# أثر الطبيعة الرقمية لجرائم المساس بأنظمة المعالجة الآلية للمعطيات في إثباتها

## *The impact of the digital nature of the automated data processing systems crimes as proof*

**د/ رامي حليم[1]**
كلية الحقوق والعلوم السياسية، جامعة البليدة 2 dr.rami.halim1@gmail.com

***تاريخ الإرسال: 2021 03/21 تاريخ القبول:31 / 03 /2021 تاريخ النشر: 28 / 05 /2021***

**ملخص:**
تثير مسألة الإثبات في جرائم المساس بأنظمة المعالجة الآلية للمعطيات العديد من المشكلات وعلى مستويات مختلفة، منها ما يتعلق بإجراءات البحث والتحري، ومنها ما هو متعلق بخصائص وطبيعة الدليل المعلوماتي. كما قد يشكل تشفير البيانات المخزنة معلوماتيا أو المنقولة عبر برتوكولات خاصة عبر شبكة الإنترنت عائقا كبيرا أمام كشف هذه الجرائم وإثباتها، ومن المؤكد أن ارتباط هذا النوع من الإجرام بالجانب التقني والتطور السريع للتكنولوجيا، جعل له طبيعة خاصة تجعل من الإجراءات الكلاسيكية في إثبات الجرائم التقليدية عاجزة عن التعامل مع مسرح جريمة افتراضي يتطلب معرفة تقنية متطورة ونمطا فريدا من المهارات الفنية في استخلاص الأدلة. الأمر الذي حتم على المشرعين في مختلف دول العالم ومنها الجزائر، على الإسراع في إرساء دعائم منظومة قانونية، لتوفير الإطار الإجرائي والموضوعي لمكافحة هذه الظاهرة الإجرامية.
**كلمات مفتاحية:** نظام معالجة آلية للمعطيات، أنظمة معلومات، دليل رقمي، تشفير بيانات.

***Abstract:***
*The issue of proving in automated data processing systems crimes raises a number of questions on various levels, particularly in terms of research and investigation procedures as well as the characteristics and nature of the information evidence. Moreover, encrypting computer*

*data, either stored or transmitted through special protocols via the internet, constitute a major obstacle to crime detection and proof. Certainly, the relationship between this type of crime, the technical aspect and the fast evolution of technology grants it a specific nature so that the classical provisions aimed at proving the conventional crimes would be unable to deal with a virtual crime scene, requiring developed technical expertise and exceptional specialized skills to obtain the evidence. Consequently, legislators of different countries all around the world, including Algeria, hasten the set-up of the pillars of a legal system, in the interest of providing a procedural and objective framework to fight against this criminal phenomenon.*

***Keywords:*** *Automated data systems; Information systems; Digital proof; Data encryption.*

**1- المؤلف المرسل:** د/ رامي حليم، **الإيميل:** dr.rami.halim1@gmail.com

**مقدمة :**

خصوصية جرائم المساس بأنظمة المعالجة الآلية للمعطيات بالنظر إلى طبيعتها الرقمية التي تميزها عن غيرها، فرضت منطقا مختلفا في التعامل معها واستيعابها على مستوى مراحل إثباتها المختلفة، من خلال تطوير اساليب البحث والتحري بما يتلاءم والمستوى التقني المتطور والمعقد لهذه الجرائم. ذلك أن العدالة الجزائية تعتمد بشكل أساسي على الأدلة التي لا تخرج عن نطاق كونها ملموسة أو مرئية أو مسموعة، من أجل إثبات الوقائع وتقصي الحقائق، وهو المألوف في ما يمكن تسميته بالجرائم التقليدية، إلا أنه ونظرا للتطور التكنولوجي الهائل في مجال المعلوماتية أصبحت العدالة في مواجهة صريحة مع أدلة يصعب التعامل معها لطبيعتها غير المادية التي تكون على شكل نبضات الكترونية غير مرئية تنساب عبر أجزاء الاجهزة المعلوماتية.

الإقرار بصعوبة التعامل مع هذه الادلة لا يقتصر فقط على مجال البحث والتحري، بل يتعداه لمرحلتي التحقيق القضائي والنهائي من أجل الربط بين الجريمة والمجرم والمجني عليه، بشكل قانوني أمام أجهزة إنفاذ وتطبيق القانون، وإن كان الإثبات في المادة الجزائية يمثل محورا أساسيا في الدراسات القانونية المتخصصة فإن إثبات الجريمة المعلوماتية أصبح يشكل هاجسا لعدة اعتبارات أبرزها طبيعتها الرقمية، ومحلها المعنوي، ووسط ارتكابها الإفتراضي، مما يجعل إشكالية هذه الدراسة تكون على النحو التالي: **كيف فرضت معالم الطبيعة الرقمية لجرائم المساس بأنظمة المعالجة الآلية للمعطيات منطقا له خصوصيته في إثباتها؟**

لذلك فإن هذه الدراسة تستمد أهميتها من خلال البحث في مدى استجابة القواعد العامة في الإثبات لمتطلبات الفضاء الرقمي وهل أصبحنا في حاجة الآن إلى قانون إجراءات جزائية معلوماتي؟ لاستجلاء مختلف جوانب هذا الموضوع اعتمدنا بشكل أساسي على المنهج التحليلي، الذي نلمسه بوضوح، وبصورة أقل على المنهجين الوصفي والاستقرائي.

