الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)

بن فردية محمد أستاذ مساعد "أ"
كلية الحقوق و العلوم السياسية جامعة بجاية، 06000 بجاية، الجزائر.

ملخص:

يمكن القول أنه بظهور شبكة الإنترنت وانتشار النظم المعلوماتية قامت تحديات لم تكن موجودة من قبل أمام القانون الجنائي بشقيه الموضوعي والإجرائي ، فعلى المستوى الموضوعي فقد ظهرت ما أطلق عليه بالجرائم المعلوماتية، أما على المستوى الإجرائي فإن جوهر إثبات هذه الجرائم هو الدليل الجنائي ذو الطبيعة الرقمية .

ويتميز الدليل الجنائي الرقمي بعدة مزايا ، فهو دليل علمي ذو طبيعة تقنية، يصعب التخلص منه ويكون قابلا للنسخ.

أما من حيث حجية هذا الدليل فإن للقاضي الجنائي سلطة واسعة في تقدير الدليل الرقمي حيث أنه لقبوله ينبغي توافر عدة شروط وهي مشروعية هذا الدليل وكذا بلوغ اقتناع القاضي درجة اليقين، وأخيرا شرط مناقشة هذا الدليل.

وتتحدد سلطة القاضي الجنائي في قبول الأدلة الجنائية الرقمية حسب طبيعة النظام السائد، فهناك النظام اللاتيني الذي يطلق عليه نظام الإثبات الحر، والنظام الأنجلوسكسوني الذي يسمى بنظام الإثبات المقيد.

Résumé :

Avec l'émergence de l'internet et la prolifération des systèmes d'information, le droit pénal, tant dans son volet substantiel que procédural, s'est heurté à des défis qui n'étaient pas connus. S'agissant de l'aspect substantiel, les textes consacrent ce qu'a été qualifié d'infractions informatiques. Quant à l'aspect procédural, l'essence de la preuve des dites infraction réside dans la preuve pénale à caractère numérique.

La preuve pénale numérique se distingue par plusieurs avantages. Il s'agit, en effet, d'une preuve scientifique et technique, d'où la difficulté de son effacement et la susceptibilité de sa reproduction.

Concernant la force probante de la preuve numérique, le juge pénal a un large pouvoir discrétionnaire quant à l'appréciation de celle-ci. Ainsi, l'acceptation de cette dernière est subordonnée à la réunion de plusieurs conditions : la légalité de la preuve, la certitude de la persuasion du juge et la discussion de l'exigence de la preuve.

Enfin, les limites du pouvoir du juge quant à l'acceptation de la preuve numérique sont déterminées en fonction du système juridique en vigueur. A ce titre, on distingue, d'une part, le système latin, appelé système de la preuve libre, et, d'autre part, le système anglo-saxon, appelé système de preuve liée.

الكلمات المفتاحية: الدليل الرقمي – الإثبات الرقمي – الدليل الجنائي – القضاء الجنائي

مقدمة

يعد الدليل الجنائي جوهر الإثبات ووسيلة لإسناد الواقعة الإجرامية إلى المتهم أو نفيها عنه، لذا فهو يكتسي أهمية في جميع مراحل الدعوى، وبه تعرف الحقيقة، ويعرف على أنه:"كل وسيلة مرخص أو مسموح بها قانونا لإثبات وجود أو عدم وجود الواقعة المرتكبة، أو صحة أو كذب وقوعها"[1].

ويهدف الدليل الجنائي إلى الإثبات، ويعرف هذا الأخير على أنه: " إقامة الدليل لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة بأشخاصها ذات أهمية قانونية، وذلك بالطرق التي حددها القانون وفق القواعد التي أخضعها لها"[2].

وتحظى نظرية الإثبات بأهمية قصوى في نطاق القانون الجنائي، طالما كان من المستحيل قانونا إدانة شخص دون أن تثبت مساهمته في الفعل الجرمي، ودون اجتماع كافة العناصر المكونة لهذه الجريمة، بل ذهب البعض إلى القول أن نظرية الإثبات تعد من أخطر نظريات القانون، بل لا يوجد في القانون نظرية تضاهيها في السيطرة والشمول واضطراد التطبيق، لأنها النظرية الوحيدة التي لا تنقطع المحاكم عن تطبيقها في كل ما يعرض عليها من القضايا[3].

