# الدليل الرقمى فى مجال الإثبات الجنائى وفقاً للتشريع الجزائرى

## وهيبة لعوارم*

إن التطور الحالى الحاصل للوسائل الإلكترونية الذى انعكس أثره على قانون العقوبات باعتبار أن الاستخدام غير المشروع للتقنية الإلكترونية أدى إلى ظهور علم جديد فى البحث الجنائى وهو علم البحث الجنائى الرقمى الذى يهتم بالدليل الرقمى بالنظر لآثار الجريمة الإلكترونية، وقد انعكس أثره أيضًا على قانون الإجراءات الجنائية، بحيث إن هذا القانون الأخير قد لا يطبق بسبب عجز القانون الأول عن استيعاب الجرائم المستحدثة التى ترتكب بالوسائل الإلكترونية، كما أن الإثبات الجنائى وهو أحد الموضوعات المهمة لهذا القانون قد تأثر بدوره بالتطور الهائل الذى لحق الأدلة الجنائية بسبب تطور طرق ارتكاب الجريمة، الأمر الذى يتعين معه تغير النظرة إلى طرق الإثبات الجنائى لكى تقترب الحقيقة العلمية فى واقعها الحالى من الحقيقة القضائية.

## مقدمة

من القواعد المستقرة فى مجال الإثبات الجنائى ومن أهم القواعد فى الإجراءات الجنائية أنه يجب على القاضى أن يبنى حكمه على أدلة طرحت أمامه لمناقشة الدليل فى الجلسة، فلا يمكنه أن يقضى بعلمه الشخصى، فإحاطته بوقائع الدعوى يجب أن يتم من خلال ما يُطرح عليه من أدلة؛ فهى الوسيلة التى ينظر من خلالها القاضى للواقعة ليبنى قناعته، وهى أيضًا جوهر الإثبات سواء فى مجال إثبات الواقعة ونسبتها إلى المتهم أو عدم إمكانية إسنادها إليه، ولها أهمية كبرى لأنها تناصر الحقيقة وتبين مرتكب الجريمة وتحول الشك إلى

* أستاذ مساعد، كلية الحقوق، جامعة عبدالرحمان ميرة، بجاية، الجزائر.

يقين، ولهذه الأهمية التى تتمتع بها حظيت باهتمام المشرع فى مختلف الأنظمة القانونية.

ولا شك فى أن التطور الحالى الذى لحق ثورة الاتصالات عن بعد وما أفرزته هذه الثورة من وسائل إلكترونية متقدمة ومتعددة قد انعكس أثره على الجرائم التى تمخضت عن ذلك، بحيث تميزت هذه الجرائم بطبيعة خاصة من حيث الوسائل التى ترتكب بها، ومن حيث المحل الذى تقع عليه، ومن حيث الجناة الذين يرتكبونها، بحيث يمكن القول إن الأساس فى خطورة هذه الجرائم يكمن فى أنها فى طبيعتها تجمع بين الذكاء الاصطناعى والذكاء البشرى، مما يجعل إثباتها جنائيًا قد يكون فى منتهى الصعوبة، كما ترجع الصعوبة كذلك إلى اختلاف الوسط الذى ترتكب فيه الجريمة، من وسط مادى إلى وسط افتراضى، وهو ما استتبع ظهور طائفة جديدة من الأدلة تتفق وطبيعة الوسط الذى ارتكبت فيه الجريمة وهى الأدلة الرقمية.

ولقد أثار هذا النوع من الأدلة الكثير من الجدل والذى يمكن إرجاعه إلى إشكاليتين رئيستين:

- الأولى فتتمثل فى مدى مشروعية الأخذ بالدليل الرقمى.
- وأما الثانية فتتمثل فى مدى قابلية الدليل الرقمى فى إثبات الوقائع مع التطور الحاصل فى مجال تقنية المعلومات.

**ولذلك فإننا سنحاول من خلال هذه الدراسة التطرق إلى المحورين التاليين:**

- مفهوم الدليل الرقمى.
- القيمة القانونية للدليل الرقمى.

## المحور الأول: مفهوم الدليل الرقمى

نظرًا للطابع الخاص الذى تتميز به الجريمة الإلكترونية، يتبين أن إثباتها يحيط به الكثير من الصعاب، ولا شك أن كشف ستر هذا النوع من الجرائم يحتاج إلى أدلة ذات طبيعة خاصة مختلفة عما ألفناه فى الجرائم التقليدية، ولما كانت عملية الإثبات الجنائى فى الوسط الافتراضى أو المعنوى ترتكز على الدليل الجنائى الرقمى، ذلك أنه الوسيلة الوحيدة لإثبات هذا النوع من الجرائم، فإننا فى هذا المحور سنتناول التعريف به فيما يلى:

**أولًا: المقصود بالدليل الرقمى.**

**ثانيًا: نطاق وأنواع الدليل الرقمى.**

### أولًا: المقصود بالدليل الرقمى

من المشكلات التى تتعلق بالدليل الإلكترونى أنه دليل غير مرئى، حيث تكون الأدلة الناتجة عن الجرائم المرتكبة فى الوسط الافتراضى عبارة عن بيانات غير مرئية لا تفصح فى الغالب عن شخصية الجانى، وتكون مسجلة إلكترونيًا، وفى الغالب مشفرة على وسائط تخزين ضوئية أو ممغنطة لا يمكن للإنسان قراءتها، وإن كان ذلك ممكنًا للآلة، والتلاعب أو التعديل الذى يحدثه الجانى فيها لا يحدث أثرًا، مما يقطع صلة المجرم بالجريمة، ويحول دون كشف شخصيته فى الغالب، ونظرًا لتلك الميزات ولميزات أخرى استوجب التطرق إلى خصائص ومميزات الدليل الرقمى، وقبل ذلك، فالمنطق يوحى لنا التطرق بداية لتعريف الدليل الرقمى.

**١ – تعريف الدليل الرقمى**

يعرف الدليل الرقمى على أنه "الدليل المأخوذ من أجهزة الحاسب الآلى ويكون فى شكل مجالات أو نبضات مغناطيسية أو كهروبائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة ويتم تقديمها فى شكل دليل يمكن الأخذ به أمام القضاء"[١]. أو " هو مكون رقمى لتقديم معلومات فى أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال وذلك من أجل الربط بين الجريمة والمجرم والمجنى عليه بشكل قانونى، يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون"[٢]، فى حين يعرفه آخر على أنه "الدليل الذى يجد له أساسًا فى العالم الافتراضى ويقود إلى الجريمة"[٣].

كما عرفه البعض بأنه يشمل "جميع البيانات الرقمية التى يمكن أن تثبت بأن هناك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجانى، أو توجد علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية مجموعة الأرقام التى تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت أو الصورة"[٤].

أو هو "معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة فى أجهزة الكمبيوتر وملحقاتها وشبكات الاتصال، ويمكن استخدامها فى أى مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شىء أو شخص له علاقة بجريمة أو جانى أو مجنى عليه"[٥].

ومن وجهة نظرنا فإن الدليل الرقمى Digital Evidence هو ذلك الدليل المشتق من النظم المعلوماتية، أو أجهزة ومعدات الكمبيوتر، أو شبكات الاتصالات، بعد تحليلها علميًا وفنيًا وتفسيرها فى شكل نصوص مكتوبة، أو رسومات أو أصوات، لتقديمها لهيئات العدالة لإثبات وقوع الجريمة من عدمها.

لكن الطبيعة غير المرئية للأدلة الإلكترونية تنعكس سلبًا على أداء الجهات التى تتعامل معها، حيث تشكل عملية فحص وتحليل تلك البيانات صعوبة بالغة أمام تلك الجهات التى مازالت الثقافة المادية هى المسيطرة عليها فى التعامل مع تلك الأدلة، مع أن الأمر مختلف بالنسبة لهذا النوع من الأدلة الرقمية التى تحتاج إلى إجراءات تتناسب مع طبيعتها غير المرئية(٦).

وتظهر هذه المشكلة على وجه الخصوص بالنسبة لجرائم الإنترنت، ومنها الجرائم التى تقع على العمليات الإلكترونية المختلفة، كالتى تقع على التجارة الإلكترونية، أو على العمليات الإلكترونية للأعمال المصرفية، أو تلك التى قد يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات، كجرائم السرقة، التزوير، الغش، الإتلاف، والجرائم التى ترتكز على البريد الإلكترونى فى ارتكابها إذ يكون من الصعب تحديد مصدر المرسل(٧).

**٢ – خصائص الدليل الرقمى**

إن البيئة الرقمية التى يعيش فيها الدليل الإلكترونى بيئة متطورة بطبيعتها، فهى تشتمل على أنواع متعددة من البيانات الرقمية تصلح منفردة أو مجتمعة لكى تكون دليلا للإدانة أو البراءة، وقد انعكس هذا العالم الرقمى على طبيعة هذا الدليل مما جعله يتصف بعدة خصائص ميزته عن الدليل الجنائى التقليدى، وهى كالتالى:

- **الدليل الرقمى دليل علمى:** يتكون هذا الدليل من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة لا تُدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات، وأدوات الحاسبات الآلية، واستخدام نظم برامجية حاسوبية، فهو يحتاج إلى مجال تقنى يتعامل معه، وهذا يعنى أنه كدليل يحتاج إلى بيئته التقنية التى يتكون فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فإن ما ينطبق على الدليل العلمى ينطبق على الدليل الإلكترونى[٨].
- **الدليل الرقمى دليل تقنى:** وهو ما يميزه عن الدليل التقليدى، من حيث إن التقنية لا تنتج اعترافًا مكتوبًا أو مالًا قدم كرشوة، أو بصمة إصبع، بل تنتج التقنية نبضات رقمية تكمن قيمتها فى إمكانية التعامل مع القطع الصلبة التى يتكون منها الحاسب الآلى مهما كان نوعه[٩].
- **صعوبة التخلص من الدليل الرقمى:** وتعتبر هذه الخاصية من أهم مميزات الدليل الرقمى باعتبارها ميزة يتمتع بها عن غيره من الأدلة، بحيث يقتضى الأمر مقارنة بين الدليل الرقمى والدليل الجينى الذى يطلق عليه الحمض النووى DNA، وذلك لاتحاد كل منها فى هذه الخاصية التى تتمثل فى صعوبة التخلص منهما من جهة، ومن جهة أخرى من الممكن إحداث تعديل فى تكوينهما معًا، وهذا ما يستوجب مقارنة الأدلة الرقمية بالأدلة التقليدية، حيث إن هذه الأخيرة تستمد قوتها فى حالة التسريع بالحصول عليها، فمثلا بصمة الإصبع إذا ما طالت المدة بين ساعة ارتكاب الجريمة وبين الحصول عليها فتكون قابلة للشك، هذا من ناحية، ومن ناحية أخرى، فالأدلة المادية يمكن

الدليل المستمد إذا ما تم تدميره كلية، أما الحال فهو مختلف بالنسبة للأدلة الرقمية؛ لأن موضوع التخلص من الدليل الرقمى بالاستعمال أو الاستعانة بخصائص التخلص من المستندات فى الحاسب الآلى؛ والشبكة الإلكترونية لا تعتبر من العوائق التى تحيل دون استرداد الملفات التى تم من قبل إلغاؤها أو محوها من الحاسب الآلى، أو إظهارها وهذا ما يعنى صعوبة إخفاء الجانى لجريمته[١٠].

