حجية الدليل الرقمي في مجال الإثبات الجنائي وموقف المشرع الليبي

د. حكيم محمد عثمان
محاضر /قسم القانون الجنائي /كلية القانون
جامعة بني وليد

المقدمة

من القواعد المستقرة في مجال الإثبات الجنائي أن القاضي لا يمكنه أن يقضي بعلمه الشخصي، فإحاطته بوقائع الدعوى يجب أن يتم من خلال ما يطرح عليه من أدلة، ومن هنا يبدو الدليل هو الوسيلة التي ينظر من خلالها القاضي للواقعة موضوع الدعوى، وعلى أساس يبني قناعته، ولهذه الأهمية التي يتمتع بها الدليل عموماً حظي باهتمام المشرع في مختلف الأنظمة القانونية من حيث تحديد شروط مشروعيته وتقدير قيمته الإثباتية، مع اختلاف النظم القانونية في الاتجاه الذي تتبناه بين موسع ومضيق.

ونتيجة لتسارع إيقاع التقدم التكنولوجي والتقني الهائل؛ وظهور الفضاء الإلكتروني ووسائل الاتصال الحديثة كالفاكس والإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية استغله مرتكبو الجرائم الإلكترونية[1] في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة، بل تجاوزت حدود الدول، وهي جرائم مبتكرة ومستحدثة تمثل ضرباً من ضروب الذكاء الإجرامي، وبذلك اختلف الوسط الذي ترتكب فيه الجريمة، من وسط مادي إلى وسط معنوي أو ما يعرف بالوسط الافتراضي، وهو ما استتبع ظهور طائفة جديدة من الأدلة تتفق وطبيعة الوسط الذي ارتكبت فيه الجريمة وهي الأدلة الرقمية ، أو ما يسمى بالأدلة الإلكترونية، ولقد أثارت هذه الأدلة الكثير من الإشكاليات التي يمكن إرجاعها إلى ما يتمتع به الدليل الرقمي الإلكتروني بصفة الحداثة، فهو إفراز التطور التقني وذو طبيعة خاصة من حيث الوسط الذي ينشأ فيه والطبيعة التي يبدو عليها، وهذا يثير التساؤل حول مشروعية الأخذ به، ومدى إمكانية البحث عن الدليل الرقمي في الوسط الافتراضي وضبطه وفقاً للقواعد التي تحكم التفتيش، وكذلك صفة الشخص الذي يقوم بجمع هذا الدليل.

وكذلك يثير التساؤل حول مقبولية الدليل الرقمي في إثبات الوقائع الجنائية، وخصوصاً إن نظام الإثبات الجنائي تحكمه قرينة البراءة والتي على أساسها يتعين دائماً الحكم بالبراءة كلما تطرق للدليل الشك، لاسيما إذا علمنا بأن مقدار التطور في مجال تقنية المعلومات يتيح العبث بالمخرجات الرقمية بما يجعل مضمونها مخالفاً للحقيقة دون أن يتسنى لغير المتخصص إدراك ذلك.

([1]) من أمثلتها قرصنة واختراق غير مشروع لأنظمة الغير وبرامجهم وتدميرها بواسطة ما يعرف بالفيروسات المعلوماتية، وتقليد برامج الغير ونسخها وكذلك جرائم السرقة الإلكترونية والنصب والتزوير وتسهيل الدعارة وانتهاك حشمة الحياة الخاصة وعرض المواد الإباحية للأطفال وانتهاك خصوصية الغير، والمعلومات المشوهة والإعلانات الكاذبة والأفلام المخلة بالآداب العامة وعمليات التجسس والإرهاب والابتزاز والسطو على أموال البنوك.

لذلك سنحاول من خلال ما سيأتي أن نبين هذه الإشكاليات التي يثيرها الدليل الرقمي وكيفية التعامل التشريعي مع هذه المسألة والتطبيقات القضائية بها ومحاولة الاستفادة من تجارب بعض الدول المتقدمة وموقف المشرع الليبي في ضوء القواعد العامة، وذلك وفق الخطة التالية:

المبحث الأول: ماهية الدليل الرقمي وأقسامه وخصائصه .

المطلب الأول: التعريف بالدليل الجنائي بشكل عام.

المطلب الثاني: تعريف الدليل الرقمي.

المطلب الثالث: تقسيمات الدليل الرقمي.

المطلب الرابع: خصائص الدليل الجنائي الرقمي.

المبحث الثاني: مدى قبول وإجازة الأدلة الرقمية في الإثبات الجنائي .

المطلب الأول: مشروعية استخدام الأدلة الرقمية كوسيلة الإثبات الجنائي.

المطلب الثاني: حجية الدليل الرقمي أمام القضاء الجنائي.

المطلب الثالث: الصعوبات التي تواجه عملية الإثبات الجنائي في جمع الأدلة الرقمية.

المطلب الرابع: تفعيل التعاون الدولي ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية المتبادلة.

المبحث الأول

ماهية الدليل الرقمي وأقسامه وخصائصه

تمهيد وتقسيم:

نظراً للطبيعة الخاصة للجرائم الرقمية فإن دليل إثباتها يختلف ويتميز عن الدليل الجنائي التقليدي، فالدليل الرقمي يعيش في بيئة متطورة بطبيعتها وتشمل على أنواع متعددة من البيانات الرقمية تصلح مجتمعة أو منفردة لكي تكون دليلاً للإدانة أو البراءة، فيعتبر الدليل الإلكتروني الوسيلة الوحيدة والرئيسية في الإثبات الجنائي بجرائم الحاسوب والإنترنت، لذلك ترتكز عملية الإثبات الجنائي للجرائم الرقمية على الدليل الجنائي الرقمي باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم، وهو محور اهتمام بحثنا هذا، لذا سنتناول في هذا المبحث توضيح ماهية هذا الدليل وخصائصه وأقسامه، وكذلك في مطلب مستقل نسبقهم بمطلب نوضح فيه مفهوم الدليل الجنائي بشكل عام، وسنتناول ذلك على النحو التالي:

المطلب الأول

الدليل في اللغة:

هو المرشد، وما يتم به الإرشاد، وما يستدل به، والدليل: الدال، والجمع: أدلة[1]، وكذلك الحق بالبينة، والبينة هي الدليل أو الحجة.

