تاريخ الاستلام: 2019/06/29 تاريخ القبول: 2019/10/02

شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية

Authentic Digital Guide In proving cyber crime

د. بن الطيبي مبارك [1] btmadrar@yahoo.fr

جامعة أحمد دراية بادرار

د/ رحموني محمد ramouni4@yahoo.fr

جامعة أحمد دراية- أدرار

ملخص

الجريمة الالكترونية من الجرائم المستحدثة، ومعالجتها من الناحية القانونية تتم في إطار شمولي باعتماد المحاور الرئيسية للحماية الجزائية، حيث أن فخصوصية التجريم يلزمها خصوصية في الإثبات وفي الملاحقة.

الكلمات المفتاحية: جريمة إلكترونية، حجية، دليل رقمي، إثبات.

Abstract:

Electronic crime is an emerging crime; Their legal treatment must take place within a holistic framework; The specificity of criminalization requires specificity in evidence as well as privacy in prosecution

key words: Electronic crime; Authentic; Digital proof; Proof

المؤلف المرسل: رحموني محمد ، **الإيميل:** *ramouni4@yahoo.fr*

مقدمة

تعتبر الجريمة الالكترونية من الجرائم المستحدثة، وعليه فإن معالجتها من الناحية القانونية يجب أن تتم في إطار شمولي، ذلك أن اعتماد المحاور الرئيسية للحماية الجزائية فيما بينها لا يخلو من التكاملية، فخصوصية التجريم يلزمها خصوصية في الاثبات وكذلك خصوصية في الملاحقة.

أما خصوصية التجريم فهي نابعة من وقوع غالبية هذه الجرائم على العالم الافتراضي دون المادي، وذلك حتى مع ملامسة بعضها للعالم المادي، فإنها تبقى من الخصوصية بما يجعلها متمايزة عن غيرها من الجرائم والتي تتطلب خصوصية في التجريم لئلا يفلت مقترفها من العقاب.

ومن ناحية خصوصية الإثبات في هذا النوع من الجرائم فإنها لا تخلو من الصعاب الجمة والتي تكتنف رصد واحتواء الدليل المتحصل من مسرح الجريمة سواء المادي أو الافتراضي، وذلك كون الأدلة الرقمية صعبة الاحتواء وسهلة الاختفاء والمحو. وكذلك انه يمكن التضليل بشأن كشفها أو الاطلاع على مضمونها[1].

من خلال هذه الورقة البحثية سنحاول أن نناقش الدليل الرقمي أو الإلكتروني ومدى حجيته في إثبات الجريمة الإلكترونية في التشريع الجزائري؟

حيث ستتم هذه المعالجة اعتمادا على منهج علمي تحليلي، لمختلف النصوص القانونية ذات العلاقة بموضوع الدراسة سواء في قانون الإجراءات الجزائية أو مختلف النصوص القانونية الخاصة الأخرى والتي تتضمن أحكاما خاصة بالجريمة المعلوماتية.

وبناء عليه تم تقسيم الدراسة إلى مبحثين: الأول يعالج مفهوم الدليل الرقمي، أما الثاني فيتناول أحكام قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية.

المبحث الأول: مفهوم الدليل الرقمي

من المعلوم أن الدليل الرقمي من المواضيع التي حظيت باهتمام فقهاء القانون الجنائي والمشرعين، وهذا في مجال الإثبات الجنائي على اختلاف نظمه، وهذا الاهتمام جاء نتيجة لكون الدليل الرقمي عامل مهم في إثبات الجريمة من عدمه، وهذا في حد ذاته يتطلب منا التعرض إلى مفهوم الدليل الرقمي من خلال تعريفه وبيان طبيعته .

المطلب الأول: تعريف الدليل الرقمي وخصائصه

نتعرض في هذا المطلب إلى بيان مختلف التعريف والدلالات المتعلقة بالدليل الرقمي، كما نعرج أيضاً على خصائصه التي تميزه عن غيره، نبين كل ذلك في النقاط الجزئية التالية:

الفرع الأول: تعريف الدليل الرقمي

الدليل الرقمي، وهو ما يعرف بأنه " الدليل الذي يجد له أساساً في العالم الافتراضي إلي الجريمة "[2] .