وتعتبر هذه الخاصية ميزة الدليل الرقمى عن غيره من الأدلة التقليدية؛ لأن هناك العديد من البرامج الحاسوبية وظيفتها استعادة البيانات التى تم حذفها أو إلغاؤها سواء تم إلغاء هذا بالأمر Delete أو عن طريق إعادة تهيئة أو تشكيل للقرص الصلب باستخدام الأمر.

- **الدليل الرقمى قابل للنسخ:** حيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر فى أنواع الأدلة التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير عن طريق نسخ طبق الأصل من الدليل[١١].
- **الدليل الرقمى يسجل المعلومات عن الجانى ورصدها وتحليلها** فى الوقت نفسه، لكونه يمكن أن يقوم بتسجيل تحركات الأفراد وسلوكياتهم وعاداتهم وبعض الأمور الخاصة بهم، لذلك فالبحث الجنائى عن الدليل الرقمى يكون بسهولة مقارنة مع الدليل المادى، كما أنه يتميز بسعة تخزينية عالية، بحيث يمكن لقرص صغير تخزين مكتبة كاملة، كما لآلة الفيديو الرقمية يمكنها تخزين مئات الصور[١٢].

بسعة تخزينية عالية، بحيث يمكن لقرص صغير تخزين مكتبة كاملة، كما لآلة الفيديو الرقمية يمكنها تخزين مئات الصور[١٢].

هذه أهم الخصائص التى يتميز بها الدليل الرقمى والذى بموجبها يتميز بذاتية خاصة مختلفة عن تلك المتواجدة فى الدليل التقليدى.

**ثانياً: نطاق وأنواع الدليل الرقمى**

الأدلة الجنائية هى كل ما يقود إلى برهان صحة الواقعة أو الوقائع موضوع التحقيق ويتم تصنيف الأدلة الجنائية إلى أربعة أنواع رئيسية هى: الأدلة القانونية، تلك التى حددها المشرع وعين حالات استخدامها ومدى حجية كل منها، والأدلة الفنية تلك التى تنبعث من رأى الخبير الفنى حول تقدير أو تقديم دليل مادى أو قولى وفق معايير ووسائل علمية معتمدة، والأدلة المادية الناتجة من عناصر مادية ناطقة بنفسها وتؤثر فى اقتناع القاضى بطريق مباشر، والأدلة القولية ويقصد بها تلك التى تنبعث من أشخاص أدركوا معلومات مفيدة للإثبات بإحدى حواسهم كالاعتراف وأقوال الشهود.

ويرى البعض أن الأدلة الجنائية الرقمية ماهى إلا مرحلة متقدمة من الأدلة المادية الملموسة التى يمكن إدراكها بإحدى الحواس الطبيعية للإنسان إلى الاستعانة بجميع ما يبتكره العلم من أجهزة مخبرية ووسائل التقنية العالية ومنها الكمبيوتر محور الأدلة الرقمية، لذا سوف نتطرق ضمن هذا المحور إلى دراسة نطاق العمل بالدليل الرقمى، وأنواع الدليل الرقمى.

**١ – نطاق العمل بالدليل الرقمى**

وجد الدليل الرقمى لإثبات الجريمة المعلوماتية – تلك التى تستخدم التقنية الرقمية والعالم الرقمى كوسيلة لها من قبل المجرمين المعلوماتيين – إذ يعتبر الدليل الأفضل لإثباتها، كونه من طبيعة الوسط الذى ارتكبت فيه، ولكن هل يعنى ذلك أن الدليل الرقمى ينحصر مجاله كدليل إثبات فقط على جرائم المعلوماتية أم يمتد لإثبات جرائم أخرى؟

بعبارة أخرى هل يوجد تلازم بين نطاق العمل بالدليل الرقمى وإثبات الجريمة المعلوماتية؟؟

يرى الفقه أن الدليل الرقمى وإن كان يصلح لإثبات الجرائم المعلوماتية فإنه يصلح أيضًا لإثبات الجرائم التقليدية، فلا تلازم بين نطاق العمل بالدليل الرقمى ومشكلة إثبات الجريمة المعلوماتية[١٣]، ويميز الفقه فى هذا الشأن بين عدة أنواع من الجرائم:

**النوع الأول: الجرائم المرتكبة بواسطة الكمبيوتر**

هى الجرائم التى يستخدم فيها الكمبيوتر والإنترنت كوسيلة مساعدة لارتكاب الجريمة، مثل استخدامه فى الغش والاحتيال وهذا النوع من الجرائم لا صلة له بالوسط الافتراضى إلا من حيث الوسيلة، فبالرغم من عدم اتصال هذه الجريمة بالنظام المعلوماتى إلا أن الدليل الرقمى يصلح كدليل لإثباتها، فلا يعتبر استخدام الكمبيوتر فى هذه الجرائم من طبيعة الفعل الجرمى، بل تستخدم كوسيلة مساعدة لارتكاب الجريمة مثل عمليات غسل الأموال أو نقل المخدرات من مكان إلى آخر، إلا أن جهاز الكمبيوتر فى هذه الحالة يظل محتفظًا بآثار رقمية يمكن أن تستخدم للإرشاد عن الفاعل.

**النوع الثانى: جرائم الإنترنت Cyber crime**

هى الجرائم التى يكون محلها جهاز الكمبيوتر فإما أن يكون الاعتداء واقعًا على الكيان المادى له، ويمكن اعتبارها فى هذه الحالة جريمة تقليدية تلحق سابقتها في الإرشاد عن الفاعل، وإما أن يكون واقعًا على الكيان المعنوى له أو على قاعدة المعلومات الرقمية، مثال جرائم القرصنة وهذا النوع من الجرائم هو الجرائم المعلوماتية والتى يكون الدليل الرقمى هو الأفضل لإثبات وجودها[١٤]، عرفها البعض بأنها سلوك إنسانى يشكل فعلًا غير مشروع قانونًا، وتقع على آلية نقل المعلومات بين مستخدمى الشبكة العالمية للمعلومات، ومن أمثلة هذه الجرائم جرائم الدخول غير المشروع لمواقع غير مصرح بها للدخول بها واستخدام عناوين غير حقيقية أو زائفة للولوج إلى الشبكة العالمية للمعلومات، كسر بروكسى أو تقنية الحماية الخاصة بالجهات المتصلة بالشبكة[١٥].

لكن يرى البعض أنه يمكن للدليل التقليدى إثبات الجريمة المعلوماتية كالشهادة رغم شدة صلتها بالدليل الرقمى[١٦]، فلا تلازم إذن بين نطاق الدليل الرقمى وإثبات الجريمة المعلوماتية، بل إن الدليل الرقمى كما يصلح لإثبات الجريمة التقليدية المرتكبة باستعمال الآلة الرقمية يصلح لإثبات الجريمة الإلكترونية[١٧].

**جـ - جرائم الشبكة العالمية**

وهى أى سلوك إنسانى يكون فعلًا غير مشروع قانونًا ويقع على أى وثيقة أو نص موجود بالشبكة، أو أنها أية جريمة يكون فيها لشبكة المعلوماتية دور فى أسلوب ارتكابها أو التوقيع على إحدى وثائقها بأية طريقة كانت[١٨]:

ومن أمثلتها قرصنة المعلومات وسرقة أرقام بطاقات الائتمان، وانتهاك الملكية الفكرية للبرامج والأفلام وغيرها، فهذه الجرائم تتطلب اتصالًا بالإنترنت على عكس جرائم الكمبيوتر التى قد يتصور حدوثها سواء كان هناك اتصال بالإنترنت أو لا[١٩].

**د – جرائم الكمبيوتر**

وهى سلوك إنسانى يشكل فعلًا غير مشروع قانونًا ويقع على أجهزة الكمبيوتر سواء وقع هذا السلوك غير المشروع على المكونات المادية أو المكونات المعنوية أو قواعد البيانات الرئيسية.

ولم يتوفر تعريف جامع يتفق عليه بسبب المتغيرات المتسارعة فى مجال تقنية الكمبيوتر وتعدد أنماط الجرائم، ولكن يمكن أن نستعمل هذا المصطلح للدلالة على الجرائم الموصوفة فى القوانين الحديثة لمكافحة جرائم الحاسوب أو الكمبيوتر، وهى تلك الجرائم التى تشمل سرقة خدمات الكمبيوتر، والدخول غير المشروع فى نظم الحاسوب المحمية، وقرصنة البرامج وتعديل أو سرقة المعلومات المخزنة إلكترونيًا، والابتزاز بواسطة الكمبيوتر، والحصول على دخول غير مصرح على سجلات البنوك أو إصدار بطاقات الائتمان أو وكالات العملاء، والاتجار فى كلمة السر، وبث الفيروسات والأوامر الهدامة[٢٠]، والتخريب لمكونات الكمبيوتر المادية كالشاشات أو الطابعة أو وسائط التخزين المرنة أو الصلبة، وكذلك الفيروسات وتعديل أو محو البيانات الرئيسية وغيرها[٢١].

أصدر المشرع الجزائرى قانونًا متخصصًا يعالج جرائم التكنولوجيا بما فيها التكنولوجيا الرقمية وهو قانون ٠٩-٠٤ المؤرخ فى ٠٥ أغسطس ٢٠٠٩

المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[٢٢]، وعرف تلك الجرائم أى الجرائم المتصلة بتكنولوجيات الإعلام والاتصال فى المادة الثانية منه الفقرة (أ) بأنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة فى قانون العقوبات وأى جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية".

٢ - أنواع الدليل الرقمى

للدليل الرقمى خاصية الالتصاق بمفهوم تكنولوجيا المعلومات من جهة تكوينه، ومقصود التنوع فى الدليل الرقمى يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه، وإنما تتعدد وسائل التوصل إليه، وفى كل الأحوال يظل الدليل المستمد منه رقميًا، ويعود سبب التنوع فى مصادر الحصول على الدليل الرقمى إلى كون الإنترنت تكتسب وجودها وحياتها من ضرورة توافر مقدمات متعددة لها، كالكمبيوتر والشبكات والمعلومات التى تتراسل، وكذلك المحتوى المادى للمعلومات كبرمجيات التعامل مع المعلومات فى العالم الافتراضى، وهذه كلها من الأدلة إذا تم فحصها لكونها تشكل قواعد اختراق، وإن كان يؤخذ فى الاعتبار الحيز المادى الذى توضع فيه الآليات التى تعمل على توصلينا بالإنترنت، وقد يستقى منها دليل أو آخر يساعد فى كشف غموض الواقعة أو وقائع أخرى قد تكون فى ذاتها جرائم أخرى أو ارتباط بالجريمة موضوع البحث، وعلى كل يمكن تقسيم الدليل الرقمى إلى ما يلى:

**أ – الورق ومخرجات الطابعات**

غالبًا ما تترك الجرائم الواقعة على الأموال أو الأشخاص آثارًا من الأوراق والمستندات بالغة الأهمية التى يتم حفظها فى الحاسب الآلى، فالكثير ممن يقومون بطباعة المعلومات بهدف المراجعة والتأكد من الشكل العام أو صحة المستند موضوع الجريمة، فالطابعات وأجهزة الحاسب الآلى ذات السرعة الفائقة تطبع الكثير من الأوراق فى وقت يسير، لذلك يعد الورق من الأدلة الرقمية التى يتم من خلالها بحث وتفتيش مسرح الجريمة[٢٣]، وللورق أربعة أنواع وهى:

* المسودة التى يتم إعدادها بخط اليد مثل تصور للعملية التى يتم برمجيتها.
* أوراق تالفة والتى تتم طباعتها للتأكد من برمجة العملية، ومن ثم إلقاؤها فى سلة المهملات.
* الأوراق التى تتم طباعتها والاحتفاظ بها لأغراض تفيد الجريمة.
* الأوراق الأساسية والمحفوظة فى الملفات العادية أو دفاتر الحسابات وخاصة التى يتم تزويرها من أجل تنفيذ الجريمة[٢٤].