الدليل في المصطلح القانوني:

يقصد بالدليل: الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، والمقصود بالحقيقة في هذا الصدد: هو كل ما يتعلق بالإجراءات والوقائع المعروضة عليه لأعمال حكم القانون عليها[2]، كما يقصد بالدليل أو العمل الإجرائي: كل إظهار لنشاط عام أو خاص داخل الخصومة أو من أجلها يؤدي مباشرة إلى التأثير في تطور رابطة الخصومة، أو بمعنى آخر: هو كل عمل يجري في الخصومة أو يهدف إلى إعدادها أو له قيمة في الخصومة، أيا كانت طبيعته أو معناه، نظمه القانون بقصد الوصول إلى تطبيق القانون الموضوعي فيها[3]، وهو الوسيلة الإثباتية المشروعة التي تسهم في تحقيق حالة اليقين لدى القاضي بطريقة سائغة يطمئن إليها[4] وهو أداة الإثبات عموما.[5]

كما أن الدليل هو: الوسيلة المتحصلة بالطرق المشروعة لتقديمها للقاضي لتحقيق حالة اليقين لديه والحكم بموجبها.[6]

والدليل هو النشاط الإجرائي الحال والمباشر من أجل الحصول على اليقين القضائي وفقاً لمبدأ الحقيقة المادية، وذلك عن طريق بحث أو تأكيد الاتهام أو نفيه.[7]

([1]) د. جميل صليبا، المعجم الفلسفي، بيروت، دار الكتاب اللبناني، الطبعة الأولى، 1970م، ص23.

([2]) د.ناصر إبراهيم محمد زكي، سلطة القاضي الجنائي في تقدير الأدلة دراسة مقارنة، أطروحة دكتوراه، جامعة الأزهر، كلية الشريعة والقانون، 1987م، ص211.

([3]) أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، 1983م، ص 473 ومابعدها.

([4]) عميد د.عبدالحافظ عبدالهادي عابد، الإثبات الجنائي بالقرائن،أطروحة دكتوراه، جامعة القاهرة 1989م، ص198.

([5]) مفهوم الإثبات أوسع من كلمة (دليل) فالإثبات أكثر عمومية، ويشمل مجموعة من الإجراءات الشكلية والموضوعية والقواعد اللازمة لكشف الحقائق وتحقيق العدالة، والدليل: مجموعة من الحقائق التي تقدم للمحكمة ويتم استخدامها لتبرئة أو لإدانة المتهم.

([6]) د.محمد عبيد سعيد يوسف، مشروعية الدليل في المجالين الجنائي والتأديبي، دراسة مقارنة بالتطبيق على تشريعات دولة الإمارات العربية المتحدة، أطروحة دكتوراه في علوم الشرطة، أكاديمية مبارك للأمن، كلية الدراسات العليا، مصر.

([7]) لواء د.أحمد ضياء الدين محمد خليل، قواعد الإجراءات الجنائية ومبادئها في القانون المصري، مطبعة كلية الشرطة، 2004م، ص316.

المطلب الثاني

تعريف الدليل الرقمي

بعد أن عرفنا الدليل بشكل عام والدليل الجنائي بشكل خاص، يمكن لنا أن نعرف الدليل الجنائي الرقمي باعتباره نوعاً متميزاً من أنواع الدليل الجنائي.

فيعرف البعض[1] الدليل الرقمي Digital evidence بأنه: الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء.

وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل: النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة تطبيق وتنفيذ القانون.[2]

أو هو: معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جانٍ أو مجني عليه.[3]

في حين عرفه البعض الآخر[4] بأنه : الدليل الذي يجد له أساس في العالم الافتراضي ويقود إلى الجريمة.

والذي يلاحظ على هذه التعريفات أنه اقتصر على مفهوم الدليل الرقمي الذي يتم استخراجه من الحاسب الآلي، ولاشك أن ذلك فيه تضييق لدائرة الأدلة الرقمية، فهي كما يمكن أن تستمد من

([1]) د.ممدوح عبدالحميد عبدالمطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، مصر، 2006م، ص88.

أيضاً راجع: د. خالد ممدوح إبراهيم، الدليل الإلكتروني في جرائم المعلوماتية، بحث منشور على الإنترنت ص2 http://www.f-law.net

([2]) خبير، عبدالناصر محمد محمود فرغلي، د.محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 12/11/2007،14م، ص13.

([3]) اللواء د.محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض، 2004م، ص234.

([4]) د.عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الإنترنت، ندوة الدليل الرقمي عبر جامعة الدول العربية، مصر، في الفترة 5-8 مارس 2006م، ص5.

الحساب الآلي، فمن الممكن أن يتحصل عليها من أية آلة رقمية أخرى، فالهاتف وآلات التصوير وغيرها من الأجهزة التي تعتمد التقنية الرقمية في تشغيلها يمكن أن تكون مصدراً للدليل الرقمي، فضلاً عن ذلك فإن هذا التعريف يخلط بين الدليل الرقمي ومسألة استخلاصه، حيث عرفه بأنه الدليل المأخوذ من الحاسب الآلي أو الكمبيوتر ... إلخ، وهذا يعني أن الدليل الرقمي لا تثبت له هذه الصفة إلا إذا تم أخذه أو استخلاصه من مصدره، وهذا برأينا ليس صحيحاً، وهو ما يصف هذا التعريف بالقصور لكونه لا يعطي تعريفاً جامعاً للدليل الرقمي.

ولذا فإننا بالاستفادة مما سبق نرى تعريف الدليل الرقمي بأنه : ((هو ذلك الدليل المشتق بواسطة النظم البرمجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال وأصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها)).

المطلب الثالث:خصائص الدليل الجنائي الرقمي

يتميز الدليل الجنائي الرقمي عن الدليل الجنائي التقليدي بالخصائص التالية:

1- الأدلة الرقمية تتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية Hardware واستخدام نظم برمجية حاسوبية Software.[1]

2- الأدلة الرقمية ليست أقل من الدليل المادي فحسب، بل تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن[2]، وذلك لأن مصطلح الدليل الرقمي يشمل كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقمياً، بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني.[3]

3- يمكن استخدام نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها ذات القيمة العلمية والحجية الثبوتية الشيء الذي لا يتوافر في أنواع الأدلة الأخرى (التقليدية) مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد، والتلف، والتغيير، عن طريق عمل نسخ طبق الأصل من الدليل.[4]

([1]) انظر، خبير عبدالناصر محمد محمود فرغلي، د.محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية، مرجع سابق، ص14.

([2]) للمزيد انظر: د.محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، مرجع سابق، ص237 ومابعدها.

([3]) رشيد بوكر، الدليل الإلكتروني ومدى حجيته في الإثبات الجنائي، رسالة ماجستير منشورة في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 27 العدد الأول.

([4]) وهذا مافعله المشرع البلجيكي، وبمقتضى قانون 28 نوفمبر 2000م تعديل قانون التحقيق الجنائي وبإضافة المادة (39 bis) التي سمحت بضبط الأدلة الرقمية، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية . انظر: عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الإنترنت، ندوة الدليل الرقمي، مرجع سابق، ص12.

4- الأدلة الرقمية يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، مما يؤدي إلى صعوبة الخلاص منها وهي خاصية من أهم خصائص الدليل الرقمي، بالمقارنة بالدليل التقليدي، فهناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي يتم حذفها أو إلغائها، سواء تم ذلك بالأمر Delete وحتى لو تم عمل إعادة تهيئة أو تشكيل للقرص الصلب hard Disk باستخدام الأمر format والبرامج التي تم إتلافها أو إخفائها، سواء كانت صوراً أو رسوماً أو كتابات أو غيرها، مما يعني صعوبة إخفاء الجاني لجريمته أو التخفي فيها عن أعين الأمن والعدالة، طالما تم علم رجال البحث والتحقيق الجنائي بوقوع الجريمة.