وإثر التقدم العلمي والتكنولوجي ظهر ما يسمى بالنظام المعلوماتي[4] مع ما يحتويه من قواعد بيانات وبرامج ومعلومات، وامتد ليشمل نسبة كبيرة من الأفراد، بفضل الشبكات المعلوماتية وما حققته من مزايا لا يمكن إنكارها على مستوى جميع الأصعدة الثقافية والعلمية والسياسية ... إلا أنها بالمقابل فتحت مجالا لمخاطر لا يستهان بها، حيث أصبح النظام المعلوماتي محلا ووسيلة لارتكاب ما أُطلق عليه بالجرائم المعلوماتية[5].

وتعتبر الجرائم المعلوماتية صنفا جديدا من الجرائم، وذلك لارتباطها بتقنية حديثة وهي تكنولوجيا المعلومات والاتصالات، فظهر بذلك نوع جديد من المجرمين[6] لينتقل بالجريمة من صورتها التقليدية إلى أخرى إلكترونية حديثة، مما استوجب تحول الدليل الجنائي من صورته التقليدية إلى الرقمية.

وإذا كان الدليل الجنائي التقليدي يشترط لقبوله أمام القضاء أن يكون صريحا ومباشرا ودالا بذاته على الواقعة المراد إثباتها، فإن الدليل الجنائي الرقمي هو الآخر يجب أن يتوافر على خصائص كي يتم قبوله أما القضاء. وعليه فإنه في إطار هذه الإشكالية يمكن طرح التساؤل الآتي: ما المقصود بالدليل الجنائي الرقمي، وما مدى حجيته أمام القضاء المقارن؟ ولغرض البحث في هذه الإشكالية فإنه سيتم معالجة هذا الموضوع بالبحث عن ماهية الدليل الجنائي الرقمي كمطلب أول، وحجية هذا الدليل أمام القضاء الجنائي المقارن كمطلب ثاني.

المطلب الأول: ماهية الدليل الجنائي الرقمي

يتم في هذا الإطار تناول كل من مفهوم الدليل الجنائي الرقمي (فرع أول)، ثم التطرق إلى تقسيمات الدليل الجنائي الرقمي(فرع ثاني)، وأخيرا الإجراءات التقنية في جمع الأدلة الرقمية(فرع ثالث).

الفرع الأول مفهوم الدليل الجنائي الرقمي

نتناول في هذا الإطار تعريف الدليل الجنائي الرقمي أولا وخصائصه ثانيا

أولا: تعريف الدليل الجنائي الرقمي:

تنوعت التعريفات التي قيلت في شأن الدليل الرقمي أو الالكتروني وتباينت بين التوسع في مفهومه والتضييق فيه، فقد عرفته المنظمة العالمية لدليل الكمبيوتر IOCE في أكتوبر 2001 بأنه" المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية"[7]

كما عرفه البعض على أنه" الدليل المأخوذ من أجهزة الحاسب الآلي يكون في شكل مجلات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة ويتم تقديمها في شكل دليل يمكن اعتباره أمام القضاء"[8]

وعرفه الدكتور عمر محمد بن يونس على أنه: "الدليل الذي يجد له أساسا في العالم الافتراضي، ويقود إلى الجريمة"[9]

أما الدكتور مصطفى محمد موسى فعرفه بأنه: " المعلومات المخزنة أو المنقولة بصفة رقمية، ويُعتمد عليها في التحقيقات، وأمام المحكمة إما بالإدانة أو البراءة"[10]

وعليه يمكن القول أن الدليل الرقمي هو ذلك الدليل الذي ينشأ في العالم الرقمي، والذي يكون على شكل مستخرج مادي يتم قبوله في جلسة المحاكمة.

ثانيا:خصائص الدليل الجنائي الرقمي:

للدليل الجنائي الرقمي عدة مزايا يتصف بها دون غيره من الأدلة الجنائية؛ فهو دليل علمي غير مرئي، ذو طبيعة تقنية، يصعب التخلص منه ويكون قابلا للنسخ وفقا للتفصيل الآتي:

1- دليل غير مرئي: أي يتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، بل إدراكها يتم باستخدام أجهزة ومعدات الحاسب الآلي (Hardware) ونظم برمجيات الحاسوب (Software).[11]

2- الدليل الرقمي دليل علمي: وبالتالي يستبعد تعارضه مع القواعد العلمية السلمية وفقا لقاعدة في القضاء المقارن مفادها " إن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة".[12]

3- الدليل الرقمي من طبيعة تقنية: حيث أن التقنية تنتج نبضات رقمية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي، فهي ذات طبيعة ديناميكية فائقة السرعة، تنتقل من مكان إلى آخر عن طريق شبكات الاتصال.[13]

4- قابلية الدليل الرقمي للنسخ: حيث أن هذه الخاصية تقلل أو تعدم مخاطر إتلاف الدليل الأصلي، حيث تتطابق طريقة النسخ مع طريقة الإنشاء، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل من الفقد والتلف، عن طريق نسخ طبق الأصل من الدليل[14].