والدليل الرقمي هو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل الرموز والنصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم يعبر عن فكر وقول يطلق عليه الكتابة الرقمية بالمعني الواسع، التي لا تشمل الكتابة التقليدية علي الورق فحسب، وإنما تشمل أيضا الكتابة التي تتم عن طريق وسائل الاتصال الحديثة (شبكة المعلومات الدولية وما في حكمها) مهما كانت الدعامة المستخدمة في تثبيتها.

ولهذا نجد بعض الاتفاقيات الدولية[3] قد تبنت هذا المفهوم الواسع للكتابة، وكذلك بعض التشريعات المقارنة.

الفرع الثاني: خصائص الدليل الرقمي

يتميز الدليل الرقمي بمجموعة من الخصائص نوردها فيما يلي[4]:

أولا: الدليل الرقمي دليل غير ملموس

والأصل أن الدليل الرقمي غير مادي ، يتكون من بيانات و معلومات ذات هيئة رقمية غير ملموسة وإخراجه في شكل مادي ملموس يتطلب الاستعانة بأجهزة الحاسب الآلي وأدواته واستخدام نظم برمجية حاسبية، ويتميز بالسرعة و السهولة وصعوبة محوه أو تحطيمه وإن حاول الجاني محو الدليل الرقمي، فإن هذه المحاولة بذاتها تسجل عليه كدليل.

ثانيا: الدليل الرقمي دليل فني

الطبيعة الفنية للدليل الرقمي تكمن في إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان قد تعرض للغش والتحريف، هذا من ناحية الجانب الايجابي، أما من حيث الجانب السلبي، فإن ذلك يتمثل في الاستخدام غير المشروع أو غير المصرح به للحاسب الآلي والانترنت وما عرف بجرائم الإلكترونية أو المعلوماتية وما يكتنف ذلك من مشكلات علي المستوى التنظيمي والقانوني والتقني، الأمر الذي يتطلب وسائل تقنية وقواعد قانونية تحيطه بسياج من الحماية وهو ما أدي إلي صدور العديد من التشريعات كمحاولة لوضع ضوابط وتنظيم قانوني بقصد توفير الحماية اللازمة للمستخدمين والقائمين على تقديم خدمة الإنترنت.

ثالثا: الدليل الرقمي يعتمد على استخدام أجهزة لتحليل وفهم فحواه

إن فهم مضمون الدليل الرقمي يعتمد على علم الكمبيوتر والذي يلعب دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون الدليل الرقمي، وهذا النوع من العلوم تتم الاستعانة به في الكشف عن مدى تلاعب بمضمون هذا الدليل، و فكرة التحليل التناظري الرقمي تبدوا من الوسائل المهمة للكشف عن مدى مصداقية الدليل، ومن خلالها يتم التأكد من مدى إمكانية حصول العبث في النسخة المستخرجة أم لا[5].

المطلب الثاني: طبيعة الدليل الإلكتروني

تتنوع الادلة الإلكترونية وطبيعتها لا تخرج عن أن تكون ذات طبيعة مادية، أو طبيعة معنوية، فالأدلة المادية يقصد بها تلك الادلة التي يمكن إدراكها بالحواس، فتتميز بطبيعة مادية محسوسة كوجود الشيء المسروق في حيازة الجاني، أو ضبط الجاني حاملا سلاحا استعمل في ارتكاب الجريمة، بمعنى آخر الادلة المادية هي التي تخرج من عناصر مادية معبرة عن نفسها، ولها تأثير في اقتناع القاضي بطريقة مباشرة.

وفيما يخص الأدلة المعنوية فهي عكس الأدلة المادية، أي ليس لها وجود مادي ملموس يعبر عنها، سواء كان هذا الأمر بالقول، أو الإيحاء أو الكتابة، فهذه الادلة يطلق عليها تعبير الأدلة الناطقة، وهذا راجع إلى أن هذه الادلة تصل للقاضي عن طريق لسان الغير كاعتراف المتهم وشهدة الشهود، وبقول آخر هي تلك الادلة الصادرة من إرادة شخصية والمتجسدة في أقوال الغير، وتؤثر في اقتناع القاضي بطرقة غر مباشرة.

