجع

قائمة المصادر:

1. القرآن الكريم.

2. القانون رقم 04-15 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الأمر 66-156 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون العقوبات الجزائري، الجريدة الرسمية، العدد 71، 2004.

3. قانون 06- 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر 66-155 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 84، الصادرة بتاريخ 24 ديسمبر 2006.

4. قانون 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 05 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، الصادرة بتاريخ 16 أوت 2009.

5. مرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 53، الصادرة بتاريخ 08 أكتوبر 2015.

6. الأمر رقم 66-155 مؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 يتضمن قانون الإجراءات الجزائية.

قائمة المراجع:

أولا: المراجع باللغة العربية

أ. الكتب

1. إبراهيم بلعليات أركان الجريمة وظروف إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، ط1، 2007.
2. أحمد الشافعي، البطلان في قانون الإجراءات الجزائية دراسة مقارنة دار هومه، الجزائر، ط5، 2005.
3. أحمد مختار عمر، معجم اللغة العربية المعاصرة، عالم الكتب، المجلد الأول، ط 2008.
4. احمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد العاشر، العدد الأول.
5. احمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2015م.
6. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009.
7. سهى عريقات، الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي، جامعة القدس، كلية الحقوق، دون تاريخ.
8. طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني لحماية المعلوماتي، دار الجامعة الجديدة، القاهرة، مصر، 2009.
9. طارق الخن، الجريمة المعلوماتية، منشورات الجامعة الافتراضية السورية، 2010-2011.
10. عائشة بن قارة، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن دار الجامعة الجديدة، الإسكندرية، مصر، 2010.

11. عادل عزام سقف الحيط، جرائم الذم والتحقير المرتكبة عبر الوسائط الإلكترونية، دار الثقافة للنشر والتوزيع، 2019.

12. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، مصر، الطبعة الأولى، 2008.

13. عبد الله أوهابية، شرح ق.إ.ج.ج، دار هومة للطباعة والنشر، الجزائر، 2011، ط 2.

14. عبد الله محمد هلال، حجية مخرجات الكمبيوتر في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، مصر، 2008.

15. عفيفي كامل عفيفي وفتوح الشاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة "، سوريا، منشورات الحلبي الحقوقية، 2003.

16. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، منشأة المعارف، الإسكندرية، مصر، 1999.

17. عمر محمد بن يونس، الدليل الرقمي، دار النشر، الطبعة الأولى، مصر، 2007.

18. عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد تلمسان، الجزائر، 2021.

19. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، سنة 2004م.

20. محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي (دراسة مقارنة)، دار الثقافة، عمان، الأردن، بدون طبعة، 2011.

21. محمد حجازي، جرائم الحاسبات والانترنت (الجرائم المعلوماتية)، المركز المصري للملكية الفكرية، القاهرة، مصر، 2005.

22. محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومه الجزائر، ط3، 2008.

23. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، مصر، 2009.

24. محمد علي قطب الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، عمان، الأردن، دون سنة.

25. محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة، دار الجامعة الجديدة 2018.

26. محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ديوان المطبوعات الجامعية، الجزائر، بدون طبعة، 1999، ج 2.

27. محمود نجيب حسني شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الثاني، دار النهضة العربية، القاهرة 2013.

28. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2005.

29. هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، الطبعة الاولى، 1992.

30. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية دراسة مقارنة، دار النهضة العربية القاهرة، مصر، ط2، 2008.

31. ياسر الأمير فاروق مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، مصر، ط1، سنة،2009.

32. المعجم الوسيط في اللغة العربية لمجموعة من علماء اللغة العربية، ج1، مطبعة مصر شركة مساهمة مصرية، 1960.

ب. الرسائل

1. حاحة عبد العالي، الآليات القانونية لمكافحة الفساد الإداري في الجزائر، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة بسكرة، 2013/2012.
2. 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.
3. سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماستر في العلوم الجنائية وعلم الإجرام، كلية الحقوق جامعة أبوبكر بلقايد، تلمسان، الجزائر، 2010.
4. محروس نصار غايب، الجريمة المعلوماتية، بحث منشور في مجلة التقني، المجموعة 24، الإصدار 9، العراق، 2011.
5. نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجيستير، جامعة الحاج لخضر-باتنة-، كلية الحقوق والعلوم السياسية، 2013.

ت. المقالات العلمية والمجلات

1. حفوظة الأمير عبد القادر وغرداين حسام، الجريمة الإلكترونية وآليات التصدي لها، الملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017.
2. سومية عكور، الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانوني والأمني، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، كلية العلوم الإستراتيجية.
3. طارق الجملي، الدليل الرقمي في مجال الإثبات الجزائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة من 28 الى 2009/10/29، الذي نظمته أكاديمية الدراسات العليا، طرابلس.
4. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري: الإثبات الجزائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجزائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض 2-1428/11/04هـ.