**ب – الأجهزة الإلكترونية ومنها:**

**– الحاسب الآلى وملحقاته**

لتحديد الجريمة على أنها جريمة معلوماتية مرتبطة بالمكان أو بالشخص يفترض وجود حاسب آلى؛ حيث بإمكان خبير الحاسب الآلى التعرف على الجهاز ومواصفاته مع تمييزه عن غيره من أجهزة الحاسب الآلى الأخرى، بالإضافة إلى كيفية تحديد أسلوب التعامل معه أثناء الضبط والتحريز[٢٥].

ويعد ضبط وحجز الحاسوب بقصد تعقب الدليل الرقمى هو الأسلوب التقليدى فى إقامة بنيان هذا الدليل.

- **الطابعات**

تقوم الطابعات باستخراج ما تم تحضيره لطباعته، وتختلف أنواعها من عادية وليزرية، ملونة وغير ملونة؛ حيث غالبًا تستخدم فى مجال التقنية المعلوماتية، ويمكن رصد الحركة الخارجية سعيا وراء الدليل التقنى بفحص الطابعات سيما الحديثة منها، إذ تتضمن الطابعات الحديثة ميزة تخزين منطقية لمجموع الصفحات التى تم استخراجها من الحاسوب، حتى فى الحالة التى يكون هذا الملف قد تم إلغاؤه، وفى هذه الحالة الأخيرة يتم استخدام برمجيات متطورة لإسترجاع ما تم اتخاذه من أوامر عبر الحاسوب، ومنها أمر الطباعة فتقوم الطابعة بطباعة ما قامت فى فترة سابقة بطباعته، وهو أمر بالضرورة يؤدى إلى الحصول على مخرجات الطابعة التى تفيد فى كشف الحقيقة[٢٦].

- **الموديم**

هى الوسيلة التى يمكن من خلالها لأجهزة الحاسب الآلى من الاتصال ببعضها البعض عبر خطوط الهاتف، كما يقوم كذلك بإرسال الفاكس والرد على المكالمات الهاتفية، وتبادل البيانات وتعديلها، ويأخذ أشكالًا متنوعة مرتبطة بتطور تقنية المعلومات.

- **الهاتف النقال**

يعتبر جهازًا إلكترونيًا حجمه صغير يفيد التواصل بين الأشخاص عبر الهواء، وقد تطور فى الآونة الأخيرة فأصبح يتمتع بأشكال ومميزات أحدث أجهزة الحاسب الآلى اليوم، وأطلق عليه عدة تسميات مثل الخلوى، المحمول، الجوال...

**جـ – وسائل التخزين، ومنها:**

**– القرص الثابت أو الصلب**

يعد الوحدة الرئيسية التى يتم من خلالها تشغيل نظام الحاسب والبرامج والبيانات، ويعد القرص الصلب المحتوى الذى يضم فى داخله مجموع البيانات الرقمية ذات الطابع الثنائى، والتى تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائى (0 - 1) الذى يتكون منه تفصيل البيانات المذكورة، ويشير العلماء إلى إمكانية القيام بفحص كلى أو جزئى للقرص الصلب.

والفحص الجزئى للقرص الصلب يؤدى إلى التعرف على محتوى البيانات ثنائية الرقم، والتى يؤدى التعامل معها إلى الكشف عن القيمة الاستردادية للبيانات المخزنة فيه سواء كانت محتويات مكتوبة أو صور أو أصوات، وكذلك ما تم حذفه من بيانات وبرمجيات وبرامج.

**– الأقراص المدمجة**

هى وحدات تخزين متنقلة تحتوى على معلومات، وتقوم بتخزين هذه المعلومات عليها وإعادة تسجيلها.

**– ذاكـــرة فـــلاش**

وهى سهلة النقل والتبادل وحجمها صغير تعمل على تخزين ونقل البيانات ولها قدرات تخزين وأحجام مختلفة ومتنوعة[٢٧]. ويعد نظام ذاكرة التخزين من مزايا نظم تشغيل الحاسوب تحديدًا، وكلما كان نظام التشغيل متطورًا كلما كان نظام ذاكرة التخزين أكثر دقة.

**- الأشرطة الممغنطة**

هى وسيلة تستخدم غالبًا فى الحفظ الاحتياطى للبيانات والمعلومات وتوضع فى مكان بعيد وآمن، وكما يقوم البعض بإيداعها لدى خزائن البنوك أو مراكز التوثيق الحكومية الأمنية.

**هـ - البطاقات الممغنطة وبطاقات الائتمان القديمة والمواد البلاستيكية المستخدمة فى إنشاء تلك البطاقات، التى قد تكون قرائن للإثبات فى الجرائم المعلوماتية(٢٨).**

**د - البرامج، ومنها:**

**- برامج نظم التشغيل**

أعدت هذه البرامج المصممة لتحديد تشغيل نظام الحاسب الآلى، والتى تقوم باستقبال وإخراج المعلومات والبيانات والتحكم فى الذاكرة والتخزين وإدارة التطبيقات.

**- برامج التطبيقات**

تعتبر برامج مصممة أساسًا لأداء وظيفة محددة كمعالجة النصوص، بالإضافة إلى إدارة قاعدة البيانات، ويتم تحميل مثل هذه البرامج فى حالة الحاجة إليها(٢٩).

وعلى كل، ووفقًا لما قررته وزارة العدل الأمريكية سنة ٢٠٠٢، فإن الدليل الرقمى يمكن تقسيمه إلى ثلاث مجموعات وهى كالتالى:

المجموعة الأولى: السجلات المحفوظة فى الحاسوب وهى الوثائق المكتوبة والمحفوظة مثل البريد الإلكترونى وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الإنترنت.

المجموعة الثانية: السجلات التى تم إنشاؤها بواسطة الحاسوب، وتعتبر مخرجات برامج الحاسوب وبالتالى لم يلمسها الإنسان مثل log files وسجلات الهاتف وفواتير أجهزة السحب الآلى ATM.

المجموعة الثالثة: السجلات التى حفظ جزء منها بالإدخال وجزء آخر تم إنشاؤه بواسطة الحاسوب، ومن الأمثلة عليها أوراق العمل المالية التى تحتوى على مدخلات تم تلقيمها إلى برامج أوراق العمل مثل Excel ومن ثم تمت معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها.

**وقد قسم البعض الدليل الرقمى إلى الأقسام الرئيسية التالية:**

- أدلة رقمية خاصة بأجهزة الحاسب الآلى وشبكاتها.
- أدلة رقمية خاصة بالشبكة العالمية للمعلومات والإنترنت.
- أدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.
- أدلة خاصة بالشبكة العالمية للمعلومات، وهذا التقسيم يتطابق مع تقسيم الجريمة عبر الحاسب الآلى(٣٠).

ويلاحظ أن التنوع فى الدليل الرقمى يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه، وإنما تتعدد وسائل التوصل إليه، وفى كل الأحوال

يظل الدليل المستمد منه رقميًا، حتى وإن اتخذ هيئة أخرى، ففى هذه الحالة فإن اعتراف القانون بهذه الهيئة الأخرى يكون مؤسسًا على طابع افتراضى مبناه أهمية الدليل الرقمى ذاته وضرورته، إلا أنه لكى يحدث تواصل بين القانون وبين الدليل المذكور - نتيجة لنقص توافر الإمكانيات الرقمية فى المحاكم - فإنه يلزم اتخاذ مسلك الافتراض من حيث اعتباره دليلًا أصليًا[٣١].

## المحور الثانى: القيمة القانونية للدليل الرقمى

إن مجرد وجود دليل يثبت وقوع الجريمة وينسبها لشخص معين لا يكفى للتعويل عليه لإصدار الحكم بالإدانة إذ يلزم أن تكون لهذا الدليل قيمة قانونية، وهذه القيمة للدليل الجنائى تتوقف على مسألتين رئيستين، الأولى المشروعية، والثانية اليقينية فى دلالته أو حجيته على الوقائع المراد إثباتها، ولذلك سنحاول فى هذا المبحث تحديد القيمة القانونية للدليل الرقمى وذلك فيما يلى:

- **مشروعية الدليل الرقمى.**
- **حجية الدليل الرقمى.**

### أولًا: مشروعية الدليل الرقمى

يشترط فى الدليل الجنائى بوجه عام أن يكون مشروعًا من حيث وجوده والحصول عليه، فمشروعية الوجود تقتضى إجازة القانون للقاضى الاستناد عليه فى تسبيب حكمه القضائى، أما مشروعية الحصول تقتضى أن يتم الحصول عليه باتباع الإجراءات التى ينص عليها القانون وفقًا لما يلى:

**١ – مشروعية وجود الدليل الرقمى**

يقصد بمشروعية الدليل إجازة القانون للقاضى الاستناد إليه لتكوين عقيدته للحكم بالإدانة، وتكمن صعوبة الاستناد إلى الدليل الرقمى فى الإثبات فى سهولة تعديل البيانات التى يحتويها. وعلى كل تتوقف مشروعية الدليل على طبيعة نظام الإثبات بحسب ما إذا كان النظام المتبع هو نظام الأدلة القانونية أو نظام الإثبات الحر أو النظام المختلط وفقًا لما يلى:

**أ – نظام الإثبات القانونى**

يُدعى هذا النظام كذلك بالنظام الأنجلوساكسونى، ووفقًا له فإن مشروعية الدليل الرقمى تعتمد على تقدير المشرع للأدلة وليس لتقدير القاضى، فالدول التى تأخذ بهذا النظام على رأسها بريطانيا، كندا والولايات المتحدة الأمريكية، تطلب شروطًا خاصة فى الأدلة بوجه عام حتى يتم الأخذ بها والقاضى وفقًا لهذا النظام مقيد بالدليل، فالمشرع هو الذى يحدد حصرًا الأدلة التى يجوز للقاضى اللجوء إليها فى الإثبات، كما يحدد القيمة الإقناعية لكل دليل، بحيث يقتصر دور القاضى على مجرد فحص الدليل للتأكد من توافر الشروط التى حددها القانون، كما أنه لا دور للقاضى فى تقدير القيمة الإقناعية للدليل.

