

جامعة المسيلة  
كلية الحقوق والعلوم السياسية  
قسم الحقوق

## الإثبات الجنائي بالأدلة الرقمية

مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق  
تخصص قانون جنائي

الأستاذ المشرف:

د. بلواضح الطيب

إعداد الطالب:

طاهري عبد المطلب

السنة الجامعية: 2014 – 2015

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

# إهداء

إلى الوالدين الكريمين أطال الله في عمرهما

إلى إخوتي عبد الحكيم، رفيق عبد الباسط، سليمان عبد الكافي، محمد عبد المحسن

إلى كل الأهل والأقارب والأصدقاء...

إلى كل من ساعدني من قريب أو بعيد في إنجاز هذه المذكرة...

إلى هؤلاء جميعا أهدي هذا العمل المتواضع...

# شكر و عرفان

في المقام الأول أتوجه إلى الله سبحانه وتعالى بالحمد والشكر، لأنه منّ علي بالتوفيق والقدرة الكبيرين لإجاز هذا البحث المتواضع، فالحمد لله حمدا طيبا مباركا فيه.

كما لا يسعني إلا أن أتقدم بجزيل الشكر والامتنان إلى أستاذي الفاضل الدكتور: بلواضح الطيب الذي تكرم علي بإشرافه وسديد توجيهاته إلى غاية إتمام هذا البحث، كما أشكر جميع أساتذة كلية الحقوق بجامعة المسيلة على المجهودات التي بذلوها من أجلنا، وجزاهم الله عنا كل خير وجعلهم نبراسا يضيء طريق كل طالب علم.

أدى التطور التكنولوجي الكبير في هذا العصر إلى إنتاج وسائل تقنية حديثة كأجهزة الحاسب الآلي وشبكة الإنترنت، وعملت تلك الوسائل على تغيير حياة الأفراد اليومية وعلاقاتهم الاجتماعية، حتى أصبح الاعتماد عليها كبيرا في شتى مجالات الحياة.

ولا شك أن الثورة المعلوماتية قد تركت آثارا إيجابية وشكلت قفزة نوعية في حياة الأفراد والدول، لما تتميز به من السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها، إلا أن هذا الجانب والآثار الإيجابية التي خلفتها لا ينفى الجوانب السلبية التي أنتجتها، والمتمثلة أساسا في ظهور جرائم مستحدثة لم تكن معهودة من قبل، واصطلح على تسميتها الكثير من الباحثين والمتخصصين **بالجرائم المعلوماتية**، والتي أصبحت في الوقت الحاضر خطرا يهدد مصالح الأفراد والدول في جميع المجالات.

ولمكافحة الجريمة المعلوماتية أصبح من الضروري إيجاد وسائل جديدة تختلف جذريا عن ما يتم استعماله في مكافحة الجريمة العادية، وذلك بسبب عجز إجراءات التحقيق التقليدية في مجارة نسق تطور هذه الجريمة، بالإضافة إلى عجز الأدلة الجنائية المادية في إثبات وقوعها، وهو ما توجب على جهات التحقيق الاعتماد على نوع جديد من الأدلة الجنائية في مجال الإثبات الجنائي تعرف **بالأدلة الجنائية الرقمية**.

إن موضوع الأدلة الجنائية من المواضيع التي هي في تطور مستمر، ويظهر صدق هذه الملاحظة سواء أتعلمت بالدليل نفسه أم بوسائل الوصول إلى الدليل، وعلى هذا الأساس تكمن أهمية موضوع **"الإثبات الجنائي بالأدلة الرقمية"** في أنها تعالج نوعا جديدا من الأدلة الجنائية من الناحيتين الفنية والقانونية، ومن جهة أخرى تعالج الإشكاليات الإجرائية التي أثارتهامثل: كيفية تفتيش أنظمة الحاسب الآلي واستخلاص الأدلة الجنائية الرقمية، معاينة

مسرح الجريمة المعلوماتية، ضبط الأدلة الجنائية الرقمية والصعوبات التي تعترض هذه العملية، وفي الأخير حجيتها أمام القضاء الجنائي في التشريعين الجزائري والفرنسي.

ولعل من بين أهم الأسباب التي دفعتني لاختيار موضوع الإثبات الجنائي بالأدلة رقمية هو رغبة مني في إثراء الدراسات الجامعية النظرية، وذلك بسبب ندرة الأبحاث والدراسات المتعلقة بتحديد ماهية الأدلة الجنائية الرقمية وحجيتها أمام القضاء الجنائي، بحيث أن هذه الأدلة لم يتم دراستها بشكل علمي وقانوني معمق في الجزائر، وإنما تم التطرق إليها في مؤلفات عامة وبشكل مقتضب دون أن يتم الإحاطة بها.

وقد اعتمدنا في بحثنا هذا على بعض الدراسات السابقة ذات الصلة على النحو التالي:

**1) دراسة محمد الأمين البشري بعنوان: الأدلة الجنائية الرقمية (مفهومها ودورها في الإثبات)، والمنشورة في المجلة العربية للدراسات الأمنية والتدريب، في العدد 33 من المجلد 17، والصادرة عن أكاديمية نايف العربية للعلوم الأمنية بالسعودية سنة 1995، تناول فيها موضوع الأدلة الجنائية الرقمية بالتعريف والتأصيل، وعالج أيضا حجيتها أمام القضاء الجنائي السعودي.**

وتوصلت هذه الدراسة إلى عدة نتائج أهمها اعتبار الأدلة الجنائية الرقمية من أكثر أنواع الأدلة المادية وفرة وثباتا، وأيضا تشكل هذه الأدلة ثروة للعدالة الجنائية متى أحسن استغلالها، ومن جهة أخرى لها حجية في الإثبات أمام المحاكم المدنية والشرعية (السعودية) لما لها من أسس علمية مؤهلة نالت بها الثقة والمصادقية.

**(2) دراسة خالد عياد الحلبي بعنوان: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت،** الصادرة عن دار الثقافة للنشر والتوزيع بالأردن سنة 2011، والتي تناول فيها الإطار الواقعي والقانوني لجرائم الحاسوب والإنترنت، بالإضافة إلى إجراءات التحقيق الفنية والقانونية، كما تناول فيها أيضا الإثبات الجنائي بواسطة الدليل الإلكتروني من خلال بيان ماهيته وطبيعته القانونية في مجال الإثبات الجنائي.

ومن خلال هذه الدراسة فإنه توصل إلى عدة نتائج أهمها أن الاعتماد على إجراءات التحقيق التقليدية غير كافية لمواجهة جرائم الحاسوب والإنترنت، وعاجزة عن التعامل مع الأدلة الإلكترونية التي تقتضي توفر وسائل فنية لاستخلاصها وتحليلها.

**(3) دراسة عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري بعنوان: الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة)،** والصادرة عن جامعة نايف العربية للعلوم الأمنية بالسعودية في سنة 2007، والتي تناول فيها الباحثان عملية الإثبات الجنائي للجريمة المعلوماتية ومدى صلاحية الطرق التقليدية لإثبات هذا النوع من الجرائم.

وتوصل الباحثان إلى عدة نتائج أهمها أن الدليل الجنائي الرقمي المحمل بملفات القرص الصلب بجهاز الحاسب الآلي، يرتبط ويتكامل مع الدليل الجنائي المادي، زيادة على ذلك أن نظم وقواعد الإثبات الجنائي التقليدية المعمول بها قاصرة في إثبات الجريمة المعلوماتية بشكل مباشر.

وانطلاقاً مما سبق ذكره، نهدف من خلال هذا موضوع إلى إزالة الغموض عن الأدلة الجنائية الرقمية، وذلك بوضع مفهوم عام له من خلال التعريف به وإبراز خصائصه وأنواعه، وسبل كشفه وضبطه من الجانبين الفني والقانوني، زيادة على ذلك معرفة مدى فاعلية الأدلة الجنائية الرقمية في إثبات الجريمة المعلوماتية، وتأثير ذلك على الاقتناع الشخصي للقاضي الجنائي في التشريعين الجزائري والفرنسي.

وعليه تكون إشكالية بحثنا كالتالي:

**ما مدى حجية الأدلة الجنائية الرقمية في التشريعين الجزائري والفرنسي ؟**

واعتمدنا في الإجابة على هذه الإشكالية المنهج التحليلي والمقارن من خلال المزج بينهما، حيث استخدمنا المنهج التحليلي في عرض الآراء الفقهية وتحليل النصوص القانونية، كما استخدمنا أيضاً المنهج المقارن أيضاً في بعض الجزئيات التي تتطلب المقارنة، وذلك من خلال بيان موقف التشريع الفرنسي من الأدلة الجنائية الرقمية، بالإضافة إلى الاستئناس في بعض الأحيان لموقف التشريعات الأخرى مثل التشريع الإنجليزي والأمريكي.

ولمعالجة هذا الموضوع والتصدي للإشكالية المطروحة، ارتأينا تقسيم البحث إلى فصلين، الأول بعنوان ماهية الدليل الجنائي الرقمي، وقد تناولنا في المبحث الأول مفهوم الدليل الجنائي الرقمي، وفي المبحث الثاني تطرقنا فيه إلى استخلاص الدليل الجنائي الرقمي، وأما الفصل الثاني فقد كان بعنوان القيمة القانونية للدليل الجنائي الرقمي، بحيث تناولنا في المبحث الأول شروط قبول الدليل الجنائي الرقمي أمام القضاء الجنائي، وفي المبحث الثاني تناولنا فيه لسلطة القاضي في تقدير الأدلة الجنائية الرقمية، وفي الختام انتهينا إلى توضيح النتائج والتوصيات التي تم التوصل إليها.

## الفصل الأول

### ماهية الدليل الجنائي الرقمي

إن الكلام عن ماهية الشيء يستلزم – بطبيعة الحال – البحث في مفهومه وتعريفه، ثم التعرض للخصائص التي يتميز بها عن غيره من الأشياء.

وعليه يتعين علينا عند بيان ماهية الدليل الجنائي الرقمي، أن نوضح مفهومه من خلال التعريف به لغويا واصطلاحيا، وبيان خصائصه وأنواعه، ثم نتعرض من جهة أخرى لكيفية استخلاص الدليل الجنائي الرقمي، وذلك استكمالا لماهيته، ومعرفة الطرق والأساليب المستعملة في جمعه وتوثيقه.

لذا سنخصص المبحث الأول من هذا الفصل لبيان مفهوم الدليل الجنائي الرقمي، وأما المبحث الثاني نفرده لاستخلاص الدليل الجنائي الرقمي.

## المبحث الأول: مفهوم الدليل الجنائي الرقمي

يقتضي الحال لمعرفة أي موضوع تناول دراسته ببيان وتحديد مفهومه بكل جوانبه، وهذا بتعريفه وتحديد خصائصه وأنواعه، والأمر سيّان بالنسبة لموضوعنا المتعلق بمفهوم الدليل الجنائي الرقمي، بحيث سنتناول تعريف الدليل الجنائي الرقمي في المطلب الأول، ونتعرض إلى خصائصه في المطلب الثاني، وفي الأخير سنفرد المطلب الثالث لأنواع الدليل الجنائي الرقمي.

### المطلب الأول: التعريف بالدليل الجنائي الرقمي

سنتعرض في هذا المطلب للتعريف اللغوي والاصطلاحي للدليل الجنائي الرقمي، وذلك وفقا للفرعين المواليين.

### الفرع الأول: التعريف اللغوي

يقصد بالدليل في اللغة ما يستدلّ به، ويقال أدلّ، وفلانا يدلّ فلان، والدليل يعني المرشد، وجمعه أدلّة<sup>1</sup>، وكذلك يقصد بالدليل البرهان، بحيث يقال أقام الدليل أي بين وبرهن<sup>2</sup>، وقد جاء في القرآن الكريم معنى الدليل بقول الله تعالى: ﴿الْم تَرَى إِلَى رَبِّكَ كَيْفَ مَدَّ الظِّلَّ وَلَوْ شَاءَ لَجَعَلَهُ سَاكِنًا ثُمَّ جَعَلْنَا الشَّمْسَ عَلَيْهِ دَلِيلًا﴾، سورة الفرقان، الآية 45.

وأما كلمة "الرقمي" فهي اسم منسوب للدليل، وأصلها "رقم"، وجمعها أرقام، وهي علامات الأعداد المعروفة: 1، 2، 3...<sup>3</sup>، وينصرف إلى معناها أيضا كلمة عدد، وجمعها أعداد.

<sup>1</sup> محمد بن أبي بكر الرازي، مختار الصحاح، دار الرسالة، الكويت، 1983، ص 209.

<sup>2</sup> المنجد الأبجدي، دار المشرق، لبنان، 1967، ص 446.

<sup>3</sup> المرجع نفسه، ص 49.

## الفرع الثاني: التعريف الاصطلاحي

بعد التطرق إلى التعريف اللغوي للدليل الجنائي الرقمي في الفرع السابق، سنتعرض في هذا الفرع للتعريف الاصطلاحي له، وذلك من خلال التعريف بالدليل الجنائي بصفة عامة، ثم ننتقل إلى التعريف الاصطلاحي للدليل الجنائي الرقمي.

### أولاً: التعريف الاصطلاحي بالدليل الجنائي

يعرف الدليل اصطلاحاً بأنه: "هو ما يلزم من العلم به علم شيء آخر"<sup>1</sup>، أي أن الدليل هو ما يمكن التوصل به إلى معرفة الحقيقة<sup>2</sup>، وأما الدليل الجنائي فقد عرف بأنه: "الحجة والبرهان وما يستدل به على صحة الواقعة"<sup>3</sup>، وفي تعريف آخر "هو كل واقعة مادية أو معنوية تؤدي إلى إثبات وقوع الجريمة، أو تحديد شخصية مرتكبيها، أو إثبات ارتكابه لها سواء تم ذلك مباشرة أو عن طريق غير مباشر"<sup>4</sup>.

ويختلف الدليل الجنائي عن الأثر، من خلال طبيعتهما الذاتية، فالدليل الجنائي يحتمل أن يكون دليلاً مادياً، كوجود أداة الجريمة أو بصمات الجاني أو دمائه في مسرح الجريمة، ويحتمل أيضاً أن يكون دليلاً معنوياً، كأقوال الشهود أو اعتراف الجاني مثلاً، بينما الأثر يكون دائماً ذو طبيعة مادية، يمكن إدراكها بالحواس<sup>5</sup>.

---

<sup>1</sup> أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، الجزء الأول، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، السعودية، 1993، ص 177.

<sup>2</sup> المرجع نفسه، ص 178.

<sup>3</sup> محمد الأمين البشري، "الأدلة الجنائية الرقمية (مفهومها ودورها في الإثبات)"، المجلة العربية للدراسات الأمنية والتدريب، العدد 33، المجلد 17، أكاديمية نايف العربية للعلوم الأمنية، السعودية، 1995، ص 105.

<sup>4</sup> محمد فاروق عبد الحميد كامل، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، السعودية، 1999، ص 185.

<sup>5</sup> المرجع نفسه، ص 185.

ومن جهة أخرى أن الأثر أعم وأشمل من الدليل الجنائي، بحيث أن هذا الأخير مرتبط فقط بماديات وقوع الجريمة ونسبتها إلى مرتكبها<sup>1</sup>، ومنه يمكن القول أنه ليس كل أثر يمكن اعتباره دليلاً جنائياً، والعكس صحيح.

### ثانياً: التعريف الاصطلاحي بالدليل الجنائي الرقمي

في ظل عدم تعريف الدليل الجنائي الرقمي من قبل المشرعين الجزائري والفرنسي، سنستعرض بعض التعريفات التي أتى بها فقهاء القانون الجنائي، فقد عرف البعض بأنه الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء<sup>2</sup>.

كما عرف أيضاً بأنه: "ذبذبات أو نبضات إلكترونية Electronic Impulses مسجلة على وسائط أو دعائم مادية"<sup>3</sup>، أو أنه: "الدليل الذي تم الحصول عليه بواسطة التقنية الفنية الإلكترونية من معطيات الحاسوب وشبكة الإنترنت، والأجهزة الإلكترونية الملحقة والمتصلة به وشبكات الاتصال، من خلال إجراءات قانونية لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة"<sup>4</sup>.

---

<sup>1</sup> محمد محمد محمد عنب، معاينة مسرح الجريمة، الجزء الثاني، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، السعودية، 1991، ص 181.

<sup>2</sup> ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006، ص 88.

<sup>3</sup> خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009، ص 176.

<sup>4</sup> خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص 230.

وعرف أيضا بأنه: "معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحاسوبية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه"<sup>1</sup>.

وهناك أيضا من يعرف الدليل الجنائي الرقمي بأنه يشمل جميع المعلومات والبيانات الرقمية التي يمكن أن تثبت أن هنالك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني، أو توجد علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت أو الصورة، أو أنه عبارة عن مجموعة من معلومات أو بيانات ذات قيمة في التحقيق، والتي جرى تخزينها أو إرسالها عبر جهاز إلكتروني<sup>2</sup>.

ومن جهة أخرى تم تعريف الدليل الجنائي الرقمي من طرف مجموعة العمل العلمية للأدلة الرقمية The scientific Working Group Digital Evidence بأنه مجموعة المعلومات القيمة التي تخزن أو ترسل في شكل رقمي<sup>3</sup>، وعرفت أيضا المنظمة الدولية لدليل الحاسوب The International Organization of Computer Evidence بأن الدليل الجنائي الرقمي هو المعلومات التي جرى تخزينها أو إرسالها في شكل ثنائي، والذي يمكن أن تعتمد عليه المحكمة<sup>4</sup>.

---

<sup>1</sup> محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، السعودية، 2004، ص 234.

<sup>2</sup> The Technical Working Group for Electronic Crime Scene Investigation, **Electronic Crime Scene Investigation**, the national institute of justice, the United States of America, 2001, p 6.

<sup>3</sup> Eoghan Casey, **Digital Evidence and Computer Crime**, Third Edition, Published by Elsevier Inc, London, 2011, p 7.

<sup>4</sup> Ibid., p 7.

بناء على ما سبق ذكره، يمكن لنا القول بأن أغلب التعريفات قد جانبت الصواب حين قدمت لنا وصفا للدليل الجنائي الرقمي من حيث تكوينه، وذلك بأنه عبارة عن مجالات أو نبضات مغناطيسية أو كهربائية، تشكل لنا معلومات أو بيانات مختلفة، إلا أنه يعاب عليها في بعض الأحيان أنها اعتمدت فقط على الأدلة المستخلصة من أجهزة الحاسب الآلي أو شبكة الإنترنت<sup>1</sup>، في حين أنه يمكن الحصول على الأدلة الجنائية الرقمية من الهواتف المحمولة الذكية، أو أجهزة تحديد المواقع G.P.S، أو أي جهاز آخر يتميز بخصائص معينة أهمها التخزين أو المعالجة.

ومن جهة أخرى يعاب أيضا على التعريفين الذي أتى بهما كل من مجموعة العمل العلمية للأدلة الرقمية ومنظمة الدولية لدليل الحاسوب، أنهما لم يوضحا المقصود بالشكل الثنائي للدليل الجنائي الرقمي، وإهمالهما لماهية المعلومات الموصوفة بأنها دليل رقمي.

وعليه تفاديا لهذه العيوب التي شابت التعريفات السابقة، يمكننا القول بأن الدليل الجنائي الرقمي هو الدليل المستخلص من أجهزة الحاسب الآلي وملحقاته، أو من شبكة الإنترنت، أو أي جهاز آخر له خاصية معالجة أو تخزين المعلومات، وهو عبارة عن مجالات أو نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة، لتشكل لنا معلومات أو بيانات مختلفة، يمكن الاعتماد عليها في مرحلة التحقيق أو المحاكمة، ومنه فهذا التعريف المقترح يعطي مفهوما شاملا للدليل الجنائي الرقمي من حيث استخلاصه، بحيث أنه لا يشمل فقط الأدلة المستخلصة من أجهزة الحاسب الآلي فقط، ومن جهة أخرى يحدد الطبيعة الفنية والتقنية له، بحيث يمكن للخبراء المتخصصين جمعها وتحليلها عبر وسائل وأساليب تقنية، لتشكل في الأخير دليلا جنائيا رقميا صالحا للإثبات.

---

<sup>1</sup> خالد عياد الحلبي، المرجع السابق، ص 230.

## المطلب الثاني: خصائص الدليل الجنائي الرقمي

تقوم خصائص الدليل الجنائي الرقمي على مدى ارتباطه بالبيئة التي نشأ فيها، وهي البيئة الافتراضية أو العالم الافتراضي، هذه البيئة ممثلة في أجهزة الحاسب الآلي بكل مكوناته المادية، المتمثلة في الأجهزة والمعدات والأدوات المادية Hardware، ومكوناته المعنوية المتمثلة أيضا في البرامج الحاسوبية Software، وعليه فهذه البيئة الافتراضية قد انعكست على طبيعة هذا الدليل، فأصبح يتصف بعدة خصائص جعلته يتميز عن الدليل الجنائي التقليدي (المادي)، وهو ما سنتطرق إليه في الفروع التالية.

### الفرع الأول: الدليل الجنائي الرقمي دليل علمي

يتطلب في استخلاص الدليل الجنائي الرقمي وتحليله طرقا غير تقليدية، بحيث يتم إجراء تجارب علمية وتقنية على جهاز الحاسب الآلي الذي استخدم في جريمة معينة<sup>1</sup>. وعليه عندما يتم البحث عن الدليل الجنائي الرقمي، يجب أن تكون هذه العملية في إطار جغرافيا النظام الافتراضي Geographic Information systems، الخاضعة لقوانين الإعلام الآلي أو البيئة المعلوماتية ككل<sup>2</sup>.

وبناء على هذه الخاصية يمكن القول أنه لا يمكن الحصول على الدليل الجنائي الرقمي أو الإطلاع عليه سوى باستخدام الوسائل والأساليب العلمية، وهذا يعود ذلك للمنشأ الذي تكون فيه هذا الدليل.

<sup>1</sup> ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية - دراسة تأصيلية تطبيقية - ، (رسالة ماجستير)، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012، ص 74.

<sup>2</sup> عمر محمد بن يونس، الدليل الرقمي (Digital Evidence)، دون دار نشر، مصر، 2006، ص 7.

## الفرع الثاني: الدليل الجنائي الرقمي ذو طبيعة تقنية

إن الخاصية العلمية للدليل الجنائي الرقمي تقتضي بالضرورة التعامل مع هذا النوع من الأدلة من قبل تقنيين في الأدلة الجنائية العلمية والبيئة الافتراضية خصوصاً<sup>1</sup>، لذا فالطبيعة التقنية للدليل تقتضي أن يكون هناك توافق بين الدليل المستخلص وبين البيئة التي تكون فيها، لأن التقنية في حد ذاتها لا تنتج لنا سكيناً يتم به اكتشاف القاتل مثلاً، وإنما ما تنتجه هو نبضات أو مجالات مغناطيسية أو كهربائية<sup>2</sup> تشكل لنا معلومات مختلفة كما سبق ذكره، ولا يمكن معالجتها وقراءتها إلا من طرف أخصائيين وتقنيين يفهمون البيئة التي نشأ فيها والقوانين الخاضعة لها هذا النوع من الأدلة.