والإشكال المثار هو حول طبيعة الدليل الإلكتروني سواء كانت مادية أو معنوية. إن الدليل الإلكتروني بأنواعه ذو طبيعة مادية مهما كان شكله وسواء كان في شكل مخرجات ورقية أو غير ورقية وغيرها ومنه نقول أن الادلة الإلكترونية لها طبيعة مادية وهذا أمر لا يمكن إنكاره باعتبار أن التطور التكنولوجي باعتبار أنه حتى وإن كانت غير ذلك فسيتم إخراجها في شكل دعامات، عبارة عن أشرطة ممغنطة أو أقراص مغناطيسية إلى غير ذلك وبالتالي فهي ستصبح ذات طبيعة مادية.

في الوقت الحالي سمح باستخراج مختلف المعلومات من جهاز الحاسوب الآلي أو التقنيات المرتبطة به، في شكل أشياء مادية ملموسة لتصبح دليل يعتمد عليه في قضية ما وتثبت به[6].

المطلب الثالث: نطاق الدليل الإلكتروني

تعتبر الجريمة الإلكترونية أو المعلوماتية نطاقا للعمل بالدليل الإلكتروني، أو محلا له، وعليه نحاول مناقشة مفهومها وخصائصها في النقاط الجزئية التالية:

الفرع الأول: تعريف الجريمة الإلكترونية

الجريمة بوجه عام هي كل نشاط يقع بما يخالف القانون، فإذا ما تم هذا النشاط أو الفعل بواسطة الوسائل التكنولوجية الحديثة الممثلة أو عبر وسائط تقنية علمية يمكن وصف النشاط أو الفعل حينئذ بالجريمة الإلكترونية، وفيما يلي نبين مختلف التعريفات المتعلقة بالجريمة الإلكترونية:

أولاً: التعريف الفقهي للجريمة الإلكترونية

لم يتوصل الفقه إلى تعريف جامع مانع للجريمة الإلكترونية، وقد تعددت التعريفات الفقهية وفق المنظور الذي تبناه الفقيه أو اعتمده من خلال العناصر المتصلة بآليات ارتكابها أو بيئة ارتكابها أو صفات مرتكبيها، ذلك ما نبينه في الآتي:

1- فمن حيث أو نمط السلوك محل التجريم:

تعرف الجريمة الإلكترونية في هذا الإطار على أنها: " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه[7]." وتعرف الجريمة الإلكترونية أيضاً بأنها "نمط من أنماط الجرائم المدونة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات[8].

2- من حيث وسيلة ارتكاب الجريمة:

من هذا التصور تتحقق الجريمة الإلكترونية باستخدام الكومبيوتر كوسيلة لارتكابها فيعرفها البعض بأنها فعل إجرامي يستخدم الكومبيوتر في ارتكابه كأداة رئيسية، ويصف هذه الجريمة مكتب تقييم التقنية في الولايات المتحدة الأمريكية فيقول بأنها " الجريمة التي تلعب فيها البيانات الكومبيوترية والبرامج المعلوماتية دورا رئيسيا[9]."

3- صفات شخصية لمرتكب الفعل (المعرفة التقنية المعلوماتية):

ومنها التعريف الذي وضعته وزارة العدل الأمريكية في دراسة أعدها معهد ستانفورت للأبحاث واعتمدتها هذه الوزارة في دليلها لعام 1979 والذي يعرفها بأنها: " أي جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها[10]."

أما منظمة التعاون الاقتصادي والتنمية OECD فقد عرفتها بأنها " كل فعل او امتناع من شأنه الاعتداء على الاموال المادية او المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[11].

ويرجح اعتماد هذا التعريف على اعتبار أنه اتسع ليشمل مختلف التصورات والاحتمالات المرتبطة بالجريمة الإلكترونية، كما أنه لا يغفل طابعها الفني والتقني، مما يعطي المجال الأوسع لما تنتجه التكنولوجيا العلمية مستقبلا في هذا المجال.

4- تعريفات تعتمد معيار محل الجريمة ووسيلة ارتكابه (الكمبيوتر)

وفي هذه الحالة يعد جهاز الكومبيوتر الضحية والوسيلة، ولتفصيل ذلك نورد التعريفات التالية:

وفق هذا المنظور يعرف الفقيه Smedinghoff الجريمة الإلكترونية بأنها: " أي ضرب من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسوب." أما الفقيه Masse فعرفها بأنها" تلك الاعتداءات التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح[12]."