5- الأدلة الجنائية الرقمية ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان.

6- يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في ذات الوقت، فالدليل الرقمي يمكن أن يسجل تحركات الفرد، كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.[1]

هذه الخصائص أكسبت الدليل الرقمي طابعاً مميزاً جعلته الأفضل لإثبات الجرائم الإلكترونية مثل جرائم الاعتداء على نظم المعالجة الآلية؛ لأنّه من طبيعة الوسط الذي ارتكبت فيه، وكذلك يصلح لأن يكون دليل إثبات في الجرائم التقليدية، ففي الجرائم المرتكبة بواسطة الحاسوب مثل جرائم غسل الأموال أو تهريب المخدرات وعلى الرغم من عدم وجود صلة بين هذه الجرائم وبين الجرائم المرتكبة عن طريق الحاسوب إلا من حيث الوسيلة أي أنه الوسيلة لارتكاب الجريمة، وعدم اتصال الجريمة بالحاسوب في مثل هذه الحالات فإن الدليل الرقمي يصلح ليكون دليلاً لإثباتها.[2]

([1]) انظر: د.ممدوح عبدالحميد عبدالمطلب، استخدام بروتوكول (TCP IP) في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات، رقم العدد 4 ، المحور الأمني والإداري، تاريخ الانعقاد 26 أبريل 2003م، والانتهاء 28 أبريل 2003م دبي، الإمارات العربية المتحدة، ص649-650.

([2]) سهى إبراهيم داود عريقات، الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي، رسالة ماجستير، قسم القانون الجنائي، كلية الحقوق، جامعة د.ن، ص18.

المطلب الرابع

تقسيمات الدليل الرقمي

نتناول في هذا المطلب أنواع الدليل الرقمي والأشكال التي يبدو عليها، وكذلك الجرائم التي يصلح الدليل الرقمي ليكون دليلاً لإثباتها، وذلك على النحو التالي:

أولاً : أنواع الدليل الرقمي وأشكاله: إن الدليل الرقمي ليس له صورة واحدة بل يوجد له العديد من الصور والأشكال، وقد قسمها البعض إلى الأقسام الرئيسية التالية[1]:

1_ انواع الدليل الرقمي :

أ- أدلة أعدت لتكون وسيلة إثبات:

وهذا النوع من الأدلة الرقمية يمكن إجماله فيما يلي:

1- السجلات التي تم إنشاؤها بواسطة الآلة تلقائياً، ويعتبر هذه السجلات من مخرجات الأدلة التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.[2]

2- السجلات التي جزء منها تم حفظه بالإدخال وجزء يتم إنشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة وتتم معالجتها من خلال برنامج خاص كإجراء العمليات الحسابية على تلك البيانات.

ب- أدلة لم تعد لتكون وسيلة إثبات:

وهذا النوع من الأدلة الرقمية نشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغباً في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهو ما يمكن أن نسميه أيضاً بالآثار المعلوماتية الرقمية، وهي تتجسد في الآثار التي يرتكبها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية.[3]

([1]) انظر: د.ممدوح عبدالحميد عبدالمطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت، مرجع سابق، ص88.

([2]) راجع: د.ممدوح عبدالحميد عبدالمطلب، زبيدة محمد قاسم، عبدالله عبدالعزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر الأعمال المصرفية والإلكترونية، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة التجارة والصناعة دبي في الفترة من 10-2003/5/12م، ص2238.

([3]) حيث يتم الاعتماد في ضبط هذا النوع من الأدلة على ما يعرف ببروتوكول IP والذي يمكن من ضبط تحركات مستخدم الشبكة تحدى الجهاز الذي يستعمله من خلال بيانات الجهاز عند مزود الخدمة . راجع في ذلك: د.عبدالفتاح بيومي حجازي، الدليل الرقمي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة معمقة في جرائم الحاسب الآلي والإنترنت، بهجات للطباعة والتجليد، مصر، 2009م، ص108-109. وهذا النظام لا يحدد شخصية مرتكب الجريمة وإنما يحدد الجهاز الذي استعملت منه، ويرى البعض إن ذلك يصلح كقرينة لاعتبار صاحب الجهاز مرتكب الجريمة إلى أن يثبت العكس . راجع: د.ممدوح عبدالحميد عبدالمطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص108.

والواقع أن هذا النوع من الأدلة لم يعد أساساً للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ربط هذه الأدلة ولو بعد فترة زمنية من نشوئها، فالاتصالات التي تجري عبر الإنترنت والمراسلات الصادرة عن الشخص أو التي يتلقاها كلها يمكن ضبطها بواسطة تقنية خاصة بذلك.[1]

وتبدو أهمية التمييز بين هذين النوعين من الأدلة.

- إن النوع الأول من الأدلة قد أُعدّ كوسيلة إثبات لبعض الوقائع فإنه عادة ما يعمد إلى حفظه للاحتجاج به لاحقاً وهو ما يقلل من إمكانية فقدانه، وعلى عكس النوع الثاني حيث لم يُعدّ ليحفظ ما يجعله عرضة لفقدان الأسباب ومنها فصل التيار الكهربائي عن الجهاز مثلاً.
- يكون الحصول على النوع الثاني من الأدلة باتباع تقنية خاصة لا تخلو من الصعوبة والتعقيد بينما يتميز النوع الثاني من الأدلة الرقمية بسهولة الحصول عليه لكونه قد أُعدّ أصلاً لأنّ يكون دليلاً على الوقائع التي يتضمنها.
- نجد أن النوع الثاني من الأدلة الرقمية هو الأكثر أهمية لكونه لم يُعدّ أصلاً ليكون أثراً لمن صدر عنه، ولذا فهو في العادة تتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها.

ويلاحظ أن التنوع في الدليل الرقمي يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه، وإنما تتعدد وسائل التوصيل إليه، وفي كل الأحوال يظل الدليل المستمد منه رقمياً، حتى وإن اتخذ هيئة أخرى، ففي هذه الحالة فإن اعتراف القانون بهذه الهيئة يكون مؤسساً على طابع افتراضي مبناه أهمية الدليل الرقمي ذاته وضرورته إلا أنه لكي يحدث تواصل بين القانون وبين الدليل المذكور – نتيجة لنقص توافر الإمكانية الرقمية في المحاكم – فإنه يلزم اتخاذ مسلك الافتراض من حيث اعتباره دليلاً أصلياً.[2]

2 _ أشكال الدليل الرقمي:

أما عن أشكال الدليل الرقمي فيمكن إيجازها في ثلاث أشكال رئيسية هي:

أ- الصورة الرقمية: وهي عبارة عن تجسيد الخصائص حول الجريمة ، وفي العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة للصورة الفوتوغرافية التقليدية وهي قد تبدو أكثر تطوراً ولكنها ليست بالصورة الأفضل من الصورة التقليدية.