وعليه انطلاقاً من الطبيعة التقنية التي يتصف بها الدليل الجنائي الرقمي، يمكن القول أن هذا الأخير قد اكتسب العديد من المميزات التي جعلته يمتاز بها عن الدليل الجنائي التقليدي (المادي)، بحيث يمكن استخراج نسخ من الدليل الجنائي الرقمي مطابقة للأصل لها نفس القيمة العلمية، وهو الشيء الذي يندم أساساً في أنواع الأدلة التقليدية (المادية) الأخرى<sup>3</sup>، مما يقدم خدمة جليلة للمحققين من حيث الحفاظ على الدليل الأصلي ضد التلف والفقان والتغيير<sup>4</sup>، بحيث تتطابق طريقة النسخ مع طريقة الإنشاء.

<sup>1</sup> ثنيان ناصر آل ثنيان، المرجع السابق، ص 74.

<sup>2</sup> عمر محمد بن يونس، المرجع السابق، ص 8.

<sup>3</sup> عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة)، جامعة نايف العربية للعلوم الأمنية، السعودية، 2007، ص 15.

<sup>4</sup> خالد عياد الحلبي، المرجع السابق، ص 232.

ومن جهة أخرى، يتميز أيضا الدليل الجنائي الرقمي عن الدليل التقليدي (المادي)، بصعوبة إزالته من حاويات التخزين، وإمكانية استرجاعه عن طريق برامج وتطبيقات خاصة، وهو ما يؤكد على صعوبة التخلص منه ولو تم استعمال أقوى البرامج في إزالته.

كما أن نشاط الجاني الذي يستهدف محو الدليل الجنائي الرقمي يسجل أيضا كدليل ضده<sup>1</sup>، لذا فكل هذه المميزات التي يتصف بها الدليل الجنائي الرقمي عن الدليل التقليدي (المادي) ناتجة عن الطبيعة التقنية له.

### الفرع الثالث: الدليل الجنائي الرقمي ذو طبيعة ثنائية

تعتبر الطبيعة الثنائية التي يختصّ بها الدليل الجنائي الرقمي امتدادا للطبيعة العلمية والتقنية لهذا الأخير، وأيضاً امتدادا للبيئة الافتراضية التي تكون فيها كما سبق ذكره، لذا فالمعلومات والبيانات التي تشكل لنا دليلاً جنائياً رقمياً تكون في الأصل شكلاً ثنائياً أو رقمياً، ومردّد ذلك أن الحاسب الآلي أو أي جهاز آخر له نفس خصائصه، يقوم باستقبال هذه البيانات والمعلومات وتحويلها إلى أرقام ثم معالجتها<sup>2</sup>.

ومنه فمضمون الطبيعة الثنائية للدليل الجنائي الرقمي، هو اختزال البيانات أو المعلومات كالنصوص أو الصور أو الصوت أو أي معلومة أخرى إلى رموز ثنائية<sup>3</sup>، وهذه الرموز الثنائية تتكون من سلسلة من رقم الصفر (0) ورقم واحد (1)<sup>4</sup>، ومثال ذلك أن الحرف (أ) يقابله في البيئة الافتراضية (11000110)<sup>5</sup>، وهكذا يتم من خلال طرق الترميز

<sup>1</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 89.

<sup>2</sup> سليمان غازي العتيبي، درجة توافر كفايات البحث عن الدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة، (رسالة ماجستير)، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2010، ص 35.

<sup>3</sup> ممدوح عبد الحميد عبد المطلب، المرجع نفسه، ص 22.

<sup>4</sup> Brian Carrier, **File System forensic Analysis**, Pearson Education (Inc), United states of America, 2005, p 22.

<sup>5</sup> سليمان غازي العتيبي، المرجع السابق، ص 35.

نقل وتمثيل البيانات المختلفة، لتكون صالحة للتعامل معها داخل الحاسب الآلي وكذا الأجهزة الرقمية، بحيث أن لغة التعامل بين تلك الأجهزة هي النظام الثنائي الرقمي، والتي تسمى في الأصل لغة الآلة.

### الفرع الرابع: الدليل الجنائي الرقمي متنوع ومتطور

إن مصطلح الدليل الجنائي الرقمي يشمل جميع البيانات والمعلومات الرقمية التي يمكن تداولها رقميا بمختلف أشكالها وأنواعها<sup>1</sup>، سواء كانت هذه الأدلة متعلقة بالحاسب الآلي أو غيرها من الأجهزة، أو شبكة الانترنت، أو شبكات الاتصال السلكية واللاسلكية، ومنه فالآثار الرقمية<sup>2</sup> المستخلصة من الحاسب الآلي أو شبكة الإنترنت، تكون ثرية جدا ومتنوعة بما تحتويه من معلومات عن وقائع قد تشكل جريمة ما، وترتقي إلى أن تصبح دليل براءة أو إدانة، ومن بين هذه المعلومات صفحات المواقع الإلكترونية المختلفة، البريد الإلكتروني، النصوص والصور والفيديوهات الرقمية، الملفات المخزنة في الكمبيوتر الشخصي، والمعلومات المتعلقة بمستخدم شبكة الإنترنت وغيرها<sup>3</sup>.

ومنه، فهذا التنوع إن دل على شيء، فإنما يدل على اتساع قاعدة الدليل الجنائي الرقمي، بحيث يمكنه أن يشمل أنواعا متعددة من المعلومات والبيانات الرقمية التي تصلح لأن تكون دليلا جنائيا ببراءة المتهم أو إدانته<sup>4</sup>.

---

<sup>1</sup>Eoghan Casey, Op.Cit., p 6.

<sup>2</sup> يقصد بالآثار الرقمية، الآثار التي يتركها مستخدم أجهزة الحاسب الآلي، أو شبكة الإنترنت، والتي قد تشكل دليلا جنائيا ببراءته أو إدانته، وعليه فمصطلح الآثار الرقمية مصطلح أعم وأشمل من مصطلح الدليل الجنائي الرقمي.

<sup>3</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 22.

<sup>4</sup> نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، (رسالة ماجستير)، جامعة الحاج لخضر - باتنة -، كلية الحقوق والعلوم السياسية، الجزائر، 2013، ص 124.

وأما خاصية التطور التي يتمتع بها الدليل الجنائي الرقمي، فهي ناتجة عن تزايد استخدام تقنية المعلومات الرقمية، بعد أن أصبحت أجهزة الحاسب الآلي وشبكة الإنترنت، تشكل مستودعا هاما للمعلومات والبيانات الرقمية<sup>1</sup>، ومن جهة أخرى أن تطورها اليومي جاء لتلبية احتياجات المستخدمين الذي أدى إلى ظهور أنواع جديدة من هذه الأدلة.

### المطلب الثالث: أنواع الدليل الجنائي الرقمي

بالرغم من أن الأدلة الجنائية الرقمية عبارة عن نبضات أو مجالات مغناطيسية أو كهربائية كما رأيناه في السابق، إلا أنها تتخذ عدة صور وأشكال تشكل لنا العديد من المعلومات والبيانات المختلفة، التي يمكن من خلالها الاعتماد عليها كوسيلة إثبات للجرائم المعلوماتية أو حتى الجرائم التقليدية، لذا يأخذ الدليل الجنائي الرقمي نوعين رئيسيين، النوع الأول يتمثل في الأدلة الجنائية الرقمية التي أعدت لتكون وسيلة إثبات، وأما النوع الثاني يتمثل في الأدلة الجنائية الرقمية التي لم تعد لتكون وسيلة إثبات.

### الفرع الأول: الأدلة الجنائية الرقمية التي أعدت لتكون وسيلة إثبات

بناء على هذا النوع، تنقسم الأدلة الجنائية الرقمية إلى قسمين، القسم الأول يتمثل في المعلومات والبيانات المنشئة تلقائيا من طرف الحاسب الآلي، وأما القسم الثاني فإنه يتمثل في المعلومات والبيانات ذات الطبيعة المختلطة.

---

<sup>1</sup> محمد الأمين البشري، الأدلة الجنائية الرقمية (مفهومها ودورها في الإثبات)، المرجع السابق، ص 93.

## أولاً: المعلومات والبيانات المنشئة تلقائياً من طرف الحاسب الآلي

وتتمثل في جميع المعلومات والبيانات الرقمية التي تم إنشاؤها بواسطة جهاز الحاسب الآلي أو أي جهاز آخر، ولا دخل للمستخدم في إنشائها<sup>1</sup>، أو السجلات التي تعتبر من مخرجات جهاز الحاسب الآلي مثل فواتير البطاقات البنكية المعدة آلياً<sup>2</sup>.

## ثانياً: المعلومات والبيانات ذات الطبيعة المختلطة

وهي المعلومات والبيانات الرقمية التي تم حفظ جزء منها بالإدخال، وجزء آخر تم إنشاؤه بواسطة الحاسب الآلي<sup>3</sup>، وأبرز مثال عن ذلك المعلومات والبيانات المدخلة والمعالجة من طرف برنامج Excel.

لذا، فكلما النوعين السابق ذكرهما تكمن أهميتهما من حيث أنهما أعدا سلفاً بغرض جعلهما وسيلة لإثبات بعض الوقائع التي تتضمنها، ولهذا يتم حفظ هذه المعلومات والبيانات الرقمية للاحتجاج بها لاحقاً، وذلك للتقليل من إمكانية فقدانها، كما يكون من السهل الحصول عليها عند الحاجة<sup>4</sup>.

## الفرع الثاني: الأدلة الجنائية الرقمية التي لم تعد لتكون وسيلة إثبات

هذا النوع من الأدلة الجنائية الرقمية نشأ دون إرادة المستخدم، ودون أن يكون راغباً في وجودها<sup>5</sup>، وتتجسد هذه الأدلة في الآثار التي يتركها المستخدم عند استعماله للحاسب الآلي أو شبكة الإنترنت، بحيث تشمل الرسائل المرسلة منه أو التي يستقبلها، وكافة الأفعال التي قام بها من خلال جهاز الحاسب الآلي أو شبكة الإنترنت<sup>6</sup>، ومثال ذلك المعلومات

<sup>1</sup> عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص 14.

<sup>2</sup> خالد عياد الحلبي، المرجع السابق، ص 234.

<sup>3</sup> عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع نفسه، ص 14.

<sup>4</sup> نعيم سعيداني، المرجع السابق، ص 129.

<sup>5</sup> خالد عياد الحلبي، المرجع نفسه، ص 234.

<sup>6</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 21.

والبيانات المضمنة في ملفات الولوج Log Files، والتي تحتوي على معلومات تتمثل في تاريخ ووقت تحميل أو إرسال ملفات المستخدم، أو الملفات الاحتياطية للنظام Backup Files التي تستعمل في حالة انهيار النظام<sup>1</sup>، أو بيانات الكوكيز Cookies<sup>2</sup>.

ومنه، تكمن أهمية هذا النوع من الأدلة في أنه قد يحمل أحيانا معلومات تفيد في الكشف عن الجريمة ومرتكبها، زيادة على ذلك إمكانية ضبط هذه الأدلة ولو بعد مرور فترة زمنية طويلة، بواسطة تقنيات وبرامج خاصة<sup>3</sup> لا تخلو من الصعوبة والتعقيد.

---

<sup>1</sup> Linda Volonino and Reynaldo Anazaldua, **Computer Forensics For Dummies**, Wiley Publishing, United States of America, 2008, p 85.

<sup>2</sup> The Technical Working Group for Electronic Crime Scene Investigation, Op.Cit., p 11.

<sup>3</sup> خالد عياد الحلبي، المرجع السابق، ص 235.

## المبحث الثاني: استخلاص الدليل الجنائي الرقمي

بعد التعرض إلى مفهوم الدليل الجنائي الرقمي في المبحث السابق واستكمالاً لماهيته، وجب علينا التطرق في هذا المبحث إلى طرق استخلاص وتوثيق الأدلة الجنائية الرقمية، وذلك محاولة منا لعرض وفهم الطرق والأساليب المستخدمة في هذا الشأن.

وعلى هذا الأساس سنتعرض في هذا المبحث إلى الطرق الفنية الحديثة في جمع الأدلة الجنائية الرقمية وذلك في المطلب الأول، أما المطلب الثاني فنخصصه لصلاحيات إجراءات التحقيق التقليدية في جمع الأدلة الجنائية الرقمية، وفي الأخير نخصص أيضاً المطلب الثالث للصعوبات المتعلقة باستخلاص الدليل الجنائي الرقمي.

### المطلب الأول: الطرق الفنية الحديثة في جمع الأدلة الجنائية الرقمية

تعد عملية الحصول على الأدلة الجنائية الرقمية أمر صعب الوصول إليه، وذلك لما تتطلبه من خبرة ومهارة كبيرة في مجال التكنولوجيا الرقمية، زيادة على ذلك تعدد صور وأشكال الجريمة المعلوماتية<sup>1</sup>، وعليه للحصول على هذا النوع من الأدلة الجنائية يجب إتباع طرق ووسائل فنية معقدة، جرى تقسيمها إلى وسائل مادية ووسائل إجرائية.

### الفرع الأول: الوسائل المادية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية

يقصد بالوسائل المادية "تلك الأدوات الفنية التي غالباً تستخدم في بيئة نظم المعلومات، والتي يمكن باستخدامها يتم تنفيذ إجراءات وأساليب التحقيق المختلفة، والتي تثبت وقوع الجريمة وتحدد شخصية مرتكبها"<sup>2</sup>، ومنه فالوسائل المادية عبارة عن أدوات أو برامج ذات

<sup>1</sup> عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص 34.

<sup>2</sup> سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، (رسالة ماجستير)، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2003، ص 98.

طبيعة تقنية يتم استخدامها في التحقيق بغرض إثبات وقوع الجريمة وتحديد مرتكبها، أو بالأحرى وسائل فنية الهدف منها جمع مختلف الأدلة الجنائية الرقمية التي يمكن من خلالها الكشف عن ملبسات الجريمة المعلوماتية، ومنه عندما يستعمل المستخدم شبكة الانترنت، فإنه يترك آثارا وراءه عن كل موقع يزوره، إذ يفتح هذا الأخير سجلا خاصا يحتوي على معلومات كثيرة من بينها نوع الحاسب الآلي والمتصفح، وعنوان IP، وكل هذه البيانات تعتبر من قبيل معلومات جد هامة في التحقيق<sup>1</sup>، ومنه فإنه يعد من بين هذه الوسائل استخدام بروتوكول IP/TCP، والبروكسي Proxy، والمعلومات التي تحتويها ملفات الكوكيز Cookies، وغيرها من الوسائل الأخرى التي سنتطرق إليها في العرض الموالي.

### أولا: استخدام بروتوكول IP/TCP

يعتبر بروتوكول IP/TCP من أكثر البروتوكولات المستخدمة في شبكة الانترنت لأنه يعتبر جزء أساسي منه، والمسؤول عن تراسل حزم البيانات عبره وتوجيهها إلى أهدافها<sup>2</sup>، فهو يوجد بكل جهاز مرتبط بالإنترنت، ويتكون من أربعة أجزاء، فيشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المترابطة، وأما الجزء الرابع يحدد الحاسب الآلي الذي تم الاتصال منه<sup>3</sup>.

زيادة على ذلك يعمل عنوان IP بشكل متزامن مع بروتوكول آخر وهو بروتوكول التحكم بالنقل TCP، والذي تكمن وظيفته في تقسيم المعلومات إلى حزم معلوماتية، ويقوم بروتوكول IP بعنوان كل حزمة مع إضافة معلومات أخرى إليها<sup>4</sup>، ومنه فيتم استخدام عنوان IP من خلال البحث عن رقم الجهاز وتحديد موقعه الجغرافي، بالإضافة إلى إمكانية مراقبة

<sup>1</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 69.

<sup>2</sup> سليمان مهجع العنزي، المرجع السابق، ص 98.

<sup>3</sup> المرجع نفسه، ص 98.

<sup>4</sup> ممدوح عبد الحميد عبد المطلب، المرجع نفسه، ص 101.

المستخدم من طرف مزود خدمة الإنترنت وتقديم المعلومات التي تفيد في التحقيق، بناء على أن لكل جهاز حاسب آلي يتصل بالإنترنت عنوان IP خاص به<sup>1</sup>.

وبناء على ما سبق ذكره، وبالرغم من المعلومات المهمة التي يحتويها بروتوكول IP/TCP، إلا أنه تثار العديد من الصعوبات في استخدامه، إذ أنه يحتوي على معلومات عن جهاز الحاسب الآلي وليس الأشخاص، لذلك فمن الصعوبة إثبات أن شخصا قد ارتكب جريمة معلوماتية، ومع ذلك يمكن أن يستخدم كقرينة ضد مالك أو صاحب هذا الجهاز إلى أن يثبت العكس<sup>2</sup>، ومن جهة أخرى إمكانية استعمال عناوين مزيفة وذلك بوضع معلومات غير صحيحة من أجل تجنب التعرف إليهم، أو حتى استخدام برامج معينة تؤمن لهم سرية تحركاتهم عبر الشبكة، وذلك بإخفاء عنوان IP عن المواقع التي يزورونها<sup>3</sup>.

### ثانياً: استخدام معلومات الكوكيز Cookies

عند زيارة مستخدم الإنترنت أي موقع من مواقع الويب، تفتح هذه الأخيرة ملفاً صغيراً على القرص الصلب يسمى كوكي Cookie بهدف جمع بعض المعلومات عنه<sup>4</sup> وتحسين عملية تصفح الموقع<sup>5</sup>، و منه فهو يسجل العديد من المعلومات التي يمكن أن تساعد في التحقيق من بينها تاريخ زيارة الموقع الإلكتروني، أو تاريخ إجراء التعديلات عليه أو الانتهاء منها، وزيادة على ذلك الاحتفاظ بكلمات السر الخاصة بالمستخدم عند زيارته للموقع<sup>6</sup>.

---

<sup>1</sup> Debra Littlejohn Shinder, **Scene of the Cyber Crime (Computer forensic Handbook)**, Publishing by Syngress (Inc), United states of America, 2002, p 240.

<sup>2</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 108.

<sup>3</sup> حارث عاصم داود، "المخاطر الأمنية في بروتوكول الإنترنت الإصدار السادس IPv6"، *المجلة العربية الدولية للمعلوماتية*، المجلد الثاني، العدد الرابع، جامعة نايف العربية للعلوم الأمنية، السعودية، 2013، ص 4.

<sup>4</sup> ممدوح عبد الحميد عبد المطلب، المرجع نفسه، ص 69.

<sup>5</sup> Steve Bunting and William Wei, **Encase Computer forensic**, Wiley Publishing (inc), United States of America, 2006, p 371.

<sup>6</sup> Ibid., p 371.

## ثالثاً: استخدام معلومات البروكسي Proxy

في بادئ الأمر تم تطوير تقنية البروكسي Proxy لاستخدامها كحواجز نارية Firewalls لشبكة الإنترنت<sup>1</sup>، والحاجز الناري عبارة عن نظام أمني يفرض توليد جميع الرزم المرسلّة أو الواردة من خلال جهاز وحيد، وتميرها من خلال الحاجز الناري<sup>2</sup>، ومنه فإن الدور الأساسي الذي تقوم به هو قيامها بدور الوسيط بين مستخدم شبكة الإنترنت وبين مواقعها، وذلك بطلب المعلومات من تلك المواقع وتقديمها للمستخدم.

ومن بين أهم ما تتميز به مزودات البروكسي Proxy هو إمكانيتها في تسريع الوصول إلى شبكة الإنترنت، بالإضافة إلى احتوائها على تدابير أمنية للتحكم بعملية الاتصال بالإنترنت، و مثال ذلك التعرف على الأشخاص المسموح لهم بالاتصال بالشبكة، وتحديد الخدمات التي يمكن استخدامها، أو حتى تحديد الأيام والأوقات المسموح بها بزيارة شبكة الإنترنت<sup>3</sup>، وعليه فكل هذه العمليات والمعلومات التي يحتويها البروكسي Proxy، يتم حفظها في قاعدة بياناته، مما يجعل دورها قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة<sup>4</sup>.

وفي الأخير، وبالرغم من المميزات التي تتمتع بها مزودات البروكسي Proxy إلا أنها تحتوي على عدة مساوئ قد تشكل عائقاً في التحقيق، من بينها منع الوصول إلى صفحات المواقع الإلكترونية معينة، أو الحصول على صفحات قديمة أو ناقصة أحياناً<sup>5</sup>، إلا أن هذا كله لا يمنعها كونها وسيلة هامة ومفيدة في التحقيق.

<sup>1</sup> Debra Littlejohn Shinder, Op.Cit., p 394.

<sup>2</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 84.

<sup>3</sup> المرجع نفسه، ص 85.

<sup>4</sup> سليمان مهجع العنزي، المرجع السابق، ص 99.

<sup>5</sup> ممدوح عبد الحميد عبد المطلب، المرجع نفسه، ص 85.

## رابعاً: استخدام برامج التتبع وكشف الاختراق

إن طبيعة عمل هذه البرامج تكمن في التعرف على محاولات الاختراق، وكشف كافة المعلومات المتعلقة بمن قام بها، وأيضاً إشعار الجهة المتضررة من هذه العملية، ومن بين هذه البرامج، برنامج Hack Tracer v1.2، فعندما يرصد أي محاولة للقرصنة أو اختراق جهاز الحاسب الآلي، يسارع بإغلاق منافذ الدخول أمام المخترق، ثم يبدأ في عملية اقتفاء أثره حتى يصل إلى الجهاز الذي حدث العملية من خلاله، ويستعرض هذا البرنامج مجموعة شاملة من بيانات المخترق من حيث عنوان IP الخاص به، وتاريخ حدوث الاختراق باليوم والساعة، وفي الأخير المعلومات الخاصة بمزود الخدمة<sup>1</sup>.

### الفرع الثاني: الوسائل الإجرائية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية

يقصد بالوسائل الإجرائية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية، تلك الإجراءات التي تستعمل أثناء تنفيذ طرق التحقيق الثابتة والمحددة والأساليب المتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها<sup>2</sup>، ومنه فالوسائل الإجرائية عبارة عن أساليب محددة قانوناً تهدف إلى إثبات وقوع الجريمة وتحدد شخصية مرتكبها، وذلك باستخدام تقنيات وبرامج إلكترونية مختلفة<sup>3</sup>، تماشياً مع إرادة المشرع في مكافحة الجرائم المعلوماتية، أو حتى الجرائم التقليدية التي تتطلب استخدام هذه الوسائل.