وحتى تستجيب خطة البحث للمتطلبات المنهجية بناء على الإشكالية المطروحة، تم تقسيم هذه الدراسة إلى محورين، تناولنا في المحور الأول الصعوبات المتعلقة بإجراءات البحث والتحري، وفي المحور الثاني الصعوبات المتعلقة بالدليل المعلوماتي.

## 1. الصعوبات المتعلقة بإجراءات البحث والتحري

صعوبات البحث والتحري في جرائم المساس بأنظمة المعالجة الآلية للمعطيات، تتعلق أساسا في كيفية تعامل الضبطية القضائية مع طبيعتها الرقمية وكيفية إجراء التفتيش واعتراض المراسلات والوصول إلى معطيات مشفرة، وكيفية الحصول على دليل الإدانة في وسط افتراضي والحفاظ عليه، وكيفية التعرف على الفاعل.[1]

لذلك فإنه من البديهي أن يكون إثبات الجرائم التي ينجم عن ارتكابها أثارا مادية ملموسة أو مرئية أيسر من تلك التي لا ينجم عنها سوى أثارا معنوية يصعب التعامل معها، وفقا لهذا المنطق فإن إثبات جرائم المساس بأنظمة المعالجة الآلية للمعطيات من الصعوبة بما كان، على اعتبار أن المعطيات والبيانات التي تتداولها الأنظمة المعلوماتية[2] تكون في شكل رموز ونبضات في شكل غير مرئي من الصعب جدا إدراكها، لاسيما مع الانتشار الواسع لأنظمة التشفير. كما أن الوسط الرقمي الذي ترتكب فيه جرائم المساس بأنظمة المعالجة الآلية للمعطيات له خصوصيته التي تنعكس بشكل واضح على الدليل الذي يستعمل في إثبات هذا النوع من الجرائم، والذي يكون بطبيعته فنيا نتيجة للعمليات التقنية المعقدة التي تستعمل في سبيل الحصول عليه.

### 1.1. غياب الاثار التقليدية في جرائم المساس بأنظمة المعالجة الآلية للمعطيات:

يتصف المجرم المعلوماتي غالبا بالذكاء والخبرة الواسعة إذا ما قارناه بالمجرم العادي، لذلك فهو يسعى دائما إلى استعمال أساليب وتدابير الحماية

الفنية، التي تعيق مهمة المحققين في استخلاص الدليل، ويجتهد في إخفاء أثار سلوكه الإجرامي لمنع التعرف عليه وتحميله المسؤولية الجزائية.

والآثار في جرائم المساس بأنظمة المعالجة الآلية للمعطيات هي كل ما يتركه المجرم بعد استخدامه للشبكة المعلوماتية أو الإنترنت، عن طريق إرسال أو استقبال رسائل وإجراء اتصالات من خلال جهاز كمبيوتر سواء كان موصولا بشبكة الإنترنت أولا.[3]

وبالرغم من أن الكثير من الآثار ذات الطبيعة الرقمية يتم تركها عن غير قصد ودون دراية المستخدم، فإن هذا النوع من الجرائم يبقى صعبة الإثبات نظرا لاختفاء الأثر المادي الذي يمكن إدراكه بالحواس أو الشهود الذين يمكن سماعهم أو حالات التلبس التي يمكن معاينتها، كما انه يمكن للجاني أن يتلاعب وبكل سهولة في البيانات محل الجريمة أو أن يمحو ملفات الذاكرة سواء قام بذلك بنفسه أو بالإعتماد على البرامج التي تتمتع بخاصية إتلاف البيانات بصورة تلقائية، لذلك فإنه يصعب الحصول على الدليل المادي الذي يثبت الصلة بين الأثر والمتهم، فإن كانت هذه الصلة إيجابية أثبتت الواقعة وإن كانت سلبية نفت المسؤولية الجزائية عن المتهم.[4]

كما أن عملية الحصول على الدليل تزداد صعوبة، عندما يتمكن المجرم المعلوماتي من إخفاء هويته حتى لا يتم تعقبه من السلطات المختصة، كأن يقوم باختراق نظام معلوماتي لشخص آخر أو عدة أنظمة معلوماتية، ومن خلالها يقوم بتنفيذ هجومه. أو أن يستعمل نظام معالجة آلية للمعطيات تابع لمكان عام أو في أحد مقاهي الإنترنت.

وهو ما يجعلنا لانتفق مع الذين يرجحون إمكانية أن يخلف الجاني أثارا مادية تقليدية كبصماته على الجهاز في حالة اتصاله المباشر بالنظام المعلوماتي في الجرائم التي تتطلب تواجده الفعلي، ذلك أن البصمات قد تثبت قيام المتهم باستعمال الجهاز لكن لا تثبت قيامه بالفعل محل التجريم والمتابعة.[5] وعليه فإن الآثار التي قد يخلفها المجرم تشمل مسرحي الجريمة الحقيقي والرقمي، ما يحتم على المحققين في هذا النوع من الجرائم، البحث فيهما معا.[6] ومع ذلك فإن إثبات

صلة الجاني بجرائم المساس بأنظمة المعالجة الآلية للمعطيات يبقى أمرا غاية في الصعوبة لأنها ترتكب في بيئة افتراضية رقمية تختفي فيها الأدلة المادية.