ثانياً: التعريف التشريعي للجريمة الإلكترونية

من المعلوم أن المشرع الجزائري وإلى وقت قريب أغفل تنظيم مجال الجريمة الإلكترونية قانونا، إلا أنه ما فتئ أن تدارك ذلك الفراغ القانوني من خلال سن قواعد قانونية لمواجهة هذه الجريمة، وذلك ما تجلى في القانون رقم 04-15 المتضمن تعديل قانون العقوبات، الذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية للمعطيات، ثم تلاه بالقانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما.

أ- تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 04-1315

بالرجوع إلى قواعد القانون 04-15 من المادة 394 مكرر إلى المادة 394 مكرر2 نجد أنه حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات، حيث حددها في المادة 394 مكرر بالآتي:

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

أما المادة 394 مكرر1 فقد أشارت إلى ما يلي:

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

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

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

ب- تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 09-1404

حددت المادة (02) منه الجريمة الإلكترونية بقولها: " يقصد في مفهوم هذا القانون بما يأتي:

- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

- منظومة معلوماتية:

أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

- معطيات معلوماتية:

أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

الفرع الثاني: خصائص الجريمة الإلكترونية

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

أولا: صعوبة اكتشاف الجريمة الإلكترونية:

توصف الجرائم الإلكترونية بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كإرسال فيروسات، وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم[15].

ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي لحصول الجريمة الإلكترونية في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الكمبيوتر الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث[16].

ثانيا: الجريمة الإلكترونية عابرة للحدود (الزمان والمكان)

المقصود بذلك أن هذا النوع من الجرائم لا يعتد بالحدود الجغرافية للدول ولا بين القارات، فمع انتشار شبكة الاتصالات بين دول العالم وأقاليمه أمكن ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم بهذه الشبكة، حيث يمكن أن يكون الجاني في بلد والمجنى عليه في بلد آخر، وهكذا فالجرائم الالكترونية تقع في أغلب الأحيان عبر حدود دولية كثيرة[17].

ثالثا: جرائم هادئة

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل والسرقة وغيرها من الجرائم، فالجرائم الالكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية الكمبيوتر[18].

رابعا: جرائم صعبة الإثبات

يعد إثبات الجريمة الإلكترونية من الصعوبة بمكان، حيث يصعب تتبعها واكتشافها، فهي لا تترك أثراً يقتفى، حيث تعتبر مجرد أرقام، فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أنها تفتقر إلى الدليل المادي التقليدي كالبصمات مثلاً [19].

ومن جهة أخرى، فهي تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها، زيادة على ذلك يعمد مرتكب الجريمة الإلكترونية إلى ممارسة الخداع عند ارتكابها والتضليل بغاية عدم التعرف على مرتكبيها.

المبحث الثاني:أحكام قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية

يتطلب قبول الدليل الرقمي كإثبات في الجريمة الالكترونية جملة من الشروط واتباع قواعد إجرائية يتعين عند مخالفتها بطلان الدليل، ذلك ما نبينه في النقاط التالية:

المطلب الأول:شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية

لا يمكن الاعتداد بالدليل الرقمي كأداة إثبات في الجريمة الالكترونية إلا إذا رافقته جملة من الشروط بمقتضاها يمكن قبوله كدليل إثبات في الجريمة الإلكترونية، وفيما يلي نبين جملة الشروط المطلوبة:

الفرع الأول:مشروعية الدليل الرقمي

الدليل الرقمي يجب أن يكون مشروعا أي أن إجراءات جمع الأدلة الرقمية المتحصلة من الحاسب الآلي إذا خالفت القواعد الإجراءات التي تنظم كيفية الحصول عليها، فإنها تكون باطلة ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجزائية[20].

فإجراءات الحصول على الأدلة الجنائية يجب أن تكون ضمن الإطار العام الذي حدده الدستور وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون باطلاً بطلاناً مطلقاً لتعلقه بالنظام العام، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها.