5- صعوبة التخلص من الدليل الرقمي: حتى في حالة إصدار أمر من الجاني بإزالته فيمكن استرجاعه عن طريق برامج الاسترجاع.

الفرع الثاني: تقسيمات الدليل الرقمي:

للدليل الرقمي أشكال مختلفة، وقد أشارت وزارة العدل الأمريكية سنة 2002 أن الدليل الرقمي يمكن تقسيمه إلى ثلاث أقسام وهي كالتالي[15]:

1- السجلات المحفوظة في الحاسوب: وتشمل الوثائق المكتوبة والمحفوظة مثل (البريد الإلكتروني ورسائل غرف الدردشة، وملفات معالجة الكلمات).

2- السجلات التي تم إنشاؤها بواسطة الحاسوب: وتعد مخرجات أصلية للحاسوب، حيث لم يشارك الأشخاص في إعدادها، مثل (سجلات الهاتف، وفواتير أجهزة السحب الآلي للنقود).

3- السجلات المختلطة: التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه عن طريق الحاسب الآلي، منها أوراق العمل المالية التي تم حفظها بالإدخال ثم معالجتها عن طريق برنامج Excel لإجراء العمليات الحسابية عليها.

في حين ذهب بعض الفقهاء إلى تقسيم الدليل الرقمي إلى:

القسم الأول: الأدلة الرقمية الخاصة بأجهزة الكمبيوتر: وتشتمل على جهاز الحاسب الآلي وملحقاته كالطابعات وكذا المواديم والأقراص المدمجة(CD) وذاكرة الفلاش (usb) والأشرطة الممغنطة.[16]

القسم الثاني: الأدلة الرقمية الخاصة بالشبكة الدولية للمعلومات (الإنترنت): كالبريد الإلكتروني وغرف المحادثات.

القسم الثالث: الأدلة الخاصة ببروتوكولات نقل وتبادل المعلومات بين الأجهزة المتصلة بشبكة الإنترنت ومن أمثلتها بروتوكول(TPC/Ip)[17]، الكوكيز(Cookies)[18].

الفرع الثالث:الإجراءات التقنية في جمع الأدلة الرقمية:

لغرض جمع الدليل الرقمي الذي يثبت الجريمة المرتكبة ونسبتها إلى المتهم، فإن الخبير أو المحقق يحتاج لمجموعة من الوسائل التي تتنوع من مادية (أولا) ووسائل إجرائية(ثانيا)

أولا: الأدوات المادية في جمع الأدلة الرقمية: وهي الأدوات الفنية التي تستخدم في بيئة النظام المعلوماتي ومن هذه الوسائل:

1- عنوان بروتوكول الإنترنت (IP، MAK، البريد الإلكتروني، برامج المحادثة): يعتبر عنوان الإنترنت المسئول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، وهو يتواجد بكل جهاز مرتبط بالإنترنت، ويتكون من أربعة أجزاء حيث أن الجزء الرابع يحدد جهاز الحاسوب الذي تم الاتصال منه، وعليه في حالة اقتراف إحدى الجرائم يكون من السهل التعرف على رقم الجهاز الذي تم من خلاله ارتكاب العملية وبالتالي تحديد الجاني [19].

2- البروكسيPROXY يعمل البروكسي كوسيط بين المستخدم والشبكة، وتقوم فكرته على أساس تلقيه طلبا من المستخدم للبحث عن صفحة ما ضمن ذاكرة (Cache) المحلية المتوفرة لديه، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فيقوم بإرسالها دون الرجوع إلى الشبكة، أما في حالة عدم تنزيلها من قبل فإنه يعمل كمزود زبون ويقوم بإرسال الطلب إلى الشبكة

العالمية حيث يستخدم أحد عناوين(IP)، ومن أهم مزاياه أن ذاكرة (cache) المتوفرة لديه تحفظ تلك المعلومات التي تم تنزيلها، وفي حالة وجود أي إشكال يتم فحص تلك العمليات المحفوظة والتي تخص المتهم والموجودة عند مزود الخدمة [20].