ومنه فقد استحدث المشرع الجزائري وسائل إجرائية هي: اعتراض المراسلات والتسرب، الذي جاء بهما القانون رقم 06-22 المؤرخ في 20/12/2006، المعدل

<sup>1</sup> سليمان مهجع العنزي، المرجع السابق، ص 100.

<sup>2</sup> خالد عياد الحلبي، المرجع السابق، ص 212.

<sup>3</sup> ثنيان آل ناصر ثنيان، المرجع السابق، ص 78.

والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية الجزائري<sup>1</sup>، ومن جهة أخرى تم استحداث أيضا الإجراءات المتمثل في المراقبة الإلكترونية الذي أتى بها القانون رقم 09-04 المؤرخ في 05/08/2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها<sup>2</sup>.

### أولا: اعتراض المراسلات

تعتبر عملية اعتراض المراسلات من بين أهم الإجراءات المستحدثة لما لها من أهمية وفائدة في جمع الأدلة الجنائية الرقمية، ومنه وجب علينا التطرق إلى هذا الإجراء من خلال مفهومه وشروطه وكيفية القيام به.

### 1) مفهوم عملية اعتراض المراسلات

عند استقراء نصوص قانون الإجراءات الجزائية الجزائري<sup>3</sup>، نجد أن المشرع الجزائري لم يعرف بإجراء اعتراض المراسلات، بل اكتفى بوضع تنظيم لهذه العملية في المواد من 65 مكرر 05 إلى غاية المادة 65 مكرر 10 من قانون الإجراءات الجزائية الجزائري، وترك أمر تعريفه للفقهاء، لذا ومن خلال نص المادة 65 مكرر 05 من نفس القانون، نجد أن عملية اعتراض المراسلات يقصد بها: "اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض"<sup>4</sup>.

<sup>1</sup> الجريدة الرسمية رقم 84، الصادرة بتاريخ 24/12/2006، ص 4.

<sup>2</sup> الجريدة الرسمية رقم 47، الصادرة بتاريخ 16/08/2009، ص 5.

<sup>3</sup> الأمر رقم 66-155 المؤرخ في 08/06/1966، المتضمن قانون الإجراءات الجزائية الجزائري، الجريدة الرسمية رقم 48، الصادرة بتاريخ 10/06/1966، المعدل والمتمم.

<sup>4</sup> نعيم سعيداني، المرجع السابق، ص 178.

وإذا بحثنا في مفهوم المراسلات، نجد أن المادة 9 الفقرة 6 من القانون رقم 03-2000 المؤرخ في 05/08/2000 والمتضمن تحديد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية<sup>1</sup>، قد نصت على تعريف المراسلات، إذ أنها: "اتصال مجسد في شكل كتابي يتم عبر مختلف الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه. لا تعتبر الكتب والمجلات والجرائد واليوميات كمادة مراسلات".

وعليه فقد حصرت المادة المراسلات في الشكل الكتابي فقط، إلى أن جاءت المادة 2 الفقرة "و" من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، التي وسعت من المفهوم التقليدي للمراسلات، وأدخلت الاتصالات الإلكترونية في مفهومها تماشيا مع التطور التكنولوجي، إذ أنها: " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"، لذا يمكننا القول أن المراسلات تعني كل رسالة مكتوبة بأي شكل من الأشكال سواء ماديا أو إلكترونيا، وسواء كانت على دعامة ورقية أو رقمية، مرسلة بأي وسيلة لعدد معين ومحدد من المرسل إليهم، باستثناء الكتب والمجلات والجرائد والحواليات التي لا تعتبر من قبيل المراسلات الخاصة<sup>2</sup>.

## (2) شروط القيام بعملية اعتراض المراسلات

حدد المشرع الجزائري من خلال قانون الإجراءات الجزائية شروط للقيام بهذا الإجراء، كونه يشكل انتهاكا لحرمة الحياة الخاصة للأفراد، واعتداء على سرية مراسلاتهم واتصالاتهم التي كفلها الدستور الجزائري لسنة 1996 من خلال المادة 39، إذ نصت على

<sup>1</sup> الجريدة الرسمية رقم 48، الصادرة بتاريخ 06/08/2000، ص 4.

<sup>2</sup> نعيم سعيداني، المرجع السابق، ص 178-179.

أن سرية المراسلات والاتصالات الخاصة بكل أشكالها محمية<sup>1</sup>، ومنه فقد وضع المشرع شروطا قانونية بهدف منع التعسف في استعمالها، وتتمثل هذه الشروط في الحصول على إذن من وكيل الجمهورية، أو من قاضي التحقيق إذا تم فتح تحقيق قضائي<sup>2</sup>، زيادة على ذلك أن يكون الإذن الصادر عن وكيل الجمهورية أو قاضي التحقيق مكتوبا، لمدة أقصاها 4 أشهر، قابلة للتجديد حسب مقتضيات البحث والتحري، وأيضا وجوب تضمينه على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة<sup>3</sup>، وفي الأخير أن يكون هذا الإجراء في الجرائم المحددة بموجب المادة 65 مكرر 5، والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

### (3) كيفية اعتراض المراسلات في الجريمة الإلكترونية

بعد سلوك الطريق القانوني للقيام بهذا الإجراء التقني، نستطيع القول أن هذه العملية عادة ما تنصب على رسائل البريد الإلكتروني E-mail، التي تحتوي على العديد من المعلومات كتاريخ إنشاء الرسالة وتاريخ إرسالها أو تلقيها، وكذا عنوان المرسل، وعنوان المرسل إليه<sup>4</sup>، ولكن تبقى المعلومات التي تحتويها حاشية رسالة البريد الإلكتروني E-mail Header هي الأهم، حيث تتضمن على عنوان IP لمرسل الرسالة، وطبقا لما تم دراسته من قبل، فعنوان IP يحتوي على معلومات تتمثل في الكمبيوتر الذي تم إرسال منه الرسالة، وأيضا الموقع الجغرافي الذي أرسلت منه، وفي الأخير معلومات مزود الخدمة الذي يتعامل معه مرسل الرسالة.

<sup>1</sup> التعديل الدستوري الجزائري لسنة 1996، الصادر بموجب المرسوم الرئاسي رقم 96-438 المؤرخ في 1996/12/07، الجريدة الرسمية رقم 76، الصادرة في 1996/12/08.

<sup>2</sup> المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري.

<sup>3</sup> المادة 65 مكرر 7 من قانون الإجراءات الجزائية الجزائري.

<sup>4</sup> نعيم سعيداني، المرجع السابق، ص 182.

## ثانيا: التسرب

نظم المشرع الجزائري هذا الإجراء من خلال المواد من 65 مكرر 11 إلى غاية المادة 65 مكرر 18 من نفس القانون، بحيث نتناول فيها مفهوم هذا الإجراء وشروطه.

### (1) مفهوم التسرب

عرفت المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري التسرب بأنه :  
"قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص والمشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف"، إذن فالتسرب هو تلك العملية المحضرها مسبقا، تهدف إلى التوغل داخل خلية إجرامية، ومعرفة نشاطاتها وكشف الأشخاص المتورطين سواء كانوا فاعلون أصليون أم شركاء، وذلك بتوفير جميع الوسائل البشرية والتقنية اللازمة<sup>1</sup>.

### (2) شروط القيام بعملية التسرب

تتمثل شروط القيام بعملية التسرب في الحصول على إذن من وكيل الجمهورية أو من قاضي التحقيق إذا تم فتح تحقيق قضائي، وأن يكون الإذن الصادر عن وكيل الجمهورية أو قاضي التحقيق مكتوبا ومسببا لمدة أقصاها 4 أشهر، قابلة للتجديد مرة واحدة لنفس الفترة حسب مقتضيات البحث والتحري، زيادة على ذلك وجوب تضمنه على هوية ضابط الشرطة القضائية التي تتم عملية التسرب تحت مسؤوليته أو عون الشرطة القضائية باعتباره مساعدا له، وأيضا أن يكون هذا الإجراء في جرائم محددة المنصوص عليها بموجب المادة 65 مكرر 5، والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات<sup>2</sup>.

<sup>1</sup> نعيم سعيداني، المرجع السابق، ص 175.

<sup>2</sup> عبد الله أوهايبة، المرجع السابق، ص 281.

### 3) كيفية التسرب في الجريمة المعلوماتية

إن عملية التسرب في نطاق الجريمة الإلكترونية تتمثل في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي، وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو اشتراكه في محادثات غرف الدردشة والظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما أسماء أو صفات وهمية<sup>1</sup>، بهدف الحصول على معلومات هامة تفيد التحقيق.

#### ثالثا: المراقبة الإلكترونية

تم استحداث هذا الإجراء بموجب القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها<sup>2</sup>.

#### 1) مفهوم المراقبة الإلكترونية

من خلال استقراء نصوص القانون رقم 09-04 السابق الذكر، لم يعرف المشرع الجزائي بإجراء المراقبة الإلكترونية بل ترك أمر تعريفها للفقهاء، ومنه فتعرف بأنها: " عمل أمني أساسي له نظام معلومات إلكتروني، يقوم فيه المراقب (بكسر القاف) بمراقبة المراقب (بفتح القاف) بواسطة الأجهزة الإلكترونية وعبر شبكة الإنترنت، لتحقيق غرض محدد وإفراغ النتيجة في ملف إلكتروني، وتحرير تقارير بالنتيجة"<sup>3</sup>.

بناء على التعريف السابق، يمكن القول أن المراقبة الإلكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه<sup>4</sup>، بحيث يقوم بها مراقب إلكتروني يتمثل في ضابط من

<sup>1</sup> نعيم سعيداني، المرجع السابق، ص 177.

<sup>2</sup> الجريدة الرسمية رقم 47، الصادرة بتاريخ 2009/08/16، ص 5.

<sup>3</sup> مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت (دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية)، دار الكتب القانونية، مصر، 2005، ص 192.

<sup>4</sup> نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، الطبعة الأولى، دار الفكر الجامعي، مصر، 2007، ص 199.

ضباط الشرطة القضائية ذي كفاءة تقنية عالية، وباستخدام تقنيات وبرامج إلكترونية فيها، لذا وبالرجوع إلى القانون رقم 09-04 الذي سبق ذكره، نجد أن المشرع الجزائري لم يعتبر هذا الإجراء طريقة من طرق الحصول على الدليل الجنائي الرقمي فقط، بل أدرجه أيضا ضمن التدابير الوقائية من الجريمة المعلوماتية<sup>1</sup> بداعي حماية النظام العام، وهذا وفقا لما أتت به نص المادة 4 من نفس القانون، إذ يمكن القيام بهذا الإجراء للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وكذا في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

## (2) شروط القيام بعملية المراقبة الإلكترونية

حدد المشرع الجزائري شروطا للجوء إلى تقنية المراقبة الإلكترونية، وهي أن يتم تنفيذ هذه العملية تحت سلطة القضاء وبإذن منه، وهو ما نصت عليه المادة 4 من القانون رقم 09-04 المذكور، بحيث لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة، زيادة على ذلك أن تكون هناك ضرورة تتطلب هذا الإجراء، وذلك عندما يكون من الصعب الوصول إلى نتيجة تهم مجرييات التحري أو التحقيق دون اللجوء إلى المراقبة الإلكترونية، وهو ما نصت عليه المادة 4 من خلال الفقرة "ج" من نفس القانون<sup>2</sup>.

<sup>1</sup> نعيم سعيداني، المرجع السابق، ص 184.

<sup>2</sup> المرجع نفسه، ص 185.

## المطلب الثاني: صلاحيات الإجراءات التقليدية في جمع الأدلة الجنائية الرقمية

سنعرض في هذا المطلب لإشكالية صلاحية الإجراءات التقليدية في جمع الأدلة الجنائية الرقمية التي أثارت جدلا فقهما كبيرا، بحيث سنكتفي بدراسة الإجراءات التقليدية المتمثلة في التفتيش والمعاينة والخبرة، وذلك لعلاقتها المباشرة بالدليل الجنائي الرقمي، وسنستبعد الشهادة والاعتراف والاستجواب باعتبارها لا تثير أي صعوبات في اتخاذها نظرا لخضوعها للقواعد العامة المقررة لها قانونا.

### الفرع الأول: التفتيش وضبط الأدلة الجنائية الرقمية

يعتبر التفتيش من أهم إجراءات التحقيق التي تفيد في الكشف عن الحقيقة، لأنه غالبا ما يسفر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم، فيعرف التفتيش بصفة عامة بأنه: "البحث في مكنون سر الأفراد على دليل للجريمة المرتكبة، أو هو البحث عن الدليل..."<sup>1</sup>، وعرف أيضا بأنه: "البحث عن الأشياء المتعلقة بالجريمة لضبطها وكل ما يفيد في كشف حقيقتها ويجب أن يكون للتفتيش سند من القانون"<sup>2</sup>، وبالنسبة للفقهاء الفرنسيين فقد عرف بأنه: "البحث الدقيق لكل عناصر الأدلة التي يمكن استخدامها في الدعوى الجزائية والتي تجري على مسكن المتهم"<sup>3</sup>، إذن يتضح أن التفتيش ما هو إلا وسيلة إجرائية تستهدف ضبط أشياء مادية تتعلق بالجريمة وتفيد في كشف حقيقتها، إلا أن ذلك يتنافر مع الطبيعة غير المادية للدليل الجنائي الرقمي<sup>4</sup>، وهو ما يجعلنا أن نطرح السؤالين التاليين: ما مدى قابلية أنظمة الحاسب الآلي وشبكاته للتفتيش؟ وكيف يتم ضبط الأدلة الجنائية الرقمية؟.

<sup>1</sup> عبد الله أوهابية، المرجع السابق، ص 266.

<sup>2</sup> خالد ممدوح إبراهيم، المرجع السابق، ص 182.

<sup>3</sup> Merle et vitu, *Traite de droit Criminel*, Paris, 1967, p 758 نقلا عن علي حسن محمد الطوابية، التفتيش

الجنائي على نظم الحاسوب والإنترنت (دراسة مقارنة)، الطبعة الأولى، عالم الكتب الحديث، الأردن، 2004، ص 12.

<sup>4</sup> نبيلة هبة هروال، المرجع السابق، ص 223.

## أولاً: مدى خضوع أنظمة الحاسب الآلي للتفتيش

يقصد بالتفتيش عن الأدلة الجنائية الرقمية إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني، أو هو التفتيش عن معطيات الحاسب الآلي غير المادية والمخزنة في الجهاز أو المخزنة في الأقراص<sup>1</sup>، وبناء على ذلك يمكن القول بأن تفتيش أنظمة الحاسب الآلي يكون بإحدى صورتين:

**(1) الصورة الأولى:** تتمثل هذه الصورة في تفتيش المكونات المادية لجهاز الحاسب الآلي<sup>2</sup>، والمكونات المادية عبارة عن مجموعة من الوحدات المتصلة ببعضها البعض بشكل يجعلها تعمل كنظام متكامل<sup>3</sup> وهي: وحدات الإدخال مثل الفأرة ولوحة المفاتيح، ووحدات الإخراج مثل شاشة الحاسب الآلي والطابعة، وأخيراً وحدة الذاكرة<sup>4</sup>.

وبناء على هذه الصورة فلا توجد أي صعوبة عند معاينة القائمين على التفتيش لمسرح الجريمة الواقعة على المكونات المادية للحاسب الآلي، نظراً لعدم التعارض بين تفتيش المكون المادي لجهاز الحاسب الآلي، مع مفهوم التفتيش التقليدي، لأنه يمثل في ذاته بحثاً عن الأدلة المادية، وكل ما يتطلبه إجراء التفتيش في هذه الحالة هو أن يتم وفقاً للقواعد القانونية التي تحكم التفتيش<sup>5</sup>.

**(2) الصورة الثانية:** تتمثل في تفتيش المكونات المعنوية لجهاز الحاسب الآلي، والمكونات المعنوية عبارة عن مجموعة من البرامج والأساليب المتعلقة بتشغيل وحدة معالجة البيانات<sup>6</sup>،

<sup>1</sup> خالد عياد الحلبي، المرجع السابق، 157.

<sup>2</sup> بكرى يوسف بكرى، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011، ص 67.

<sup>3</sup> خالد عياد الحلبي، المرجع نفسه، ص 158.

<sup>4</sup> علي حسن محمد الطويلة، المرجع السابق، ص 19.

<sup>5</sup> بكرى يوسف بكرى، المرجع نفسه، ص 68.

البيانات<sup>1</sup>، وتتقسم إلى كيانات أساسية تضم البرامج الضرورية التي يتم تشغيل واستخدام جهاز الحاسب الآلي، وكيانات تطبيقية تضم برامج تمكن للمستخدم من أن ينفذ بواسطته عملاً معيناً<sup>2</sup>.

وبناء على الصورة الثانية، فقد ثار خلافاً فقهيًا حول إمكانية تفتيش المكونات المعنوية للحاسب الآلي، إذ رأى جانب من الفقه أنه متى كانت الغاية من التفتيش ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة، فإن هذا المفهوم يمتد حتى يشمل جميع المعلومات والبيانات الرقمية بمختلف أشكالها<sup>3</sup>، وسبب ذلك أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط أي شيء، فإن ذلك يجب تفسيره بحيث يشمل جميع المعلومات والبيانات المادية أو المعنوية<sup>4</sup>، ومن جهة أخرى ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب الآلي غير المحسوسة (المعنوية)، لذلك فإنه يقترح لمواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسب الآلي لا بد أن يشمل المواد المعالجة عن طريق الحاسب الآلي أو بياناته<sup>5</sup>.

وعليه، يتضح موقف المشرع الجزائري من خلال القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إذ نص صراحة على تفتيش أنظمة الحاسب الآلي، وذلك بموجب نص المادة 05 منه، بحيث يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية، **الدخول بغرض التفتيش** ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، وكذا منظومة تخزين معلوماتية.

<sup>1</sup> علي حسن محمد الطوالة، المرجع نفسه، ص 24.

<sup>2</sup> المرجع نفسه، ص 24.

<sup>3</sup> عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006، ص 378.

<sup>4</sup> خالد ممدوح إبراهيم، المرجع السابق، ص 197.

<sup>5</sup> المرجع نفسه، ص 197.

وإلى جانب المشرع الجزائري، نص أيضا المشرع الفرنسي على تفتيش أنظمة الحاسب الآلي من خلال المادة 94 من قانون الإجراءات الجزائية، إذ نصت على أنه: "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة"، وتجدر الإشارة أن هذه المادة قد جرى تعديلها بموجب المادة 42 من القانون رقم 545-2004 المؤرخ في 21/06/2004 المتعلق بالثقة في الاقتصاد الرقمي، والذي أضاف لنص المادة عبارة "المعطيات المعلوماتية"<sup>1</sup>.

### ثانيا: مدى خضوع شبكات الحاسب الآلي للتفتيش

مما لا شك فيه أن الطبيعة التقنية الرقمية قد زادت من الصعوبات التي تواجه القائمين على التفتيش والضبط في الجرائم المعلوماتية، فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكات الحاسب الآلي في أماكن قد تكون على مسافات بعيدة عن الموقع المادي الذي يتم فيه التفتيش، كما قد يكون الموقع الفعلي للبيانات والمعلومات ضمن الاختصاص القضائي لدولة أخرى، وهو ما يعقد ويصعب من عملية التفتيش وضبط الأدلة الجنائية الرقمية<sup>2</sup>، وعلى هذا الأساس نميز بين احتمالين اثنين في تفتيش شبكات الحاسب الآلي:

**1) الاحتمال الأول: أن يكون الحاسب الآلي للمشتبه فيه أو المتهم متصلا بحاسب آلي آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة، وبناء على هذا الاحتمال الذي يشكل عائقا أمام السلطات القائمة على التفتيش وضبط الأدلة الجنائية الرقمية، عمدت بعض التشريعات الإجرائية إلى حل هذه المشكلة من خلال نصها على إجازة تفتيش أنظمة الحاسب الآلي، وتسجيل كل البيانات اللازمة كأدلة إثبات لإدانة المتهم أمام المحكمة<sup>3</sup>.**

<sup>1</sup> نعيم سعيداني، المرجع السابق، ص 147.

<sup>2</sup> أسامة بن غانم العبيدي، "التفتيش عن الدليل في الجرائم المعلوماتية"، المجلة العربية للدراسات الأمنية والتدريب، العدد 58، المجلد 29، أكاديمية نايف العربية للعلوم الأمنية، السعودية، (دون سنة النشر)، ص 91.

<sup>3</sup> نعيم سعيداني، المرجع السابق، ص 149.

وهو نفس المسار الذي اتخذته المشرع الجزائري، إذا نص في الفقرة الثانية من المادة 05 من القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أنه في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقاً من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقاً بذلك.

وإلى جانب المشرع الجزائري، نجد المشرع الفرنسي قد حسم هذه المسألة أيضاً بمناسبة تعديله قانون الإجراءات الجزائية بموجب القانون 239-2003 الصادر في 2003/03/18، والذي أجاز فيه من خلال نص المادة 17 لضباط الشرطة القضائية أو تحت مسؤوليتهم أعوان الشرطة القضائية بتمديد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الحاسب الآلي الأصلي محل التفتيش<sup>1</sup>.

(2) الاحتمال الثاني: اتصال الحاسب الآلي للمشتبه فيه أو المتهم بحاسب آلي آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة، وهو أن يقوم مرتكبي الجريمة المعلوماتية بتخزين بياناتهم في أنظمة معلوماتية خارج إقليم الدولة بهدف عرقلة سلطات التحقيق في جمع الأدلة<sup>2</sup>، لذا ولحل هذه المسألة يرى جانب من الفقه أن تفتيش أنظمة الحاسب الآلي العابر للحدود لا بد أن يتم في إطار اتفاقيات تعاون ثنائية أو دولية تجيز هذا الامتداد، وبالتالي لا يجوز القيام بذلك التفتيش العابر للحدود في ظل غياب تلك الاتفاقية، أو على الأقل الحصول على إذن الدولة الأخرى<sup>3</sup>.

<sup>1</sup> المرجع نفسه، ص 150.

<sup>2</sup> عبد الفتاح بيومي حجازي، المرجع السابق، ص 382.

<sup>3</sup> خالد ممدوح إبراهيم، المرجع السابق، ص 205.

ولمواجهة هذا الاحتمال نجد أن المشرع الجزائري قد أجاز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج الإقليم الوطني، وهو ما نصت عليه الفقرة الثالثة من المادة 05 من القانون 09-04 السابق الذكر، بحيث إذا تبين مسبقاً بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة ووفقاً لمبدأ المعاملة بالمثل، والملاحظ على هذه الفقرة أنها مأخوذة حرفياً من نص الفقرة الثانية من المادة 57 من قانون الإجراءات الجزائية الفرنسي.