### 2.1. الطبيعة الرقمية لمسرح جرائم المساس بأنظمة المعالجة الآلية للمعطيات:

يعتبر مسرح الجريمة العنصر الاساسي في إجراءات البحث والتحري التي يقوم بها رجال الضبطية القضائية المختصين نوعيا وإقليميا، لذلك فإن أوليتهم القصوى هي الحفاظ على مسرح الجريمة والأدلة التي يحتويها،[7] وما يميز جرائم المساس بأنظمة المعالجة الآلية للمعطيات، هو أن الافعال المكونة للركن المادي فيها يمكن أن تتجزأ على أكثر من مكان واحد، ويمكن أن تتعدى إقليم الدولة الواحدة، لأن ارتكابها لا يشرط التواجد الفعلي أو المادي للجاني في مكان الجريمة.

ويزداد الأمر تعقيدا عندما تكون المسافة بين الفعل المجرم والمعطيات محل الاعتداء كبيرة لدرجة تتجاوز حدود الدولة الواحدة، وهو ما يتولد عنه الصعوبات المتعلقة بمعيار التجريم المعتمد في مختلف التشريعات، ومشكلات المتابعة القضائية ابتداء من إجراءات البحث والتحري والتحقيق، التي قد تكون في أكثر من دولة[8] وصولا إلى التنازع القضائي الإيجابي عندما يعقد الاختصاص لأكثر من قضاء للنظر في القضية.

تجدر الإشارة في هذا الإطار إلى أن العديد من الدول وفي غياب اتفاقيات تعاون أمني وقضائي، تعتبر أن الدخول إلى أنظمة معلوماتية موجودة في إقليم دولة أخرى مساسا بسيادتها،[9] ومثال ذلك القضاء الأمريكي الذي يعقد الإختصاص لنفسه في كل الجرائم التي وقعت في الخارج ومست آثارها مصالح أمريكية أو عرضتها للخطر، إعمالا لمبدأ الإختصاص الشخصي.[10]

وهو نفس الإتجاه الذي سار فيه القضاء الإنجليزي، حيث ينعقد الإختصاص للمحاكم البريطانية، متى كان ثمة ارتباط بين الواقعة المرتكبة وبريطانيا، عملاً بقانون إساءة استخدام الحاسوب الصادر سنة 1990 ( The Computer Misuse Act of 1990) حتى وإن كانت هذه الواقعة قد حدثت في الخارج وبصرف النظر عن محل إقامة الجاني.[11] أما في فرنسا فينعقد

الإختصاص في جرائم الإنترنت التي وقعت في الخارج، للقضاء الفرنسي متى كانت الظروف الواقعة تبرر مصلحة فرنسا في إعمال قانونها عليها، عملاً بقانون العقوبات الجديد.[12]

وبالرغم من سعي الدول إلى عقد اتفاقيات ثنائية من أجل إزالة الحواجز التي تقيد الإجراءات الجزائية، فإن الواقع العملي أثبت أن العائق الفعلي هو مبدأ ازدواجية التجريم الذي يضمن توافق الدول على تجريم نفس الفعل وهو ما يتطلب قوانين جنائية أكثر مرونة.[13]

### 2.1. القصور التشريعي وغياب التنسيق الدولي في مواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات:

خصوصية جرائم المساس بأنظمة المعالجة الآلية للمعطيات وأساليب مكافحتها، فضحت القصور التشريعي في جانبيه الموضوعي والإجرائي، وإن كانت الدول سارعت إلى تدعيم منظوماتها القانونية بنصوص لمواكبة التطور المتسارع للظاهرة، فإن غالبية هذه النصوص تفتقد إلى الدقة من حيث تحديد السلوك المجرم، ولا تضمن الشرعية اللازمة لسلامة إجراءات المتابعة من العيوب، وهو ما يثير إشكالات كبيرة أمام القضاء من حيث القبول والحجية.

في الجزائر تم تناول هذا الجانب من خلال القانون 09-04[14] الذي يعتبر نوعيا من حيث الصياغة ومرافقته لنصوص قانون العقوبات المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات.[15]

وبالرغم من أن بعض الدول سارعت إلى جعل قوانينها الداخلية أكثر ملاءمة للتطور في مجال تكنولوجيا المعلومات، إلا أن ذلك يبقى غير كاف لإرساء دعائم التعاون الدولي في مجال مكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات. فعدم وجود مفهوم مشترك لهذه الأخيرة صعب من إجراءات ملاحقة المجرمين الذين يرتكبون أفعال مجرمة من دول تبيح قوانينها السارية هذه الأفعال، كما أن اعتماد بعض الدول على قواعد قانونية إجرائية تقليدية جعل التنسيق في ما بينها في غاية الصعوبة لاسيما عندما يتعلق الأمر بعمليات الإستدلال والتحقيق.