ولذا فإن النظم التى تتبنى هذا النظام لا يمكن فى ظلها الاعتراف للدليل الرقمى بأية قيمة إثباتية ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه يهدر قيمته الإثباتية مهما توافرت فيه شروط اليقين، فلا يجوز للقاضى أن يستند إليه لتكوين عقيدته[٣٢].

وتجدر الإشارة إلى أن الدليل فى هذا النظام تحكمه قواعد خاصة لقبوله أمام المحاكم سواء تعلقت هذه القواعد بمضمون الأدلة من بينها قاعدة استبعاد شهادة السماع، أو تعلقت بكيفية تقديم الأدلة والتى تدعى بقاعدة الدليل الأفضل[٣٣]، ومادام أن الدليل الرقمى يعد من قبيل شهادة السماع لكونه يتضمن أقوالًا أو مواد قام بوضعها الإنسان فى الحاسوب[٣٤].

ويعاب على هذا النظام أن من شأنه تقييد القاضى على نحو يفقده سلطته فى الحكم بما يتفق مع الواقع، فيحكم بما يخالف قناعته وفقًا للأدلة المطروحة عليه[٣٥].

**ب - نظام الإثبات الحر**

يسود نظام الإثبات الحر الأنظمة اللاتينية، ووفقًا له يتمتع القاضى الجنائى بحرية مطلقة فى شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للاستناد إليها فى تكوين قناعته، فله أن يبنى هذه القناعة على أى دليل وإن لم يكن منصوصًا عليه، فالمشرع فى مثل هذا النظام لا يحفل بالنص على أدلة الإثبات ولا يتدخل فى تحديد القيمة الإقناعية للدليل، فكل الأدلة تتساوى قيمتها الإثباتية فى نظره، والقاضى هو الذى يختار من بين ما يُطرح عليه ما يراه صالحًا- له مطلق الحرية فى قبول الدليل أو رفضه - للوصول إلى الحقيقة، فللقاضى دور إيجابى فى مجال الإثبات، فالإثبات فى هذا النظام يتبع نظام الإثبات الحر، إذ أن الإثبات فيه لا يرسم طريقًا محددًا يتبعه القاضى، بل يترك حرية تقدير أدلة الإثبات للقاضى وفقًا لمبدأ حرية القاضى فى الاقتناع[٣٦].

وتشمل القوانين ذات الصياغة اللاتينية القانون الفرنسى والقوانين الأخرى التى تأثرت به كالقانون الإيطالى والإسبانى وقوانين أمريكا اللاتينية،

وكذا القانون المصرى والجزائرى هذا الأخير الذى كرس مبدأ الاقتناع كأصل عام فى المادة ٢١٢ /١ من قانون الإجراءات الجزائية التى نصت على أنه: "يجوز إثبات الجرائم بأى طريق من طرق الإثبات ماعدا الأحوال التى ينص فيها القانون على غير ذلك، وللقاضى أن يصدر حكمه تبعًا لاقتناعه الخاص"، كما يتضمن القانون الألمانى ذلك، حيث أنه إن لم يكن لاتينى النزعة إلا أنه يتشابه فى صياغته مع القانون الفرنسى، لذلك يتضح أن مبدأ حرية الإثبات يعد بمثابة إقرار ضمنى من المشرع لفتح مجال لنوع من الأدلة العلمية التى يكتشفها العلم الحديث، وذلك لمواجهة الجرائم المستحدثة كبصمة الصوت والبصمة الوراثية والدليل الرقمى خاصة، وبالتالى فهذا الأخير شأنه شأن باقى الأدلة الأخرى(٣٧).

**جـ - النظام المختلط**

لقد حاول هذا النظام التوفيق بين النظامين اللاتينى والأنجلوسكسونى مع تلافى سلبيات كل النظامين، والمتمثلة فى إمكانية تعسف القاضى أثناء استعماله للسلطة التقديرية فى الاقتناع بالدليل من عدمه فى النظام اللاتينى، وكما أن القاضى فى النظام الأنجلوسكسونى يكون دوره سلبيًا ومقيدًا فى مسألة الإثبات لتقييده بالأدلة القانونية.

ويقوم هذا النظام بالجمع بين النظامين، وذلك عن طريق تحديد القانون لأدلة معينة للإثبات فى بعض الجرائم من خلال تقييد سلطة القاضى فى الإثبات، ومثال ذلك منح حجية للمحاضر المحررة فى بعض المخالفات بالنسبة لما ورد فيها إلى أن يثبت العكس، وتقييد سلطة القاضى فى إثبات بعض الجرائم بأدلة معينة، ولقد أخذ المشرع الجزائرى بمبدأ حرية الإثبات

كأصل عام فى المادة ٢١٢ السابق الإشارة إليها، إلا أنه يتضح من خلال هذه المادة وقوفًا عند عبارة "ماعدا الأحوال التى ينص فيها القانون على غير ذلك" أن المشرع الجزائرى وكاستثناء أخذ بمبدأ الأدلة القانونية، إذ قيد فى إثبات بعض الجرائم كجريمة الزنى المعاقب عليها فى نص المادة ٣٣٩ من قانون العقوبات والتى لا يمكن إثباتها إلا بالطرق التى أوردها على سبيل الحصر فى نص المادة ٣٤١ من قانون العقوبات(٣٨).

أما بالنسبة للأدلة الرقمية فقد قضى البعض أن السجلات الإلكترونية تتميز بكونها غير مرئية فى ذاتها، وبالتالى لا يمكن إسنادها كدليل فى المحكمة، إلا فى حالة تحويلها إلى أدلة مرئية ومقروءة عن طريق مخرجات الطباعة، فتكون مقبولة سواء كانت هى الأصل أو نسخة من الأصل(٣٩).

ونجد أن المشرع الجزائرى جعل طريقة الإثبات بالكتابة مقبولة مهما كانت الوسيلة التى تتضمنها وكذا طرق إرسالها، وكذلك ساوى بين الكتابة فى الشكل الإلكترونى بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذى أصدرها، وأن تكون معدة و محفوظة فى ظروف تتضمن سلامتها.

**٢ - مشروعية الحصول على الدليل الرقمى**

يُشترط فى الدليل الجنائى لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة، وذلك يقتضى أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط المحددة قانونًا، ونحن هنا إذ نبحث مشروعية الدليل الرقمى فإننا سنقتصر على ما يثيره جمع هذا الدليل من إشكاليات قانونية، بالنظر إلى طبيعته الخاصة، ولذا فإن الإشكاليات العامة لجمع الأدلة والتى بدورها لا تقتصر على الدليل الرقمى لن تكون موضع بحث منا، ويمكننا القول إن ما

مشروعية الحصول عليه يتركز بشكل أساسى فى إجراءات التفتيش للبحث عن هذا الدليل، وذلك يثير نقطتين وهما مضمون إجراء التفتيش وغايته، مشروعيته وأنواعه، ونعرض لذلك فيما يلى:

**أ – مضمون التفتيش وغايته**

**– مضمون التفتيش**

عرف البعض التفتيش على أنه "إجراء من إجراءات التحقيق يقوم به موظف مختص طبقًا للإجراءات المقررة قانونًا، فى محل يتمتع بحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم"(٤٠)، أو "هو إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة فى مستودع السر، غالبًا ما يسفر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم، وهو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تسهم فى بيان الحقيقة"(٤١).

لم يورد المشرع الجزائرى تعريفًا خاصًا للتفتيش، بقدر ما اعتبره إجراءً من إجراءات التحقيق وأحاطه بضوابط صارمة لأن فيه مساس بحريات الأشخاص وبكرامتهم، ما يؤكد ذلك الدستور الجزائرى إذ نص فى المادة ٤٠ منه: "لا تفتيش إلا بمقتضى القانون وفى إطار احترامه ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة"، وجسده المشرع فى أحكام المادة ٤٤ من قانون الإجراءات الجزائية المعدل والمتمم التى بينت إجراءات التفتيش كما يلى:

- وجود إذن مكتوب صادر من وكيل الجمهورية أو قاضى التحقيق.
- الاستظهار بالإذن قبل دخول المسكن المراد تفتيشه.

- أن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.
- حضور الشخص المعنى بتفتيش مسكنه أو من ينوب عنه، وفى حالة رفض الحضور يستدعى ضابط الشرطة القضائية شاهدين من الموظفين الخاضعين لسلطته.

أما التفتيش فى الأماكن العامة، وهى التى يرتادها العامة فى كل وقت ولا تتمتع بحرمة المنزل، فلا إذن فيها، وهى نوعين، الأماكن العامة بطبيعتها على وجه دائم مثل الشوارع والحدائق العامة، والأماكن العامة بالتخصيص أو المصادفة وهى التى يرتادها الجمهور فى أوقات محددة كالمقاهى والمطاعم[٤٢].

ولا يخرج معنى التفتيش فى الوسط الافتراضى عن المعنى السابق كأصل عام حسب غالبية الفقه، فهو كذلك إجراء من إجراءات التحقيق بهدف الوصول إلى أدلة ومواجهتها بالمتهم المنسوبة إليه التهمة، إلا أن محل التفتيش يختلف فى الوسط الافتراضى عنه فى الوسط المادى؛ حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات بما تحتويه من مدخلات وتخزين ومخرجات، وذلك من أجل البحث عن الأفعال والسلوكيات المرتكبة غير المشروعة والتى تشكل جناية أو جنحة[٤٣].

ولما كان التفتيش إجراءًا من إجراءات التحقيق كان ينبغى أن يمارس من ذى صفة وهو مأمور الضبط القضائى أو جهة التحقيق حسب الأحوال، فهل لهؤلاء القدرة على تفتيش الوسط الافتراضى وضبط ما يسفر عنه التفتيش من أدلة؟

نـص القـانون الجزائـرى (٤/٩) المـؤرخ فـى ٢٠٠٩/٨/٥، المتـضمن قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فـى المـادة الخامسة منـه علـى أنـه "يـجوز للسلطات القـضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة معلوماتية.

يلاحظ إذن بأن التفتيش فى الوضعيات المشار إليها يأخذ منحنيين فهو إما أن يكون عملًا من أعمال التحقيق تقوم به السلطات القضائية المختصة، وإما يكون من أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطة المختصة، وفى كلتا الحالتين فإن المستهدف هنا هو جهاز الكمبيوتر بمكوناته المادية والمعنوية.

وفى هذا الصدد صرحت الاتفاقية الأوروبية فى شأن جرائم السير بحق الدول الأعضاء فى تفتيش أجهزة الكمبيوتر فى إطار الإجراءات الجنائية، وذلك من خلال المادة ١٩ من القسم الرابع حيث نصت على "أن لكل طرف الحق فى أن يسن من القوانين ما هو ضرورى لتمكين السلطات المختصة بالتفتيش أو الدخول إلى:

- نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة به.
- الوسائط التى يتم تخزين معلومات الكمبيوتر بها ما دامت مخزنة فى إقليمها.

- غاية التفتيش

من خلال ما تقدم يمكن القول إن الغاية من التفتيش هو الوصول إلى رصد الدليل الرقمى ومعرفة المجرم المعلوماتى وتقديمه للمحاكمة، غير أن الطابع الفنى لهذه الجرائم يجعل الأمر أكثر تعقيدًا.