3- برامج التتبع: تقوم هذه البرامج بالتعرف على محاولات الاختراق وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ومثاله برنامج Hack tracer وهو مصمم للعمل في الأجهزة المكتبية، وعندما يرصد محاولة للاختراق يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ بعملية مطاردة تستهدف اقتفاء أثر مرتكب عملية الاختراق، حتى يصل إلى الجهاز الذي حدثت منه العملية [21].

4- نظام كشف الاختراق: يرمز له ب IDS وهي برامج تقوم بمراقبة بعض العمليات التي تتم على مستوى الشبكة أو الحاسب، مع تحليلها بحثا عن وجود أي إشارة تدل على وجود تهديد، حيث أنه يسجل الأحداث فور وقوعها ويقارن نتائج التحاليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية، وفي حالة اكتشافه لأحدى هذه الصفات يقوم بإنذار مدير النظام ويسجل البيانات الخاصة بذلك الاعتداء[22].

ثانيا: الوسائل الإجرائية: ويقصد بها تلك العمليات التي تهدف إلى جمع الدليل الرقمي، وذلك بتحديد وقوع الجريمة، وانتهاء بنسبتها لمرتكبها، ومن هذه الوسائل:

1- اقتفاء الأثر: تتم عملية تتبع المجرم المعلوماتي خصوصا في حالة إذا لم يقم بمحو آثاره، وهذا عن طريق اقتفاء أثره باستخدام مجموعة من البرامج المساعدة وصولا إلى الحاسب الذي تمت منه العملية.

2- الاستعانة بالذكاء الاصطناعي: يمكن الاستعانة به في حصر الحقائق والاحتمالات والأسباب والفرضيات ومن ثم استنتاج النتائج على ضوء عمليات حسابية يتم تحليلها بالكمبيوتر وفق برامج صممت خصيصا لذلك، حيث أنها تعتمد على نظرية الاحتمالات بإعطاء كافة الاحتمالات، ثم أكثر الاحتمالات وصولا إلى الاحتمال الأقوى، مع إعطاء الأسباب [23].

3- التوقيف خلال فترة التحقيق: من العوامل المساعدة في جمع الأدلة الرقمية وسائل التحفظ على المتهم، ولعل من أبرزها التوقيف الذي يعتبر من إجراءات التحقيق وفق ضوابط حددها القانون وهذا للمحافظة على الأدلة من عملية الإتلاف أو الإخفاء [24].

المبحث الثاني: حجية الدليل الرقمي أمام القضاء الجزائي:

يتمتع القاضي الجزائي بسلطة واسعة في تقدير الأدلة حتى وإن كانت علمية مثل الدليل الرقمي، فإن لقبوله يجب توافر شروط معينة (كفرع أول) ثم على أي أساس تتحدد سلطة القاضي الجنائي في قبول الأدلة الرقمية (كفرع ثاني).

الفرع الأول: شروط قبول الدليل الرقمي أمام القضاء:

الدليل الرقمي مثله مثل باقي الأدلة التقليدية لكي يتم قبوله أمام القضاء الجزائي لا بد أن يتوافر على مجموعة من الشروط وإلا تم رفضه، وتتمثل هذه الشروط في:

أولا: مشروعية الدليل الرقمي:

في مقبوليته يشترط أن يتم الحصول عليه بطرق مشروعة موافقة للقانون، وعليه فإن استخدام وسائل غير مشروعة للحصول على الأدلة الرقمية يترتب عليها بطلان الإجراءات وعدم صلاحيتها لأن تكون أدلة إدانة في المواد الجزائية، ومن هذه الإجراءات استخدام الإكراه المادي أو المعنوي، أو الغش ضد الجاني مثلا لفك شفرة الدخول إلى النظام[25].

ويعتبر مشروعية الدليل إحدى أهم ما أوصى به المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات، والذي عقد في عاصمة البرازيل في الفترة 4-9 سبتمبر 1994 في مجال حركة إصلاح الإجراءات الجنائية بالتوصية رقم 18 التي تنص" كل الأدلة التي يتم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة، ولا يمكن التمسك بها أو مراعاتها" كما أشار إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في جرائم الحاسب الآلي والجرائم التقليدية في بيئة تكنولوجيا المعلومات وإلا ترتب عليه بطلان الإجراء، فضلا عن تقرير المسؤولية لرجل السلطة العامة الذي انتهك القانون[26].