([1]) خالد ممدوح إبراهيم، زبيدة قاسم، عبدالله عبدالعزيز، مرجع سابق، ص2.

([2]) انظر: د.عمر محمد بن يونس ، مذكرات في الإثبات الجنائي عبر الإنترنت، ندوة الدليل الرقمي، مرجع سابق، ص12.

ب- التسجيلات الصوتية: وهي التسجيلات التي يتم ضبط وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الإنترنت والهاتف ... إلخ.

ج- النصوص المكتوبة: وتشمل النصوص التي يتم كتابتها بواسطة الآلة الرقمية ومنها الوسائل عبر البريد الإلكتروني، والهاتف المحمول (النقال) والبيانات المسجلة بأجهزة الحاسب الآلي...إلخ.

ثانياً : نطاق العمل بالدليل الرقمي:

إن الاهتمام الذي يحظى به الدليل الرقمي قياساً بغيره من الأدلة الأخرى هو زياده و انتشار استخدام تقنية المعلومات الرقمية، والتي تعاظم دورها مع دخول الإنترنت شتى مجالات الحياة، وأصبح بذلك هذا الوسط مرتعاً لطائفة من الجناة يطلق عليهم اسم المجرمين المعلوماتيين، فالجرائم التي يرتكبها هؤلاء تقع في الوسط الافتراضي أو ما يمكن تسميته بالعالم الرقمي، ولذا كان الدليل الرقمي هو الدليل الأفضل لإثبات هذا النوع من الجرائم؛ لأنّه من طبيعة الوسط الذي ارتكبت فيه، ومن هنا بدت أهمية هذا النوع من الأدلة، ولكن أيعني ذلك أن الدليل الرقمي ينحصر مجاله كدليل إثبات فقط على جرائم المعلوماتية؟

يجب التنويه إلى أنه لا تلازم بين نطاق العمل بالدليل الرقمي ومشكلة إثبات الجريمة المعلوماتية، فمن ناحية فإن الدليل الرقمي مثلما يصلح لأثبات الجريمة المعلوماتية وهو الدليل الأفضل لإثباتها، فإنه من ناحية أخرى يصلح لإثبات الجرائم التقليدية إن جاز التعبير، حيث يميز الفقه في هذا الشأن بين نوعين من الجرائم[1]:

أ- الجرائم المرتكبة بواسطة الآلة: وهذا النوع من الجرائم يستخدم فيه الحاسب الآلي والإنترنت كوسيلة مساعدة لارتكاب الجريمة، مثل استخدامه في الغش أو الاحتيال أو غسل الأموال أو لتهريب المخدرات، وهذا النوع من الجرائم لا صلة له بالوسط الافتراضي إلا من حيث الوسيلة – وبكلمة أوضح فإن الجريمة في هذه الحالة هي جريمة تقليدية استعملت في ارتكابها أداة رقمية، فبرغم عدم اتصال هذه الجريمة بالنظام المعلوماتي فإن الدليل الرقمي يصلح كدليل لإثباتها.

ب- جرائم الإنترنت والآلة الرقمية: وهذا النوع من الجرائم يكون محله جهاز الحاسب الآلي أو الآلة بصفة عامة، بحيث يكون الاعتداء واقعاً إما على الكيان المادي للآلة وهذه يمكن اعتبارها جريمة تقليدية تلحق النوع الأول وإما يكون الاعتداء واقعاً على الكيان المعنوى للحاسب أو الآلة أو على قاعدة البيانات التي قد تكون على شبكة المعلومات العالمية، مثل انتهاك الملكية الفكرية،

(1) د.ممدوح عبدالحميد عبدالمطلب، زبيدة محمد قاسم، عبدالله عبدالعزيز، مرجع سابق، ص2237.

وجرائم القرصنة وغيرها، وهذا النوع من الجرائم هو ما يمكن تسميته بجرائم المعلوماتية، والتي يكون الدليل الرقمي هو الدليل الأفضل لإثباتها إن وجد.[1]

ولذلك نجد أن الجريمة المعلوماتية رغم ارتباطها بالدليل الرقمي إلا أن إثباتها لا يقتصر عليه، فمن الممكن إثباتها بأدلة الإثبات التقليدية كالشهادة والاعتراف وغيرها.[2]

ولذلك يمكن القول إنه لا تلازم بين مشكلة الدليل الرقمي وإثبات الجريمة المعلوماتية، فلهذه الأخيرة إشكاليات قانونية أخرى لا شأن لها بالدليل الرقمي، فإذا كانت غاية الدليل عموماً هي إثبات الجريمة ونسبها إلى مرتكبها، فإن هذا الدليل لا يكون قاصراً في تقديرنا إذا اقتصر على مجرد إثبات وقوع الجريمة دون تحديد مقترفها؛ إذ مع ذلك تصح تسميته كدليل، وتبدو أهمية هذا النوع من الأدلة بالنسبة للجريمة المعلوماتية لصعوبة إثبات وقوعها عادة.

المبحث الثاني

مدى قبول وإجازة الأدلة الرقمية في الإثبات الجنائي

تمهيد وتقسيم:

مجرد وجود دليل يثبت وقوع الجريمة وينسبها لشخص معين لا يكفي للتعويل عليه لإصدار الحكم بالإدانة؛ إذ يلزم أن تكون لهذا الدليل قيمة قانونية، وهذه القيمة للدليل الجنائي تتوقف على عدة مسائل، الأولى مشروعية هذا الدليل وكيفية استخدامه، والثانية حجية واليقين في دلالته على الوقائع المراد إثباتها، والثالثة معرفة الصعوبات التي تواجه عملية الإثبات في الأدلة الرقمية، ولذلك سنحاول في هذا المبحث الإجابة على كل ذلك من خلال المطالب التالية:

([1]) هناك خلاف في الفقه حول تحديد مفهوم الجريمة المعلوماتية وليس في نيتنا التعرض لهذا الخلاف . راجع بشأن ذلك راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، بحث مقدم للمؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الإنترنت، الفترة 2-4 يوليو 2008م، منشور على الإنترنت، ص5 http://www.f-law.net

([2]) مع الملاحظ أن بعض الأدلة التقليدية تحتاج لتطوير مناسب مع الطبيعة الخاصة لهذه الجرائم، فالخبرة مثلاً تصلح لإثبات الجريمة المعلوماتية إلا أنها تحتاج إلى أن يكون الخبير متمتعاً بمستوى عالٍ من العلم والمهارة الفنية التي تمكنه من شق طريقه بنجاح في مجال إثبات هذه الطائف من الجرائم . د.علي محمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم ضمن أعمال المؤتمر العلمي حول الجوانب القانونية والأمنية للعمليات الإلكترونية ونظمه، أكاديمية شرطة دبي في الفترة من 26-2003/4/28م، ص22 منشور على الإنترنت http://www.f-law.net.