### ثالثاً: مدى صلاحية ضبط الدليل الجنائي الرقمي

يترتب على التفتيش نشوء الحق في ضبط الأشياء التي تفيد في الكشف عن الجريمة المرتكبة<sup>1</sup>، وذلك بوضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبها<sup>2</sup>، وفي هذا الصدد لا تثير عملية الضبط أي صعوبة إذا ما تعلق في ضبط المكونات المادية للحاسب الآلي، بل يقع الإشكال في مدى صلاحية المكونات المعنوية للضبط، لهذا فقد انقسم الفقهاء في هذا الأمر إلى اتجاهين:

**(1) الاتجاه الأول:** يرى أصحاب هذا الاتجاه أنه لا يمكن تصور إجراء الضبط على الكيانات المعنوية وذلك لانقضاء الكيان المادي عنها، بالإضافة إلى أن البيانات والمعلومات لا تعتبر من قبيل الأشياء المادية، وبالتالي لا يقع الضبط عليها، ولتجاوز هذا الإشكال اقترحوا أن يتدخل المشرع ويوسع من دائرة الأشياء التي يمكن أن يرد عليها الضبط، لتشمل جميع البيانات والمعلومات الرقمية بكافة أنواعها<sup>3</sup>.

<sup>1</sup> بكرى يوسف بكرى، المرجع السابق، ص 128.

<sup>2</sup> خالد عياد الحلبي، المرجع السابق، ص 168.

<sup>3</sup> علي حسن محمد الطوالة، المرجع السابق، ص 145.

**(2) الاتجاه الثاني:** يرى أنصار هذا الاتجاه أنه لا يوجد ما يمنع من أن يرد الضبط على البيانات والمعلومات الرقمية، وذلك أن الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة، وبالتالي يمتد هذا المفهوم ليشمل جميع البيانات الرقمية بمختلف أشكالها<sup>1</sup>.

وقد تدخل المشرع الجزائري لحل هذا الإشكال، وذلك ما نص عليه في المادة 06 من القانون 04-09، بحيث عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار وفقا للقواعد المقررة في قانون الإجراءات الجزائية، وإلى جانب المشرع الجزائري نجد المشرع الفرنسي قد تدخل أيضا بموجب تعديله لقانون الإجراءات الجزائية من خلال القانون رقم 2003/239 أين استحدثت الفقرة الثالثة من المادة 57، والتي نصت أيضا على نسخ جميع المعلومات والبيانات الرقمية الناتجة عن التفتيش على دعامات التخزين الإلكترونية وتحريزها<sup>2</sup>.

زيادة على ذلك، وإذا كان الدليل الجنائي الرقمي يخضع في ضبطه إلى قواعد تحريز الأدلة الجنائية، إلا أنه وبالنظر إلى الطبيعة التقنية والفنية التي يختص بها، فإن عملية ضبطه تستوجب بعض الإجراءات الخاصة لحمايته والحفاظ عليه من العبث والتلف، وهو ما نص عليه المشرع الجزائري من خلال نص المادة 06 في فقرتها الثانية من القانون رقم 04-09 إذ يجب في كل الأحوال على السلطة القائمة على التفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، ومن بين هذه الإجراءات:

<sup>1</sup> المرجع نفسه، ص 146.

<sup>2</sup> نعيم سعيداني، المرجع السابق، ص 160.

ضبط الدعائم الأصلية دون نسخها، عدم تعريض الأقراص والأشرطة الممغنطة لدرجات الحرارة العالية ولا إلى الرطوبة، وأيضا عدم الضغط عليها بوضع أشياء ثقيلة<sup>1</sup>.

### الفرع الثاني: المعاينة

يقصد بالمعاينة في علم التحقيق الجنائي "مشاهدة المكان الذي ارتكبت فيه الجريمة وعمل وصف شامل له، سواء بالكتابة أو بالرسم التخطيطي أو بالتصوير لإثبات حالته بالكيفية التي تركها بها الجاني"<sup>2</sup>، إذن تعتبر المعاينة وسيلة جد هامة لتكوين الفكرة الأولى عن كيفية ارتكاب الجريمة، بالإضافة إلى أنها تعد من أهم مصادر الأدلة الجنائية المادية، ولكن هل يمكن أن نتصور القيام بإجراء معاينة في الجريمة المعلوماتية؟<sup>3</sup>

### أولا: صلاحية المعاينة في كشف وضبط الدليل الجنائي الرقمي

بالرغم من أن المعاينة تعتبر من أهم إجراءات التحقيق، إلا أن البعض يرى أن دورها يتضاءل في الكشف عن الجريمة المعلوماتية، وسبب ذلك أن الجريمة التقليدية تجري غالبا على مسرح جريمة تخلف آثار مادية، وهذا المسرح يعطي المجال أمام جهة البحث والتحري في الكشف عن غموض الجريمة، على عكس مسرح الجريمة المعلوماتية الذي يتضاءل فيه دور المعاينة، بسبب أن الجريمة المعلوماتية قلما تخلف آثار مادية<sup>3</sup>، بالإضافة إلى إمكانية التلاعب في الأدلة الجنائية الرقمية عن بعد عن طريق محوها أو إتلافها<sup>4</sup>.

<sup>1</sup> نبيلة هبة هرول، المرجع السابق، ص 273.

<sup>2</sup> خالد ممدوح إبراهيم، المرجع السابق، ص 149.

<sup>3</sup> عبد الفتاح بيومي حجازي، المرجع السابق، ص 314.

<sup>4</sup> نبيلة هبة هرول، المرجع نفسه، ص 217.

وعليه ولتجاوز هذا الإشكال، ينبغي على الفنيين القائمين على عملية المعاينة، التعامل مع مسرح الجريمة المعلوماتية على أنه مسرحان<sup>1</sup>:

- 1) **مسرح تقليدي (مادي):** ويشمل هذا المسرح جميع المكونات المادية للحاسب الآلي، ويمكن أن يحتوي على آثار مادية مثل بصمات الجاني أو وسائط تخزين رقمية، أو أوراق.
- 2) **مسرح افتراضي (رقمي):** ويقع داخل العالم الافتراضي (الرقمي) لجهاز الحاسب الآلي، ويحتوي على جميع المعلومات والبيانات الرقمية المخزنة فيه والتي تفيد في التحقيق<sup>2</sup>.

### ثانياً: إجراءات المعاينة في العالم الافتراضي

حتى تصبح لمعاينة مسرح الجريمة المعلوماتية فائدة عملية في الكشف عن ملامسات الجريمة، ينبغي مراعاة العديد من الإجراءات والخطوات الفنية، منها ما يكون قبل القيام بإجراء المعاينة، ومنها ما يكون بعدها.

#### 1) الإجراءات والخطوات الفنية المتخذة قبل القيام بإجراء المعاينة

عادة ما تكون هذه الإجراءات والخطوات تحضيرية، غرضها تهيئة الوسائل البشرية والمادية للقيام بإجراء المعاينة، ويتم ذلك بإعداد خطة عمل تحتوي على إعداد شامل للأدوات المستعملة في المعاينة، وتقسيم المهام بين الفنيين القائمين على هذا الإجراء<sup>3</sup>، بالإضافة إلى توفير معلومات مسبقة عن مكان الجريمة وعن نوع وعدد الأجهزة المراد معاينتها، وذلك لتحديد إمكانيات التعامل معها فنياً من حيث الضبط والتأمين وحفظ المعلومات، وتأمين التيار

---

<sup>1</sup> فاطمة زهرة بوعناد، "مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانونية، العدد الأول، (دون دار نشر)، الجزائر، 2013، ص 68.

<sup>2</sup> المرجع نفسه، ص 68.

<sup>3</sup> كاظم محمد عطيات ومحمد رضوان هلال، "كيفية التعامل التقني والأمن مع أوعية الجريمة الرقمية في مسرح الجريمة لضمان حيدة الدليل المستخلص"، المجلة العربية الدولية للمعلوماتية، العدد 5، المجلد 3، السعودية، 2014، ص 45.

الكهربائي تجنباً لتلفها<sup>1</sup>، كما أنه يجب في هذا المرحلة توفير الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل وفك التشفير<sup>2</sup>.

## (2) الإجراءات والخطوات الفنية المتخذة أثناء القيام بإجراء المعاينة

بعد القيام بالإجراءات التحضيرية التي سبق ذكرها، يقوم الفنيون القائمون على إجراء المعاينة بتصوير جهاز الحاسب الآلي وكافة مكوناته المادية<sup>3</sup>، مع التركيز على تصوير الأجزاء الخلفية له ومراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة<sup>4</sup>.

زيادة على ذلك، القيام بملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل ملحقات الحاسب الآلي<sup>5</sup>، وأيضا التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة، وكذا الشرائط والأقراص المضغوطة وفحصها<sup>6</sup>.

بعد ذلك يتم البحث في جهاز الحاسب الآلي – بعد تشغيله طبعا – عن الآثار الرقمية التي خلفها المستخدم، وذلك باستعمال كافة الوسائل التقنية كالدخول إلى السجلات والملفات، وفي هذه المرحلة يجب تعطيل حركة الاتصالات السلكية واللاسلكية بشبكة الإنترنت تجنباً لتلف الدليل الجنائي الرقمي أو التلاعب به وتخريبه عمداً عن بعد، وفي حالة ضبط معلومات أو بيانات رقمية، يجب مراعاة قواعد تحريز الأدلة الجنائية الرقمية، والتي تتطلب تخزينها عناية فائقة للدعائم مادية وفحصها واستعمالها لاحقاً.

<sup>1</sup> نبيلة هبة هروال، المرجع السابق، ص 219.

<sup>2</sup> المرجع نفسه، ص 219.

<sup>3</sup> كاظم محمد عطيات ومحمد رضوان هلال، المرجع السابق، ص 45.

<sup>4</sup> خالد ممدوح إبراهيم، المرجع السابق، 172.

<sup>5</sup> كاظم محمد عطيات ومحمد رضوان هلال، المرجع نفسه، ص 46.

<sup>6</sup> خالد ممدوح إبراهيم، المرجع نفسه، ص 173.

## الفرع الثالث: الخبرة

الخبرة القضائية هي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة<sup>1</sup>، إذن فالخبرة وسيلة لتحديد التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلاً مستقلاً وإنما هي تقييم فني لهذا الدليل<sup>2</sup>، وعليه ما أهمية الخبرة في مجال استخلاص الأدلة الجنائية الرقمية؟، وما هي الضوابط التي تحكم عمل الخبير في مجال الجريمة المعلوماتية؟.

### أولاً: أهمية الخبرة في كشف وتحليل الدليل الجنائي الرقمي

الخبير هو شخص مختص فنياً في مجال من المجالات الفنية أو العلمية أو غيرها من المجالات الأخرى، ويستطيع من خلال ما لديه من معلومات وخبرة إبداء الرأي في أمر من الأمور المتعلقة بالقضية التي تحتاج إلى خبرة فنية خاصة<sup>3</sup>، وإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمر ضروري، فالاستعانة به في مجال الجريمة المعلوماتية أكثر من الضروري<sup>4</sup>، وذلك بسبب أن عملية استخلاص الأدلة الجنائية الرقمية تتطلب مهارة ودراية كبيرة في مجال الحاسب الآلي، ولهذا كان لزاماً أن يتم اللجوء إلى خبير فني ومتخصص<sup>5</sup>.

<sup>1</sup> فاطمة زهرة بوعناد، المرجع السابق، ص 71.

<sup>2</sup> عبد الفتاح بيومي حجازي، المرجع السابق، ص 321.

<sup>3</sup> خالد ممدوح إبراهيم، المرجع السابق، ص 285.

<sup>4</sup> نعيم سعيداني، المرجع السابق، ص 166.

<sup>5</sup> ثنيان ناصر آل ثنيان، المرجع السابق، ص 108.

ونظرا لطبيعة عمل الخبير في هذا المجال، اهتم المشرع الجزائري مثل المشرع الفرنسي بتنظيم أعمال الخبرة وكيفية اللجوء إليها وذلك من خلال المواد من 143 إلى المادة 156 من قانون الإجراءات الجزائية الجزائري، بحيث نصت المادة 143 من نفس القانون أنه لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بنذب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها، ومن جهة أخرى أيضا نص المشرع الجزائري من خلال نص المادة 05 في فقرتها الأخيرة من القانون رقم 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنه يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

وعليه يمكن القول أنه دائما هناك حاجة ماسة إلى خبراء وفنيين من أجل القيام بالعديد من المهام التقنية مثل الكشف عن الأدلة الجنائية الرقمية وتحليلها، أو إصلاح الدليل وإعادة تجميعه من المكونات المادية للحاسب الآلي، أو التأكد من أن الدليل لم يتم العبث به<sup>1</sup>.

### ثانيا: الضوابط التي تحكم عمل الخبير في مجال الجريمة المعلوماتية

مما لا شك فيه عند قيام الخبير بمزاولة مهامه، يجب أن تتوفر مجموعة من الضوابط القانونية والفنية، فأما الضوابط القانونية هي أن يتم اختياره من قائمة الخبراء المعدة سلفا، وهو ما نصت عليه المادة 144 من قانون الإجراءات الجزائية، بحيث يختار الخبراء من الجدول الذي تعدده المجالس القضائية بعد استطلاع رأي النيابة العامة... واستثناء يجوز للجهات القضائية بصفة استثنائية أن تختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول، ويجب على الخبير أيضا أن يكون قد أدى اليمين القانونية وذلك لكي لا يترتب

<sup>1</sup> خالد ممدوح إبراهيم، المرجع السابق، ص 302.

على عمله البطلان، وهو ما نصت عليه المادة 145 من نفس قانون، وذلك بأن **يحنف** الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس<sup>1</sup>، وبعد ذلك يقوم الخبير بمزاولة مهامه المحددة له، وبعد انتهائه من عمله يعد تقريرا كتابيا مفصلا لما توصل إليه من نتائج، ويودعه خلال المدة المحددة له في الأمر أو الحكم بالندب.

وأما الضوابط الفنية فيجب على الخبير أن يكون ملما بكل ما يتعلق بالحاسب الآلي وملحقاته<sup>2</sup>، بالإضافة إلى وجوب تمكنه وفهمه البيئة التي يعمل فيها، والقدرة على أداء المهام الموكلة له دون أن يترتب على ذلك ضررا للدليل الجنائي الرقمي المراد استخلاصه<sup>3</sup>.

### المطلب الثالث: الصعوبات المتعلقة باستخلاص الدليل الجنائي الرقمي

بالرغم من الجهود المبذولة في مكافحة الجريمة المعلوماتية وذلك بوضع قواعد موضوعية لمواجهتها، وإجراء تعديلات في القواعد الإجرائية لتطوير أساليب مكافحتها، إلا أن هناك معوقات وصعوبات ما تزال تعترض عملية استخلاص الأدلة الجنائية الرقمية، ويمكن أن نجلها في صعوبات متعلقة بالدليل الجنائي الرقمي، وصعوبات متعلقة بجهات التحقيق، وفي الأخير إلى الصعوبات التشريعية وهو ما سنتعرض إليه في الفرعين المواليين.

<sup>1</sup> إبراهيم بلعليات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، 2012، ص 304.

<sup>2</sup> عبد الفتاح بيومي حجازي، المرجع السابق، ص 330.

<sup>3</sup> المرجع نفسه، ص 331.

## الفرع الأول: الصعوبات المتعلقة بالدليل الجنائي الرقمي

تتمثل الصعوبات المتعلقة بالدليل الجنائي الرقمي فيما يلي:

### أولاً: الطبيعة غير المرئية للدليل الجنائي الرقمي

دائماً ما يكون الدليل الجنائي في الجريمة التقليدية مرئياً ذو طبيعة مادية، بحيث يمكن للقائمين على عملية التحقيق بمعاينة مسرح الجريمة، وضبط أي دليل يفيد في الكشف عن ملبساتها<sup>1</sup>، ولكن في الجريمة المعلوماتية وكما تم ذكره في السابق تقع في بيئة مختلفة تماماً عن بيئة الجريمة التقليدية، إذ تكون فيها الأدلة عبارة عن نبضات أو مجالات مغناطيسية أو كهربائية مشكلة معلومات وبيانات رقمية في العالم الافتراضي<sup>2</sup>، ومنه فعدم رؤية الدليل الجنائي الرقمي يشكل العديد من الصعوبات من خلال جمعه وتحليله، مما يتوجب توفر لدى المحققين الفنيين دراية كافية ومهارة كبيرة في التعامل مع هذا النوع من الأدلة<sup>3</sup>.

### ثانياً: سهولة تدمير ومحو الدليل الجنائي الرقمي

يعد تدمير ومحو الأدلة الجنائية الرقمية من بين أكبر الصعوبات التي تعترض عملية الاستخلاص، نظراً للسهولة التي تتميز بها هذه العملية واستغراقها لوقت قصير جداً<sup>4</sup>، فمرتكبي الجريمة المعلوماتية يتميزون بالذكاء والإتقان الفني للعمل الذي يقومون به، ولذلك فإنهم يسعون دائماً لمحو وتدمير أو حتى تعديل أي دليل يؤدي إلى إدانتهم<sup>5</sup>، عن طريق التلاعب غير المرئي في أنظمة الحاسب الآلي ومحتوياته.

<sup>1</sup> ثيان ناصر آل ثيان، المرجع السابق، ص 117.

<sup>2</sup> عبد الفتاح بيومي حجازي، المرجع السابق، ص 78.

<sup>3</sup> المرجع نفسه، ص 79.

<sup>4</sup> هشام محمد فريد رستم، "أصول التحقيق الجنائي الفني"، في بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2004، ص 429.

<sup>5</sup> Eoghan Casey, Op.Cit., p 6.

### ثالثاً: إعاقة الوصول إلى الدليل الجنائي الرقمي

يلجأ مرتكبي الجريمة المعلوماتية دائماً لابتكار أحدث الوسائل والأساليب لعرقلة جمع أدلة الإدانة، ومن بين هذه الوسائل استخدام تقنية التشفير<sup>1</sup>، أو فرض تدابير أمنية لمنع وعرقلة عملية التفتيش والاطلاع عن الأدلة أو ضبطها وذلك باستخدام كلمات سر<sup>2</sup>، أو لجوء مرتكب الجريمة المعلوماتية إلى إخفاء هويته وخاصة عند استخدام شبكة الإنترنت، وذلك باستعمال العديد من البرامج والتطبيقات التي تعمل على طمس هويته في شبكة الإنترنت<sup>3</sup>.

### رابعاً: ضخامة البيانات المتعين فحصها

لعل من بين أكبر الصعوبات التي تواجه رجال الضبط وسلطات التحقيق في استخلاص الأدلة الجنائية الرقمية، هو الكم الهائل للمعلومات والبيانات المراد فحصها وتحليلها<sup>4</sup>. فضلاً عن ضرورة توفر الخبرة الفنية للمحقق في مجال الحاسب الآلي وملحقاته، يتعين كذلك أن يتوافر لديه القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة في جهاز الحاسب الآلي أو في دعائم التخزين الرقمية<sup>5</sup>، لذلك ولمواجهة هذه الصعوبة وتجاوزها وجب الاستعانة بخبراء فنيين في مجال الحاسب الآلي<sup>6</sup>، بداعي معرفتهم معرفتهم بمكان وكيفية جمع المعلومات والبيانات التي يمكن أن تفيد التحقيق، في ظل الصعوبة البالغة لفحص كل أنظمة الحاسب الآلي.

<sup>1</sup> عبد الفتاح بيومي حجازي، المرجع السابق، ص 89.

<sup>2</sup> هشام محمد فريد رستم، المرجع السابق، ص 427.

<sup>3</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 121.

<sup>4</sup> ثنيان ناصر آل ثنيان، المرجع السابق، ص 131.

<sup>5</sup> المرجع نفسه، ص 131.

<sup>6</sup> هشام محمد فريد رستم، المرجع نفسه، ص 431.

## الفرع الثاني: الصعوبات المتعلقة بجهات التحقيق

يتطلب استخلاص الأدلة الجنائية الرقمية وفحصها إلى مهارات وخبرات خاصة في مجال الحاسب الآلي، بالإضافة إلى أساسيات وأصول التحقيق الجنائي الفني المطبقة في مجال الجرائم التقليدية<sup>1</sup>، لذا فنقص خبرة المحققين وعدم متابعتهم للمستجدات الحاصلة في مجال الحاسب الآلي، وعدم معرفتهم للأساليب والتقنيات المستعملة في ارتكاب الجريمة المعلوماتية يشكل عائق كبير في جمع الأدلة الجنائية الرقمية وتحليلها.

لذلك وتجاوز هذه الصعوبات وجب تخصيص وحدات خاصة لديها الإلمام الكافي بتقنيات الحاسب الآلي<sup>2</sup>، بالإضافة إلى تعديل مناهج التدريب والدراسة في كل أكاديميات الشرطة عن طريق إدخال مواد جديدة لدراسة تقنيات الحاسب الآلي ونظم المعلومات<sup>3</sup>، وأيضا تكثيف البعثات التكوينية إلى الخارج قصد الاحتكاك بالبلدان التي تملك الخبرة الكافية في هذا المجال.

إلا أن البعض يرى بأن هذه الحلول لا تكفي في تطوير وتكوين خبراء متخصصين في جمع الأدلة الجنائية الرقمية، وذلك لعدة أسباب من بينها ضعف الميزانيات المالية المقررة للتكوين والوقت الكبير الذي تستهلكه هذه العملية<sup>4</sup>، زيادة على ذلك أن انتشار الحاسب الآلي على نطاق واسع وتعدد أنظمتها وبرامجها وتطورها بشكل سريع، يجعل ملاحقتها من حيث الإعداد والتدريب عليها أمر يتسم بالصعوبة<sup>5</sup>، لذا وتماشيا مع اتجاه تطوير وتكوين خبراء متخصصين في مجال جمع الأدلة الجنائية الرقمية، بادرت مختلف الدول في إنشاء وحدات

<sup>1</sup> هشام محمد فريد رستم، المرجع السابق، ص 437.

<sup>2</sup> محمد الأمين البشري، التحقيق في الجرائم المستحدثة، المرجع السابق، ص 109.

<sup>3</sup> نبيلة هبة هروال، المرجع السابق، ص 101.

<sup>4</sup> عبد الفتاح بيومي حجازي، المرجع السابق، ص 125.

<sup>5</sup> المرجع نفسه، ص 126.

متخصصة في مجال البحث والتحري عن الجريمة المعلوماتية، ومن بين هذه الدول فرنسا التي استحدثت وحدات متخصصة وغير متخصصة ضمن جهازي الشرطة والدرك لمكافحة الجريمة المعلوماتية، وذلك بإنشاء المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات بموجب المرسوم الوزاري المشترك رقم 405-2000 المؤرخ في 2000/05/15، والذي يعد من بين أهم مهامه تقديم المساعدة التقنية لجهات التحقيق<sup>1</sup>.