ثانيا: بلوغ اقتناع القاضي درجة اليقين:

يعتبر شرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة تقليدية أو حديثة[27]، فالدليل الرقمي يجب أن يكون غير قابل للشك إذ أن هذا الأخير يفسر لمصلحة المتهم، طبقا للمادة 45 من الدستور الجزائري[28]، وإذا كان القاضي في الجرائم التقليدية يستطيع الوصول إلى اليقين عن طريق الحس والمعاينة والتحليل والاستنتاج، فإن الجزم بوقوع الجريمة المعلوماتية يحتاج من القاضي نوعا آخر من المعرفة العلمية بالأمور المعلوماتية، إذ أن الجهل بهذه الأمور يؤدي إلى التشكيك في قيمة الدليل وبالتالي يقضي بالحكم بالبراءة، ويستفيد المتهم المعلوماتي من هذا الشك.

ويعتبر الرأي الغالب في الفقه الكندي أن مخرجات الحاسوب تتوافر على درجة عالية من اليقينية، وهو ما ذهب إليه القضاء الأمريكي إلى أن أفضل أدلة الإثبات هي النسخ المستخرجة من البيانات المخزنة في الحاسوب.

ثالثا: شرط مناقشة الدليل الرقمي:

من أهم قواعد الإجراءات أن القاضي لا يبني حكمه إلا على أدلة طرحت أمامه في الجلسة، ويترتب عن ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى، وأن تُمنح للخصوم فرصة الإطلاع عليه ومناقشته، وهو ما قضت به المادة 2/212 ق.إ.ج.ج [29] وهو ما ينطبق كذلك على الدليل الرقمي أيا كان شكل ذلك الدليل، وتقوم مناقشة الدليل على أمرين اثنين؛ أولهما إتاحة الفرصة للخصوم للإطلاع على الدليل الرقمي والرد عليه حتى يتمكن الخصوم من استيفاء حقوق الدفاع ومواجهة هذه الأدلة، أما الأمر الثاني أن يكون للدليل الرقمي أصل في أوراق الدعوى وذلك حتى يكون اقتناع القاضي مبني على أساس[30].

ولقد أدرج المشرع الجزائري مبدأ المواجهة وأحاطه بضمانات قوية في المادتين 100، 101 ق.إ.ج.ج

الفرع الثاني: سلطة القاضي الجنائي في قبول الأدلة الرقمية:

تتحدد سلطة القاضي الجنائي في قبول الدليل الرقمي حسب طبيعة نظام الإثبات السائد، وتنقسم هذه الأنظمة إلى: النظام اللاتيني (أولا)، النظام الأنجلوسكسوني(ثانيا) وهذا كما يلي:

أولا: النظام اللاتيني: يطلق عليه بنظام الأدلة الإقناعية (نظام الإثبات الحر) وفيه أن المشرع لا يحدد أدلة الإثبات ووسائله بل يترك الحرية للقاضي في تأسيس حكمه وفقا لاقتناعه الشخصي وبدون أن يفرض عليه دليل معين، ومن هذه التشريعات نجد كلا من الفرنسي والجزائري والمصري حيث أن المشرع الجزائري كرس المبدأ في نص المادة 1/212 ق.إ.ج.ج[31].

وبتطور دور الإثبات العلمي مع ظهور الدليل الرقمي جعل القاضي في هذا النظام يضطر للتعامل مع الأدلة المستحدثة بغية اكتشاف الجرائم، ونتيجة لهذا المبدأ فإن القاضي غير مقيد بالأدلة التي يقدمها أطراف الدعوى لأن من حقه أن يبادر بنفسه لاتخاذ جميع الإجراءات بحثا عن الأدلة اللازمة لتكوين قناعته، وفي سبيل ذلك له أن يوجه أوامر إلى مزود خدمة الإنترنت من أجل جمع الأدلة الرقمية كعناوين المواقع التي اطلع عليها المتهم، والملفات والحوارات التي شارك فيها، والرسائل التي أرسلها واستقبلها، كما له أن يأمر مشغل النظام بتقدير المعلومات اللازمة لاختراق النظام والولوج إلى داخله؛ كالإفصاح عن الكلمات السرية والشفرات الخاصة بتشغيل البرامج المختلفة، وله أن يأمر بتفتيش الحاسب الآلي،[32] كما أن القاضي الجنائي وفق هذه التشريعات له أن يتأكد أولا من قبول الدليل ومدى صحته ومصداقيته.