المطلب الأول

مشروعية استخدام الأدلة الرقمية كوسيلة الإثبات الجنائي

أولاً: مشروعية وجود الدليل الرقمي:

فالقيمة القانونية للدليل الرقمي في مجال الإثبات الجنائي تتمثل في مشروعية وجود الدليل الرقمي وأن يكون الدليل معترف به، وبمعنى آخر أن يكون القانون يجيز للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة، ويمكن القول إن النظم القانونية تختلف في موقفها من الأدلة التي تقبل كأساس بالإدانة، فهناك اتجاهان رئيسيان، الأول: نظام الأدلة القانونية، والثاني: نظام الإثبات الحر.

1- نظام الأدلة القانونية (المقيد):

ويسمى أيضاً بنظام الأدلة المحدد وفيه تكون الأدلة محصورة سلفاً من قبل المشرع[1]، بل إن قوتها التدليلية محددة ولا يجوز للقاضي أن يخرج عليها أو يبني عليها حكمه على خلافها، فلا سبيل للاستناد إلى أي دليل لم ينص القانون عليه صراحة ضمن أدلة الإثبات، كما أنه لا دور للقاضي في تقدير القيمة الإقناعية للدليل، حيث إن القانون قيّد القاضي بقائمة من الأدلة التي حددت قيمتها الإثباتية، وهذا النظام ينتمي للنظام ذات الثقافة الأنجلوسكسونية، مثل المملكة المتحدة (بريطانيا) والولايات المتحدة الأمريكية، ولذا فإن النظم التي تتبنى هذا النظام لا يمكن في ظلها الاعتراف للدليل الرقمي بأنه قيمة إثباتية، ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه يهدر قيمته الإثباتية مهما توافرت فيه شروط اليقين، فلا يجوز للقاضي أن يستند إليه لتكوين عقيدته.[2]

ويعاب على هذا النظام تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع فيحكم بما يتفق مع الواقع، فيحكم بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فسيصبح القاضي كالآلة في إطاعته لنصوص القانون، فإن هذا النظام بدأ ينحصر نطاقه حتى في الدول التي تعتبر الأكثر اعتناقاً له.[3]

([1]) د.هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية دراسة مقارنة، د.ط، د.ن، 1999م، ص49.

([2]) وتطبيقاً لهذا الفهم نص قانون الإثبات في المواد الجنائية البريطاني على قبول الدليل الرقمي وحدد قيمته الإثباتية وطبيعة النظام القانوني في بريطانية . راجع: علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية، مرجع سابق، ص30.

([3]) د.هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص91.

2- نظام الإثبات الحر (الاقتناعية):

ويعرف بحرية الاقتناع، وفيه لا يحدد المشرع أدلة الإثبات ووسائله، بل يترك للقاضي الحرية في أن يؤسس حكمه على أي دليل وفقاً لاقتناعه الشخصي دون أن يفرض عليه دليلاً بعينه، والاعتراف للقاضي بسلطة تقدير قيمة الدليل، فهو يقوم على أساس أن القوة الإثباتية (المقنعة) لكل دليل ليست مفروضة على القاضي مقدماً من المشرع، وإنما هي مرتبطة بما ترتبه من إقناع القاضي بحقيقة واقعة معينة، وبما يمليه عليه وجدانه وضميره، ويسود هذا النظام في ظل الأنظمة اللاتينية.[1]

وعليه فإنه في مثل هذا النظام لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود على اعتبار أن المشرع لا يعهد عنه سياسة النص على قائمة الأدلة والإثبات، ولذلك فمسألة قبول الدليل الرقمي لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي.

3- موقف المشرع الليبي من الدليل الرقمي:

قد تبنت بعض التشريعات نظام الإثبات المقيد أو ما يعرف بنظام الأدلة القانونية مع تمتع القاضي بسلطة واسعة في تقدير الدليل ((الاتجاه المختلط))[2] فالبعض الآخر من التشريعات تبنى نظام الأدلة القانونية الحرة، وقد أخذ المشرع الليبي بنظام الجمع بين النظامين، ويستند هذا الرأي إلى أن المشرع الليبي قد نص في قانون الإجراءات الجنائية على مجموعة من الأدلة ونظم طرق الحصول عليها، ومن ثم فإن هذا المسلك يعني أن المشرع لا يحظى بغيرها في مجال الإثبات الجنائي، فالنص على تلك الأدلة دليل على أن المشرع أراد اعتماد نظام للأدلة يجب أن يتقيد به القاضي، غير أن هذا النظام يعطيه – أي للقاضي – سلطة في تقدير الأدلة بموجب المادة 275 من قانون الإجراءات الجنائية [3]، وكأن المشرع الليبي أراد أن يجمع بين النظامين، ولذا فإنه وفقاً لهذا الرأي لا يمكن للقاضي أن يبني قناعته على غير الأدلة المنصوص عليها، فإن استند على دليل غير منصوص عليه كان حكمه باطلاً لمخالفة القانون.

وخلافاً لذلك يرى البعض إلى أن المشرع الليبي قد تبنى نظام الإثبات الحر، ولا يمكن القول إنه قد أخذ بنظام الإثبات المقيد لكونه قد نص على طائفة من الأدلة دون سواها لأن ذلك يتناقض وما قررته المادة 275 من قانون الإجراءات الجنائية، ومضمون هذه المادة هو الذي يستند إليه للقول أن المشرع

([1]) وهذا النظام هو السائد في التشريعات الجنائية المعاصرة كالتشريع المصري في المادة 302 من قانون الإجراءات الجنائية ، والتشريع العماني في المادة 215 من قانون الإجراءات الجزائية العماني، والقانون السوري واللبناني والفرنسي.

([2]) وهي التي تجمع ما بين النظامين اللاتيني والأنجلوسكسوني.

([3]) أستاذنا د.أحمد الصادق الجهاني، محاضرات ألقيت على الطلبة الدراسات العليا، جامعة قاريونس، 2003-2004م، غير منشورة، وتنص المادة 275 على أنه : ((يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته))، ومع ذلك لا يجوز له أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة.

الليبي قد تبنى نظام الإثبات الحر لا المقيد[1]، ولذلك فإن هذا الرأي يؤدي إلى القول إن كل الأدلة تتساوى من حيث قبولها قانوناً أمام القضاء بما في ذلك الدليل الرقمي.