ويستخلص بالنسبة للمشرع الجزائرى المبادرة على مواكبة التطور القانونى على المستوى الدولى تماشيًا مع التطور التكنولوجي بتمهيد الطريق أمام استخلاص الدليل الرقمى فى القانون رقم (٤/٩) المشار إليه سلفًا بالنص فى المادة (٦) منه على حجز المعطيات المعلوماتية؛ وذلك بإفراغها أو نسخها على دعامة تخزين إلكترونية تكون قابلة للحجز أو الوضع فى أحراز.

لكن مع ذلك فإن الصعوبة تظل قائمة أمام القائمين بالتفتيش فالتخزين الإلكترونى للبيانات أو تشفيرها يجعلها بمنأى عن وضع اليد على الدليل المستخلص منها، هذا فضلًا عما قد تثيره مشكلة تخزين المعلومات عن طريق جهاز مرتبط بالخارج وبواسطة شبكة الاتصال عن بعد وما يترتب على ذلك من المساس بسيادة الدول، وهذا التصور كله يطرح أمامنا تساؤلات حول مواصفات الدليل الرقمى فى حد ذاته ومدى توافر شروط معينة للأخذ به.

ومن البديهى القول وإعمالًا بالقواعد العامة فإنه من الضرورى أن تتوفر فى الدليل الرقمى المشروعية بمعنى أنه لا يكون مستخلصًا بطريقة مخالفة لأحكام القانون ولا مبادئ دستورية خاصة منها ما يتعلق بحماية الحريات الأساسية، وهو ما أكدته محتويات الاتفاقية الأوروبية بتاريخ ١٩٨١/١٠/٢٨ والمتعلقة بحماية الأشخاص تجاه مخاطر المعالجة الآلية

للبيانات ذات الطبيعة الشخصية ومما نصت عليه: "أن تكون الأدلة المضبوطة دقيقة وصحيحة مستمدة بطريقة شرعية"(٤٤).

ويعد تفتيش نظام الحاسوب والإنترنت من أخطر المراحل حال اتخاذ الإجراءات الجنائية ضد مرتكب الجريمة الإلكترونية، لكون محل التفتيش هنا – وهو الحاسوب والشبكات – محل جدل فقهى متزايد خاصة بالنسبة للكيان المعنوى للحاسوب أى البرامج والبيانات الإلكترونية التى بطبيعتها ليس لها أى كيان مادى محسوس، لذا نتناول تبعًا مسألة مشروعية التفتيش فى الوسط الافتراضى.

**ب – مشروعية التفتيش فى الوسط الافتراضى**

**– مكونات الوسط الافتراضى**

إن الإشكالية التى تطرح هى تحديد المقصود بمصطلح (شىء) الذى يفترض أن يكون محلًا للتفتيش والضبط فما مدى انطباق لفظ شىء على الوسط الافتراضى؟

ولذلك أهمية عملية، فإذا كانت هذه المكونات لا تكتسب صفة الشىء بالمعنى الذى يعبر عنه النص القانونى فإنها لا يمكن أن تكون محلًا للتفتيش؟

لقد ثار خلاف تشريعى وفقهى بشأن مدى جواز تفتيش المكونات المعنوية للحاسوب تمهيدًا لضبط الأدلة الرقمية، فذهب الرأى الأول إلى جواز تفتيش نظم الحاسوب، ويستند فى ذلك إلى عمومية نصوص التفتيش، وذلك من خلال توسيع تفسير عبارة ضبط أى شىء لتشمل المكونات غير المادية للحاسوب فالمادة (٤٨٧) عقوبات كندى مثلًا تقضى بإمكانية إصدار أمر قضائى لتفتيش وضبط أى شىء... تتوافر بشأنه أسس ومبررات معقولة تدعو

للاعتقاد بأن جريمة قد وقعت أو يشتبه في وقوعها، وحتى الآن فإن هذا النص يفسر بوضوح تام على أنه يسمح بتفتيش المكونات المعنوية للحاسوب[٤٥]، أو بصورة عامة التفتيش عن الدليل الرقمي.

ويذهب هذا الرأى إلى أن التفتيش والضبط لا يقتصران على الأشياء المادية، لأن الغاية من التفتيش هى البحث عن دليل بشأن الجريمة، فتحديد مدلول كلمة شيء يعنى كل ما يشغل حيزًا ماديًا فى فراغ معين، ولما كانت البرامج تشغل حيزًا ماديًا فى ذاكرة الحاسب الآلى ويمكن قياسها بمقياس معين، وتأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها ذات كيان مادى وتتشابه مع التيار الكهربائى الذى اعتبره الفقه والقضاء من قبيل الأشياء المادية، ومن ثم فهى تعد أشياءً بالمعنى العلمى للكلمة.

أما الرأى الثانى فيرى أن المقصود بلفظ الشيء هو ما كان ماديًا، ولذا فإن الوسط الافتراضى والبيانات غير المرئية أو الملموسة لا يمكن اعتبارها شيئا، ومن ثم سينحصر عنها النص القانونى الذى استعمل مصطلح شيء، ما يجعل تفتيش الوسط الافتراضى وضبط محتوياته مخالفًا للقانون، ولذلك يقترح هذا الرأى لمواجهة هذا القصور التشريعى أن يتم تعديل النصوص الخاصة بالتفتيش، وبهذا الاتجاه أخذت بعض التشريعات فنصت صراحة على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلى، ومن ذلك ما نُصَّ عليه فى قانون إساءة استعمال الحاسب الآلى فى انجلترا الصادر سنة ١٩٩٠، وهو ما نصت عليه أيضًا اتفاقية بودابست لسنة ٢٠٠١ فى المادة ١٩/١-٣[٤٦].

وفى فرنسا يرى بعض الفقهاء أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة، وبالتالى لا تعتبر

شيئًا ماديًا بالمعنى المألوف، وقد استجاب المشرع الفرنسى لهذه التغيرات وقام بتعديل نصوص التفتيش بالقانون رقم ٢٠٠٤/٥٤٥ المؤرخ فى ٢١ يونيو ٢٠٠٤، حيث قام بإضافة عبارة "المعطيات المعلوماتية" فى المادة (٩٤) من قانون الإجراءات الجزائية، لتصبح المادة على النحو التالى: "يباشر التفتيش فى جميع الأماكن التى يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدًا لإظهار الحقيقة"(٤٧).

أما فى الجزائر فإن المشرع الجزائرى جرم أفعال المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم (١٥/٤) المؤرخ فى ١٠ نوفمبر ٢٠٠٤ المعدل والمتمم لقانون العقوبات وبالتالى اعترف بالوسط الافتراضى حينما جرم مختلف الأفعال الواقعة والماسة بأنظمة المعالجة الآلية للمعطيات باستحداثه لقسم سابع مكرر سماه المساس بأنظمة المعالجة الآلية للمعطيات وأفرد له ثمانى مواد من المادة (٣٩٤) مكرر إلى المادة (٣٩٤) مكرر (٧) وعدد تلك الأفعال والتى تتمثل فى:

- الدخول أو البقاء عن طريق الغش فى كل أو جزء من منظومة للمعالجة الآلية للمعطيات.
- حذف أو تغيير لمعطيات المنظومة.
- تخريب نظام اشتغال المنظومة.
- الإدخال بطريق الغش معطيات فى نظام المعالجة الآلية أو الإزالة أو التعديل بطريق المعطيات التى يتضمنها.
- التصميم أو البحث أو التجميع أو توفير أو نشر أو الاتجار فى معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية.

كما أصدر قانون (٤/٩) المؤرخ فى ٥ أغسطس ٢٠٠٩ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المشار إليه سلفًا، إذ عرف فى المادة (٢) فقرة "ب" منه المنظومة المعلوماتية أو ما يسمى بالوسط الافتراضى بأنه: "أى نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذًا لبرنامج معين"، كما عرف المعطيات المعلوماتية فى الفقرة "ج" من ذات المادة بأنها: "أى عملية عرض للوقائع أو المعلومات أو المفاهيم فى شكل جاهز للمعالجة داخل منظومة معلوماتية، بما فى ذلك البرامج المناسبة التى من شأنها جعل منظومة معلوماتية تؤدى وظيفتها"، أما الفقرة "و" فعرفت الاتصالات الإلكترونية بأنها: "أى تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أى وسيلة إلكترونية".

وهناك اتجاه توفيقى يرى ضرورة إهمال الجدل الدائر حول مصطلح الشىء والعبرة عنده بالواقع، فالضبط لا يمكن وقوعه عمليًا إلا على أشياء مادية، ولذلك فإن المشكلة ليست مشكلة مصطلح عبر عنه النص القانونى، وإنما هى تتعلق بإمكانية اتخاذ الإجراء، وترتيبًا على ذلك فإن تفتيش الوسط الافتراضى يكون صحيحًا إذا أسفر عن وجود بيانات اتخذت فيما بعد شكلًا ماديًا، وهذا الاتجاه قد أخذ به قانون الإجراءات الألمانى فى القسم (٩٤) حينما نص على أن الأدلة المضبوطة يجب أن تكون ملموسة، ولذلك فإن البيانات إذا تمت طباعتها تعد أشياء ملموسة وبالتالى يمكن ضبطها[٤٨].

**جـ - أنواع التفتيش**

يعتبر التفتيش عن الدليل الرقمى فى الوسط الافتراضى وضبط محتوياته مشروعًا. وتتمثل أنواعه فيما يلى:

**- تفتيش المنظومة المعلوماتية عن بعد**

أجاز القانون الجزائرى بموجب القانون (٤/٩) المشار إليه سلفًا بتفتيش المنظومة المعلوماتية عن بعد ويقتضى ذلك الدخول إليها دون إذن صاحبها والولوج إلى كيان المنطقى للحاسوب، فالتفتيش هنا يستهدف أشياء معنوية وليست مادية، كالبرامج وقواعد البيانات، ولأن هذه قد تكون وسيلة لارتكاب جريمة أو تخزين معلومة بشأنها سيما إذا كانت هذه المعلومات غير مرتبطة بعد بأية دعامة مادية وإن كان المشرع الجزائرى - كما رأينا - قد أجاز إفراغ أو نسخ تلك المعلومات المشكوك فيها أو التى من شأنها الإفادة فى الكشف عن الجريمة أو مرتكبيها على دعامة تخزين إلكترونية تكون قابلة للحجز كما أوردت ذلك المادة (٦) المشار إليها أعلاه من القانون السالف الذكر، ودعائم تخزين المعلومات مختلفة منها: الأشرطة المغناطيسية والأقراص الصلبة، والأقراص اللينة ومنها كذلك المنتجات البصرية، أما إذا كانت تلك البرامج مندمجة مع كيان مادى كالقرص الصلب أو المرن فإنه من السهل الوصول إليها وضبطها كدليل إثبات ضد المتهم يقدم أمام القضاء[٤٩].

فالتفتيش عن بعد للمنظومة المعلوماتية حسب المادة (٥) من القانون (٤/٩) سواء عن قرب أى بطريقة مباشرة أو عن طريق الولوج عن بعد يأخذ طريقين:

الطريق الأول: الدخول إلى منظومة معلوماتية أو جزء منها وكذا المعطيات أو البيانات المعلوماتية المخزنة فيها.