وأما في الجزائر فإنه تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام تحت وصاية القيادة العامة للدرك الوطني، بموجب المرسوم الرئاسي رقم 183-04 المؤرخ في 2004/06/26<sup>2</sup>، وقد نصت المادة 04 منه على العديد من المهام الموكلة إلى هذا المعهد أهمها إجراء الخبرات والفحوص العلمية بناء على طلب من القضاة والمحققين أو السلطات المؤهلة، بالإضافة إلى المساعدة التقنية والفنية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية والتقنية، الرامية إلى تجميع وتحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة، ويحتوي هذا المعهد على قسم الإعلام الآلي الذي يختص بالتحقيق من خلال جمع الأدلة الجنائية الرقمية وتحليلها<sup>3</sup>.

وبالإضافة إلى المعهد الوطني للأدلة الجنائية وعلم الإجرام، تم استحداث أيضا المعهد الوطني للبحث في علم التحقيق الجنائي تحت وصاية المديرية العامة للأمن الوطني، بموجب المرسوم الرئاسي رقم 432-04 المؤرخ في 2004/12/29<sup>4</sup>، والذي نص أيضا في المادة 05 منه على مجموعة من المهام من بينها إعداد تقارير الخبرة، وأيضا القيام بالتكوين وتجديد المعارف في ميدان علم التحقيق الجنائي والإجرام، ويحتوي هذا المعهد على مصلحة

<sup>1</sup> سعيداني نعيم، المرجع السابق، ص 188.

<sup>2</sup> الجريدة الرسمية رقم 41، الصادرة بتاريخ 2004/06/27، ص 18.

<sup>3</sup> سعيداني نعيم، المرجع نفسه، ص 189.

<sup>4</sup> الجريدة الرسمية رقم 84، الصادرة بتاريخ 2004/12/29، ص 24.

الخبرات الخاصة بالدلائل التكنولوجية<sup>1</sup>، بحيث تكلف بتحليل الدلائل المادية التي تم جمعها إثر معاينة المخالفات والتحريات في ميدان الجريمة المعلوماتية وإعداد تقارير الخبرة.

### الفرع الثالث: الصعوبات التشريعية

يعد القصور التشريعي في مجال استخلاص الأدلة الجنائية الرقمية من بين أكبر الصعوبات التي تعترض الخبراء والفنيين المتخصصين في مكافحة الجريمة المعلوماتية، وهو ما جعل الدول تعمل على تحديث منظوماتها القانونية من خلال تعديل قوانينها الإجرائية، وقد كانت الجزائر من بين هذه الدول التي استحدثت آليات قانونية تسهل من عملية جمع الأدلة الجنائية الرقمية، وذلك من خلال ما أتى به في القانون رقم 09-04 المؤرخ في 2009/08/05 والمتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي أتى بإجراءات وأساليب تقنية تتمثل في مراقبة الاتصالات الإلكترونية (المادة 04)، وتفتيش المنظومة المعلوماتية (المادة 05)، وحجز المعطيات المعلوماتية (المادتين 06 و 07)، زيادة على ذلك أيضا قام المشرع الجزائري بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك بهدف تنسيق ومساعدة السلطات القضائية في التحريات بما في ذلك تجميع المعلومات وإنجاز الخبرات.

---

<sup>1</sup> قرار وزاري مشترك مؤرخ في 2007/04/14 والمتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية رقم 36، الصادرة بتاريخ 2007/06/03، ص 14.

وأما المشرع الفرنسي فقد كان السباق في تعديل قوانينه لمواجهة القصور التشريعي في مجال استخلاص الأدلة الجنائية الرقمية، بحيث قام بتعديل قانون الإجراءات الجزائية بموجب القانون رقم 239-2003 والمؤرخ في 18/03/2003، وأتى بالعديد من القواعد القانونية التي تسهل من عملية جمع الأدلة الجنائية الرقمية، من بينها ما نصت به المادة 17 من نفس القانون، بحيث أجازت لضباط الشرطة القضائية أو تحت مسؤوليتهم أعوان الشرطة القضائية الدخول إلى الأنظمة المعلوماتية وتفتيشها وحجز كل ما يفيد الكشف عن الجريمة.

وعلى هذا الأساس وبالرغم من الجهود المبذولة في مجال تطوير تقنيات استخلاص الأدلة الجنائية الرقمية، إلا أن التحدي ما يزال قائماً حول مجارة نسق تطور الجريمة المعلوماتية وتطور أساليب ارتكابها، عن طريق التحديث الدوري للتشريعات الداخلية سواء ما تعلق منها بالجانب الموضوعي أو الإجرائي، زيادة على ذلك تطوير مهارات الخبراء المتخصصين والمحققين وذلك للحصول على أحسن النتائج في مجال جمع الأدلة الجنائية الرقمية.

## الفصل الثاني

### القيمة القانونية للدليل الجنائي الرقمي

بعد بيان ماهية الدليل الجنائي الرقمي في الفصل الأول، يتبقى لنا البحث في القيمة القانونية للأدلة الجنائية الرقمية في مجال الإثبات الجنائي، وذلك بسبب أن هذا النوع من الأدلة ما يزال يثير العديد من الإشكاليات حوله نظرا للطابع الخاص الذي يتميز به عن غيره من الأدلة الجنائية الأخرى.

لذا سنتعرض في هذا الفصل ومن خلال المبحث الأول إلى شروط قبول الدليل الجنائي الرقمي أمام القضاء الجنائي، وأما المبحث الثاني سنتطرق فيه لسلطة القاضي في تقدير الأدلة الجنائية الرقمية.

## المبحث الأول: شروط قبول الدليل الجنائي الرقمي أمام القضاء الجنائي

إن مجرد وجود دليل يثبت وقوع الجريمة وينسبها لشخص معين لا يكفي للاعتماد عليه لإصدار الحكم بالإدانة، إذ يجب أن يكون لهذا الدليل قيمة قانونية<sup>1</sup>، وهذه القيمة تتوقف على خضوعه للقواعد المقررة في الإثبات الجنائي، وهو كذلك بالنسبة للدليل الجنائي الرقمي الذي يجب أيضا أن يخضع مثل باقي الأدلة لقواعد الإثبات الجنائي، وذلك بأن يتصف الدليل بالمشروعية، وأن يكون أيضا يقينيا في دلالاته على الوقائع المراد إثباتها، وفي الأخير خضوعه للمناقشة.

### المطلب الأول: مشروعية الدليل الجنائي الرقمي

بناء على مبدأ مشروعية الدليل الجنائي، يجب على القاضي أن يستمد اقتناعه بالإدانة من أدلة صحيحة ومشروعة<sup>2</sup>، وذلك من خلال ضرورة اتفاق الإجراء مع القواعد القانونية والأنظمة الثابتة للمجتمع، والهدف من ذلك هو تقرير الضمانات الأساسية للأفراد وحماية حرياتهم وحقوقهم الشخصية من تعسف سلطة التحقيق في غير الحالات التي رخص القانون فيها بذلك<sup>3</sup>، ومنه فقاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضا مراعاة إعلانات حقوق الإنسان والمواثيق والاتفاقيات الدولية وقواعد النظام العام<sup>4</sup>.

<sup>1</sup> خالد عياد الحلبي، المرجع السابق، ص 235.

<sup>2</sup> نصر الدين مروك، محاضرات في الإثبات الجنائي (النظرية العامة للإثبات الجنائي)، الجزء الأول، دار هومة، الجزائر، 2003، ص 519.

<sup>3</sup> كمال محمد عواد، الضوابط الشرعية والقانونية للأدلة الجنائية (في الفقه الإسلامي والقانون الوضعي)، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011، ص 165.

<sup>4</sup> أحمد عبد اللاه هلال، "حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة)"، في بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2004، ص 429.

وتطبيقا لما أوردناه سابقا، تتمثل مشروعية الدليل الجنائي الرقمي في مشروعية وجوده ومشروعية الحصول عليه، والذي سنتناوله في الفرعين المواليين.

### الفرع الأول: مشروعية وجود الدليل الجنائي الرقمي

يقصد بمشروعية الوجود أن يكون الدليل الجنائي الرقمي معترفاً به، بمعنى أن القانون يجيز للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة<sup>1</sup>، ويتحدد موقف القوانين من مشروعية وجود الدليل الجنائي الرقمي بحسب طبيعة نظام الإثبات السائد في الدولة.

#### أولاً: مشروعية وجود الدليل الجنائي الرقمي في نظام الإثبات المقيد (القانوني)

بناء على هذا النظام فإن المشرع هو الذي يحدد على سبيل الحصر الأدلة الجنائية التي يجوز للقاضي اللجوء إليها في الإثبات، كما يحدد القوة الإقناعية لكل دليل جنائي، بحيث يقتصر دور القاضي في فحص الدليل والتأكد من توافر الشروط التي حددها القانون، وعليه فلا سبيل للاستناد إلى أي دليل لم ينص القانون عليه صراحة ضمن أدلة الإثبات<sup>2</sup>، ففي بريطانيا مثلاً والتي تتبنى نظام الإثبات المقيد (القانوني) قد أصدرت في 1984 قانون البوليس والإثبات الجنائي<sup>3</sup>، والذي احتوى فيه تنظيمًا محددًا لمسألة قبول الأدلة الجنائية الرقمية بمختلف أشكالها كأدلة إثبات في المواد الجنائية<sup>4</sup>.

---

<sup>1</sup> خالد عياد الحلبي، المرجع السابق، ص 235-236.

<sup>2</sup> المرجع نفسه، ص 236.

<sup>3</sup> علي حسن محمد الطوالة، المرجع السابق، ص 196.

<sup>4</sup> المرجع نفسه، ص 197.

## ثانيا: مشروعية وجود الدليل الجنائي الرقمي في نظام الإثبات الحر

وفقا لهذا النظام يتمتع القاضي بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه، لأن القانون لا يلزمه في تكوين اقتناعه بأدلة جنائية محددة، بل يمكن له أن يعتمد على أي دليل جنائي يراه مناسباً وإن لم يكن منصوصاً عليه قانوناً<sup>1</sup>.

وعليه ففي مثل هذا النظام الذي يقوم على حرية الإثبات الجنائي، لا تثار مشكلة مشروعية وجود الدليل الجنائي الرقمي، على اعتبار أن المشرع ليس مطالب بتحديد أدلة الإثبات بتاتا لأن الأصل في الأدلة مشروعية وجودها في هذه الحالة<sup>2</sup>، وهو نفس ما اتجه إليه المشرعين الجزائري والفرنسي على اعتبار أنهما يتبنيان نظام الإثبات الحر.

## الفرع الثاني: مشروعية الحصول على الدليل الجنائي الرقمي

سنتناول في هذا الفرع مشروعية الحصول على الدليل الجنائي الرقمي من خلال دراسة الأسس التي تقوم عليها، وكيفية معالجة كلا التشريعين الجزائري والفرنسي لها.

## أولاً: أسس مشروعية الحصول على الدليل الجنائي الرقمي

يشترط في الدليل الجنائي الرقمي لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعاً، وذلك من خلال أن يكون الإجراء المتبع في استخلاص الدليل الجنائي الرقمي مشروعاً<sup>3</sup>، عن طريق مراعاة القواعد الموضوعية والشكلية أثناء اتخاذ أي إجراء.

<sup>1</sup> خالد عياد الحلبي، المرجع السابق، ص 237.

<sup>2</sup> المرجع نفسه، ص 238.

<sup>3</sup> كمال محمد عواد، المرجع السابق، ص 167.

وتتمثل القواعد الموضوعية في أن يكون الإجراء الذي يستهدف استخلاص الدليل الجنائي الرقمي عملاً إرادياً صادراً من شخص له صلاحية القيام به بناء على سبب معين، زيادة على ذلك يجب أن يكون المحل الذي يرد عليه الإجراء محددًا أو قابلًا للتحديد وأن يكون مشروعاً، وأما بالنسبة للقواعد الشكلية فيجب الالتزام باحترام كيفية مباشرة تنفيذ هذا الإجراء<sup>1</sup>، ودائماً ما تكون القواعد الشكلية محددة بموجب القانون.

وعلى هذا الأساس فإن مخالفة القواعد الإجرائية التي تستهدف استخلاص الدليل الجنائي الرقمي يؤدي إلى بطلانها، وبالتالي بطلان الدليل الناتج عنها، ولا تصلح في الأخير لأن تكون أدلة جنائية يبنى عليها الحكم بالبراءة أو بالإدانة.

### ثانياً: مشروعية الحصول على الدليل الجنائي الرقمي في التشريعين الجزائري والفرنسي

دائماً ما يفترن الحديث عن مشروعية الحصول على الأدلة الجنائية بوجوب حماية واحترام حقوق الإنسان، على اعتبار أن جميع الإجراءات القانونية التي تستهدف الحصول على الأدلة الجنائية تمس بحقوق الأفراد وحياتهم، ومن بين هذه الحقوق الحق في الخصوصية، لذا فإن اتخاذ إجراء المراقبة الإلكترونية أو اعتراض المراسلات يمثل دون أدنى شك اعتداء على الحياة الخاصة، هذا الذي جعلها موضوع اهتمام كبير من قبل الإعلانات والمواثيق الدولية<sup>2</sup>، ومثال ذلك ما نصت عليه المادة 12 من الإعلان العالمي لحقوق الإنسان، إذ: "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات".

<sup>1</sup> كمال محمد عواد، المرجع السابق، ص 167 - 170.

<sup>2</sup> معتصم خميس مشعشع، "إثبات الجريمة بالأدلة العلمية"، مجلة الشريعة والقانون، العدد 56، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2013، ص 34.

ومن جهة أخرى وتماشيا مع الاتجاه الدولي في إقرار هذا الحق وحمائته، قامت العديد من التشريعات ومن بينها التشريع الجزائري بتأكيد الحق في الخصوصية وحمائته، وذلك من خلال ما نص عليه في المادة 39 من الدستور، بحيث نصت على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، وحميها القانون"، وأضافت نفس المادة في فقرتها الثانية أن: "سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"، وتأتي الحماية القانونية لهذا الحق المنصوص عليه في الدستور من خلال قانون العقوبات، وذلك بما أتت به نص المادة 303 مكرر من قانون العقوبات<sup>1</sup>، إذ: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دينار جزائري إلى 300.000 دينار جزائري، كل من تعدد المساس بحرمة الحياة الخاصة للأشخاص، وبأية تقنية خاصة كانت وذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه...".

وأما فيما يخص المشرع الفرنسي فقد كان السباق في حماية الحياة الخاصة، وذلك بموجب إصداره لقانون رقم 70-643 المؤرخ في 17/07/1970، بالإضافة إلى القانون رقم 78-17 الصادر في 1978 والمتعلق بالمعالجة الإلكترونية للبيانات الرسمية، والذي تضمن حماية البيانات الشخصية المرتبطة بالحياة الخاصة للأفراد<sup>2</sup>، زيادة على ذلك ما نص عليه قانون العقوبات الفرنسي بتجريم العديد من الأفعال التي تمس بالبيانات الإلكترونية الشخصية، مثل ما نصت عليه المادة 226 مكرر 1 التي تعاقب كل من يقوم بمعالجة إلكترونية للبيانات الشخصية من دون ترخيص، وكذا ما نصت عليه المادة 226 مكرر 21 التي عاقبت على الانحراف عن الغرض من المعالجة الإلكترونية للبيانات الشخصية.

---

<sup>1</sup> الأمر رقم 66-156 المؤرخ في 08/06/1966، المتضمن قانون العقوبات، الجريدة الرسمية رقم 49، الصادرة بتاريخ 11/06/1966، المعدل والمتمم.

<sup>2</sup> سوزان عدنان الأستاذة، "انتهاك حرمة الحياة الخاصة عبر الإنترنت (دراسة مقارنة)"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الثالث، المجلد 29، سوريا، 2013، ص 437.

إنّ وبناء على ما سبق ذكره، فقد حرص كل من المشرعين الجزائري والفرنسي على حماية الحياة الخاصة للفرد، وذلك بالرفع من مكانة هذا الحق وجعله في مصاف الحقوق الدستورية، بالإضافة إلى تقرير عقوبات على كل الأفعال التي تخل به، ولكن هذا لا يعني أنه لا يمكن المساس بهذا الحق بتاتا، إذ وضع القانون استثناءات على هذه القاعدة الدستورية، وذلك بإمكانية المساس بهذا الحق إذا اقتضت الضرورة<sup>1</sup>، من خلال القيام بإجراءات تفتيش أنظمة الحاسب الآلي أو مراقبة الاتصالات الإلكترونية بغية استخلاص الأدلة الجنائية الرقمية، وذلك بشرط احترام الإجراءات الخاصة بها والمنصوص عليها قانونا.

وعلى هذا الأساس، وفي إطار مشروعية الحصول على الدليل الجنائي الرقمي، فالمشرع الفرنسي وبالرغم من أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة والنزاهة في البحث عن الحقيقة، إلا أن الفقه والقضاء اعتمدا هذا المبدأ<sup>2</sup> في مجال استخلاص الأدلة الجنائية بصفة عامة، بحيث تم قبول استخدام الوسائل العلمية الحديثة في بحث واستخلاص الأدلة الجنائية – والتي من بينها الأدلة الرقمية – تحت تحفظ، وهو أن يتم الحصول عليها بطريقة مشروعة ونزيهة<sup>3</sup>.

---

<sup>1</sup> عبر على هذا الاستثناء نص المادة 3 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إذ جاء فيها: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

<sup>2</sup> علي حسن محمد الطوالة، المرجع السابق، ص 187.

<sup>3</sup> أحمد عبد اللاه هلال، المرجع السابق، ص 753.

## المطلب الثاني: يقينية الدليل الجنائي الرقمي

إن الهدف الذي تسعى إليه كافة التشريعات الإجرائية هو أن يصيب القاضي الحقيقة في حكمه، سواء بالبراءة أو بالإدانة، والحقيقة لا يمكن الوصول إليها إلا باليقين، ومنه تكمن أهمية يقينية الأدلة الجنائية في اتصاله المباشر لما سيؤول إليه حكم القاضي في الدعوى العمومية، لذا وجب علينا وفي هذا المطلب أن نبين مفهوم يقينية الأدلة الجنائية الرقمية، بالإضافة إلى بيان القواعد التي تحكمها.

### الفرع الأول: مفهوم مبدأ يقينية الدليل الجنائي الرقمي

اليقين بصفة عامة هو عبارة عن "حالة ذهنية أو عقلانية تؤكد وجود الحقيقة، ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة عالية من التوكيد"<sup>1</sup>، لذا عندما يصل القاضي إلى اليقين فإنه يصبح في هذه المرحلة مقتنعا بالحقيقة، لأن اليقين في الأصل هو وسيلة لاقتناع القاضي، أو بعبارة أخرى أن اقتناع القاضي بالحقيقة هو ثمرة اليقين وليس اليقين ذاته<sup>2</sup>.

ومنه فالوصول إلى اليقين يكون عن طريق نوعين من المعرفة، الأولى تتمثل في المعرفة الحسية التي تدركها الحواس، والثانية تتمثل في المعرفة العقلية التي يقوم بها العقل عن طريق التحليل والاستنتاج<sup>3</sup>.

<sup>1</sup> نصر الدين مروك، المرجع السابق، ص 491.

<sup>2</sup> المرجع نفسه، ص 491.

<sup>3</sup> أحمد عبد اللاه هلال، المرجع السابق، ص 739.

وأما اليقين في مجال الأدلة الجنائية الرقمية، فإنه يشترط في هذا النوع من الأدلة مثل باقي الأدلة الجنائية الأخرى، بحيث أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، وذلك أنه لا مجال لدحض قرينة البراءة وافترض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين<sup>1</sup>.

ويمكن الوصول إلى اليقين في هذه الحالة من خلال ما يعرض من الأدلة الرقمية بمختلف أنواعها وأشكالها، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه<sup>2</sup>.

وفي حالة عدم قدرة أدلة الإدانة على إحداث القطع أو اليقين يترتب عليه استمرار حالة البراءة التي يكفي لتأكيد وجودها حينئذ مجرد الشك في ثبوت تلك الإدانة، انطلاقاً من أن الحكم بالإدانة يستوجب اليقين بوجود هذه الإدانة، وذلك لأنها إثبات على خلاف الأصل الذي لا يمكن إثبات عكسه إلا بمقتضى حالة من اليقين تتساوى في نتائجها مع تلك المسلم بوجودها نتيجة لمبدأ افتراض البراءة<sup>3</sup>.

### الفرع الثاني: القواعد التي تحكم مبدأ يقينية الأدلة الجنائية الرقمية

نظراً للطبيعة التقنية التي يتميز بها الدليل الجنائي تم وضع قواعد محددة من طرف مختصين تحكم يقينيتها، وذلك بواسطة استعمال وسائل فنية من طبيعة هذا الدليل تمكن من فحصه والتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه<sup>4</sup>.

<sup>1</sup> علي حسن محمد الطوالية، المرجع السابق، ص 190.

<sup>2</sup> المرجع نفسه، ص 191.

<sup>3</sup> أحمد عبد اللاه هلال، المرجع السابق، ص 740.

<sup>4</sup> خالد عياد الحلبي، المرجع السابق، ص 249.

## أولاً: تقييم الدليل الجنائي الرقمي من حيث سلامته من العبث

تعتبر صلاحية الأدلة الجنائية الرقمية المستخلصة والتأكد من سلامتها من القواعد الأساسية التي يقوم عليها التحقيق الجنائي<sup>1</sup>، وعليه فإن مضمون عملية تقييم الدليل الجنائي الرقمي هو التأكد من سلامته من العبث عبر إتباع مجموعة من الطرق أهمها استعمال عملية التحليل التناظري الرقمي، التي تعتبر من بين الوسائل المهمة للكشف عن مصداقية الدليل الرقمي، من خلال القيام بعملية مقارنة الدليل الجنائي الرقمي (الأصلي) المقدم للقضاء بالنسخة المستخرجة<sup>2</sup>.

وفي حالة عدم الحصول على النسخة الأصلية للدليل الجنائي الرقمي، أو في حالة وقوع تعديل أو إتلاف النسخة الأصلية، فيمكن في هذه الحالة التأكد من سلامة هذا الدليل من العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات، أو باللجوء إلى نوع آخر من الأدلة الرقمية والذي يطلق عليه باسم الدليل الرقمي المحايد<sup>3</sup>، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يساهم في التأكد من مدى سلامة الدليل الجنائي الرقمي<sup>4</sup>.

لذا وتفادياً لحصول أي إتلاف أو تعديل للدليل الجنائي الرقمي، يوصي المختصون دائماً بالحفاظ على الدليل الجنائي الرقمي الأصلي، واستغلال الميزة التي يتمتع بها وهي استخراج العديد من النسخ المطابقة له<sup>5</sup>.