الأشكال المختلفة للدليل الرقمي في ضوء الأدلة المعتمدة في قانون الإجراءات الجنائية وتحديد موقف المشرع الليبي من ذلك:

1- **الصور والتسجيلات الرقمية:** لم ينص المشرع الليبي على الدليل في شكل صور أو تسجيلات أو رسائل نصية مثل الوارد على المختلفات تطبيقات الهواتف الذكية وصفحات التواصل الاجتماعي (الدردشة) فردية أو جماعية، ولكن يمكن اعتبارها من قبيل القرائن على أن يتم الحصول عليه بطريقة مشروعة لا تنطوي على انتهاك لحرمة الحياة الخاصة وإن كانت قيمته أدنى من قيمة الدليل في الإثبات.[2]

2- **المستندات الرقمية:** قد يكون الدليل الرقمي في شكل نص مكتوب على دعامة أو أي وسائط إلكترونية حديثة ثابتة أو متحركة أو محمولة، وما يمكن أن يستخرج ويسترد من بيانات أو صور ورسائل نصية من مختلف أجهزة الحاسوب والهواتف الذكية في شكل أو هيئة ورقية وهناك إشارة يستفاد منه قبول المشرع للدليل المكتوب أو ما يسمى المحررات كدليل إثبات، وهو ما نصت عليه المادة 274 من قانون الإجراءات الجنائية الليبي بشأن محاضر المخالفات ويمكن القول إن الدليل الرقمي إذا ما أخذ شكل النص المكتوب فإنه يستمد مشروعيته من أن يأخذ حكم المحررات والتي يعترف المشرع الليبي بها كوسيلة إثبات أمام القضاء الجنائي.

تطبيقات على اعتراف المشرع الليبي بالدليل الرقمي في عدة قانونين خاصة:

هناك بعض النصوص التي وردت في تشريعات خاصة اعتمد فيها المشرع بالدليل الرقمي صراحة كدليل إثبات لبعض الجرائم.

نص المادة (67) من قانون رقم (1) لسنة 2005م بشأن المصارف فقرة (2-3) على الآتي:

- يعتد بالمستندات والتوقيعات الإلكترونية التي تتم في إطار المعاملات المصرفية وما يتصل بها من معاملات أخرى، وتكن لها الحجية في إثبات ما تتضمنه من بيانات.

([1]) د.مأمون سلامة، الإجراءات الجنائية في القانون الليبي، ج2، ط الأولى، منشورات الجامعة الليبية، بنغازي، 1970م، ص170.

([2]) د.مأمون سلامة، الإجراءات الجنائية في القانون الليبي، مرجع سابق، ص217-218.

- تعتبر مخرجات الحاسوب المتعلقة بالمعاملات المصرفية وفقاً للمنصوص عليه في الفقرة السابقة بمثابة الدفاتر القانونية المنصوص عليها في القانون التجاري والقوانين المكملة له .
- للمصارف أن تحتفظ للمدة المقررة في القانون بنسخ مصغرة على أقراص صلبة أو مرنة أو مضغوطة أو غير ذلك من أحداث التقنية الحديثة في مجال حفظ البيانات أو المعلومات بدلاً من أصول الدفاتر والسجلات والكشوفات والوثائق والمراسلات والبرقيات والإشعارات وغيرها من الأوراق المتصلة بأعمالها وتكون لهذه النسخ المصغرة حجية الأصل في الإثبات.[1]

نص المادة (6) مكرر من القانون رقم (10) لسنة 1428 هـ بإضافة مادة للقانون رقم 70 لسنة 1973م بشأن إقامة حد الزنى وتعديل بعض أحكام قانون العقوبات على أنه ((تثبت جريمة الزنى ... باعتراف الجاني أو بشهادة أربع شهود أو بأية وسيلة إثبات علمية أخرى وهي تحليل الحامض النووي DNA وكذلك الدليل الرقمي بوصفه من الأدلة العلمية الحديثة))[2].

نص المادة (62) فقرة (1) من قانون الاتصالات الليبي لسنة 2013م حيث نصت المادة على الآتي: ((مزودو خدمات شبكة المعلومات الدولية "الإنترنت" غير مسئولين عن الأخطاء التي يرتكبها المستفيدون إلا في الحالات الآتية:

- إذا ساهم مع المستفيدة بالخدمة في ارتكاب مخالفة أو تسبب في الإضرار بالغير أو إذا سهل للمستفيد بالخدمة إجراء ذلك)).

ثانياً : مشروعية حصول واستخدام وسائل جمع الأدلة الرقمية:

إن التطور التقني في شبكة الإنترنت سوف يقود دون شك إلى تغير كبير، وإن لم يكن كلياً في المفاهيم السائدة حول الدليل، ويقود مثل هذا القول في الحقيقة إلى إعلان انضمام الخبرة التقنية إلى علم الخبر المتميزة بتصنيف التعامل مع موضوع الدعوى ، من حيث ضرورة الاستعانة بالمختصين في مجال النزاع.[3]

([1]) يلاحظ على هذا النص أنه متعلق بالمعاملات المصرفية وما يتصل بها وما يدخل في حكمها دون سواها، ولقد ذكرنا سابقاً إلى عدم وجود موانع قانونية عن العمل بالدليل الرقمي المكتوب لإثبات أي جريمة وفقاً للقواعد العامة.

([2]) فاستعمال مصطلح بأية وسيلة إثبات علمية فيه دلالة على العموم، ولذلك يجب العمل بهذا النص على عمومه، والقول بغير ذلك هو تخصيص للنص، فتكتسب كل الأدلة العلمية الحجية في مجال إثبات جريمة الزنى، ويدخل في ذلك الدليل الرقمي بوصفه من ضمن الأدلة العلمية.

([3]) د.هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، مصر، 1994م، ص141 ومابعدها.

ويعد كل من المعاينة التفتيش والشهادة أحد وسائل جمع الأدلة ولكل منها قواعد ويتم اتباعها.

المعاينة:

يرى البعض[1] أن أهمية المعاينة تتضاءل في الجريمة المعلوماتية وذلك لندرة تخلف آثار مادية عند ارتكاب الجريمة المعلوماتية، لذلك عند إجراء المعاينة بعد وقوع الجريمة في المجال الإلكتروني يجب مراعاة الضوابط التالية:

1- تصوير الحاسب والأجهزة الطرفية به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

2- إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كافٍ حتى يستعد من الناحية الفنية العملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة.

3- العناية بالطريقة التي تم بها إعداد النظام.

4- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

5- التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة.

6- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة.

ندب الخبراء:

الخبرة هي إجراء يتعلق بموضوع يتطلب إلماماً بعلم أو فن معينة لإمكان استخلاص الدليل منه، لذلك فإن الخبرة تفترض وجود شيء مادي أو واقعة يستظهر منه الخبير رأيه، وإذا كان لندب الخبراء أهمية في الجرائم التقليدية، فإن أهميتها أكثر وضرورتها أشد في إجراءات جمع أدلة المكونات المعنوية في كل وحدات التخزين وتحليلها وكشف أي تلاعب في البرامج والمعلومات.[2]

والخبير في سبيل أداء مهمته مقيد في اللجوء إلى الأساليب والوسائل المشروعة التي يمكن من خلالها الحصول على الدليل العلمي دون إخلال بما يحفظ للإنسان حقوقه الأساسية ويكفل له عدم إهدار كرامته.