كأن يستخدم أعضاء الضابطة العدلية طرقًا معلوماتية في أعمال التنصت على المحادثات الهاتفية ، ومن أمثلة الطرق غير المشروعة التي يمكن أن تستخدم في الحصول على الأدلة الناتجة عن الجرائم المعلوماتية، الإكراه المادي والمعنوي في مواجهة المتهم المعلوماتي من أجل فك شفرة نظام من النظم المعلوماتية أو الوصول إلى دائرة حل التشفير أو الوصول إلى ملفات البيانات المخزنة، أو التحريض على ارتكاب الجريمة المعلوماتية من قبل أعضاء الضابطة العدلية، كالتحريض على الغش أو التزوير المعلوماتي أو التجسس المعلوماتي، والاستخدام غير المصرح به للحاسوب، والتنصت، والمراقبة الإلكترونية عن بُعد.

ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 1981/1/28م على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة، ومستمدة بطرق مشروعة، ومدة حفظها محددة زمنيًا، وعدم إفشائها أو استعمالها في غير الأغراض المخصصة لها، وحق الشخص المعني في التعرف والاطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة[21].

الفرع الثاني: يقينية الدليل الرقمي

يُشترط في الأدلة المستخرجة من الحاسوب والإنترنت أن تكون غير قابلة للشك، وتقترب نحو الحقيقة الواقعية قدر المستطاع، وتبتعد عن الظنون والتخمينات، حتى يمكن الحكم بالإدانة، ذلك أنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين.

الفرع الثالث: إمكانية مناقشة الدليل الرقمي

ويعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة فالقاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى، إذ لا يسوغ للقاضي أن يبني قراره إلا على الادلة المقدمة له في معرض المرافعات والتي حصل المناقشة فيها حضوريا أمامه[22].وهذا يعني أن الأدلة المتحصلة من جرائم الحاسوب والإنترنت سواء كانت مطبوعة أم بيانات

معروضة على شاشة الحاسوب ، أم كانت بيانات مدرجة في حاملات البيانات ، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية ، كل هذه ستكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات ، يجب أن يعرض في الجلسة بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات الحواسيب.

وبعد هذه المناقشة يكون للقاضي الحرية والاجتهاد في الحكم في الجرائم المعلوماتية وعدم الاعتماد على رأي الغير، إلا إذا كان هذا الغير من الخبراء، وقد ارتاح ضميره إلى التقرير المحرر منه وقرر الاستناد إليه ضمن حكمه وبناء عليه يكون متولدا من عقيدته وليس من تقرير الخبير[23].

المطلب الثاني: حجية الدليل الرقمي في الجريمة الإلكترونية

تعد مرحلة الحكم بمثابة المرحلة الحاسمة في الدعوى الجنائية، ذلك أن غاية هذه الأخيرة هي الوصول إلى حكم حاسم لها، حائز لقوة إنهائها، ولهذا فإن الحكم يمثل أهم إجراءات الدعوى لأنه يمثل غايتها، وعملية تقدير الأدلة تشكل جوهر هذا الحكم، حيث لا يمكن الوصول إليه وإدراكه مالم يمارس القاضي سلطته التقديرية على الأدلة محل الوقائع وفي مجال جرائم الإلكترونية فإن الدليل الإلكتروني هو الأكثر تواجدا، وهذا الدليل وكغيره من الأدلة يخضع لتقدير المحكمة[24].

المشرع الجزائري وكغيره من التشريعات المنتمية إلى النظام ذات الأصل اللاتيني لم يفرد نصوصا خاصة تحضر على القاضي مقدما قبول أو عدم قبول أي دليل بما في ذلك الدليل الرقمي وهذا أمر منطقي على اعتبار أن الجزائر تعتمد على مبدأ حرية الإثبات كقاعدة عامة في المواد الجزائية من خلال المواد 212، و307 من قانون الإجراءات الجزائية[25].

ولأن الدليل الرقمي يعتبر من الأدلة العلمية يتطلب دراية خاصة لا يمتلكها القاضي، فلا يمكن ان ينازع في قيمته الإثباتية وذلك لامتيازه بقوة استدلالية من الناحية العلمية.