في الأخير فإن غياب اتفاقيات للتعاون بين الدول في مكافحة هذه الظاهرة الإجرامية أو عدم كفاية بنودها -إن وجدت للتصدي لهذه الظاهرة- يحتم على الدول إيجاد صيغ أكثر فعالية من أجل تسهيل تسليم المجرمين وتبادل المعلومات، مثل ما هو الحال بالنسبة لاتفاقية التعاون في المجال القضائي بين الجزائر والولايات المتحدة الأمريكية بتاريخ 07 أفريل 2010.[16]

**2. الصعوبات المتعلقة بالدليل المعلوماتي**

يعرف الدليل المعلوماتي بأنه "الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم".[17] ويعرف كذلك بأنه "ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي أوشبكات الاتصال من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها بشكل نصوص مكتوبة أو رسومات أو صور وأشكال وأصوات لإثبات وقوع الجريمة، لتقرير البراءة أو الإدانة فيها.[18]

كما يعرف بأنه"الدليل الذي يشمل جميع البينات الرقمية التي يمكن أن تثبت أن هناك جريمة قد أرتكبت أو توجد علاقة بين الجريمة والجاني، أو بين الجريمة والمتضرر منها. والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت أو الصورة"[19] أو "الدليل آلذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة أو هو تلك المعلومات آلتي يقبلها المنطق و العقل و يعتمدها العلم و يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحاتقها وشبكات الإتصال، ويمكن استخدامها في أي

مرحلة من مراحل التحقيق أو المحاكمة، لإثبات حقيقة فعل أو شيئ له علاقة بجريمة ما أو المجني عليه".[20]

لكن ما يؤخذ على هذه التعاريف، هو عدم دقتها في أغلب الأحيان وخلطها بين مفاهيم متعددة، ذلك أن واضعيها لا يلمون بالجانب التقني المتخصص والمعمق بالشكل الكافي الذي يسمح لهم بوضع تعاريف دقيقة توازن بين الشق القانوني والتقني، هذا من جهة ومن جهة أخرى، صعوبة وضع تعريف شامل ودقيق نظرا للتطور المستمر والسريع لتكنولوجيا المعلومات.

فاعتبار الدليل مجموعة من البيانات يتم إدخالها للنظام المعلوماتي يجعله يتطابق مع باقي المفاهيم الأخرى كبرامج المعلوماتية المتعلقة بالتطبيقات أو أنظمة التشغيل كما أنه ثبت قصور التعريفات التي تربط الدليل المعلوماتي بجهاز الحاسوب، من خلال التكنولوجيا التي وسعت البيئة الرقمية إلى العديد من الاستخدامات كالهواتف الذكية وبطاقات الدفع مثلا.

**1.2 النسبية في خصائص الدليل المعلوماتي:**

درج استعمال العديد من المصطلحات للتعبير عن الدليل المعلوماتي(preuve Informatique)، الدليل الالكتروني ( prevue électronique) وكذلك دليل تكنولوجيات المعلومات (IT Evidence)،[21] إلا أنها تقريبا تؤدي نفس المعنى ولا يوجد اتفاق صريح على تعريف واحد، نظرا للطبيعة الفنية والتقنية لهذا النوع من الأدلة، المتغيرة بحسب اتساع مجالات استخدام المعلوماتية، وهو ما حذا بالتشريعات الداخلية للدول ومن بينها التشريع الجزائري، إلى تجنب اعطاء تعريف للدليل المعلوماتي، وأن ما هو موجود في البحوث العلمية المتخصصة، هو اجتهادات فقهية لإيجاد تعريف إطار شامل ودقيق. إلا أن المسالة التي تلقى إجماعا في ما يتعلق بالدليل المعلوماتي هي صعوبة الحصول عليه وفهمه وكيفية التعامل معه في الإثبات، خاصة وأن الأمر غالبا ما يتطلب إعادة عرض كافة العمليات الآلية التي تمت من أجل الحصول عليه.

وتنعكس البيئة الرقمية التي تمثل الوسط الطبيعي للدليل المعلوماتي على خصائصه ومميزاته، فهو دليل علمي لاختلافه عن الدليل التقليدي من حيث هيئته غير الملموسة، وطريقة الحصول عليه التي تطلب برمجيات خاصة ونظم معلوماتية مؤهلة تقنيا للتعامل معه واستخلاصه. كما أنه الدليل المعلوماتي هو دليل تقني نسبة إلى البيئة التقنية التي يتكون فيها، والتأهيل التقني اللازم للتعامل معه من طرف تقنيين ومتخصصين، إضافة إلى أنه متنوع ومتطور، لإمكانية اتخاذه كافة أنواع وأشكال البيانات الممكن تداولها رقميا كالصور والتسجيلات على سبيل المثال.

وبالرغم من أغلب الدراسات تتناول مسألة خصائص الدليل المعلوماتي كنوع مستحدث من الأدلة، إلا أننا نجد بأن هذه الخصوصية نسبية إلى حد ما في بعض الحالات، وأن ما يمكن أن يميز الدليل الجزائي المعلوماتي يمكن سحبه كذلك على الدليل الجزائي التقليدي، أو على الأقل لا ينفرد وحده بهذه الخصوصية، والأدلة على ذلك كثيرة. فالتسليم بأن الدليل المعلوماتي دليل يصعب التخلص منه على اعتبار أن أي إلغاء لمعطيات تم إدخالها للنظام المعلوماتي، يمكن استردادها في ما بعد لتوفر برمجيات يمكن بمقتضاها القيام بهذه المهمة، يتعارض تماما مع جانب من الفقه الذين يرجعون صعوبة الإثبات في جرائم المساس بأنظمة المعالجة الآلية للمعطيات إلى سهولة وسرعة التخلص من أدلة الإثبات.