والمتتبع لأحكام القضاء الجنائي يلمس توسعاً في الاعتماد على الخبرة ورأي الخبراء، فقد قضت المحكمة العليا الليبية في الطعن الجنائي رقم 18/66ق ((ليس لمحكمة الاستئناف أن تخوض في صميم المسائل الفنية التي أبدى فيها الخبير رأيه الفني؛ لأنّ استعانة القاضي بأهل الخبرة في المسائل الفنية التي

([1]) المرجع نفسه، ص59.

([2]) علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية، مرجع سابق، ص285.

يتعذر عليه إدراكها يتطلب منه أن يضع في الاعتبار أي رأي الخبراء فيما يتعلق بالمسائل الفنية وألا يطرح رأيهم إلا لأسباب سائغة مقبولة)) .

التفتيش:

وفقاً لنص المادة (39) من قانون الإجراءات الجنائية الليبي التي تنص على أنه : ((لا يجوز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة ...إلخ))، فما يفهم من ذلك أن التفتيش يقتصر على ما يمكن اعتباره شيئاً لذلك هل يعتبر الوسط الافتراضي شيئاً يمكن تفتيشه ولذا فإن لفظ شيء يثير إشكالية من حيث مدى اعتبار البيانات المخزنة بالوسط الافتراضي أشياء يمكن ضبطها.

وعليه فإنه من الممكن أن يكون الوسط الافتراضي محلاً للتفتيش كما يمكن أن يكون محتوياته محلاً للضبط، ولا يعترض على ذلك بأن القانون يوجب تحريز المضبوطات وهو ما يتفق وطبيعة المخرجات الرقمية، فهذا ليس صحيحاً من وجهة نظرنا، ذلك أن هذه المخرجات يمكن تحريزها بطريقة تتفق وطبيعتها بوضعها في حالة فصلها عن مصدرها في قرص مضغوط ((CD)) وتحريز هذا القرص بالطريقة المنصوص عليها قانوناً، كما يمكن تحريزها إذا كانت في شكل نصوص بعد طباعتها وتحويلها للشكل المادي الملموس.[1]

ومما تقدم نخلص إلى أن الكيان المعنوي أو الوسط الافتراضي والبيانات المتحصلة فيه ينطبق عليه لفظ الشئ ، ولذا فإن تفتيش ذلك الوسط يعد صحيحاً وفقاً للقانون كما تعد البيانات الموجودة بذلك الوسط أشياء مما يصح ضبطها.ولكن المشكلة تكمن في حالة ارتكاب الجريمة بواسطة منظومة من الحواسيب تتوزع في أكثر من دولة، والسؤال الذي يطرح هنا هل يمكن تفتيش تلك الحواسيب للبحث عن أدلة تتعلق بتلك الجريمة بما في ذلك الأجهزة الموجودة في إقليم ودولة أخرى.

يجب أن نشير هنا إلى أن الوسط الافتراضي لشبكة الإنترنت لا يرتبط بنطاق إقليم دولة ما، فإن مكان تفتيش الحاسوب هو المكان الذي يتواجد فيه، فإن اختصاص الدولة بالتحقيق في جريمة ما وإن كان يخولها تطبيق قانون إجراءاتها بشأن هذا التحقيق بصرف النظر عن مكان وقوع الجريمة ما دامت خاضعة لقانون العقوبات الخاصة بها، إلا أن ذلك لا يعني أن تباشر الدولة هذه الإجراءات خارج إقليمها[2]؛ لأن ذلك من مظاهر السيادة، لذلك فمن المتعذر قانوناً مباشرة الدولة المختصة بالتحقيق

([1]) تنص المادة 44 من قانون الإجراءات الجنائية الليبي على أنه ((توضع الأشياء والأوراق التي تضبط في حرز مغلق وتربط كلما أمكن، ويختم عليه ويكتب على شريط داخل الختم تاريخ المحضر المحرر بضبط تلك الأشياء ويشار إلى الموضوع الذي حصل الضبط من أجله)).

([2]) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، ج1، 2011م، ص20.

لأي إجراء بشأن الجريمة خارج إقليمها على الرغم من اختصاصها بالتحقيق فيها، ولكن تستطيع الدولة حل هذه الإشكالية في حال وجود دليل على جهاز خارج إقليمها من خلال الإنابة القضائية للدولة الأخرى، بحيث تقوم بتفويض تلك الدولة بالقيام ببعض إجراءات البحث وجمع الأدلة وإرسالها لها.[1]

ولكن ماذا لو كان النظام المعلوماتي المراد تفتيشه يمتد لمسكن آخر غير منزل المتهم فهل يمكن تفتيشه في هذه الحالة ؟

لقد حسمت بعض القوانين هذه المسألة بحيث أجازت التفتيش بهذه الحالة دون الحاجة لأذن مسبق من أي جهة ولكن بشرط أن لا يكون النظام المعلوماتي يمتد لدولة أخرى، ومن هذه الأنظمة القانونية قانون جرائم الحاسوب الهولندي بالمادة (25/أ)[2] ولكنني أرى عدم إمكانية تطبيق هذه الحالة في ضوء نصوص القانون الليبي؛ لأنّ هذا النوع من التفتيش ينطوي في الواقع على معنى تفتيش غير المتهم ولذلك لا يمكن للقائم بالتفتيش تطبيق هذه الحالة إلا في الحالات التي يسمح له القانون بتفتيش غير المتهم أو منزله.[3]

المطب الثاني:حجية الدليل الرقمي أمام القضاء الجنائي

إن حجية المخرجات المتحصلة من الحاسوب هي قوتها الاستدلالية على صدق نسبة الفعل إلى شخص معين أو كذبه، أو هي قيمة ما يتمتع به المخرج المتحصل من الكمبيوتر بأنواعه المختلفة الورقية والإلكترونية والمصغرات الفيلمية من قوة الاستدلالية في كشف الحقيقة.[4]

فإن مجرد الحصول على الدليل الرقمي وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة؛ إذ الطبيعة الفنية الخاصة للدليل الرقمي تمكن من العبث بمضمونه على نحو تحرف الحقيقة دون أن يكون في قدرة غير المتخصصين إدراك ذلك العبث، ولذلك تثور فكرة الشك في مصداقيتها كأدلة للإثبات الجنائي، فهل من شأن ذلك استبعاد الدليل الرقمي من دائرة أدلة الإثبات الجنائي لتعارضه وقرينة البراءة؟

لقد اختلفت أنظمة الإثبات في تقديرها لحجية المخرجات ففي القوانين ذات الصياغة اللاتينية ومنها النظام الليبي، فإن حجية الأدلة الرقمية لا تثير صعوبات لمدى حرية تقديم هذه الأدلة لإثبات

([1]) وبهذا الشأن قضت إحدى الحاكم الألمانية في جريمة غش ارتكبت في ألمانيا بأن الحصول على البيانات الخاصة بهذه الجريمة والمخزنة بشبكات اتصال موجودة في سويسرا لا يتحقق إلا بطلب المساعدة من الحكومة السويسرية، وفي واقعة نشر فيروس Love bug عام 2000م الذي تسبب في إتلاف المعلومات في أجهزة الحاسب الآلي، فعندما الخبراء الأمريكيون بأن هذا الفيروس أرسل من الفلبين فإن تفتيش منزل المشتبه فيه تقتضي تعاون السلطات الفلبينية والحصول على إذن من قاضي التحقيق بالفلبين.