ثانيا: النظام الأنجلوسكسوني: يطلق عليه بنظام الإثبات المحدد أو نظام الأدلة القانونية، حيث أن المشرع يحدد فيه الأدلة مسبقا، فلا يجوز للقاضي أن يخرج عليها، وعليه فإنه في حالة توافر الدليل على شروط حددها وقيدها المشرع يكون القاضي ملزما بتأسيس حكمه حتى وإن كان القاضي غير مقتنع به. ومن الدول التي أخذت به إنجلترا وأمريكا وجنوب أفريقيا[33].

ويحكم الدليل في هذا النظام قاعدتان؛ الأولى قاعدة استبعاد شهادة السماع، والثانية قاعدة الدليل الأفضل

1- قاعدة استبعاد شهادة السماع: والمقصود بها تلك الشهادة التي يكون الشاهد الذي أدلى بها قد سمعها ولم يشارك في وضعها بإحدى حواسه، ويعتبر الدليل الرقمي شهادة سماع كونه يتضمن أقوالا ومواد قام بوضعها الإنسان في الحاسوب؛ فهي في الحقيقة حدثت خارج المحكمة وبالتالي يتم استبعادها من طرف هذه الأخيرة، إلا أن هناك حالات استثنائية يتم فيها قبول شهادة السماع كدليل في الدعوى الجزائية أهمها: البيانات والمعلومات التي يتم الحصول عليها من الكمبيوتر، وقد قبل القضاء الإنجليزي هذا النوع من الأدلة في العديد من المناسبات مثالها قضية (R.V.Wood) حيث أن المحكمة أجابت في هذا الإطار"أن الورقة الناتجة عن الكمبيوتر مقبولة وفقا للشريعة العامة وتصلح للإثبات" وقد قبلتها على أساس أنها شهادة مباشرة [34].

2- قاعدة الدليل الأفضل: والمقصود بها أنه لأجل إثبات محتويات كتابة أو سجل أو صورة فإن أصل الكتابة أو السجل أو الصورة يكون مطلوبا، وهو ما أقره القانون الأمريكي في المادة 1002 من قانون الإثبات بنصها "باستثناء ما هو مقرر في هذا القانون أو بقانون خاص يصدر عن الكونجرس فإنه عند إثبات مضمون الكتابة والتسجيل والصورة فإنه يلزم توافر أصل الكتابة والتسجيل والصورة "، إلا أنه مع ظهور المستندات الإلكترونية حدث تعديل في قانون الإثبات؛ ففي المادة 1/101 من قانون الإثبات الأمريكي سمح الاعتراف بالمواد الإلكترونية كي تحظى بذات الاهتمام التي تحظى به الأدلة الأخرى.

وقد ذهب المشرع الأمريكي أبعد من ذلك في نص المادة 3/1001 وهذا في إطار اعتباره أن الكتابة الموجودة داخل الجهاز في صورة كهرومغناطيسية من قبيل النسخة الأصلية وبالتالي لا تصطدم مع قاعدة الدليل الأفضل وورد فيها " إذا كانت البيانات مخزنة في جهاز حاسوب أو مماثل، فإن مخرجات الطباعة أو أي مخرجات أخرى يمكن قراءتها بالنظر إلى ما تم إظهارها وتبرز انعكاسا دقيقا للبيانات تعد بيانات أصلية" [35]

هذا وقد أقر القانون الأمريكي في المادة 1003 من قانون الإثبات الأمريكي " أن النسخة المطابقة للأصل تُقبل كالأصل إلا إذا - أولا: أثير حولها تساؤل جدي يتعلق بجديتها وأصالتها – ثانيا إذا كانت الظروف لا تسمح بقبول النسخة المطابقة للأصل لكي تحل محل الأصل."

الخاتمة:

من خلال ما سبق يتضح أن الدليل الإلكتروني ومن خلال طبيعته الفنية يصلح لأن يكون دليلا لإثبات الجريمة الإلكترونية بالرغم من أنه دليل غير مادي، فقد يسهل إخفاؤه كما يسهل إثباته في ذات الوقت، ضف إلى ذلك أن الجريمة ومن رائها دليل إثباتها قد يكونا متصلين بدولة أخرى،مما يزيد في صعوبة الحصول عليه الأمر الذي قد ينجم عنه تنازع في الاختصاص القضائي لتمسك كل دولة بسيادتها، كما أن عملية الإثبات هذه تحتاج إلى الخبرة التقنية والفنية والتي قد لا تتوافر في رجال إنفاذ القانون.