### 2.2 شروط قبول الدليل المعلوماتي:

إن أول ما يثار بشأن الدليل المعلوماتي هو مدى إمكانية قبوله كدليل وذلك نظرا للأشكال المختلفة التي يمكن أن يكون عليها، والتي تجعل قبوله أمام الجهات القضائية يتوقف على ضوابط معينة منصوص عليها قانونا، تلتزم بها جهات التحقيق في إجراءات الحصول عليه، ليكون دليل إثبات يعول عليه القضاء في أحكامه، ويستمد حجيته من نتائج وآثار أصل البراءة، المتمثلة أساسا في أولا: أن يكون الدليل المعلوماتي مشروعا، وثانيا:أن يكون الدليل المعلوماتي يقينيا، وثالثا: أن تتم مناقشة الدليل في الجلسة.

### 1.2.2 أن يكون الدليل المعلوماتي مشروعا

المقصود بمشروعية الدليل هو أن يعترف المشرع بهذا الدليل من خلال تصنيفه في قائمة الأدلة القانونية، التي يجيز القانون فيها للقاضي الاستناد إليه في تكوين عقيدته، وهو ما يسمى بمشروعية الوجود من جهة، ومن جهة أخرى أن يتفق الإجراء الذي تم الحصول من خلاله على الدليل المعلوماتي مع القواعد القانونية،[22] وهو ما يسمى مشروعية الحصول على الدليل المعلوماتي.

أما بالنسبة لمشروعية الحصول على الدليل المعلوماتي، فالمقصود بها هو الحصول على الدليل وتقديمه للقضاء أو إقامته أمامه بالطرق التي رسمها القانون، وأن أي خروج عن هذه القواعد يجعل الدليل غير مشروع لا يعتد بقيمته القانونية مهما كانت دلالته في الكشف عن الحقيقة، وفي هذا الإطار، فقد أكد المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد بالبرازيل في الفترة من 04 إلى 09 سبتمبر 1994 في قراره الصادر حول القواعد الإجرائية في بيئة جرائم الحاسوب، على أن الانتهاكات غير المشروعة لحقوق الإنسان التي يرتكبها رجال السلطة العامة، يمكن أن تبطل الدليل المتحصل عليه، بالإضافة إلى تقرير المسؤولية الجنائية لرجل السلطة العامة الذي انتهك القانون.[23]

ويشكل نظام الإثبات الذي تتبناه الدولة، المعيار الأساسي الذي تتحدد على أساسه مشروعية الدليل من حيث الوجود. ففي نظام الإثبات المقيد، والذي يعرف بنظام الأدلة القانونية، تكون أدلة الإثبات محصورة، ولا يمكن للقاضي الإستناد على دليل غير منصوص عليه صراحة ضمن أدلة الإثبات، ولا يكون بذلك لقناعة القاضي أي دور في تقدير الأدلة أو البحث عنها. أما في نظام الإثبات الحر، الذي لا يحدد أدلة الإثبات، فإن مسألة مشروعية الدليل المعلوماتي من حيث الوجود لا تطرح تماما، نظرا لاضطلاع القاضي في هذا النظام بدور إيجابي في البحث عن الأدلة وتقدير قوتها الثبوتية، وهو النظام الذي تبناه المشرع الجزائري، وعبر عنه صراحة في نص المادة 212 من قانون الإجراءات الجزائية.

لذلك كان من المنطقي أن يستبعد القاضي كل دليل معلوماتي تم الحصول عليه بطريقة غير مشروعة،[24] وأن لا يستند عليه في حكمه مهما كانت قيمته القانونية وقوته الثبوتية، وهو ما ذهب إليه المشرع الإنجليزي الذي أكد على أن كل دليل تم التوصل إليه بطريقة مباشرة أو غير مباشرة، وكان متضمنا اعتداء على الحقوق الاساسية للمواطن، يتعين استبعاده من جلسة المرافعات، حتى ولو كان دليلا ملائما أو موضوعيا يتصل بموضوع النزاع مباشرة يثبته أو يساهم في إثباته.[25]

### 2.2.2 أن يكون الدليل المعلوماتي يقينيا

بمعنى أن يكون الدليل مبنيا على الجزم واليقين وغير قابل للشك، لذلك فإنه يتوجب التأكد من سلامة الدليل أولا من العبث، كأن يتعرض للتغيير أو التعديل أو الحذف أو الطمس، وثانيا من الخطأ في استخلاصه، بأن يتم التحقق من سلامة الإجراءات الفنية المستخدمة في الحصول عليه، من خلال الاعتماد على الأساليب التي أثبتت كفاءتها في استخلاص الأدلة الموثوقة. هذا من جهة، ومن جهة أخرى، سلامة الوسائل المستعملة كالبرمجيات وغيرها من أي عيب قد يؤثر على مصداقية الدليل، وذلك بإخضاعها لعدة تجارب للوقوف على مدى دقتها. حتى أن القضاء الأمريكي استبعد المخرجات الناتجة عن حاسوب لا يؤدي وظائفه بصورة سليمة أو كان القائم عليه غير موثوق.[26]

كما يشترط قانون الشرطة والإثبات في بريطانيا لسنة 1984، أن تكون البيانات دقيقة وناتجة عن الحاسوب بصورة سليمة، لاعتبار الدليل يقينيا.[27]

### 3.2.2 أن تتم مناقشة الدليل المعلوماتي في الجلسة

يشترط المشرع الجزائري كغيره من المشرعين وجوب مناقشة الأدلة في الجلسة، ونص على ذلك صراحة في المادة 212 من قانون الإجراءات الجزائية،[28] التي تؤكد على أنه لا يسوغ للقاضي أن يبني قراره إلا على الأدلة

المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه. وعليه فإن حرية الدليل في المادة الجزائية مشروطة بأن يكون الدليل الذي يستند إليه القاضي قد تم إتاحته للخصوم ومناقشته بالجلسة. إلا أنه تجد الإشارة إلى أن خصوصية الجريمة المعلوماتية تجعل من حضور الخبير في الجلسة أمرا ضروريا لتوضيح المسائل التقنية التي تلعب دورا هاما في اقتناع القاضي الجزائي بالدليل الرقمي.[29]

### 3.2 حجية الدليل المعلوماتي

درجت مختلف التشريعات ومنها التشريع الجزائري على تقسيم مراحل إثبات الجرائم إلى مرحلة البحث والتحري التي تعتبر مرحلة تمهيدية تجمع فيها الاستدلالات ومرحلة التحقيق القضائي التي تمحص فيها الأدلة تحت إشراف قضائي، أخير مرحلة المحاكمة أو كما تسمى في الممارسة القضائية بالتحقيق النهائي، لأن فيها تناقش الأدلة ترجيحا للإدانة في حال كفاية أدلة الإتهام أو الحكم بالبراءة في حال عدم كفايتها.

إن المقصود بحجية الدليل المعلوماتي، هو قيمة ما يتمتع من قوة استدلالية، لذلك فهي تختلف باختلاف أنظمة الإثبات الرئيسية وهي نظام الإثبات المقيد، نظام الإثبات الحر ونظام الإثبات المختلط.

بالنسبة لنظام الإثبات المقيد فإن الأدلة فيه تكون محصورة ومحددة مسبقا بنصوص قانونية،[30] ودور القاضي في هذا النظام يقتصر على تطبيق القانون من حيث وجود الدليل وتوافر شروطه،[31] لذلك فإن القوة الإثباتية للأدلة المعلوماتية فيه تكون محدودة، لاسيما وأن هذا النظام يعمل بقاعدة الدليل الأفضل أو المحرر الأصلي بمعنى استبعاد الدليل في صورة نسخة إذا كان من الممكن الحصول على الدليل في صورته الأصلية،[32] الأمر الذي يكون من الصعب تحقيقه بالنظر إلى خصائص الدليل المعلوماتي والوسط الرقمي الذي يستنبط منه.

يختلف الأمر في ظل نظام الإثبات الحر، لأن حجية الأدلة المعلوماتية لا تطرح أي إشكال بالنظر إلى مبادئ هذا النظام التي تقوم على حرية الإثبات وسلطة القاضي الواسعة في تقدير الأدلة وبناء قناعته على أي دليل يطرح أمامه في الجلسة، وهو الاتجاه الذي نؤيده بالنظر إلى الكفاءة التي حققتها النظم المعلوماتية الحديثة، والتي تبرهن على وضوح الأدلة المعلوماتية ودقتها في إثبات العلاقة بين الجاني والضحية أو بين الجاني والسلوك الإجرامي.

أما حجية الدليل المعلوماتي في نظام الإثبات المختلط محاطة بالغموض والتعقيد نظرا إلى أن المشرع في هذا النظام يحدد أدلة الإثبات من جهة ويمنح القاضي سلطة تقديرها من جهة أخرى، وليتم قبول الدليل المعلوماتي أمام المحكمة فإنه يتم اعتباره طريقة من طرق الإثبات لأنه بالنسبة إليهم وسائل الإثبات محددة على سبيل الحصر ولا يمكن بأي حال من الأحوال الخروج عنها.[33]

ويبقى موقف المشرع الجزائري واضحا من خلال نص المادة 212 من قانون الإجراءات الجزائية التي تنص 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، وتؤكد المادة أنه لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه، وبهذا فإن المشرع الجزائري يكون قد كرس قاعدتين جوهريتين، الأولى هي قاعدة الاقتناع الحر للقاضي الجزائي والثانية هي حرية اختيار وسائل الإثبات.

هذا الأمر يتجلى بوضوح أكبر في ما ذهبت إليه المادة 307 من قانون الإجراءات الجزائية بتأكيدها على أن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي قد وصلوا بها إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير 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.

**الخاتمة:**

إن إثبات جرائم المساس بأنظمة المعالجة الآلية للمعطيات وضبط الأدلة الرقمية والتعامل معها لتحديد قيمتها في الإثبات، من المواضيع ذات الأهمية العلمية والعملية، لذلك فإنه من المنطقي أن تتم معالجتها لوضع اليد على مواضع النقص في الأنظمة القانونية، وهو الهدف من دراستنا التي توصلنا فيها إلى أنه من الضروري التعرض بالدراسة والفحص للعوامل المؤثرة في إثبات الجريمة المعلوماتية والمتأتية أصلا من طبيعتها الرقمية ووسط ارتكابها الافتراضي.