وحتى وأن وقع الشك في المصداقية الدليل بسبب إمكانية العبث به ، و كذا لوجود خطأ في الحصول عليه ، فالقاضي لا يمكن أن يفصل فيها باعتبارها مسألة فنية والرأي هنا يعود إلى الخبير ، فإذا سلم الدليل من العبث و توافره فيه كل الشروط ، فإن على القاضي القبول بهذا الدليل ، لذلك فإن رفض القاضي لرأي الخبير يكون فيه تعارض مع نفسه، وعليه فإن الدليل العلمي ومنه الدليل الرقمي أصبح يقيد حرية القاضي في تقدير الأدلة، ويلزمه الحكم حتى ولو لم مقتنعا بصحة الواقعة المطروحة أمامه.

وهناك من يذهب خلافا لذلك ويكأد أن الأدلة العلمية ليست دليلا مستقلا، بل هي عبارة عن قرائن قرينة قضائية يعتمد عليه وحده في الإثبات، وإما قرينة تكميلية لا تصلح كدليل وحيد في الإثبات، بل على القاضي الاستعانة بأهل الخبرة، فرأي هذا الاتجاه أن الدليل العلمي و الرقمي مهما علا شأنهم في الإثبات الجنائي إلا أن سلطة القاضي الجنائي محددة و مسيطرة في الحقيقة و خلالها يمكن للقاضي أن يفسر الشك لصالح المتهم وأن يستبعد الأدلة التي يتم الحصول عليها بطريقة غير مشروعة و هو أمر ضروري و هذا ما جعل الحقيقة العلمية قضائية.

وتكمن مهمة القاضي في الرقابة القانونية على التقرير الفني وهو ما ورد في نص المادة 212 من قانون الإجراءات الجزائية، كما أن المادة 215 من قانون الإجراءات الجزائية، تؤكد على أن:" لا تعتبر المحاضر والتقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك."

وهو الأمر الذي أخذ به المشرع الجزائري حيث يقرر مبدأ الاقتناع الشخصي للقاضي الجزائري والذي يجعله يبسط سلطاته على جميع الأدلة بدون استثناء بما فيها تقرير الخبير[26].

مما سبق يمكن القول إنه في القانون الجزائري لا يوجد ما يتضمن قواعد خاصة بالدليل الإلكتروني لا في قانون الإجراءات الجزائية ولا حتى في القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها[27]، وعليه فالدليل الرقمي

سيكون مشروعا من حيث الوجود استصحابا للأصل في الأدلة مشروعية وجودها وذلك باعتباره من الوسائل العلمية الحديثة في الإثبات الجنائي، ولا يطرح أي إشكال من حيث اعتباره حجة، خاصة إذا تم استخلاصه وفق ضمانات قانونية وفنية تضمن صحته وسلامته، حيث يخضع للاقتناع الشخصي للقاضي كباقي الأدلة المقدمة في الدعوى[28].

خاتمة

بالرغم من كل تلك المزايا التي تحققها التكنولوجيا الحديثة ، إلا أن الواقع قد أثبت أن لها العديد من الانعكاسات السلبية الخطيرة من جراء إساءة استخدامها وهو ما يتجلى في ظهور العديد من الظواهر الإجرامية ذات الطابع التقني، أو ما يعرف بالجرائم المعلوماتية.

إن هذا النوع من الجرائم يشكل فيها الحصول على الدليل الإجرامي أحد أهم الصعوبات التي تحول دون مكافحة هذا النوع من الجرائم، أو على الأقل تجعل من هذه المكافحة شيئا صعبا، لكونه جملة من البيانات أو الإشارات الكترونية لا يفقهها الكثير من الناس من جهة ومن جهة أخرى يسهل طمس الدليل ومحوه كلياً من قبل الفاعل.

وعليه فإن النظم القانونية ونظرا لخصوصية الدليل الإلكتروني وطبيعته فإن التعامل معه يجب أن يتماشى مع هذه الطبيعة، بحث يجب أن لا يكون الحصول على هذا الدليل إلا بالطرق المشروعة والضوابط القانونية التي حددها المشرع، وبالأخص وجوب احترام وعدم انتهاك الحريات الشخصية، نظرا لسهولة انتهاكها أثناء عمليات البحث والتحري وتحصيل الأدلة في هذا النوع من الجرائم؛ ليبقى هذا الدليل بعد الحصول عليه وفق الضوابط والشروط القانونية خاضعا للسلطة التقديرية للقاضي، يعمل سلطته إن شاء أخذ بهذا الدليل وحكم بمقتضاه واستنادا عليه وإن شاء استبعده وحكم وفقا لقناعته الشخصية وتبعا لما استقر في خلده.