ومن النتائج التي يمكن حصرها في هذا الإطار:

1- إن التقدم العلمي والتكنولوجي أوجد جرائم من نوع جديد، وبالتالي كان إثباتها هو الآخر من النوع غير المألوف أُطلق عليه بالدليل الرقمي؛ الذي هو عبارة عن معلومات مخزنة على شكل نبضات مغناطيسية في أجهزة الحاسوب وملحقاته.

2- من خصائص هذا الدليل الرقمي أنه يصعب الحصول عليه لأنه ذو طبيعة غير مرئية، وسهل الإتلاف، إلا أن التطور التقني أوجد برامج يمكن عن طريقها إسترجاع الدليل الرقمي بالرغم من عملية محوه.

3- القصور الواضح في التشريع الجزائري وفي الكثير من التشريعات حول طرق الحصول على الدليل الرقمي، مما يسهل عملية إفلات المجرمين من العدالة.

4- حتى يتم قبول الدليل الرقمي أمام القضاء ينبغي أن يتوافر على مجموعة من الشروط المتفق عليه بين الأنظمة القضائية منها شرط مشروعية الدليل و يقينيته، مع ضرورة مناقشته في وقائع الجلسة.

وهناك جملة من التوصيات التي ينبغي الإشارة إليها وهي:

- دعوة القضاء إلى قبول الدليل الرقمي كدليل أصلي ثابت لا يقبل التشكيك ولا يطعن فيه إلا بعدم المشروعية فقط.
- إدخال الوسائل الحديثة في جمع الدليل الرقمي كأساليب قانونية ضمن نطاق قانون الإجراءات الجزائية.
- تدريب الخبراء والمحققين وحتى قضاة الحكم على كيفية التعامل مع الدليل الرقمي للحد من ظاهرة الإجرام المعلوماتي.

الهوامش:

(1) طه أحمد طه متولي، الدليل العلمي وأثره في الإثبات الجنائي، رسالة للحصول على درجة الدكتوراه في الحقوق، جامعة طنطا، 2007 ص 10.

(2) خالد ممدوح إبراهيم، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، 2009 ص 177.

(3) هلالي عبد اللاه أحمد، النظرية العامة لإثبات الجنائي، (دراسة مقارنة)، المجلد 01، دار النهضة العربية، القاهرة. (د.س.ن) ص 20.

(4) يطلق مصطلح النظام المعلوماتي على الحاسب بما يشتمله من شاشة عرض ولوحة مفاتيح، بالإضافة إلى المكونات الأخرى المتصلة به من طابعات وماسحات ضوئية وشبكة المعلومات، وبما يشتمل عليها من برامج وقواعد بيانات. للمزيد راجع أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الإسكندرية، 2006 ص 19.

(5) عرف الفقيه الألماني تيدمان الجريمة المعلوماتية" كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يستخدم عن طريق الحاسب" للمزيد راجع قارة أمال، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون، كلية الحقوق بن عكنون، 2002 ص17.

(6) في إحدى الدراسات تم تقسيم المجرمين المعلوماتيين إلى ستة أقسام: المجموعة الأولى: العاملون المتذمرون غير الراضين عن منشأتهم، المجموعة الثانية: العاملون داخل المنشأة يجدون رغبة للاختراق وتحدي ذكاء مصممي النظام، المجموعة الثالثة: العاملون داخل المنشأة لديهم مشاكل خاصة تدفعهم لارتكاب الجرائم، المجموعة الرابعة: عملاء المنشأة لديهم مشاكل مع منشأتهم ويريدون الانتقام، المجموعة الخامسة: أفراد لديهم دوافع سياسية لاختراق نظم المعلومات السرية، المجموعة السادسة: مجرمون بطبيعتهم سواء بمساعدة النظام المعلوماتي أو من غيره. للمزيد راجع أحمد خليفة الملط، المرجع السابق، ص62.

(7) مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1 ، مطابع الشرطة القاهرة، 2008 ص213.

(8) ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر 2006 ص88.

(9) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة عين شمس، 2004 ص969.

(10) مصطفى محمد موسى، المرجع السابق، ص 217.

(11) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، ص61.

(12) عمر محمد أبو بكر بن يونس، المرجع السابق، ص977.