الطريق الثانى: الدخول إلى منظومة تخزين معلوماتية.

**- تمديد التفتيش من منظومة معلوماتية إلى أخرى أو جزء منها**

يبدو أن المشرع تفطَّن إلى تقنية ذات أهمية بالغة فى عالم المعلوماتية ويتعلق الأمر بارتباط شبكة الحواسب ببعضها البعض وبالتالى وجود ترابط بين الأنظمة المعلوماتية، فمن المعلوم أن شبكة الإنترنت هى نفسها شبكة ممتدة من خلال اتصال أجهزة الحواسب الآلية اتصالًا سلكيًا أو لا سلكيًا فتكون مرتبطة ببعضها البعض فى مكان واحد وهو ما يطلق عليه الشبكة المحلية، أو موزعة ومرتبطة بواسطة خطوط الهاتف أو بواسطة الأقمار الصناعية ويطلق عليها بالشبكة الممتدة، ومما يستخلص أن القانون (٤/٩) وفى المادة الخامسة منه، وتحسبًا لما قد يقبل عليه المجرم الإلكترونى أو الجانى مستعمل أجهزة الحاسوب بغرض ارتكاب الجريمة من محاولات تهريب المعلومات وتسريبها من جهاز لآخر أو لطرفيه لتخزينها أو إخفائها فإن الوضع هنا يستدعى وفق ما تصوره المشرع طابع السرعة والدقة فى تعقب آثار وخطوات هذه الأفعال(٥٠).

**- تمديد التفتيش خارج حدود الدولة**

الأصل أنه لا يجوز امتداد التفتيش فى الوسط الافتراضى خارج حدود الدولة احترامًا لمبدأ السيادة، إذ من القواعد المتفق عليها أن نطاق تطبيق قانون الإجراءات الجنائية يرتبط بنطاق تطبيق قانون العقوبات، فكلما كان هذا الأخير

واجب التطبيق طبق الأول، ومن القواعد المتفق عليها أيضًا أنه لا تلازم بين تطبيق قانون العقوبات وارتكاب الجريمة على إقليم الدولة، إذ قد ترتكب خارج إقليمها ومع ذلك يكون قانونها واجب التطبيق، كالاختصاص وفقًا لمبدأ العينية والشخصية والعالمية، فضلًا عن ذلك فإن الجريمة قد ترتكب فى إقليم دولة ما وتمتد آثارها إلى إقليم دولة أخرى، فإذا كانت هذه الدولة مختصة بالتحقيق فى هذه الجريمة لأن قانون عقوباتها واجب التطبيق، ومع ذلك يجوز الحصول على الأدلة الموجودة فى وسط افتراضى خارج حدود الدولة تطبيقًا لاتفاقات الإنابة القضائية، أو وفقًا لنظام تبادل المساعدات، كما لا يجوز تفتيش النظام المعلوماتى الممتد لمنزل غير المتهم إلا فى الأحوال التى يجوز فيها تفتيش منزل غير المتهم.

علينا بداية أن نشير إلى أن الوسط الافتراضى للشبكة المعلوماتية لا يرتبط بنطاق إقليم دولة ما، ولذا فإن مكان تفتيشه هو المكان الذى يوجد به الحاسب الآلى المراد تفتيشه.

إن اختصاص الدولة بالتحقيق فى جريمة ما وإن كان يخولها تطبيق قانون إجراءاتها بشأن هذا التحقيق بصرف النظر عن مكان وقوع الجريمة مادامت خاضعة لقانون العقوبات الخاص بها، إلا أن ذلك لا يعنى أن تباشر الدولة هذه الإجراءات خارج إقليمها، إذ يتعذر على الدولة مباشرة اختصاصاتها بالتحقيق خارج إقليمها، لأن ذلك من مظاهر سيادتها فلا يسمح لها بممارسته على إقليم دولة أخرى، ولذا فمن المتعذر قانونًا مباشرة الدولة المختصة بالتحقيق لأى إجراء خارج إقليمها بشأن الجريمة رغم انعقاد اختصاصها بالتحقيق فيها، ولذا تبدو مشكلة الحصول على دليل بشأن بعض الجرائم إذا

كان الدليل المراد الحصول عليه يوجد فى جهاز موجود فى دولة أخرى فى إطار الإشكالية المعروضة، إذ لن تتمكن سلطات التحقيق من الحصول عليه، ولذا تبدو اتفاقيات الإنابة القضائية هى السبيل لتحصيل هذا الدليل، بحيث تفوض الدولة الأخرى فى جمع هذا الدليل وإرساله لدولة التحقيق، وقد نصت المادة (٢٥ /أ) من قانون الحاسوب الهولندى على الاعتداد بالدليل المتحصل عليه فى إقليم دولة أخرى إذا تم ذلك تنفيذًا لاتفاقيات التعاون الأمنى والقضائى، وأحيانًا تكون تلك الدولة مختصة هى الأخرى بالتحقيق فى هذه الجريمة، ولذا فإن هى لم ترغب فى مباشرة التحقيق بشأنها قد تتطوع بتزويد دولة التحقيق بالبيانات التى تم ضبطها وفقًا لما يعرف بنظام تبادل المعلومات أو المساعدات، وقد نصت اتفاقية بودابست على هذا النظام فى المادة (١/٢٥) بقولها (تقوم الدول الأطراف بالاتفاقية بتقديم المساعدات المتبادلة لبعضها البعض إلى أقصى حد ممكن، وذلك للأغراض الخاصة بعمليات التحقيق أو الإجراءات المتعلقة بالجرائم التى لها علاقة بنظم وبيانات الكمبيوتر، أو بالنسبة لتجميع الأدلة الخاصة بالجريمة فى شكل إلكترونى).

وغنى عن البيان أن تفتيش الوسط الافتراضى يأخذ حكم المكان الذى توجد به الآلة، فإذا وجد فى مكان يصدق عليه وصف المنزل وجب الالتزام فى تفتيشه بالأحكام الخاصة بتفتيش المنازل.

غير أن السؤال الذى يُطرح هنا ما الحكم لو كانت النهاية الطرفية للنظام المعلوماتى المراد تفتيشه تمتد لمنزل آخر غير منزل المتهم فهل يمكن تفتيشه فى هذه الحالة؟

لقد حسمت بعض القوانين هذه المسألة بإجازة التفتيش فى هذا الحالة، كالقانون الهولندى بالمادة (٢٥/أ) من قانون جرائم الحاسوب ودون حاجة للحصول على إذن مسبق من أية جهة شريطة ألا تكون النهاية الطرفية لذلك النظام فى إقليم دولة آخر[٥١]، ونحن نعتقد أن هذا الحكم لا يمكن إعماله بإطلاق فى ضوء نصوص القانون الليبى، لأن هذا النوع من التفتيش ينطوى فى الحقيقة على معنى تفتيش غير المتهم، ولذلك فإنه لا يجوز إعماله إلا فى الأحوال التى يجوز فيها للقائم بالتفتيش تفتيش غير المتهم أو منزله.

يشترط فى القائم بالتفتيش أن يكون متمتعًا بصفة حددها القانون، ولذلك قد يصعب على هؤلاء القيام بالتفتيش فى الوسط الافتراضى لقلة أو لانعدام الثقافة الفنية التى يستلزمها هذا الإجراء، ولا سبيل لتجاوز هذه الإشكالية فى الوضع الراهن إلا بالاعتماد على الخبرة، مع العلم أن هذا النظام يظل قاصرًا فى مواجهة حالة الاستعجال كالتى تجسدها حالة التلبس.

ومما تقدم نخلص إلى أن الكيان المعنوى أو الوسط الافتراضى، والبيانات المتحصلة منه ينطبق عليها لفظ الشىء، ولذا فإن تفتيش ذلك الوسط يعد صحيحًا وفقًا للقانون، كما تعد البيانات الموجودة بذلك الوسط أشياء مما يصح ضبطها.

وكما هو الشأن فى مختلف التشريعات فالتفتيش "غايته ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد فى كشف الحقيقة فى شأنها".

**ثانياً: حجية الدليل الرقمى**

إن مجرد الحصول على الدليل الرقمى وتقديمه للقضاء لا يكفى لاعتماده كدليل للإدانة، إذ أن الطبيعة الفنية الخاصة للدليل الرقمى تُمكِّن من العبث بمضمونه

على نحو يحرِّف الحقيقة دون أن يكون فى قدرة غير المتخصص إدراك ذلك العبث، فضلًا عن ذلك فإن نسبة الخطأ فى إجراءات الحصول على دليل صادق فى الإخبار عن الحقيقة تبدو عالية فى مثل هذا النوع من الأدلة، ولذلك تثور فكرة الشك فى مصداقيتها كأدلة للإثبات الجنائى، فهل من شأن ذلك استبعاد الدليل الرقمى من دائرة أدلة الإثبات الجنائى لتعارضه مع قرينة البراءة؟ لذا سنحاول دراسة مسألتين وهما، تقدير الدليل الرقمى، وسائل تقسيم الدليل الرقمى فيما يلى:

**١ – تقدير الدليل الرقمى**

فى ظل النظم القانونية التى تعتمد النظام اللاتينى فى الإثبات – كالنظام القانونى الجزائرى – فإن القاضى يملك سلطة واسعة فى تقييم الدليل من حيث قيمته التدليلية، فللقاضى قبول الدليل أو رفضه وهو يعتمد فى ذلك على مدى اقتناعه الشخصى بذلك الدليل، وهذا المعنى هو ما نصت عليه المادة (٢١٢) من قانون الإجراءات الجزائية الجزائرى، فهل يمكن للقاضى الجنائى وفقًا لهذا النظام أن يُعمل سلطته التقديرية لقبول هذا الدليل أو رفضه بما يمكنه من استبعاد الدليل الرقمى لعدم الاقتناع به أو للشك فى مصداقيته؟

إن سلطة القاضى الجنائى فى تقدير الدليل لا يمكن أن نتوسع فى شأنها بحيث يقال إن هذه السلطة تمتد لتشمل الأدلة العلمية، فالقاضى بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الرقمى، فضلًا عن ذلك فإن هذا الدليل يتمتع من حيث قوته التدليلية بقيمة إثباتيه قد تصل إلى حد اليقين، فهذا هو شأن الأدلة العلمية عمومًا، فالدليل الرقمى من حيث تدليله على الواقع تتوافر فيه شروط اليقين، مما لا يمكن معه القبول بممارسة القاضى

لسلطته فى التأكد من ثبوت تلك الوقائع التى يعبر عنها ذلك الدليل، ولكن هذا لا يناقض ما سبق أن قدمناه من أن الدليل الرقمى هو موضع شك من حيث سلامته من العبث من ناحية وصحة الإجراءات المتبعة فى الحصول عليه من ناحية أخرى، حيث يشكك فى سلامة الدليل الرقمى من ناحيتين:

**الأولى:** الدليل الرقمى من الممكن خضوعه للعبث للخروج به على نحو يخالف الحقيقة ومن ثم فقد يقدم هذا الدليل معبرًا عن واقعة معينة صنع أساسًا لأجل التعبير عنها خلافًا للحقيقة، وذلك دون أن يكون فى استطاعة غير المتخصص إدراك ذلك العبث، على نحو يمكن معه القول إن ذلك قد أصبح هو الشأن فى النظر لسائر الأدلة الرقمية التى قد تقدم للقضاء، فالتقنية الحديثة تمكّن من العبث بالدليل الرقمى بسهولة ويسر بحيث يظهر وكأنه نسخة أصلية فى تعبيرها عن الحقيقة.