---

<sup>1</sup> Ankit Agarwal and others., "Systematic Digital Forensic Investigation Model", in: International Journal of Computer Science and Security (IJCSS), Volume 5, Issue 1, United states of America, 2011, p 119.

<sup>2</sup> خالد عياد الحلبي، المرجع السابق، ص 249.

<sup>3</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 125.

<sup>4</sup> خالد عياد الحلبي، المرجع نفسه، ص 249.

<sup>5</sup> Debra Littlejohn Shinder, Op.Cit., p 552.

## ثانياً: تقييم الدليل الجنائي الرقمي من حيث السلامة الفنية لإجراءات استخلاصه

أثناء إتباع جملة من الأساليب والإجراءات التقنية للحصول على الأدلة الجنائية الرقمية، يمكن أن تعترى هذه الإجراءات أخطاء قد تشكك في سلامة النتائج، لذا يجب في هذه الحالة الاعتماد على اختبارات محددة كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الجنائي الرقمي<sup>1</sup>، ويتمثل مضمونها في:

### (1) التأكد من دقة الأدوات المستخدمة في استخلاص الدليل الجنائي الرقمي

يكون التأكد من دقة الأدوات المستخدمة في استخلاص الدليل الجنائي الرقمي بالتحقق من مدى قدرة هذه الأدوات على عرض كافة البيانات المتعلقة بالدليل الجنائي الرقمي<sup>2</sup>، بالإضافة إلى خضوع هذه الأدوات لاختبار فني يمكن من خلاله التأكد من أنها لا تعرض بيانات إضافية جديدة<sup>3</sup>.

### (2) الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل

تبين الدراسات العلمية في مجال تقنية المعلومات على الطرق السليمة التي يجب إتباعها في الحصول على الدليل الجنائي الرقمي، لذا فالاعتماد على الأدوات التي أوضحت الدراسات العلمية عدم كفاءتها، يؤثر بصفة مباشرة على مصداقية الأدلة الجنائية الرقمية المستمدة منها<sup>4</sup>، وبالتالي يتعدى التأثير حتى إلى يقين القاضي الذي يقوم باستبعاد هذه الأدلة نتيجة عدم مصداقيتها.

<sup>1</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 127.

<sup>2</sup> خالد عياد الحلبي، المرجع السابق، ص 250.

<sup>3</sup> ممدوح عبد الحميد عبد المطلب، المرجع نفسه، ص 251.

<sup>4</sup> خالد عياد الحلبي، المرجع نفسه، ص 251.

## المطلب الثالث: مناقشة الأدلة الجنائية الرقمية

يعتبر مبدأ مناقشة الأدلة الجنائية من أهم الضوابط التي تصل بالحكم إلى العدالة التي ينشدها الجميع، بحيث تطرح جميع الأدلة المتوفرة في ساحة المحكمة، ويتسنى من خلال ذلك مناقشتها وتمحيصها.

وعليه سنتعرض في الفرعين المواليين لمفهوم مبدأ مناقشة الأدلة الجنائية، ومن جهة أخرى سنتعرض إلى مضمون مناقشة الأدلة الجنائية الرقمية بصفة خاصة.

### الفرع الأول: مفهوم مبدأ مناقشة الأدلة الجنائية

يقصد بمناقشة الأدلة الجنائية بصفة عامة "أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة، وخضعت لحرية مناقشة أطراف الدعوى"<sup>1</sup>، وقد نص عليها المشرع الجزائري من خلال المادة 2/212 من قانون الإجراءات الجزائية بقولها: "...ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه"، ونص عليها أيضا المشرع الفرنسي بناء على المادة 2/427 من قانون الإجراءات الجزائية الفرنسي، بحيث جاء فيها: "...لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحاكمة ونوقشت أمامه في مواجهة الأطراف".

وبناء على ذلك فإنه لا يجوز للقاضي أن يبني حكمه على أي دليل كان، بل يجب أن يكون هذا الدليل قد طرح بجلسة المرافعة وتمت مناقشته عن طريق إتاحة الخصوم الاطلاع على الأدلة بصفة حضورية في جلسة المحاكمة<sup>2</sup>.

<sup>1</sup> نصر الدين مروك، المرجع السابق، ص 637.

<sup>2</sup> المرجع نفسه، ص 458.

والغرض من التأكيد على وجوب احترام هذا المبدأ هو أنه يشكل ضماناً هامة من ضمانات المحاكمة العادلة، وذلك بوجوب احترام الحق في الدفاع، بالإضافة إلى تفادي اعتماد القاضي في حكمه على معلوماته الشخصية أو معلومات الغير<sup>1</sup>، إلا إذا كان الغير من الخبراء، وقد ارتاح ضميره إلى التقرير المحرر من قبله فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى العمومية المعروضة عليه<sup>2</sup>.

كما يستند مبدأ مناقشة الأدلة الجنائية على قواعد أساسية تتمثل في شفوية المرافعة، والتي يعني بها وجوب أن تجري المرافعة شفويا – أي بصوت مسموع – لجميع إجراءات المحاكمة، فالشهود والخبراء يدلون بأقوالهم شفويا أمام القاضي ويناقشون فيها أيضا شفويا<sup>3</sup>.

وأما القاعدة الأخرى، فتتمثل في المواجهة بين الخصوم، والمقصود من هذه القاعدة ليس المواجهة في حد ذاتها، ولكن المواجهة التي يقصدها بها هي مواجهة أدلة كل خصم للآخر، بحيث يتاح لكل منهما إبداء أدلته ودفاعاته، وفي النهاية يتسنى للقاضي تكوين اقتناعه من خلال هذه المواجهة<sup>4</sup>.

وعليه يترتب الإخلال بمناقشة الأدلة الجنائية بطلان الأدلة وعدم الاعتداد بها، وذلك بسبب أن الإخلال بمبدأ المناقشة يحرم خصوم الدعوى العمومية من الاطلاع على الأدلة وإبداء دفوعاتهم، وهو ما يتنافى مع قواعد المحاكمة العادلة.

---

<sup>1</sup> نصر الدين مروك، المرجع السابق، ص 641.

<sup>2</sup> نعيم سعيداني، المرجع السابق، ص 219.

<sup>3</sup> كمال محمد عواد، المرجع السابق، ص 362.

<sup>4</sup> المرجع نفسه، ص 364.

## الفرع الثاني: مضمون مناقشة الأدلة الجنائية الرقمية

انطلاقاً مما سبق ذكره، وبعد التطرق إلى المفهوم العام لمبدأ مناقشة الأدلة الجنائية، يمكن لنا القول أن الأدلة الجنائية الرقمية بمختلف أنواعها وأشكالها، سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسب الآلي، كلها ستكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة<sup>1</sup>، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة العالم الافتراضي، يجب أن يعرض في الجلسة بصفة مباشرة أمام القاضي، هذه الأحكام تنطبق على كافة الأدلة المستخلصة من أجهزة الحاسب الآلي أو من الأجهزة الأخرى المماثلة له، أو حتى من شبكاته<sup>2</sup>.

وبالنسبة لشهود الجريمة المعلوماتية الذين يكون قد سبق أن سمعت أقوالهم، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام هيئة المحكمة<sup>3</sup>.

وعلى هذا الأساس فمناقشة الأدلة الجنائية الرقمية قد تتطلب مؤهلات تقنية ومعارف فنية غير التي تتوفر في القاضي، وهو ما يؤدي بنا إلى القول بضرورة التأهيل التقني والفني للقضاة لمواكبة المناقشة العلمية للأدلة الجنائية الرقمية<sup>4</sup>، وذلك بسبب أن هذا النوع من الأدلة أصبح غير مقتصر على إثبات الجريمة المعلوماتية فقط، بل أصبح بالإمكان الاعتماد عليه لإثبات الجريمة التقليدية نظراً للتطور الكبير الذي تشهد الجريمة.

---

<sup>1</sup> أحمد عبد اللاه هاللي، المرجع السابق، ص 748.

<sup>2</sup> المرجع نفسه، ص 748.

<sup>3</sup> علي حسن محمد الطويلة، المرجع السابق، ص 193.

<sup>4</sup> المرجع نفسه، ص 195.

## المبحث الثاني: سلطة القاضي في تقدير الأدلة الجنائية الرقمية

إن أعظم ما يقع على عاتق القاضي هو تقدير أدلة الإثبات والافتناع بها، وذلك حتى لا يدان بريء ولا يفلت مجرماً، فالقاضي قبل أن يصدر حكمه يقوم بالبحث عن الحقيقة، وهو في سبيل ذلك يقوم بفحص الأدلة الجنائية وي طرحها في الجلسة ليتناولها الخصوم بالفحص سعياً للوصول إلى الحقيقة التي ترضي ضميره، وتكون اقتناعه الشخصي لتحقيق العدالة.

وعليه فتختلف سلطة القاضي الجنائي في تقدير أدلة الإثبات من دولة إلى أخرى حسب ما تعتقه كل دولة من أنظمة الإثبات، ووفقاً لما كشفت عنه الدراسات التاريخية المقارنة في هذا المجال فإنه يوجد نظامين: نظام الإثبات المقيد (القانوني) ونظام الإثبات الحر.

وعلى هذا الأساس فمن الضروري لنا أن نتعرض لكلا النظامين لمعرفة مدى إعمال القاضي لسلطته التقديرية في تعامله مع هذا النوع من الأدلة، كما يجب علينا بيان موقف بعض التشريعات من الدليل الجنائي الرقمي، لذا سنتعرض في هذا المبحث للسلطة التقديرية للقاضي الجنائي في نظام الإثبات المقيد (القانوني) وذلك في المطلب الأول، وأما المطلب الثاني فخصصناه للسلطة التقديرية للقاضي الجنائي في نظام الإثبات الحر.

## المطلب الأول: السلطة التقديرية للقاضي الجنائي في نظام الإثبات المقيد (القانوني)

يعتبر نظام الإثبات المقيد (القانوني) من أقدم أنظمة الإثبات الجنائية، حيث كان الكهنة في العصور القديمة هم الذين يحددون طرق ووسائل الإثبات إلى أن وجدت الدولة بمفهومها الحديث فتولت هي بنفسها ذلك<sup>1</sup>، ومنه لبيان السلطة التقديرية للقاضي الجنائي في هذا النظام، وجب علينا التعرض إلى مفهومه، وبيان موقف بعض التشريعات – التي تتبنى نظام الإثبات المقيد (القانوني) – من الأدلة الجنائية الرقمية.

### الفرع الأول: مفهوم نظام الإثبات المقيد (القانوني)

سنتعرض في هذا الفرع إلى الأسس التي يقوم عليها نظام الإثبات المقيد (القانوني) بالإضافة إلى أبرز الانتقادات الموجهة له.

#### أولاً: الأسس التي يقوم عليها نظام الإثبات المقيد (القانوني)

يقوم نظام الإثبات المقيد (القانوني) على مبدئين رئيسيين وهما: مبدأ تحديد أدلة الإثبات، ومبدأ اقتناع المشرع بدلا من القاضي<sup>2</sup>، ومنه فالمشرع هو الذي يكون له الدور الرئيسي في الإثبات من خلال التحديد المسبق للأدلة، والقاضي في هذا الحالة يتقيد في حكمه بالبراءة أو بالإدانة بالأدلة التي حددها القانون، دون إعماله لاقتناعه الشخصي بصحة الأدلة المقدمة له إذ يقوم اقتناع المشرع محل اقتناع القاضي، وهكذا فإن اليقين القانوني يقوم أساسا على افتراض صحة الدليل بغض النظر عن حقيقة الواقع أو اختلاف ظروف الدعوى<sup>3</sup>.

<sup>1</sup> بوزيد أغليس، تلازم مبدأ الإثبات الحر بالاقتناع الذاتي للقاضي الجنائي (دراسة تحليلية مقارنة بين القانون الجزائري والقانون المصري وبعض القوانين العربية)، دار الهدى، الجزائر، 2010، ص 108.

<sup>2</sup> أحمد كوثر خالد، الإثبات الجنائي بالوسائل العلمية (دراسة تحليلية مقارنة)، الطبعة الأولى، مكتب التفسير للنشر والإعلان، العراق، 2007، ص 33.

<sup>3</sup> نصر الدين مروك، المرجع السابق، ص 56.

ومنه يظهر دور القاضي في هذا النظام كمطبق للقانون من حيث مراعاة توافر الدليل الجنائي وشروطه، بحيث إذا لم تتوفر هذه الشروط والشكليات التي يتطلبها القانون في الدليل، فإن القاضي لا يستطيع أن يحكم بالإدانة، ويصرف النظر عن اقتناعه الشخصي حتى ولو اقتنع بأن المتهم مدان في الجريمة المسندة إليه<sup>1</sup>.

### ثانياً: أهم الانتقادات الموجهة لنظام الإثبات المقيد (القانوني)

أعيب على نظام الإثبات المقيد (القانوني) بأنه أخرج القاضي من وظيفته الطبيعية والحقيقية، والمتمثلة في فحص الدليل وتقديره وإعمال اقتناعه الشخصي، وإقحام المشرع في هذه الأمور التي لا صلة له بها<sup>2</sup>، بالإضافة إلى أنه قام بتقنين اليقين في نصوص قانونية عامة ومحددة مسبقاً، رغم أن اليقين حالة لحظية مرتبطة بقاضي الموضوع لا بتقدير المشرع، كما أن هذا النظام أيضاً وضع القاضي في قالب جامد للإثبات، مما أدى إلى إفلات حالات كثيرة من العقاب<sup>3</sup>، وذلك من خلال تقاضي الجناة في الوقوع في هذه الطرق المحددة سلفاً ليفلتوا كلياً من المتابعة الجزائية، لأنهم مدركون أن القاضي مقيد لا تخرج سلطته في الإثبات عن تلك الوسائل<sup>4</sup>.

وعليه فبالرغم من هذه العيوب التي لحقت بهذا النظام إلا أنه مازال يطبق حتى الآن في بعض التشريعات الجنائية المقارنة ومنها التشريع الإنجليزي والأمريكي، بالإضافة إلى قيامهما بالتخفيف من حدة هذا النظام تماشياً مع التطور الحاصل في وسائل الإثبات.

<sup>1</sup> أحمد عبد اللاه هاللي، المرجع السابق، ص 726.

<sup>2</sup> نصر الدين مروي، المرجع السابق، ص 57.

<sup>3</sup> المرجع نفسه، ص 58.

<sup>4</sup> بوزيد أغليس، المرجع السابق، ص 108.

## الفرع الثاني: موقف التشريعات الآخذة بنظام الإثبات المقيد من الأدلة الجنائية الرقمية

تعتبر إنجلترا والولايات المتحدة الأمريكية من طليعة الدول التي تعتمد على نظام الإثبات المقيد (القانوني)، وبناء عليه سنتعرض في هذا الفرع لموقف كليهما إزاء الأدلة الجنائية الرقمية.

### أولاً: موقف التشريع الإنجليزي من الأدلة الجنائية الرقمية

تعتبر إنجلترا من بين أول الدول التي أصدرت قانوناً خاصاً بالحاسب الآلي، وهو قانون إساءة استخدام الحاسب الصادر في 1990/06/29، وهذا القانون في الحقيقة لم يتطرق لقواعد قبول الأدلة الناتجة عن أجهزة الحاسب الآلي، بسبب أن قانون البوليس والإثبات الجنائي الصادر في سنة 1984 والذي حل محل قانون الإثبات الجنائي لعام 1965، قد احتوى تنظيمياً محدداً لمسألة قبول الأدلة الجنائية الرقمية<sup>1</sup>.

وإذا نظرنا إلى قانون البوليس والإثبات الجنائي لوجدنا أن الأدلة الناتجة عن الحاسب الآلي لا تقبل كدليل إلا إذا استكملت اختبارات الثقة المنصوص عليها في المادة 69 من نفس القانون، بحيث أن عدم قبول هذا النوع من الأدلة راجع إلى إما وجود سبب معقول يدعو إلى الاعتقاد بأن هذا الدليل غير دقيق أو أن بياناته غير سليمة، وإما أن الحاسب الآلي الذي استخرج منه الدليل الجنائي الرقمي لا يعمل بكفاءة وبصورة سليمة، وقد اقترح بعض الفقهاء بإضافة حالة ثالثة وهي حالة استخدام جهاز الحاسب الآلي بشكل غير مصرح به<sup>2</sup>، وبالتالي عدم قبول الأدلة الناتجة عن هذا الاستعمال.

<sup>1</sup> أحمد عبد اللاه هلال، المرجع السابق، ص 727.

<sup>2</sup> المرجع نفسه، ص 728.

وزيادة على ما سبق ذكره، حددت إنجلترا قواعد أخرى خاصة بمقبولية الأدلة الجنائية الرقمية أمام القضاء، واعتبرتها بمثابة مبادئ يجب مراعاتها من طرف الأجهزة المكلفة باستخلاص هذا النوع من الأدلة، وتتمثل في ألا يقوم الخبير المكلف بفحص الحاسب الآلي بأي تغيير في البيانات الموجودة في الجهاز، وإذا اضطر الخبير للدخول في البيانات أو إجراء تغيير بسيط يجب أن يقدم تفسيراً مقنعاً لهذا التغيير<sup>1</sup>.

كما يجب تسجيل وتوثيق كل الخطوات التي قام بها الخبير في عملية جمع وتحليل الأدلة، وإخضاعها للاختبار للتحقق من مصداقية النتائج المتحصل عليها من طرف الخبير، ومنه فإن عدم احترام هذه الشروط يؤدي إلى استبعادها مباشرة من طرف القاضي ولو اقتنع بأن المتهم مدان.

### ثانياً: موقف التشريع الأمريكي من الأدلة الجنائية الرقمية

وبالنسبة للولايات المتحدة الأمريكية فقد تناولت بعض القوانين مسألة قبول الأدلة الجنائية الرقمية، ومن ذلك على سبيل المثال ما نص عليه قانون الحاسب الآلي الصادر في سنة 1984 في ولاية آيوا، وذلك بأن الأدلة الناتجة عن الحاسب الآلي تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه<sup>2</sup>، وأيضاً ما احتوى عليه قانون الإثبات الصادر في سنة 1983 في ولاية كاليفورنيا، وذلك بأن النسخ المستخرجة من البيانات التي يحتويها جهاز الحاسب الآلي تكون مقبولة بوصفها أفضل وأنسب الأدلة المتاحة لإثبات هذه البيانات<sup>3</sup>.

<sup>1</sup> Association of Chief Police Officers (of England, Wales, Northern Ireland), **Good Practice for Computer Based Electronic Evidence**, Version 5, October 2011, p 6.

<sup>2</sup> علي حسن محمد الطوالة، المرجع السابق، ص 197.

<sup>3</sup> المرجع نفسه، ص 197.

وتشترط المحاكم في الولايات المتحدة الأمريكية لقبول الأدلة الجنائية الرقمية بصفة عامة أن يكون جهاز الحاسب الآلي يؤدي وظائفه بصورة سليمة<sup>1</sup>، وأيضاً أن يكون الدليل الرقمي المستخلص ذو صلة وطيدة بالقضية المعروضة أمامها، وأن يكون هناك ارتباط بين الواقعة والأشخاص المشتبه فيهم<sup>2</sup>، بالإضافة إلى أن يكون محل ثقة ومعتمد كشرط لقبوله<sup>3</sup>. وعليه يقوم القضاء بتحديد درجة مصداقية وفاعلية هذا الدليل عن طريق إخضاعه لاختبار "داوبورت"، والذي هو عبارة عن اختبار قانوني لتقرير صلاحية الدليل العلمي وصلته بالواقعة الإجرامية، ونشأ هذا الاختبار بموجب قرار المحكمة العليا في الولايات المتحدة الأمريكية، والتي أصدرته في قضية "داوبورت" ضد "ميريل دو للصناعات الدوائية" في سنة 1993<sup>4</sup>.

وبناء على هذا الاختبار تنحصر مسؤولية القاضي أثناء الجلسة في تحديد سلامة المنهجية المتبعة والطرق الفنية المتخذة في استخلاص الأدلة الجنائية الرقمية<sup>5</sup>، وذلك من خلال استخدام أربعة معايير أساسية، يتمثل المعيار الأول (التجربة والاختبار) في التحقق من أنه سبق وأن تم تجربة الطريقة المتبعة في استخلاص الدليل الجنائي الرقمي والحصول على نفس النتائج عند المقارنة، وأما المعيار الثاني (نسبة الخطأ) يتمثل في التحقق من إمكانية وجود نسبة خطأ محتملة ترافق استخدام طريقة الاستخلاص والتحليل، وبالنسبة للمعيار الثالث (النشر) فهو يتعلق بنشر الطريقة المتبعة في استخلاص الدليل ومراجعتها من قبل المختصين في هذا المجال، وأخيراً يتمثل المعيار الرابع (القبول) بقبول طريقة الاستخلاص

---

<sup>1</sup> أحمد عبد اللاه هاللي، المرجع السابق، ص 729.

<sup>2</sup> Peter Sommer, **Digital Evidence, Digital Investigation and E-Disclosure (A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers)**, Third Edition, Information Assurance Advisory Council (I.A.A.C), United Kingdom, 2011, p 30.

<sup>3</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 130.

<sup>4</sup> Steve Bunting and William Wei, Op.Cit., p 500 – 501.

<sup>5</sup> ممدوح عبد الحميد عبد المطلب، المرجع نفسه، ص 130.

من قبل المختصين المنتسبين للمجموعات العلمية والمتخصصة في وضع أنسب الوسائل والأساليب الواجب استخدامها في استخلاص الأدلة الجنائية الرقمية<sup>1</sup>.

وتجدر الإشارة أنه قبل ظهور اختبار "داوبورت" كانت محاكم الولايات المتحدة الأمريكية تتبنى اختبار "فراي" في تقرير صلاحية الدليل العلمي بصفة عامة، والذي صدر بموجب قرار المحكمة العليا للولايات المتحدة الأمريكية في سنة 1923، وكان اختبار "فراي" مقتصرًا فقط على معيارين وهما التجربة والاختبار بالإضافة إلى معيار القبول<sup>2</sup>، إلا أنه قد ثبت عجزه في مواجهة أنواع جديدة من الأدلة العلمية والتي من بينها الأدلة الجنائية الرقمية، مما تحتم على الخبراء والمختصين في إيجاد معايير أخرى تتماشى مع تطور الأدلة الجنائية<sup>3</sup>.

لذا وفي حالة عدم توفر هذه الشروط التي قررها القانون، يقوم القاضي باستبعاد الدليل الجنائي الرقمي مباشرة، بسبب أن دور القاضي في هذا النظام سلبي يقتصر فقط على مراعاة توفر الشروط القانونية المتطلبة في الدليل الجنائي التي حددها المشرع.

---

<sup>1</sup> ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 131.

<sup>2</sup> Linda Volonino and Reynaldo Anazaldua, Op.Cit., p 83.

<sup>3</sup> Ibid., p 83.