(13) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع عمان 2011 ص 232.

(14) وهو ما أخذ به المشرع البلجيكي، بمقتضى القانون الصادر في 28 نوفمبر 2000، بإضافة المادة 39 من قانون التحقيق الجنائي، التي أجازت ضبط الأدلة الرقمية مثل: نسخ المواد المخزنة في نظام المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية. للمزيد راجع، عمر محمد أبو بكر بن يونس، المرجع السابق، ص 978.

(15) عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، بحث مقدم إلى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية الرياض ص 14.

(16) ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر 2006 ص 88.

(17) بروتوكول (TPC/IP) ويعتبر من أهم وأشهر البروتوكولات المستخدمة في شبكة الإنترنت ويتكون من: بروتوكول(User Datagsam protocol/UDP)،بروتوكول (Transmission Control Protocol/TCP)، بروتوكول(Internet /IP Protocol) ومن مميزات هذه البروتوكولات أنها تقوم بالتعاون فيما بينها بنقل المعلومات الخاصة بالمستخدم وفقا لنظام هيكلة تبادل المعلومات المعروف باسم (TCP/IP with OSI). للمزيد راجع سيدي محمد لبشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية، دراسة تحليلية تطبيقية، رسالة الماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض 2010 ص 73.

(18) الكوكيز (COOKIES): أداة يتم من خلالها جمع البيانات التعريفية الخاصة بالمستخدم عن طريق الإتصال بين الخادم (Server) والقرص الصلب لحاسب المستخدم. للمزيد راجع سيدي محمد لبشير، المرجع السابق، ص 73.

(19)، (20) خالد ممدوح إبراهيم، المرجع السابق ص 304.

(21) ومن أمثلة هذه البرامج برنامج Hack tracer v 1.2 يتكون من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الإختراق، يحتوي على إسم وتاريخ الواقعة وعنوان IP الذي تمت من خلاله عملية الاختراق واسم الدولة التي تمت منها المحاولة، وصولا إلى الحاسوب الذي تمت منع عملية الاختراق. أنظر، خالد ممدوح إبراهيم، المرجع السابق ص 306

(22)،(23) خالد ممدوح إبراهيم، المرجع السابق ص 306، 308.

(24) خالد عياد الحلبي، المرجع السابق ص 215.

(25) علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، 26-28 أفريل 2003 ص38

(26) للمزيد راجع عائشة بن قارة مصطفى، المرجع السابق ص218 مأخوذ من:

XV(15eme) Congrès International de droit pénal ، Rio de Janeiro ،Brésil، 4-9 septembre 1994، Association Internationale de droit pénal، R.I.D.P ، 1er et 2eme trimestres 1995، p38.

(27) الجزء الذي يتضمن الإقتناع الشخصي للقاضي الجزائي من نص المادة 307 من قانون الإجراءات الجزائية الجزائري.. ... ولم يضع القانون لهم سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم : هل لديكم إقتناع شخصي ؟

(28) نص المادة 45 من المرسوم الرئاسي رقم 96-438 المتعلق بإصدار نص تعديل الدستور الجزائري ورد فيها" كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية إدانته، مع كل الضمانات التي يتطلبها القانون ".

(29) المادة 02/212 ق.إ.ج.ج "ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

(30) المادة 01/212 ق.إ.ج.ج " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص..."

(31) وهو ما أكدته محكمة النقض المصرية بقولها" إنه محظور على القاضي أن يبني حكمه على دليل لم يطرح أمامه في الجلسة، يستوي في ذلك أن يكون دليلا على الإدانة أو البراءة، وذلك كي يتسنى للخصوم الإطلاع عليه والإدلاء برأيهم فيه". للمزيد راجع عائشة بن قارة مصطفى، المرجع السابق ص273.

(32) أنظر في هذا الإطار عائشة بن قارة مصطفى، المرجع السابق ص194.

(33) شيماء عبد الغاني محمد عطا لله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة الإسكندرية، 2007 ص 387.

(34) للمزيد راجع عمر محمد أبو بكر بن يونس، المرجع السابق، ص958.

(35) وقد عرفت المنظمة الدولية لأدلة الحاسوب (IOCE) النسخة المطابقة للأصل بأنها: نسخة رقمية دقيقة لكل البيانات أو المعلومات الموجودة في البنود الأصلية".

Duplicate Digital Evidence is ''an accurate digital reproduction of all data objects contained on the original physical item''.