**الثانية:** وإن كانت نسبة الخطأ الفنى فى الحصول على الدليل الرقمى نادرة للغاية، إلا أنها تظل ممكنة، ويرجع الخطأ فى الحصول على الدليل الرقمى لسببين، وهما:

السبب الأول: الخطأ فى استخدام الأداة المناسبة فى الحصول على الدليل الرقمى، ويرجع ذلك للخلل فى الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة.

السبب الثانى: الخطأ فى استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن ١٠٠٪ ويحدث هذا غالبًا بسبب وسائل اختزال البيانات أو

بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التى تم تقييمها.

ومن ذلك فإننا نخلص إلى أن الشك فى الدليل الرقمى لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه، ولكنها تؤثر فى مصداقيته، ولكن هل يمكن التثبت من سلامة الدليل الرقمى من حيث العيوب؟

وبكلمة أوضح هل من الممكن أن يُضفى على الدليل الرقمى اليقين من خلال إخضاعه للتقييم الفنى الذى يمكّن من تفادى تلك العيوب التى تشوبه؟ وما موقف القاضى الجنائى من هذا الدليل إذا ما خضع لمثل ذلك التقييم؟

مثلما يخضع الدليل الرقمى لقواعد معينة تحكم طرق الحصول عليه، فإنه يخضع لقواعد أخرى للحكم على قيمته التدليلية، وذلك يرجع للطبيعة الفنية لهذا الدليل، وعليه فهناك وسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وصحة الإجراءات المتبعة فى الحصول عليه، وسوف نحاول فيما يلى تناول بعض هذه الوسائل[٥٢].

**٢ – وسائل تقييم الدليل الرقمى**

سوف نتناول وسائل تقييم الدليل الرقمى من حيث سلامته من العبث، ثم وسائل تقييمه من حيث سلامة الإجراءات المتبعة للحصول عليه من الناحية الفنية وذلك على النحو التالى:

**أ – تقييم الدليل الرقمى من حيث سلامته من العبث**

يمكن التأكد من سلامة الدليل الرقمى من العبث بعدة طرق نذكر منها:

- يلعب علم الكمبيوتر دورًا مهمًا فى تقديم المعلومات الفنية التى تسهم فى فهم مضمون وهيئة الدليل الرقمى، وهذه العلوم يستعان بها فى كشف مدى التلاعب بمضمون هذا الدليل، وتبدو فكرة التحليل التناظرى الرقمى من الوسائل المهمة للكشف عن مصداقية الدليل الرقمى، ومن خلالها تتم مقارنة الدليل الرقمى المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن خلال ذلك يتم التأكد من مدى حصول عبث فى النسخة المستخرجة أم لا[٥٣].
- حتى فى حالة عدم الحصول على النسخة الأصلية للدليل الرقمى أو فى حالة أن العبث قد وقع على النسخة الأصلية، ففى الإمكان التأكد من سلامة الدليل الرقمى من التبديل أو العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات.
- هناك نوع من الأدلة الرقمية يسمى بالدليل المحايد، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يسهم فى التأكد من مدى سلامة الدليل الرقمى المقصود من حيث عدم حصول تعديل أو تغيير فى النظام (الكمبيوترى). فمن خلال هذه الطرق يمكن التأكد من سلامة الدليل الرقمى ومطابقته للواقع.

**ب – تقييم الدليل الرقمى من حيث السلامة الفنية للإجراءات المستخدمة فى الحصول عليه**

عادة تتبع جملة من الإجراءات الفنية للحصول على الدليل الرقمى، وقد قدمنا أن هذه الإجراءات من الممكن أن يعتريها خطأ قد يشكك فى سلامة نتائجها، ولذا فإنه يمكن فى هذا الشأن اعتماد ما يعرف باختبارات (داو بورت)[٥٤]

كوسيلة للتأكد من سلامة الإجراءات المتبعة فى الحصول على الدليل الرقمى من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات، ولذا فإننا سنعرض باختصار للخطوات التى تتبع للتأكد من سلامة هذه الإجراءات من الناحية الفنية.

من خلال ما تقدم يمكن الوقوف على سلامة الدليل الرقمى، فإذا توافرت فى الدليل الرقمى الشروط العامة لما يمكن أن يمثل أساسًا لانبعاث الثقة فيه، فإنه قد يبدو من غير المقبول أن يعيد القاضى تقييم هذا الدليل وطرحه من جديد على بساط البحث، فالدليل الرقمى بوصفه دليلًا علميًا فإن دلالته قاطعة بشأن الواقعة المستشهد به عنها، فإذا سلمنا سابقًا بإمكانية التشكيك فى سلامة الدليل الرقمى بسبب قابليته للعبث ونسبة الخطأ فى إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضى أن يقطع فى شأنهما برأي حاسم وإن لم يقطع به أهل الاختصاص، ولذلك فإذا توافرت فى الدليل الرقمى الشروط المذكورة سابقًا بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استنادًا لسلطة القاضى التقديرية وفقًا للمادة ٢١٢ من قانون الإجراءات الجزائية، إذ سلطة القاضى فى رد الدليل استنادًا لفكرة الشك يلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك فى الدليل، وهو ما لا يستطيع القاضى الجزم به متى توافرت فى هذا الدليل شروط السلامة، بحيث يقتصر دور القاضى على بحث صلة الدليل بالجريمة.

مع ملاحظة أنه قد يكون الدليل الرقمى متضمنًا إثبات الجريمة ومرتكبها معًا، فجسم الجريمة المعلوماتية عادة هو الدليل الرقمى ذاته، وقد يكون هذا الجسم "الدليل الرقمى" متضمنًا ما يفيد نسبة الجريمة لشخص ما،

كما لو أرسل شخص لآخر رسالة عبر البريد الإلكترونى تتضمن فيروسات تؤدى إلى إتلاف الموقع الإلكترونى الخاص بذلك الشخص، فإن هذه الرسالة بذاتها تعد دليلًا على وقوع الجريمة، وفى الوقت نفسه ستعد دليلًا على نسبة ارتكابها لشخص معين وهو المرسل إذا تضمنت بيانات تدل على شخصية.

ومما تقدم نخلص إلى أن الدليل الرقمى يصلح لإثبات الجريمة التى ترتكب باستعمال الآلة الرقمية – حاسوب – هاتف،... الخ، أو الجريمة التى ترتكب ضد الكيان المعنوى للآلة أو ضد شبكة المعلومات العالمية.

بالإضافة إلى ذلك فإن هذا الدليل يصلح لإثبات الجرائم إذا ما استعملت الآلة الرقمية للتمهيد لارتكاب الجريمة أو لإخفاء معالمها، كالمراسلات التى يبعث بها الجانى لشريكه وتتضمن معلومات عن جريمة ينويان ارتكابها أو يطلب منه إخفاء معالم هذه الجريمة، فتلك المراسلة تصلح كدليل إثبات لهذه الجريمة حال وقوعها رغم أنها لم ترتكب ضد الآلة الرقمية ولا بواسطتها.

## الخاتمة

نخلص إلى القول إن البيئة الرقمية التى يعيش فيها الدليل الإلكترونى بيئة متطورة بطبيعتها تشتمل على أنواع متعددة من البيانات الرقمية أو مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التى يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر فى شكل صور أو تسجيلات صوتية أو مرئية تصلح لكى تكون دليلا للإدانة أو البراءة، وقد انعكس هذا العالم الرقمى على طبيعة هذا الدليل الرقمى مما جعله يمتاز بصفة الدليل العلمى والتقنى الذى يصعب التخلص منه إذ هذه المسألة لا تعتبر من العوائق التى

تحيل دون استرداد الملفات التى تم من قبل إلغائها أو محوها من الحاسب الآلى أو إظهارها وهذا ما يعنى صعوبة إخفاء الجانى لجريمته، كما أنه دليل قابل للنسخ ويسجل المعلومات عن الجانى ورصدها وتحليلها فى الوقت نفسه، وعلى كل يتميز الدليل الرقمى بصعوبة محوه أو تحطيمه، ويمكن كشف محاولة الجانى محو هذا الدليل لتتخذ بذاتها دليلا ضده، كما أن الدليل الرقمى ليس له صورة واحدة، بل يوجد له العديد من الصور والأشكال والتى تظهر كأدلة رقمية خاصة بأجهزة الحاسب الآلى وشبكاتها، وأدلة رقمية خاصة بالشبكة العالمية لمعلومات الإنترنت، وأدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات، وأدلة خاصة بالشبكة العالمية للمعلومات، فمجرد وجود دليل يثبت وقوع الجريمة وينسبها لشخص معين لا يكفى للتعويل عليه لإصدار الحكم بالإدانة إذ يلزم أن تكون لهذا الدليل قيمة قانونية، وهذه القيمة للدليل الجنائى تتوقف على مسألتين رئيستين الأولى المشروعيةً، والثانية اليقينية فى دلالته على الوقائع المراد إثباتها إذ له حجية قاطعة فى الدلالة على الوقائع التى يتضمنها، ويمكن التغلب على مشكلة الشك فى مصداقيته من خلال إخضاعه لاختبارات تمكن من التأكد من صحته.

ولذا يمكننا القول إن ما يثيره الدليل الرقمى من حيث مشروعية الحصول عليه يتركز بشكل أساسى فى إجراءات التفتيش للبحث عن هذا الدليل، ولا يخرج معنى التفتيش فى الوسط الافتراضى عن المعنى التقليدى له، إلا أن محل التفتيش يختلف فى الوسط الافتراضى عنه فى الوسط المادى، حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات، وذلك من أجل البحث عن الأفعال الإجرامية.

**ولكن**، وحسب التشريع الجزائرى، وعلى خلاف مقتضيات القواعد العامة للتفتيش باعتباره من إجراءات التحقيق لجميع الأدلة والقرائن، خرج المشرع عن هذه القاعدة بحيث جعل التفتيش مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة المعلوماتية من خلال القيام بعمليات المراقبة التقنية المسبقة وفق القانون المستحدث رقم (٤/٩) المؤرخ فى ٥ أغسطس ٢٠٠٩ المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، فيكون بذلك قد خرج عن القواعد العامة وجعل التفتيش على الأدلة الرقمية المنصب على المنظومة المعلوماتية إجراء وقائى فى مواجهة المجرم المعلوماتى دون توجيه الاتهام لأى شخص.