وبالرغم من أننا لم نلمس من خلال دراستنا للمنظومة القانونية في الجزائر قصورا تشريعيا أو عدم ملاءمة نصوص قانون الإجراءات الجزائية أو القوانين الخاصة لهذا النوع من الجرائم، بل أن ما وقفنا عليه في النظام القانوني الجزائري هو توافر النصوص القانونية التي توضح كيفية التعامل مع الأدلة الرقمية عن طريق تعليمات وإرشادات وحتى إجراءات معيارية، فإن التحديات الحقيقية في إثبات الجريمة المعلوماتية يمكن إجمالها في مواكبة التطور السريع لتكنولوجيا المعلومات لتسهيل ضبط المتهمين وإثبات إدانتهم وتوحيد القوانين التي تعنى بحماية البيانات الشخصية لمستخدمي الأنظمة المعلوماتية عالمياً مع تضمين القوانين الداخلية للدول قواعد إجرائية خاصة تنسجم مع طبيعة الجريمة المعلوماتية.

كما أنه يتوجب على موردي خدمة الإنترنت في العالم، الالتزام بتوفير تسهيلات للجهات القضائية بهدف الحصول على معلومات وبيانات تخص المتهمين، لاسيما في إطار الإنابات القضائية الدولية التي لا يمكن أن تتجسد إلا في وجود تنسيق دولي تنظمه اتفاقيات دولية نتيجة الطبيعة العابرة للحدود لهذا النوع من الجرائم.

## التهميش و الإحالات :

[1] Christiane FERAL-SCHUHL, 1999, « Cyber droit, le droit à l'épreuve de l'Internet », Paris, Dunod, p. 45.

[2] عرفت المادة 2/ب من القانون 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنظومة المعلوماتية على أنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

[3] يوسف مناصرة، 2016-2017، الاثبات الالكتروني قي القانون المقارن، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر1، الجزائر، ص: 60، نقلا عن: Geneviève CAMMAS, « Traçabilité et protection des communications », article publié dans la revue « Droit et Patrimoine » « dossier : La traçabilité », édition n° :93, Paris, 2001.

[4] عبد الفتاح مراد،1991، التحقيق الجنائي الفني والبحث الجنائي، القاهرة، دار الكتب المصرية، ص 73.

[5] محمد حماد مرهج الهيتي، 2006، جرائم الحاسوب، الطبعة الأولى، عمان، دار المناهج للنشر والتوزيع، ص 226-227.

[6]مناصرة يوسف، المرجع السابق، ص: 62. نقلا عن: Geneviève CAMMAS, « Traçabilité et protection des communications », article publié dans la revue « Droit et Patrimoine » « dossier : La traçabilité », édition n° :93, Paris, 2001.

[7] تنص المادة 43 من قانون الإجراءات الجزائية على أنه يحظر في مكان ارتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي.

[8] تنص المادة 40 من قانون الإجراءات الجزائية "يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر. يجوز تمديد الإختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة

المعالجة الآلية للمعطيات وجرائم تبييض الاموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".

[9] محمود علي حمودة، من 26 إلى 28 أفريل 2003، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، الإمارات العربية المتحدة، ص 05.

[10] موسى مسعود ارحومة، 28، 29 أكتوبر 2009، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول، حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ص 19، منشور على الموقع: iefpedia.com تاريخ الإطلاع: 2020/11/28 على الساعة 19:46، نقلا عن: USA V. Thomas, no. cr – 94 – 20019 – 9 (w. d. tenn. 1994) مشار إليها عند عمر محمد بن يونس الجرائم الناشئة عن استخدام الإنترنت، ص908.

[11] موسى مسعود ارحومة، المرجع السابق، ص 19، نقلا عن: U. S. V. Truesdale 152 F. 3d 443 (5th Cir. 1998) مشار إليها عند عمر محمد بن يونس الجرائم الناشئة عن استخدام الإنترنت، ص910.

[12] موسى مسعود ارحومة، المرجع السابق، ص 19، نقلا عن عمر محمد بن يونس الجرائم الناشئة عن استخدام الإنترنت، ص911.

[13] محمد الأمين البشري، نوفمبر 2000، التحقيق في جرائم الحاسب الآلي والإنترنت المجلة العربية للدراسات الأمنية والتدريب، عدد 30 السعودية، ص 373.

[14] القانون 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[15] المشرع الفرنسي هو أول أقر حماية المعالجة الآلية للمعطيات بموجب القانون 88-19 المتعلق بالغش المعلوماتي، أما المشرع الجزائري فقد تناولها من خلال قانون العقوبات بموجب القانون 04-15 في القسم السابع مكرر في الفصل الثالث للباب الثاني من الكتاب الثالث تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات".

[16] تتيح هذه الاتفاقية إمكانية جمع الشهادات أو تصريحات الشهود وتقديم الوثائق والملفات وغيرها من عناصر الإثبات وتحديد مكان وهوية الأشخاص والأغراض وتسليم الوثائق القانونية والتحويل المؤقت للأشخاص الموقوفين للإدلاء بشهاداتهم أو أي مساعدة أخرى وكذا تنفيذ الأوامر بالتفتيش والحجز.

[17] مناصرة يوسف، المرجع السابق، ص: 18-19. نقلا عن: Raphael d'ASSGNIES directeur de CELOG, Alexandre DREVET «La preuve dans l'environnement

numérique & collecte probatoire, bonne pratique en cas de situations pré-contentieuses», les cahiers techniques de CELOG, 2014, p 6.

[18] عائشة بن قارة، 2010، حجية الدليل الالكتروني في مجال الاثبات الجنائي في القانون الجزائري والقانون المقارن،مصر، دار الجامعة الجديدة، ص 53.

[19] نفس المرجع، ص 54.