## المطلب الثاني: السلطة التقديرية للقاضي الجنائي في نظام الإثبات الحر

ظهر نظام الإثبات الحر كبديل لنظام الإثبات المقيد (القانوني) انطلاقاً من الانتقادات التي وجهت إلى هذا الأخير، باعتباره نظام يتميز بالصرامة في عملية الإثبات الجنائي، لذا تحتم على الفقهاء إيجاد نظام آخر أكثر مرونة تماشياً مع التطور الحاصل في أدلة الإثبات الجنائية، لذا ولبين السلطة التقديرية للقاضي الجنائي في هذا النظام، وجب علينا التعرض إلى مفهومه، وبيان موقف بعض التشريعات – التي تتبنى نظام الإثبات الحر – من الأدلة الجنائية الرقمية.

### الفرع الأول: مفهوم نظام الإثبات الحر

سنعرض في هذا الفرع إلى الأسس التي يقوم عليها نظام الإثبات الحر بالإضافة إلى أبرز الانتقادات الموجهة له.

#### أولاً: الأسس التي يقوم عليها نظام الإثبات الحر

يقوم نظام الإثبات الحر على مبدئين رئيسيين وهما: مبدأ إطلاق أدلة الإثبات، ومبدأ الاقتناع الشخصي للقاضي<sup>1</sup>، ويتمثل مبدأ إطلاق أدلة الإثبات في قبول جميع الأدلة في الإثبات وحظر فرض أدلة معينة<sup>2</sup>، فالنيابة العامة التي تمثل سلطة الاتهام يكون لها إثبات التهمة بكل طرق الإثبات، وللمتهم أيضاً أن يدفع عن نفسه إسناد الفعل المجرم بكل طرق الإثبات، وأما القاضي له كل الحرية في إجراء التحقيق والبحث في الأدلة المقدمة له من أطراف الدعوى العمومية في الجلسة، وذلك حتى يستقر يقينه وعقيدته<sup>3</sup>.

<sup>1</sup> أحمد كوثر خالد، المرجع السابق، ص 32.

<sup>2</sup> معتصم خميس مشعشع، المرجع السابق، ص 29.

<sup>3</sup> نصر الدين مروك، المرجع السابق، ص 61.

لذا وبناء على هذه القاعدة، فالقانون لا يرسم طرقاً محددة للإثبات يقيد بها القاضي الجنائي، بل يترك حرية الإثبات لجميع أطراف الدعوى العمومية في أن يقدموا ما يرون أنه مناسب لاقتناع القاضي<sup>1</sup>.

وأما فيما يخص مبدأ الاقتناع الشخصي، فالقاضي حر في تكوين عقيدته دون أن يكون عليه أي رقيب إلا ضميره، أو أن يطالب ببيان سبب اقتناعه بدليل دون آخر<sup>2</sup>، مرتكزا في ذلك على قبوله لجميع الأدلة المطروحة أمامه في الجلسة، ولا يحظر أو يفرض عليه أي دليل محدد، ولا يتقيد إلا بقيد مشروعية الدليل وأنه قد تم طرحه للمناقشة بالجلسة، زيادة على ذلك قيامه بوزن كل دليل على حدى والتنسيق بينها، وله أن يهدر أي دليل مهما كانت قيمته طالما أنه لم يطمئن إليه<sup>3</sup>.

#### ثانياً: القيود الواردة على الاقتناع الشخصي للقاضي

بالرغم من الحرية الكبيرة التي يتمتع بها القاضي في نظام الإثبات الحر، إلا أن هذه الحرية ليست مطلقة بل تخضع لقيود خاصة حرصت أغلب التشريعات الأخذ بها النظام على النص عليها في تقنيناتها الإجرائية.

وتتمثل هذه القيود في أن يبني القاضي اقتناعه على الجرم واليقين لا على الظن والترجيح، وهنا لا نقصد بالجرم واليقين المطلقين، وإنما يكفي أن يكون كلا المفهومين نسبيين، انطلاقاً من ضرورة أن تبنى عقيدة القاضي على أساس احتمالات ذات درجة عالية من الثقة<sup>4</sup>.

<sup>1</sup> أحمد عبد اللاه هلالى، المرجع السابق، ص 718.

<sup>2</sup> نصر الدين مروك، المرجع السابق، ص 61.

<sup>3</sup> نعيم سعيداني، المرجع السابق، ص 228.

<sup>4</sup> نصر الدين مروك، المرجع نفسه، ص 645.

زيادة على ذلك وجوب طرح الأدلة بالجلسة لمناقشتها والتحقق منها، وهو ما رأيناه سابقا في مبدأ مناقشة الأدلة الجنائية الرقمية، وذلك أنه لا يجوز للقاضي أن يبني اقتناعه إلا على الأدلة التي طرحت أمامه بالجلسة وخضعت لمناقشة جميع أطراف الدعوى العمومية، ويترتب على هذا القيد عدم جواز أن يحكم القاضي بناء على معلوماته الشخصية أو بناء على رأي الغير.

ومن جهة أخرى يجب على القاضي أن يذكر مضمون هذه الأدلة ومآلها في الحكم بيانا كافيا، بحيث لا يكفي مجرد الإشارة إليها فقط، كما يجب أن لا تكون الأدلة التي يستند عليها القاضي في تقرير حكم البراءة أو الإدانة متناقضة ينفي بعضها البعض الآخر<sup>1</sup>.

### ثالثا: أهم الانتقادات الموجهة لنظام الإثبات الحر

بالرغم من المزايا التي يتصف بها نظام الإثبات الحر، إلا أنه أعيب عليه بأنه أفقد القاضي حياده، وذلك بالسماح له بالبحث عن الحقيقة بأي طريقة متاحة، مما يؤدي إلى إمكانية اللجوء لبعض الوسائل التي تؤدي لانتهاك حرية المتهم دون النظر إلى مصلحته أو حقه في الدفاع، خاصة أن إجراءات البحث والتحري ليس لها صفة الأعمال القضائية بل تتصف بالبوليسية، مما يجعل الأدلة التي يتم جمعها في هذه المرحلة محل شك وريبة<sup>2</sup>.

زيادة على ذلك إمكانية تأثر ضمير القاضي ببعض العوامل والبواعث المختلفة حينما يكون بصدد تحليل وتقييم الوقائع والأدلة الناتجة عنها من أجل الوصول إلى الاقتناع الذي سيبنى عليه حكمه، ويزداد خطر هذا التأثير خصوصا إذا تعلق الأمر بوقائع الإجرامية تؤدي إلى عقوبات شديدة كعقوبة الإعدام أو السجن المؤبد، وهو ما يشكل تهديدا وخطرا على الحريات الفردية، ويتحتم على المشرع تقييده دائما لتجنب انحراف القاضي.

<sup>1</sup> نصر الدين مروك، المرجع السابق، ص 646.

<sup>2</sup> المرجع نفسه، ص 63.

## الفرع الثاني: موقف التشريعات الآخذة بنظام الإثبات الحر من الأدلة الجنائية الرقمية

بعد بيان مفهوم نظام الإثبات الحر والأسس التي يقوم عليها، ووصولنا إلى أن هذا النظام قد أعطى للقاضي الحرية في تقدير الأدلة الجنائية (بضوابط)، يتوجب علينا إذن معرفة موقف التشريعات الآخذة بهذا النظام من الأدلة الجنائية الرقمية، ومن بين هذه التشريعات سنتعرض لموقف التشريعين الفرنسي والجزائري.

### أولاً: موقف التشريع الفرنسي من الأدلة الجنائية الرقمية

يعتبر التشريع الفرنسي من أوائل التشريعات التي تبنت نظام الإثبات الحر، وذلك طبقاً لما جاء في نص المادة 427 من قانون الإجراءات الجزائية الفرنسي بحيث نصت على أنه: "يجوز إثبات الجرائم بكل طرق الإثبات ما لم ينص القانون على خلاف ذلك، ويحكم القاضي وفقاً لاقتناعه الشخصي..."، وأيضاً نصت عليه المادة 304 من نفس القانون على أن: "...يقسم المحلفون على أن يصدرُوا قراراتهم طبقاً لضمائرهم واقتناعهم الشخصي..."، ومنه فمبدأ الاقتناع الشخصي للقاضي يمتد ليشمل جميع الجهات القضائية الجزائية (محكمة الجناح والمخالفات ومحكمة الجنايات)، كما يشمل أيضاً جميع مراحل الدعوى العمومية<sup>1</sup>.

وبالحديث عن موقف المشرع الفرنسي من الأدلة الجنائية الرقمية، يمكن القول أن هذا النوع من الأدلة لا يثير أي صعوبة ما دام المشرع يتبنى نظام الإثبات الحر، سواء تعلق الأمر بمدى حرية تقديم هذه الأدلة لإثبات الجريمة المعلوماتية، أو بمدى حرية القاضي في تقديرها<sup>2</sup>، وهو عكس التشريعات التي تتبنى نظام الإثبات المقيد (القانوني) مثل إنجلترا، والتي ألزمت باحترام طرق تقديم الدليل الجنائي الرقمي وإخضاعه لاختبارات الثقة<sup>3</sup>.

<sup>1</sup> أحمد عبد اللاه هلال، المرجع السابق، ص 721.

<sup>2</sup> المرجع نفسه، ص 721.

<sup>3</sup> Peter Sommer, Op.Cit., p 80.

بالإضافة إلى أن الفقهاء الفرنسيين يدرسون مسألة قبول الأدلة الجنائية الرقمية أمام القضاء الجنائي ضمن مجال أوسع وهو مسألة قبول الأدلة الناتجة عن الأجهزة الإلكترونية الأخرى غير أجهزة الحاسب الآلي، مثل الأدلة الناتجة عن أجهزة التصوير، وكاميرات المراقبة، والرادارات، وأجهزة تسجيل الأصوات وغيرها، وبالتالي فقد قضت محكمة النقض الفرنسية في قرار صادر بتاريخ 1987/04/28 أن أشرطة التسجيل الممغنطة التي يكون لها قيمة في الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي، ومنه فالتسجيل الصوتي إلكترونيًا بواسطة أجهزة خاصة بذلك، لا يحتمل الخطأ ويصعب التلاعب به، ويمكن للخبراء الفنيين أن يكتشفوا أي تلاعب أو محاولة إتلافه بواسطة وسائل تقنية عالية الكفاءة<sup>1</sup>.

كذلك الأدلة الناتجة عن أجهزة الحاسب الآلي، فأي محاولة لإتلاف الدليل الجنائي الرقمي أو إزالته يسجل أيضًا كدليل ضده، وهي من بين أهم المميزات التي تتمتع بها مقارنة بالأدلة المادية (التقليدية)<sup>2</sup>.

ومنه يتبين لنا أن المشرع الفرنسي قد اعتمد على هذه الأدلة – والتي من بينها الأدلة الجنائية الرقمية – إدراكًا منه على قطعية نتائجها، لكن بشرط خضوعها لجملة من الشروط أهمها أن يتم الحصول عليها بطريقة مشروعة ونزيهة، وأن يتم مناقشتها حضورًا من لدن جميع أطراف الدعوى العمومية<sup>3</sup>.

<sup>1</sup> علي حسن محمد الطوالة، المرجع السابق، ص 199.

<sup>2</sup> عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص 15.

<sup>3</sup> أحمد عبد اللاه هلال، المرجع السابق، ص 722.

## ثانياً: موقف التشريع الجزائري من الأدلة الجنائية الرقمية

قبل بيان موقف المشرع الجزائري من الأدلة الجنائية الرقمية، يمكن القول بعد استقراء نصوص قانون الإجراءات الجزائرية أن المشرع الجزائري قد أخذ بنظام الإثبات الحر شأنه كشأن المشرع الفرنسي، وذلك من خلال تكريس مبدأ الاقتناع الشخصي للقاضي<sup>1</sup>، وقد نصت المادة 212 من قانون الإجراءات الجزائرية على أنه: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص..."، كما نصت أيضا المادة 307 من نفس القانون على نفس المبدأ بقولها: "...إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها ولم يضع لها القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم، هل لديكم اقتناع شخصي؟".

والملاحظ على نص المادة 212 من قانون الإجراءات الجزائرية بأنها أوردت استثناء بعدم جواز إثبات بعض الجرائم بأي طريق من طرق الإثبات، وهذا يعني أن المشرع في هذه الحالة قد أخذ بنظام الإثبات المقيد (القانوني) استثناء في بعض الجرائم المحددة حصرا بموجب القانون، ومثال ذلك جريمة الزنا التي نصت عليها المادة 339 من قانون العقوبات، والتي حددت المادة 341 من نفس القانون الأدلة المثبتة لها على سبيل الحصر<sup>2</sup>.

<sup>1</sup> بوزيد أغليس، المرجع السابق، ص 110.

<sup>2</sup> نصت المادة 341 من قانون العقوبات على أن: "الدليل الذي يقبل عن ارتكاب الجريمة المعاقب عليها بالمادة 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".

لذا وبالرجوع إلى موقف المشرع الجزائري من الأدلة الجنائية الرقمية، وانطلاقاً من نص المادة 212 من قانون الإجراءات الجزائية، والتي أجاز فيها المشرع إثبات الجرائم بأي طريق من طرق الإثبات، ومنح من خلالها للقاضي الحرية في تقدير الدليل بناء على اقتناعه الشخصي، يمكن القول أن المشرع سلك ما سلكه المشرع الفرنسي من خلال اعتبار الدليل الجنائي الرقمي مثل باقي الأدلة الجنائية الأخرى، وأن السلطة التقديرية التي يتمتع بها القاضي تمتد لتشمل جميع الأدلة الجنائية بما فيها الأدلة الرقمية<sup>1</sup>، وبالتالي فإن هذا النوع من الأدلة أيضاً لا يثير إشكالا بالنسبة للمشرع الجزائري ما دام يعتنق حرية الإثبات، والقاضي مطالب فقط باحترام القواعد العامة المتعلقة بقبول الأدلة الجنائية أمام القضاء، التي قد تأخذ شكل محاضر على إثر القيام بإجراء التفتيش أو اعتراض المراسلات مثلاً، أو تأخذ أيضاً شكل تقرير خبرة فنية بمناسبة معاينة أو فحص وتحليل الأدلة الجنائية الرقمية الناتجة عن أجهزة الحاسب الآلي وملحقاته<sup>2</sup>.

وعليه فإذا تعلق الأمر بالمحاضر فالمشرع الجزائري اعتبرها كقاعدة عامة مجرد استدلالات ما لم ينص القانون على خلاف ذلك وهو ما أورده المادة 215 من قانون الإجراءات الجزائية بقولها: "لا تعتبر المحاضر والتقارير المثبتة للجنايات أو الجرح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك"، كما نصت أيضاً المادة 214 من نفس القانون على أنه: "لا يكون للمحاضر أو التقرير قوة الإثبات إلا إذا كان صحيحاً في الشكل ويكون قد حرره واضعه أثناء مباشرة أعمال وظيفته وأورد فيه عن موضوع داخل في نطاق اختصاصه ما قد رآه أو سمعه أو عاينه بنفسه".

<sup>1</sup> نعيم سعيداني، المرجع السابق، ص 228 - 229.

<sup>2</sup> المرجع نفسه، ص 229.

إلا أن المحاضر التي يخول القانون فيها لضباط الشرطة القضائية إعدادها بنص خاص لإثبات جنحة معينة، فإن هذه المحاضر تتميز بحجية ما لم يدحضها دليل عكسي وذلك وفقا لما نصت عليه المادة 216 من نفس القانون بحيث جاء فيها: "في الأحوال التي يخول القانون فيها بنص خاص لضباط الشرطة القضائية أو أعوانهم أو للموظفين وأعوانهم الموكلة إليهم بعض مهام الضبط القضائي سلطة إثبات جنح في محاضر أو تقارير، تكون لهذه المحاضر أو التقارير حجيتها ما لم يدحضها دليل عكسي بالكتابة أو شهادة شهود".

وأما بالنسبة لتقارير الخبرة الفنية فإن المشرع الجزائري اعتبرها كذلك مثل باقي أدلة الإثبات من خلال خضوعها للسلطة التقديرية للقاضي، وهو ما أكدته المادة 215 المذكورة أعلاه، لكن الطبيعة العلمية والتقنية للجريمة المعلوماتية غالبا ما تفرض على القاضي الاستناد عليها في تكوين اقتناعه الشخصي والتقيد بما توصل إليه الخبير<sup>1</sup>، بناء على أن القاضي لا يمكنه إدراك المبادئ العلمية للدلائل الجنائي الرقمي بالرغم من تكوينه القانوني<sup>2</sup>.

وعليه نصل في الأخير ولبيان سلطة القاضي في تقدير الأدلة الجنائية الرقمية يجب التمييز بين أمرين، الأمر الأول يتمثل في القيمة القاطعة للدليل، والأمر الثاني الظروف والملابسات التي وجد فيها هذا الدليل<sup>3</sup>، ومنه فتقدير القاضي لا يتناول الأمر الأول، وذلك لأن قيمة الدليل تقوم على أسس علمية دقيقة، ولا حرية للقاضي في مناقشة الحقائق العلمية الثابتة، وأما الظروف والملابسات التي وجد فيها هذا الدليل وأحاطت به، فإنها تدخل في نطاق تقديره الشخصي.

<sup>1</sup> نعيم سعيداني، المرجع السابق، ص 230.

<sup>2</sup> خالد عياد الحلبي، المرجع السابق، ص 247.

<sup>3</sup> أحمد عبد اللاه هلال، المرجع السابق، ص 724.

لذا فالاعتماد على الأدلة الجنائية الرقمية والتعامل معها من طرف الهيئات القضائية الجزائرية لا تثير أي إشكال قانوني مادام التشريعين الجزائري والفرنسي يتبنيان نظام الإثبات الحر، ومن جهة أخرى لا تثير أي إشكال تقني بسبب وضوح الأدلة الجنائية الرقمية ودقتها في الإثبات، زيادة على ذلك إمكانية تعقبها واستخلاصها والوصول إلى مصادرها بدقة، نظرا لقيامها على نظريات حسابية مؤكدة لا يشوبها أي شك، وهو ما يقوي من يقينيتها في الإثبات<sup>1</sup>.

---

<sup>1</sup> محمد الأمين البشري، التحقيق في الجرائم المستحدثة، المرجع السابق، ص 251.

## خاتمة

إن دراسة موضوع الإثبات الجنائي بالأدلة الرقمية كان الهدف الأساسي منه هو معرفة مدى حجيتها في مجال الإثبات الجنائي انطلاقاً من التشريعين الجزائري والفرنسي، على اعتبار أن هذا النوع من الأدلة لا يقتصر فقط على إثبات الجريمة المعلوماتية فحسب، بل يمكن لها أيضاً إثبات الجريمة التقليدية.

ومن خلال ما تقدم عرضه نخلص إلى أن الدليل الجنائي الرقمي هو الدليل المستخلص من أجهزة الحاسب الآلي وملحقاته، أو من شبكة الإنترنت، أو أي جهاز آخر له خاصية المعالجة أو تخزين المعلومات، وهو في الحقيقة عبارة عن مجالات أو نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة، لتشكل لنا معلومات أو بيانات مختلفة، يمكن الاعتماد عليها في مرحلة التحقيق والمحاكمة.

كما أن الدليل الجنائي الرقمي يتميز عن باقي الأدلة الجنائية الأخرى بأنه دليل علمي ذو طبيعة تقنية، وذلك من خلال أن استخلاصه وتحليله يتطلب طرقاً وأساليب غير تقليدية قائمة على علوم الحاسب الآلي وقوانينه، كما أنه ذو طبيعة ثنائية لأن المعلومات والبيانات المستخلصة من أجهزة الحاسب الآلي أو من شبكاته، هي في الأصل تحمل شكلاً رقمياً (0 و1)، زيادة على ذلك أيضاً أنه دليل متنوع ومتطور، فهو يشمل جميع المعلومات والبيانات المخزنة أو المعالجة بواسطة الحاسب الآلي أو ملحقاته أو حتى المتداولة في شبكة الإنترنت.

ومن جهة أخرى، وإدراكا من المشرع الجزائري لأهمية هذا النوع من الأدلة، فقد عمل على استحداث قواعد إجرائية جديدة تتماشى مع خصوصية الجريمة المعلوماتية وأدلتها أسوة بما عمل به المشرع الفرنسي، وانطلاقا من عجز القواعد الإجرائية التقليدية في التعامل مع الأدلة الجنائية الرقمية.

وعلى هذا الأساس يمكن القول أنه مهما علت القيمة العلمية والفنية للدليل الجنائي الرقمي في الإثبات، إلا أنه يجب أن يتمتع القاضي بالسلطة التقديرية، لأن هذه الأخيرة تكون لازمة لكي تجعل من الحقيقة العلمية حقيقة قضائية.

وعليه من خلال دراستنا لهذا الموضوع توصلنا إلى النتائج التالية:

**1) أن التشريعين الفرنسي والجزائري لم يعرفا الدليل الجنائي الرقمي، وذلك بسبب أنهما يعتمدان على نظام الإثبات الحر الذي لا يفرض على القاضي الاعتماد على أدلة جنائية معينة، زيادة على ذلك أنهما يعتبران هذا النوع من الأدلة مثلها مثل باقي الأدلة الجنائية الأخرى.**

**2) لاستخلاص الأدلة الجنائية الرقمية وتحليلها يتطلب ذلك أساليب وطرق غير تقليدية، وهو ما دفع بالمشرع الجزائري إلى استحداث قواعد قانونية خاصة بهذا الشأن أسوة بالمشرع الفرنسي، وكان ذلك من خلال سن القانون رقم 06-22 المؤرخ في 2006/12/20 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية الجزائري، والذي أتى بإجراء اعتراض المراسلات والتسرب، وكذلك القانون رقم 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والذي نص أيضا على إجراء المراقبة الإلكترونية وكذلك تفتيش أنظمة الحاسب الآلي وضبط الأدلة الناتجة عنها.**

**3** هناك صعوبة تكتنف الدليل الجنائي الرقمي سواء من حيث طرق الحصول عليه أو من حيث طبيعته، فالحصول عليه قد يحتاج إلى القيام بعمليات فنية وعلمية معقدة، كما وأن طبيعته غير المادية تسهل لمرتكبي الجريمة المعلوماتية إخفائه وإتلافه أو حتى تشفيره لحيلولة دون الوصول إليه.

**4** لكي يكون للأدلة الجنائية الرقمية حجية في مجال الإثبات الجنائي، يجب أن يكون قد تم الحصول عليه بطريقة مشروعة، وذلك من خلال احترام جميع الشروط القانونية المتعلقة بإجراءات التحقيق المتخذة في سبيل استخلاص الأدلة الجنائية الرقمية (مثل الشروط المتعلقة بالتفتيش أو اعتراض المراسلات أو المراقبة الإلكترونية)، زيادة على ذلك يجب أن تكون هذه الأدلة غير قابلة للشك أي يقينية، كما يجب أيضا أن يتم طرحها للمناقشة أمام جميع أطراف الدعوى العمومية، وعدم احترام هذه الشروط يؤدي إلى بطلان الأدلة الناتجة عنها، وعدم جواز الأخذ بها في إثبات الجريمة المعلوماتية.