الهوامش:

[1] - عبد اللطيف محمود ربايعة،" الجرائم الالكترونية " (التجريم والملاحقة والإثبات)، مقدم إلى المؤتمر الأول للجرائم الالكترونية في فلسطين المنعقد في جامعة النجاح الوطنية نابلس، 17 نيسان 2016، ص.02.

[2] - عمر محمد أبوبكر بن يونس ، الجرائم الناشئة عن استخدام الإنترنت ، دار النهضة العربية ، القاهرة ، 2004 م ص 969 .

[3] - نذكر منها علي سبيل المثال : أ- اتفاقية نيويورك بشأن التقادم في البيوع الدولية للبضائع 1972 : تشير هذه الاتفاقية في مادتها التاسعة إلي أن مصطلح الكتابة ينصرف أيضا إلي المراسلات التي توجه في شكل برقية أو تلكس .ب- اتفاقية الأمم المتحدة بشأن النقل متعدد الوسائل للبضائع 1980 : حيث اعتبرت في الفقرة الثانية من المادة الخامسة منها السندات الرقمية المستخرجة من وسائل الاتصال الحديثة من ضمن السندات الكتابية بشرط أن تكون هذه السندات واضحة العبارة و مفهومة . ج- اتفاقية هامبورج 1987 الخاصة بنقل البضائع بحراً : و جاء في الفقرة الثامنة من مادتها الأولي أن مصطلح الكتابة يشمل البرقية و التلكس .

[4] - مفتاح بوبكر المطردي، الجرمة الإلكترونية وآليات التغلب على تحدياتها، ورقة مقدمة إلي المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-25 / 9 / 2012 ، ص.22.

[5] - طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي,، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون، جامعة قار يونس، طرابلس، ص.11.

[6] - هلال آمنة، الإثبات الجنائي بالدليل الإلكتروني، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2014/ 2015، ص.10.

7 - محروس نصار غايب، الجريمة المعلوماتية، مقال منشور على الموقع الإلكتروني، www.iasj.net/iasj?func=fulltext&aId=28397 أطلع عليه بتاريخ: 2017/03/12 الساعة 00:17.

[8] - محروس نصار غايب، الجريمة المعلوماتية، المرجع السابق، ص 11.

9 - نفس المرجع، ص 13.

10 - هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة . أسيوط ، مصر، ص5 ومايليها .

11 - عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية ، بيروت، لبنان،2003، ص3.

[12] - محروس نصار غايب، الجريمة المعلوماتية، المرجع السابق، ص 13.

[13] - القانون 04-15، المؤرخ في 10 نوفمبر 2010، المتضمن تعديل قانون العقوبات، الجريدة الرسمية، العدد 71 لسنة 2004.

[14] - القانون 09-04، المؤرخ 05 أوت 2009، المتعلق المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.، في الجريدة الرسمية، العدد 47 لسنة 2009.

[15] - محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، مصر، ص 31.

16 - نائلة عادل محمد فريد قورة .جرائم الحاسب الالي الاقتصادية. منشورات الحلبي الطبعة الاولى 2005 ص 52.

17 - عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، ص 42

[18] - عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 46.

19 - رستم هشام، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة، العدد(2)، 1999، ص 11.

[20] - نور الهدى محمود، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة، العدد 11، جوان 2017، ص.920.

[21] - علي حسن الطوالبه، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي "دراسة مقارنة"، مركز الإعلام الأمني، 2009، ص.10.

[22] - المادة 212 من قانون الإجراءات الجزائية.

[23] - نور الهدى محمود، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة، العدد 11، جوان 2017، ص.919.

[24] - أيمن علاء الدين بصيلة، الحماية الجنائية الإجرائية للتجارة الإلكترونية، مذكرة ماستر في القانون الجنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة أم البواقي، 2017/ 2018، ص.64.

[25] - أيمن علاء الدين بصيلة،، المرجع السابق، ص.66.

[26] - بن قدوم سهيلة، بسام ليدية، الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر في القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2017/ 2018، ص.83.

[27] - القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها،

[28] - أيمن علاء الدين بصيلة، المرجع السابق، ص.66.