وإن مجرد الحصول على الدليل الرقمى وتقديمه للقضاء لا يكفى لاعتماده كدليل للإدانة، إذ الطبيعة الفنية الخاصة للدليل الرقمى تُمكِّن من العبث بمضمونه على نحو يحرِّف الحقيقة دون أن يكون فى قدرة غير المتخصص إدراك ذلك العبث، وعليه فإنه فى مثل هذا النظام لا تثور مشكلة مشروعية الدليل الرقمى من حيث الوجود، على اعتبار أن المشرع لا يُعهد عنه سياسة النص على قائمة لأدلة الإثبات، ولذلك فمسألة قبول الدليل الرقمى لا ينال منها سوى مدى اقتناع القاضى به إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائى.

مع ملاحظة أن المشرع الجزائرى استحدث جهة مختصة بمكافحة الجريمة المعلوماتية تتبع جهاز الشرطة، بحيث يتم تأهيل أفرادها للتعامل مع النظام المعلوماتى بما يمكنهم من تفتيش الوسط الافتراضى وضبط محتوياته بموجب القانون (٤/٩) المؤرخ فى ٥ أغسطس ٢٠٠٩ السابق الإشارة

إليه والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وهى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

**وختامًا فنكون قد توصلنا إلى أهم التوصيات والمتمثلة فى:**

- ضرورة النص صراحة على الأدلة الرقمية كأدلة إثبات فى المجال الجنائى والاعتراف لها بحجية قاطعة باعتبارها استثناءً على سلطة القاضى الجنائى فى تقدير الدليل، مع إمكانية النص على وسائل التأكد من سلامة الدليل الرقمى باعتبارها شرطًا لقبول هذا الدليل النص صراحة على جواز تفتيش الوسط الافتراضى وضبط محتوياته.
- التوسع فى عقد الاتفاقيات الدولية للاستفادة من نظام الإنابة القضائية والمساعدات القضائية الدولية المتبادلة وتبادل المعلومات فى المجال المعلوماتى لتفادى مشكلة البحث عن الدليل الرقمى خارج حدود الدولة.

# المراجـــع


١ – على محمود على حموده، الأدلة المحصلة من الوسائل الإلكترونية فى إطار نظرية الإثبات الجنائى، المؤتمر العالمى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، ٢٦-٢٨ نيسان، أكاديمية شرطة دبى، دورية مركز البحوث والدراسات، العدد الأول، ٢٠٠٣، ص ٢١.

٢ – ممدوح عبدالحميد عبدالمطلب، البحث والتحقيق الجنائى الرقمى فى جرائم الكمبيوتر والإنترنت، القاهرة، دار الكتب القانونية، ٢٠٠٦، ص ٨٨.

٣ – عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٤، ص ٩٦٩؛ عمر محمد بن يونس، مذكرات فى الإثبات الجنائى عبر الإنترنت، ندوة الدليل الرقمى، مصر، جامعة الدول العربية، ٥- ٨ مارس٢٠٠٦، ص٥.

4 - Eoghan Casey, Digital Evidence and Computer Crime, London, Academic Press, 2000, p. 260.

٥ – محمد الأمين البشرى، التحقيق فى الجرائم المستحدثة، الطبعة الأولى،الرياض، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٤، ص ٢٣٤؛ محمد الأمين البشرى، الأدلة الجنائية مفهومها ودورها فى الإثبات، المجلة العربية للدراسات الأمنية، المجلد ١٧، العدد ٣٣، أبريل، ٢٠٠٢، ص ١١٩.

٦ – عبدالفتاح بيومى حجازى، الدليل الجنائى والتزوير فى جرائم الكمبيوتر والإنترنت، القاهرة، دار الكتب القانونية، ٢٠٠٤، ص ص ٦٣-٦٤.

٧ – محمود صالح العادلي، الفراغ التشريعى فى مجال مكافحة الجرائم الإلكترونية، بحث منشور فى منتدى قوانين قطر، على الموقع الإلكترونى:
http://www.echoroukonline.com

٨ – عائشة بن قارة، حجية الدليل الإلكترونى فى مجال الإثبات الجنائى فى القانون الجزائرى والقانون المقارن، الإسكندرية، دار الجامعة الجديدة، ٢٠١٠، ص ٦١-٦٢.

٩ – عمر محمد أبو بكر أبو يونس، المرجع السابق، ص ٧.

١٠ – المرجع السابق، ص ص ٩٨١-٩٨٢.

١١ – عائشة بن قارة، مرجع سابق، ص ص ٦٣ -٦٤.

١٢ – ممدوح عبدالحميد عبدالمطلب، مرجع سابق، ص ٨٩؛ عائشة بن قارة، المرجع السابق، ص ٦٤.

١٣ – ممدوح عبدالحميد عبدالمطلب؛ زبيدة محمد قاسم؛ عبدالله عبدالعزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس المنعقد في الفترة من ١٠-١٢، غرفة تجارة وصناعة دبي، مايو ٢٠٠٣، ص ٢٢٣٧.

١٤ – راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، بحث مقدم للمؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الإنترنت، ٢- ٤ يونيو ٢٠٠٨، ص ٥ وما بعدها، على الموقع الإلكتروني: http://www.f-law.net.

١٥ – عائشة بن قارة، مرجع سابق، ص ٧٢.

١٦ – علي محمود علي حمودة، مرجع سابق، ص ٢٣.

١٧ – طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، انظر الموقع الإلكتروني التالي: www.startimes.com.

18 - Eoghan Casey, Digital Evidence and Computer Crime, New York, Academic Press, 2000, p. 259.

١٩ – ممدوح عبدالحميد عبدالمطلب، مرجع سابق، ص ٨٨؛ وعائشة بن قارة، مرجع سابق، ص ٧٢.

20 - Ronald L. Mendle, Investigating Computer Crimes: A Primer for Security Manager, New York, Charles Thomas , 1998, p. 131.

٢١ – عائشة بن قارة، المرجع السابق، ص ٧٢.

٢٢ – قانون (٠٩-٠٤) المؤرخ في ٢٠٠٩/٠٨/٥ يتضمن قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، عدد ٤٧، الصادرة بتاريخ ٢٠٠٩/٠٨/١٦.

٢٣ – عبدالله حسين على محمود، مرجع سابق، ص ٣٩٧.

٢٤ – محمد الأمين البشرى، مرجع سابق، ص ٧١.

٢٥ – عبدالله حسين على محمود، مرجع سابق، ص ٣٩٨.

٢٦ – عمر أبو بكر يونس، مرجع سابق، ص ١٠١٨.

٢٧ – محمد الأمين البشرى، مرجع سابق، ص ص ٧١-٧٢.

٢٨ – عبدالله حسين على محمود، مرجع سابق، ص ص ٣٩٩-٤٠٠.

٢٩ – محمد الأمين البشرى، مرجع سابق، ص٧٢.

٣٠ – ممدوح عبدالحميد عبدالمطلب، البحث والتحقيق الجنائى الرقمى فى جرائم الحاسب الآلى والإنترنت، مرجع سابق، ص ٨٨.

٣١ – عمر محمد بن يونس، مذكرات فى الإثبات الجنائى عبر الإنترنت، ندوة الدليل الرقمى، مرجع سابق، ص ص ١٢.

٣٢ – هلالى عبدالإله أحمد، حجية المخرجات الكمبيوترية فى المواد الجنائية، دراسة مقارنة، بدون ناشر، ١٩٩٩، ص ٤٩.

٣٣ – عائشة بن قارة، مرجع سابق، ص ١٩٦.

٣٤ – عمر محمد أبو بكر بن يونس، المرجع السابق، ص ٩٦٠.

٣٥ – نجد بريطانيا مثلًا قد بدأت تخفف من غلوائه، حيث ظهر فيها ما يعرف بقاعدة الإدانة دون أدنى شك، والتى مفادها أن القاضى يستطيع أن يكوِّن عقيدته من أى دليل وإن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قاطعًا فى دلالته، انظر: هلالى عبدالإله أحمد، مرجع سابق، ص ٩١.

٣٦ – هلالى عبدالإله أحمد، المرجع السابق، ص ص ٢٩ – ٣٤ .

٣٧ – عائشة بن قارة، مرجع سابق، ص ١٠٣.

٣٨ – تثبت جريمة الزنا وفقًا للمادة ٣٤١ من قانون العقوبات الجزائرى إما بناء على محضر قضائى يحرره أحد رجال الضبط القضائى عن حالة التلبس، وإما بالإقرار الوارد فى رسائل أو مستندات صادرة عن المتهم أو بإقرار قضائى.

٣٩ – هلالى عبدالإله أحمد، مرجع سابق، ص ص ٦٤-٦٥.

٤٠ – عوض محمد عوض، قانون الإجراءات الجنائى، الجزء الأول، القاهرة، مؤسسة الثقافة الجامعية، ٢٠٠٥، ص ٤٧٥.

٤١ – عائشة بن قارة، مرجع سابق، ص ص ٨٧–٨٨.

٤٢ – محمود نجيب حسنى، شرح قانون العقوبات، القسم العام، القاهرة، دار النهضة العربية، ١٩٨٨، ص ٥٨١.

٤٣ – على محمود على حمودة، مرجع سابق، ص ٢٤.

٤٤ – زبيحة زيدان، الجريمة المعلوماتية فى التشريع الجزائرى والدولى، مليله، الجزائر، دار الهدى، ٢٠١٣، ص ١٧٣.

٤٥ – هلالى عبدالإله أحمد، تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى، دراسة مقارنة، القاهرة، دار النهضة العربية، ٢٠٠٦، ص ٢٠١.

٤٦ – على محمود على حمودة، مرجع سابق، ص ص ٢٥ –٢٦.

٤٧ – عائشة بن قارة، مرجع سابق، ص ٩١.

٤٨ – هلالى عبدالإله أحمد، تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى، مرجع سابق، ص ٢٠٢.

٤٩ – زبيحة زيدان، مرجع سابق، ص ص ١٣٤–١٣٥.

٥٠ – المرجع السابق، ص ص ١٣٩–١٤٠.

٥١ – على حسن الطوالبة، دعاوى الجرائم الإلكترونية وأدلة إثباتها فى التشريعات العربية بين الواقع والمأمول، ورقة علمية مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا فى الدول العربية، السودان، ٢٣ – ٢٥ ديسمبر، ٢٠١٢، ص ص ١٣–١٤.

٥٢ – ممدوح عبدالحميد عبدالمطلب؛ زبيده محمد قاسم؛ عبدالله عبدالعزيز، مرجع سابق، ص ٢٢٥٣.

٥٣ – المرجع السابق، ص ص ٢٢٤١–٢٢٤٧.

٥٤ – المرجع السابق، ص ص ٢٢٤٨ – ٢٢٤٩.

# DIGITAL GUIDE IN CRIMINAL EVIDENCE FIELD ACCORDING TO ALGERIAN LEGISLATION

**Waheba El Awarem**

The current development of electronic means, is reflected in Penal law as the illegal use of electronic technology led to the appearance of a new science in criminal research.

The digital criminal research science is concerned with the digital evidence relative to electronic crimes. The effect is also reflected in the criminal procedural law; where this law may not be applied due to the inability of the first law to adopt the new crimes committed via electronic means. Moreover, the criminal evidence is one of the important topics in such law that is affected by the enormous development of criminal evidence due to the developed ways of crime committing. This requires to alter the perspective of criminal evidence in order to approximate the scientific truth in current reality to the judicial truth.