5. ناصر محمد البقهي، أثر التحويل مجتمع معلوماتي على الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف بن عبد العزيز الدراسات الأمن الفكري بجامعة الملك سعود المملكة السعودية من 22 الى 25 جمادى الأولى 1430 هـ.

6. حكيمة جاب الله، فريدة بن عمروش، التكنولوجيا الرقمية: قراءة في المفاهيم وبعض الأبعاد النظرية، المجلة العلمية للتكنولوجيا وعلوم الإعاقة، المجلد 3، العدد 1، 2021.

7. رشيدة بوكر، الدليل الإلكتروني ومدى حجيته في الإثبات الجزائي في القانون الجزائري مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، سوريا، المجلد27، العدد 02، 2011.

8. سميرة عبد الدايم الجرائم المستحدثة بين الموضوع والوسيلة، المجلة النقدية للقانون والعلوم السياسة، المجلد 16 العدد 2 تيزي وزو، 2021.

9. ميسون الحمداني، ميسون خلف حمد الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي، مجلة كلية القانون، جامعة النهرين، 2016.

10. نواف مزيد السريحي، الاستدلال والدليل في القران الكريم، مجلة الدراسات العربية، جامعة المنيا، كلية العلوم، العدد 25، م2، 2012

ثانيا: المراجع باللغة الأجنبية

1. Myriam Quéméner, Magistrat, Les spécificités juridiques de la preuve numérique (1) AJ Pénal 2014.

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

ملخص:

تهدف هذه المذكرة إلى تسليط الضوء على مدى حجية الدليل الرقمي في إثبات الجرائم الإلكترونية، في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصالات، وما أفرزه من أنماط جديدة من الجرائم، أضحت تشكل تحديا حقيقيا للمنظومة القانونية التقليدية، سواء من حيث الاكتشاف أو الإثبات.

في الفصل الأول، تم تناول الإطار المفاهيمي، حيث تم الوقوف على مفهوم الجريمة الإلكترونية، من خلال تعريفاتها الفقهية والتشريعية، وبيان خصائصها وأنواعها، بالإضافة إلى التعريف بـالدليل الرقمي، وخصائصه التي تجعله مختلفا عن وسائل الإثبات التقليدية، وأبرز أنواعه وأشكاله من صور رقمية، وتسجيلات صوتية، ومحررات إلكترونية.

أما في الفصل الثاني، فقد تم التركيز على الطبيعة القانونية للدليل الرقمي في التشريع الجزائري، من خلال استعراض إجراءات جمعه، سواء العامة أو الخاصة، والتحديات المرتبطة باستخلاصه، خصوصا ما يتعلق بمراقبة الاتصالات واعتراض المراسلات، ومدى احترامها للضمانات القانونية. كما تطرقت المذكرة إلى شروط قبول الدليل الرقمي أمام القضاء، من حيث مشروعيته، والجزاءات المترتبة على انتهاك تلك المشروعية، بالإضافة إلى استعراض سلطة القاضي الجزائي في تقدير هذا النوع من الأدلة، ومدى قناعته بها، في ظل ما يواجه من صعوبات تقنية وتشريعية.

وقد خلصت الدراسة إلى أن الدليل الرقمي، رغم فعاليته وأهميته في مواجهة الجرائم الإلكترونية، لا يزال يطرح تحديات قانونية وتقنية، تستدعي تحديث الأطر التشريعية وتعزيز الكفاءة القضائية في التعامل مع هذا النوع من الإثبات.

Abstract :

This thesis aims to shed light on the evidentiary value of digital evidence in the context of proving cybercrimes, in light of the rapid advancement of information and communication technologies, which has led to the emergence of new forms of crime that pose significant challenges to traditional legal systems—particularly in terms of detection and proof.

In Chapter One, the theoretical and conceptual framework was addressed by examining the nature of cybercrime, including doctrinal and legislative definitions, its key characteristics, and its various types. It also explores the concept of digital evidence, highlighting its unique features that distinguish it from traditional forms of criminal evidence, along with its different types and forms such as digital images, electronic documents, and audio recordings.

Chapter Two focuses on the legal framework governing digital evidence under Algerian law. It presents the procedures for collecting digital evidence, both general and specific, and the challenges associated with extracting it—especially those related to the surveillance of electronic communications and interception of correspondence, while ensuring adherence to legal safeguards. The chapter also examines the admissibility of digital evidence before Algerian courts, addressing its legality and the procedural consequences of its invalidity. Moreover, it analyzes the discretionary power of the criminal judge in evaluating and being convinced by this type of evidence, considering the technical and legislative challenges it presents.

The study concludes that, despite the effectiveness and importance of digital evidence in combating cybercrime, it still raises numerous legal and technical challenges that necessitate legislative reform and enhanced judicial capacity to deal with this emerging mode of proof.

الكلمات المفتاحية: الدليل الرقمي، الإثبات، الجريمة الإلكترونية، التشريع الجزائري.