[20] أشرف قنديل عبد القادر، 2015، الإثبات الجنائي في الجريمة الإلكترونية، الإسكندرية دار الجامعة الجديدة، ص 123 124.

[21] مناصرة يوسف، المرجع السابق، ص 18، نقلا عن: Jean-Raphaël DEMARCHI, « Les preuves scientifiques et le procès pénal », L. G. D. J, Lextenso édition, 2012, PARIS, p 42-43, p 385.

[22] أحمد فتحي سرور، 1997، الشرعية والإجراءات الجنائية، القاهرة، دار النهضة العربية ص 105.

[23] أمير فرج يوسف، 2008، الجرائم المعلوماتية على شبكة الانترنت، الإسكندرية، دار المطبوعات الجامعية، ص 314.

[24] من أمثلة الطرق غير المشروعة في الحصول على الدليل المعلوماتي، قيام ضباط الشرطة القضائية بعملية التفتيش دون الحصول على إذن مسبق من السلطات المختصة.

[25] عبد اللاه أحمد هلالي، 1997، حجية المخرجات الكمبيوترية في المواد الجنائية، القاهرة دار النهضة العربية، الطبعة الأولى، ص 128- 129.

[26] نفس المرجع، ص 95.

[27] علي حسن محمد الطوالبة، 2004، التفتيش الجنائي على نظم الحاسوب والإنترنت الطبعة الأولى، الأردن، عالم الكتب الحديث، ص 191.

[28] المادة 212 من قانون الإجراءات الجزائية الجزائري يقابلها نص المادة 427 من قانون الإجراءات الجزائية الفرنسي.

[29] أشرف عبد القادر قنديل، 2015، الإثبات الجنائي في الجريمة الإلكترونية، الإسكندرية مصر، دار الجامعة الجديدة للنشر، ص 174.

[30] نظام الإثبات المقيد أو القانوني لا يمنح الحق للقاضي بالحرية في تكوين اقتناعه الشخصي، بل يكون مقيدا بالقواعد والأسس التي حددها المشرع سلفا، لذلك فإن دور القاضي في هذا النظام يقتصر على تطبيق القانون من حيث وجود الدليل وتوافر شروطه.

[31] Charles GILLIERON, 1946, « l'évolution de la preuve pénale », revue pénale suisse, Berne, p 197.

[32] هلالي عبد اللاه أحمد، المرجع السابق، ص 94.

[33] فتوح الشاذلي، عفيفي كامل عفيفي، 2003، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، لبنان، منشورات الحلبي الحقوقية، ص 395.

## قائمة المراجع:


- **المؤلفات باللغة العربية**:

1- أحمد فتحي سرور، 1997، الشرعية والإجراءات الجنائية، القاهرة، دار النهضة العربية

2- أشرف قنديل عبد القادر، 2015، الإثبات الجنائي في الجريمة الإلكترونية، الإسكندرية دار الجامعة الجديدة.

3- أشرف عبد القادر قنديل، 2015، الإثبات الجنائي في الجريمة الإلكترونية، الإسكندرية مصر، دار الجامعة الجديدة للنشر.

4- أمير فرج يوسف، 2008، الجرائم المعلوماتية على شبكة الانترنت، الإسكندرية، دار المطبوعات الجامعية.

5- عائشة بن قارة، 2010، حجية الدليل الالكتروني في مجال الاثبات الجنائي في القانون الجزائري والقانون المقارن،مصر، دار الجامعة الجديدة.

6- عبد اللاه أحمد هلالي، 1997، حجية المخرجات الكمبيوترية في المواد الجنائية، القاهرة دار النهضة العربية، الطبعة الأولى.

7- عبد الفتاح مراد،1991، التحقيق الجنائي الفني والبحث الجنائي، القاهرة، دار الكتب المصرية.

8- علي حسن محمد الطوالبة، 2004، التفتيش الجنائي على نظم الحاسوب والإنترنت الطبعة الأولى، الأردن، عالم الكتب الحديث.

9- فتوح الشاذلي، عفيفي كامل عفيفي، 2003، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، لبنان، منشورات الحلبي الحقوقية.

10- محمد حماد مرهج الهيتي، 2006، جرائم الحاسوب، الطبعة الأولى، عمان، دار المناهج للنشر والتوزيع.

- **المؤلفات باللغات الأجنبية**:

1- Christiane FERAL-SCHUHL, 1999, « Cyber droit, le droit à l'épreuve de l'Internet », Paris, Dunod

- **الأطروحات**:

1- يوسف مناصرة، 2016-2017، الاثبات الالكتروني قي القانون المقارن، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر1، الجزائر.

- **المقالات باللغة العربية**:

1- محمد الأمين البشري، نوفمبر 2000، التحقيق في جرائم الحاسب الآلي والإنترنت المجلة العربية للدراسات الأمنية والتدريب، عدد 30 السعودية.

- **المقالات باللغات الأجنبية**:

1- Charles GILLIERON, 1946, « l'évolution de la preuve pénale », revue pénale suisse, Berne.

- **المداخلات**:

1- محمود علي حمودة، من 26 إلى 28 أفريل 2003، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، الإمارات العربية المتحدة.

2- موسى مسعود ارحومة، 28، 29 أكتوبر 2009، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول، حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس.

- **النصوص القانونية:**

1- الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 08 يوليو 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد 48، سنة 1966، المعدل والمتمم.

2- القانون 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.