**5** إذا كانت السلطة التقديرية للقاضي الجزائي في التشريعات الآخذة بنظام الإثبات الحر (مثل التشريع الجزائري والفرنسي) لا تتناول القيمة العلمية القاطعة للدليل الجنائي الرقمي، فإنها يمكنها أن تناقش الظروف والملابسات التي وجد فيها هذا الدليل، وذلك على خلاف التشريعات الآخذة بنظام الإثبات المقيد (القانوني) حيث يقوم المشرع بالدور الإيجابي في عملية الإثبات، من خلال تنظيمه لقواعد قبول الأدلة الجنائية الرقمية، وينحصر دور القاضي في هذا النظام في مراعاة توفر الأدلة وشروطها القانونية.

وبعد أن تعرضنا لأبرز النتائج التي توصلنا إليها، نوصي بـ:

- (1) **العمل على تحديث القواعد القانونية الإجرائية** لكي تتماشى مع خاصية تطور الجريمة المعلوماتية ووسائل إثباتها، والاعتماد عليها حتى في إثبات الجريمة التقليدية.
- (2) **عند القيام بإجراء المعاينة أو التفتيش داخل أنظمة الحاسب الآلي** يجب على الخبراء الفنيين والمتخصصين **باحترام جميع قواعد السلامة المتعلقة بالحفاظ على الأدلة الجنائية الرقمية**، وذلك من خلال إثبات الحالة التي تكون عليها توصيلات الحاسب الآلي وملحقاته عن طريق التصوير، و**تعطيل** كافة الاتصالات السلكية اللاسلكية الموصولة بجهاز الحاسب الآلي لمنع تخريب الأدلة الموجودة أو محوها.
- (3) **الاهتمام بالخبرة العلمية** لما لها من دور فعال في مجال الإثبات الجنائي، وذلك من خلال الاعتراف بقيمتها في الإثبات دون إخراجها من دائرة السلطة التقديرية للقاضي.
- (4) **في إطار نية الجزائر الاعتماد على بروتوكول الاتصال بشبكة الإنترنت** ذو الإصدار السادس IPv6، والتخلي عن العمل بالإصدار الرابع IPv4، **نوصي بتعزيز الحماية الأمنية لعنوان IP من التزييف أو العبث**، باعتبارها أداة مهمة في الإثبات.
- (5) **تحقيق التعاون والتنسيق بين جهاز العدالة والشركات المزودة لخدمة الاتصالات السلكية واللاسلكية وشبكة الإنترنت**، وذلك بتقديم جميع المعلومات التي تفيد في التحقيق.
- (6) **العمل على تكوين القضاة والخبراء الفنيين وإرسالهم إلى دورات فنية متخصصة** في مجال التعامل مع الأدلة الجنائية الرقمية.

7) تعزيز التعاون مع البلدان الأخرى وأخذ الخبرات عنها سواء في مجال إعداد الخبراء المتخصصين أو في مجال البحث والتحري، ونذكر منها إنجلترا والولايات المتحدة الأمريكية وفرنسا، وبالنسبة للدول العربية نجد دولة الإمارات العربية المتحدة التي قطعت أشواطاً كبيرة في مجال الاعتماد على الأدلة الجنائية الرقمية في الإثبات الجنائي.

8) إدراج موضوع الأدلة العلمية في المقررات الدراسية سواء في الجامعات أو في معاهد التكوين الخاصة بالقضاة والمحامين لإزالة الغموض الذي يكتنف هذه الأدلة وحجبتها في الإثبات الجنائي.

وفي ختام هذا البحث لا يسعني سوى القول إن أصبت فمن الله وذلك فضل الله يؤتيه من يشاء من عباده والله ذو الفضل العظيم ، وإن أخطأت فمني وأتحمّل وحدي عواقبه، وأسأل الله سبحانه وتعالى أن يديم علينا نعمة الإيمان والتوفيق.

## قائمة المراجع

أولاً: باللغة العربية

### 1- الكتب

#### أ- الكتب العامة

- إبراهيم بلعليات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، 2012.
- أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، الجزء الأول، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، السعودية، 1993.
- بوزيد أغليس، تلازم مبدأ الإثبات الحر بالافتناع الذاتي للقاضي الجزائري (دراسة تحليلية مقارنة بين القانون الجزائري والقانون المصري وبعض القوانين العربية)، دار الهدى، الجزائر، 2010.
- عبد الله أوهابية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، الطبعة الرابعة، دار هومة، الجزائر، 2013.
- كمال محمد عواد، الضوابط الشرعية والقانونية للأدلة الجنائية (في الفقه الإسلامي والقانون الوضعي)، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011.
- محمد فاروق عبد الحميد كامل، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، السعودية، 1999.
- محمد محمد محمد عنب، معاينة مسرح الجريمة، الجزء الثاني، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، السعودية، 1991.
- نصر الدين مروك، محاضرات في الإثبات الجنائي (النظرية العامة للإثبات الجنائي)، الجزء الأول، دار هومة، الجزائر، 2003.

## ب- الكتب المتخصصة

- بكرى يوسف بكرى، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011.
- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011.
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009.
- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006.
- عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة)، جامعة نايف العربية للعلوم الأمنية، السعودية، 2007.
- علي حسن محمد الطوالة، التفتيش الجنائي على نظم الحاسوب والإنترنت (دراسة مقارنة)، الطبعة الأولى، عالم الكتب الحديث، الأردن، 2004.
- عمر محمد بن يونس، الدليل الرقمي (Digital Evidence)، (دون دار نشر)، مصر، 2006.
- محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، السعودية، 2004.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006.
- مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت (دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية)، دار الكتب القانونية، مصر، 2005.

- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، الطبعة الأولى، دار الفكر الجامعي، مصر، 2007.

## 2- المقالات والدراسات

- أحمد عبد اللاه هلال، "حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة)"، في بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2004، ص 429.
- أسامة بن غانم العبيدي، "التفتيش عن الدليل في الجرائم المعلوماتية"، المجلة العربية للدراسات الأمنية والتدريب، العدد 58، المجلد 29، أكاديمية نايف العربية للعلوم الأمنية، السعودية، (دون سنة النشر).
- حارث عاصم داود، "المخاطر الأمنية في بروتوكول الإنترنت الإصدار السادس IPv6"، المجلة العربية الدولية للمعلوماتية، العدد 4، المجلد 2، جامعة نايف العربية للعلوم الأمنية، السعودية، 2013.
- سوزان عدنان الأستاذ، "انتهاك حرمة الحياة الخاصة عبر الإنترنت (دراسة مقارنة)"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الثالث، المجلد 29، سوريا، 2013.
- فاطمة زهرة بوعناد، "مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانونية، العدد الأول، (دون دار نشر)، الجزائر، 2013.
- كاظم محمد عطيات ومحمد رضوان هلال، "كيفية التعامل التقني والأمن مع أوعية الجريمة الرقمية في مسرح الجريمة لضمان حيدة الدليل المستخلص"، المجلة العربية الدولية للمعلوماتية، العدد 5، المجلد 3، جامعة نايف العربية للعلوم الأمنية، السعودية، 2014.

• محمد الأمين بشرى، "الأدلة الجنائية الرقمية (مفهومها ودورها في الإثبات)"، **المجلة العربية للدراسات الأمنية والتدريب**، العدد 33، المجلد 17، أكاديمية نايف العربية للعلوم الأمنية، السعودية، 1995.

• معتصم خميس مشعشع، "إثبات الجريمة بالأدلة العلمية"، **مجلة الشريعة والقانون**، العدد 56، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2013.

• هشام محمد فريد رستم، "أصول التحقيق الجنائي الفني"، في **بحوث مؤتمر القانون والكمبيوتر والإنترنت**، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2004.

### 3- الرسائل الجامعية

• ثنيان ناصر آل ثنيان، **إثبات الجريمة الإلكترونية - دراسة تأصيلية تطبيقية -** ، (رسالة ماجستير)، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012.

• سليمان غازي العتيبي، **درجة توافر كفايات البحث عن الدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة**، (رسالة ماجستير)، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2010.

• سليمان مهجع العنزي، **وسائل التحقيق في جرائم نظم المعلومات**، (رسالة ماجستير)، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2003.

• نعيم سعيداني، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، (رسالة ماجستير)، جامعة الحاج لخضر - باتنة -، كلية الحقوق والعلوم السياسية، الجزائر، 2013.

### 4- النصوص القانونية

• القانون رقم 03-2000 المؤرخ في 05/08/2000 والمتضمن تحديد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الجريدة الرسمية رقم 48، الصادرة بتاريخ 06/08/2000.

- القانون رقم 06-22 المؤرخ في 20/12/2006، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية الجزائري، الجريدة الرسمية رقم 84، الصادرة بتاريخ 24/12/2006.
- القانون رقم 09-04 المؤرخ في 05/08/2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، الصادرة بتاريخ 16/08/2009.
- الأمر رقم 66-155 المؤرخ في 08/06/1966، المتضمن قانون الإجراءات الجزائية الجزائري، الجريدة الرسمية رقم 48، الصادرة بتاريخ 10/06/1966، المعدل والمتمم.
- الأمر رقم 66-156 المؤرخ في 08/06/1966، المتضمن قانون العقوبات، الجريدة الرسمية رقم 49، الصادرة بتاريخ 11/06/1966، المعدل والمتمم.
- المرسوم الرئاسي رقم 183-04 المؤرخ في 26/06/2004، المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية رقم 41، الصادرة بتاريخ 27/06/2004.
- المرسوم الرئاسي رقم 432-04 المؤرخ في 29/12/2004، المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية رقم 84، الصادرة بتاريخ 29/12/2004.
- قرار وزاري مشترك مؤرخ في 14/04/2007 والمتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية رقم 36، الصادرة بتاريخ 03/06/2007.

#### 5- المعاجم والقواميس

- محمد بن أبي بكر الرازي، مختار الصحاح، دار الرسالة، الكويت، 1983.
- المنجد الأبجدي، دار المشرق، لبنان، 1967.

### 1- Ouvrages

- Brian Carrier, **File System forensic Analysis**, Pearson Education (Inc), United states of America, 2005.
- Debra Littlejohn Shinder, **Scene of the Cyber Crime (Computer forensic Handbook)**, Publishing by Syngress (Inc), United states of America, 2002.
- Eoghan Casey, **Digital Evidence and Computer Crime**, Third Edition, Published by Elsevier Inc, London, 2011.
- Linda Volonino and Reynaldo Anazaldua, **Computer Forensics For Dummies**, Wiley Publishing, United States of America, 2008.
- Peter Sommer, **Digital Evidence, Digital Investigation and E-Disclosure (A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers)**, Third Edition, Information Assurance Advisory Council (I.A.A.C), United Kingdom, 2011.
- Steve Bunting and William Wei, **Encase Computer forensic**, Wiley Publishing (inc), United States of America, 2006.
- The Technical Working Group for Electronic Crime Scene Investigation, **Electronic Crime Scene Investigation**, the national institute of justice, the United States of America, 2001.

### 2- Articles et études

- Ankit Agarwal and others., "**Systematic Digital Forensic Investigation Model**", in: International Journal of Computer Science and Security (IJCSS), Volume 5, Issue 1, United states of America, 2011, p 119.

### 3- Sources documentaire

- Association of Chief Police Officers (of England, Wales, Northern Ireland ), **Good Practice for Computer Based Electronic Evidence**, Version 5, October 2011.

## الفهرس

أ-ث	مقدمة.....
01	الفصل الأول: ماهية الدليل الجنائي الرقمي.....
02	المبحث الأول: مفهوم الدليل الجنائي الرقمي.....
02	المطلب الأول: التعريف بالدليل الجنائي الرقمي.....
02	الفرع الأول: التعريف اللغوي.....
03	الفرع الثاني: التعريف الاصطلاحي.....
03	أولاً: التعريف الاصطلاحي بالدليل الجنائي.....
04	ثانياً: التعريف الاصطلاحي بالدليل الجنائي الرقمي.....
07	المطلب الثاني: خصائص الدليل الجنائي الرقمي.....
07	الفرع الأول: الدليل الجنائي الرقمي دليل علمي.....
08	الفرع الثاني: الدليل الجنائي الرقمي ذو طبيعة تقنية.....
09	الفرع الثالث: الدليل الجنائي الرقمي ذو طبيعة ثنائية.....
10	الفرع الرابع: الدليل الجنائي الرقمي متنوع ومتطور.....
11	المطلب الثالث: أنواع الدليل الجنائي الرقمي.....
11	الفرع الأول: الأدلة الجنائية الرقمية التي أعدت لتكون وسيلة إثبات.....
12	أولاً: المعلومات والبيانات المنشئة تلقائياً من طرف الحاسب الآلي.....
12	ثانياً: المعلومات والبيانات ذات الطبيعة المختلطة.....
12	الفرع الثاني: الأدلة الجنائية الرقمية التي لم تعد لتكون وسيلة إثبات.....
14	المبحث الثاني: استخلاص الدليل الجنائي الرقمي.....
14	المطلب الأول: الطرق الفنية الحديثة في جمع الأدلة الجنائية الرقمية.....
14	الفرع الأول: الوسائل المادية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية.....
15	أولاً: استخدام بروتوكول IP\TCP.....

16	ثانيا: استخدام معلومات الكوكيز Cookies.....
17	ثالثا: استخدام معلومات البروكسي Proxy.....
18	رابعا: استخدام برامج التتبع وكشف الاختراق.....
18	الفرع الثاني: الوسائل الإجرائية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية....
19	أولا: اعتراض المراسلات.....
19	(4) مفهوم عملية اعتراض المراسلات.....
20	(5) شروط القيام بعملية اعتراض المراسلات.....
21	(6) كيفية اعتراض المراسلات في الجريمة الإلكترونية.....
22	ثانيا: التسرب.....
22	(1) مفهوم التسرب.....
22	(2) شروط القيام بعملية التسرب.....
23	(3) كيفية التسرب في الجريمة المعلوماتية.....
23	ثالثا: المراقبة الإلكترونية.....
23	(1) مفهوم المراقبة الإلكترونية.....
24	(2) شروط القيام بعملية المراقبة الإلكترونية.....
25	المطلب الثاني: صلاحيات الإجراءات التقليدية في جمع الأدلة الجنائية الرقمية.....
25	الفرع الأول: التفتيش وضبط الأدلة الجنائية الرقمية.....
26	أولا: مدى خضوع أنظمة الحاسب الآلي للتفتيش.....
28	ثانيا: مدى خضوع شبكات الحاسب الآلي للتفتيش.....
30	ثالثا: مدى صلاحية ضبط الدليل الجنائي الرقمي.....

32	الفرع الثاني: المعاينة.....
32	أولاً: صلاحية المعاينة في كشف وضبط الدليل الجنائي الرقمي.....
33	ثانياً: إجراءات المعاينة في العالم الافتراضي.....
33	(1) الإجراءات والخطوات الفنية المتخذة قبل القيام بإجراء المعاينة.....
34	(2) الإجراءات والخطوات الفنية المتخذة أثناء القيام بالمعاينة.....
35	الفرع الثالث: الخبرة.....
35	أولاً: أهمية الخبرة في كشف وتحليل الدليل الجنائي الرقمي.....
36	ثانياً: الضوابط التي تحكم عمل الخبير في مجال الجريمة المعلوماتية.....
37	المطلب الثالث: الصعوبات المتعلقة باستخلاص الدليل الجنائي الرقمي.....
38	الفرع الأول: الصعوبات المتعلقة بالدليل الجنائي الرقمي.....
38	أولاً: الطبيعة غير المرئية للدليل الجنائي الرقمي.....
38	ثانياً: سهولة تدمير ومحو الدليل الجنائي الرقمي.....
39	ثالثاً: إعاقة الوصول إلى الدليل الجنائي الرقمي.....
39	رابعاً: ضخامة البيانات المتعين فحصها.....
40	الفرع الثاني: الصعوبات المتعلقة بجهات التحقيق.....
42	الفرع الثالث: الصعوبات التشريعية.....
44	الفصل الثاني: القيمة القانونية للدليل الجنائي الرقمي.....
45	المبحث الأول: شروط قبول الدليل الجنائي الرقمي أمام القضاء الجنائي.....
45	المطلب الأول: مشروعية الدليل الجنائي الرقمي.....
46	الفرع الأول: مشروعية وجود الدليل الجنائي الرقمي.....
46	أولاً: مشروعية وجود الدليل الجنائي الرقمي في نظام الإثبات المقيد (القانوني).....

47	ثانيا: مشروعية وجود الدليل الجنائي الرقمي في نظام الإثبات الحر.....
47	الفرع الثاني: مشروعية الحصول على الدليل الجنائي الرقمي.....
47	أولا: أسس مشروعية الحصول على الدليل الجنائي الرقمي.....
48	ثانيا: مشروعية الحصول على الدليل الجنائي الرقمي في التشريع الجزائري والفرنسي
51	المطلب الثاني: يقينية الدليل الجنائي الرقمي.....
51	الفرع الأول: مفهوم مبدأ يقينية الدليل الجنائي الرقمي.....
52	الفرع الثاني: القواعد التي تحكم مبدأ يقينية الأدلة الجنائية الرقمية.....
53	أولا: تقييم الدليل الجنائي الرقمي من حيث سلامته من العبث.....
54	ثانيا: تقييم الدليل الجنائي الرقمي من حيث السلامة الفنية لإجراءات استخلاصه.....
55	المطلب الثالث: مناقشة الأدلة الجنائية الرقمية.....
55	الفرع الأول: مفهوم مبدأ مناقشة الأدلة الجنائية.....
57	الفرع الثاني: مضمون مناقشة الأدلة الجنائية الرقمية.....
58	المبحث الثاني: سلطة القاضي في تقدير الأدلة الجنائية الرقمية.....
59	المطلب الأول: السلطة التقديرية للقاضي الجنائي في نظام الإثبات المقيد (القانوني).....
59	الفرع الأول: مفهوم نظام الإثبات المقيد (القانوني).....
59	أولا: الأسس التي يقوم عليها نظام الإثبات المقيد (القانوني).....
60	ثانيا: أهم الانتقادات الموجهة لنظام الإثبات المقيد (القانوني).....
61	الفرع الثاني: موقف التشريعات الآخذة بنظام الإثبات المقيد من الأدلة الجنائية الرقمية
61	أولا: موقف التشريع الإنجليزي من الأدلة الجنائية الرقمية.....
62	ثانيا: موقف التشريع الأمريكي من الأدلة الجنائية الرقمية.....
65	المطلب الثاني: السلطة التقديرية للقاضي الجنائي في نظام الإثبات الحر.....

65	الفرع الأول: مفهوم نظام الإثبات الحر.....
65	أولاً: الأسس التي يقوم عليها نظام الإثبات الحر.....
66	ثانياً: القيود الواردة على الاقتناع الشخصي للقاضي.....
67	ثالثاً: أهم الانتقادات الموجهة لنظام الإثبات الحر.....
68	الفرع الثاني: موقف التشريعات الآخذة بنظام الإثبات الحر من الأدلة الجنائية الرقمية..
68	أولاً: موقف التشريع الفرنسي من الأدلة الجنائية الرقمية.....
70	ثانياً: موقف التشريع الجزائري من الأدلة الجنائية الرقمية.....
74	خاتمة.....
79	قائمة المراجع.....
85	الفهرس.....

## ملخص

لقد حاولنا من خلال هذا البحث معالجة موضوع الإثبات الجنائي بالأدلة الرقمية في التشريعين الجزائري والفرنسي، وهو الأمر الذي ساعدنا في الكشف عن غموض هذا النوع من الأدلة، من خلال التعريف بها وبيان أنواعها، وإبراز الخصائص التي تميزها عن غيرها من الأدلة الجنائية الأخرى.

كما تعرضنا أيضا للطرق والأساليب الفنية المستخدمة في استخلاص الأدلة الجنائية الرقمية، ووصلنا إلى أن المشرع الجزائري وإدراكا منه لأهمية هذه الأدلة، قد عمل على استحداث إجراءات تتناسب وطبيعة هذا النوع من الأدلة أسوة بما عمل به المشرع الفرنسي، وانطلاقا من عجز القواعد الإجرائية التقليدية في التعامل مع الأدلة الجنائية الرقمية.

ومن جهة أخرى لكي يكون للأدلة الجنائية الرقمية حجية في مجال الإثبات الجنائي، يجب أن يكون قد تم الحصول عليها بطريقة مشروعة، زيادة على ذلك أن تكون هذه الأدلة غير قابلة للشك أي يقينية، وأن يتم طرحها أيضا للمناقشة أمام جميع أطراف الدعوى العمومية، وأن عدم احترام هذه الشروط يؤدي إلى بطلانها وعدم جواز الأخذ بها.

وفي الأخير نصل وليبيان سلطة القاضي في تقدير الأدلة الجنائية الرقمية يجب التمييز بين أمرين، الأمر الأول يتمثل في القيمة القاطعة للدليل، والأمر الثاني الظروف والملابسات التي وجد فيها هذا الدليل، فتقدير القاضي لا يتناول الأمر الأول لأن قيمة الدليل تقوم على أسس علمية دقيقة، ولا حرية للقاضي في مناقشة الحقائق العلمية الثابتة، وأما الظروف والملابسات التي وجد فيها هذا الدليل وأحاطت به، فإنها تدخل في نطاق تقديره الشخصي.

## **Abstract**

We have tried through this research address the issue of proof of criminal digital evidence in Algerian and French pieces of legislation, which has helped us in the detection of ambiguity of this type of evidence, through the definition of the statement types, and to highlight the characteristics that distinguish them from other forensic evidence.

Also we were ways and techniques used in the extraction of digital forensics, and we got to the Algerian legislature Aware of the importance of this evidence, may work on the development of procedures that are appropriate and the nature of this type of evidence similar to what was done by the French legislature, and from the inability of traditional procedural rules in dealing with digital forensics.

On the other hand in order to be forensic digital authoritative in the field of criminal evidence, you must have obtained a legitimate manner, increased by the fact that this evidence be not be any doubt uncertain, And that it is also put forward for discussion in front of a sheet of all parties to the proceedings, and that failure to respect these conditions lead to the invalidity of her and the inadmissibility of taking them.

And in the last blade to indicate the power of the judge in the estimation of digital forensics must distinguish between two things, the first thing is the cutting of the guide value, and the second thing is the circumstances in which such evidence exists, the judge does not deal with the first order because the guide value based on the basis of accurate scientific , no freedom of the judge in the fixed discuss scientific facts, and the conditions and circumstances in which such evidence exists, and took him, they fall within the scope of his discretion.