([2]) نقلاً عن د. علي حسن الطوالبة، مشروعية الدليل الرقمي المستمد من التفتيش الجنائي، دراسة مقارنة، جامعة العلوم التطبيقية، البحرين، كلية الحقوق، بحث منشور على الإنترنت من قبل مركز الإعلام الأمني، ص13-14 www.policemc.gov.

([3]) راجع المادتين 78 و180 من قانون الإجراءات الجنائية الليبي.

([4]) د.هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية، مرجع سابق، ص22، راجع أيضاً: د.علي حسن الطوالبة، مشروعية الدليل الإلكتروني، مرجع سابق، ص25.

جرائم الحاسوب والإنترنت ، ولا لمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة باعتبارها أدلة إثبات في المواد الجنائية، وهذا المعنى هو ما نصت عليه المادة 275 من قانون الإجراءات الجنائية، فهل يمكن للقاضي الجنائي وفقاً لهذا النظام أن يعمل سلطته التقديرية لقبول هذا الدليل أو رفضه بما يمكنه من استبعاد تلك الصور؟

يقال إن هذه السلطة تمتد لتشمل الأدلة العلمية، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الرقمي ، فضلاً عن ذلك فإن هذا الدليل يتمتع من حيث قوته التدليلية بقيمة إثباته قد تصل إلى حد اليقين، فهذا هو شأن الأدلة العلمية عموماً.فالدليل الرقمي من حيث تدليله على الواقع تتوافر فيه شروط اليقين، مما لا يمكن معه القبول بممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع التي يعبر عنها ذلك الدليل، ولكن هنا لا يناقض ما سبق أن قدمناه من أن الدليل الرقمي هو موضع شك من حيث سلامته من العبث من ناحية وصحة الإجراءات المتبعة في الحصول عليه، من ناحية أخرى، حيث يشكك في سلامة الدليل الرقمي من ناحيتين:

- أن الدليل الرقمي هو موضع شك من حيث سلامته من العبث من ناحية وصحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى[1]، ومن ثم فقد يقوم هذا الدليل معبراً عن واقعة معينة صنع أساساً لأجل التعبير عنها خلافاً للحقيقة، وذلك دون أن يكون في استطاعة غير المتخصص إدراك ذلك العبث، فالتقنية الحديثة تمكن من العبث بالدليل الرقمي بسهولة بحيث يظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة.[2]

([1]) محمد نافع فالح رشدان العدواني، حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، تشرين الثاني، 2015م، ص103.

([2]) طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، كلية القانون، جامعة قاريونس، بحث منشور على الإنترنت.

وإن كانت نسبة الخطأ الفني في الحصول على الدليل الرقمي نادرة للغاية لا أنها تظل ممكنة، ويرجع الخطأ في الحصول على الدليل الرقمي لسببين:

– الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الرقمي، ويرجع ذلك الخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة.

– الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات الاستخدام الأداة تقل نسبة صوابها عن 100% ويحدث هذا غالباً بسبب اختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها.

- إن سلطة القاضي الجنائي في تقدير الدليل لا يمكن أن نتوسع في شأنها بحيث يقال إن هذه السلطة تمتد لتشمل الأدلة العلمية ومنها الدليل الرقمي، فالقاضي بثقافته القانونية لا يمكن إدراك الحقائق المتعلقة بأصالة الدليل الإلكتروني.[1]

ومن ذلك فإننا نخلص إلى أن الشك في الدليل الرقمي لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه ولكنها تؤثر في مصداقيته، ولكن هل يمكن التثبت من سلامة الدليل الرقمي من حيث العيوب؟ وبكلمة أوضح هل من الممكن أن يُضفى على الدليل الرقمي اليقين من خلال إخضاعه للتقييم الفني الذي يمكّن من تفادي تلك العيوب التي تشوبه وما موقف القاضي الجنائي من هذا الدليل إذا ما خضع لمثل ذلك التقييم؟

فإذا سلمنا سابقاً بإمكانية التشكيك في سلامة الدليل الرقمي بسبب قابليته للعبث ونسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنها برأي حاسم وإن لم يقطع به أهل الاختصاص، ولذلك فإذا توافرت في الدليل الرقمي السلامة من العبث والخطأ، فإن هذا الدليل لا يمكن رده استناداً لسلطة القاضي التقديرية وفقاً لنص المادة (274) من قانون الإجراءات الجنائية الليبي.

وهنا ننوه إلى عدم الخلط بين الشك الذي يشوب الدليل الرقمي بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه وبين القيمة الإقناعية لهذا الدليل، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية فالقول فيها هو قول أهل الخبرة، فإن سلم الدليل من العبث والخطأ، فإنه لن يكون للقاضي سوى القبول بهذا الدليل ولا يمكن التشكيك في قيمته التدليلية.

وخلاصة القول ووفقاً للقواعد العامة في القانون الليبي لا يوجد نص صريح بقبول الأدلة الرقمية ومع ذلك يحكم بها، حيث تستمد الأدلة الرقمية في شكل نصوص مشروعيتها باعتبارها تأخذ حكم المحررات التي يقبل بها القانون الليبي كأدلة إثبات.

([1]) محمد نافع فالح رشدان، المرجع السابق، ص103.

المطلب الثالث

الصعوبات التي تواجه عملية الإثبات الجنائي في جمع الأدلة الرقمية

تتسم جرائم الكمبيوتر بصعوبة اكتشافها وإثباتها، فالجريمة المعلوماتية تتم في بيئة أو إطار لا علاقة له بالأوراق أو المستندات بل تتم بواسطة الحاسب الآلي أو الشبكة العالمية ويمكن للجاني عن طريق نبضات إلكترونية لا ترى العبث في بيانات الحاسب الآلي أو برامجه وذلك في وقت قياسي قد يكون جزءا من الثانية، وهذه البيانات أو المعلومات التي يتم العبث بها يمكن محوها كذلك في زمن قياسي قبل أن تصل يد العدالة إليه، سيما وأن عملية الضبط لا تتم سوى بمعرفة خبير فني أو متخصص.[1]

ولذلك فإن التحقيق في الجرائم الإلكترونية يظل يواجه صعوبات وتحديات متعددة من أجل جمع الأدلة الرقمية من أجهزة الحاسب الآلي أو الشبكات الرقمية نذكر منها:

أولاً: صعوبات تتعلق بالحصول على الدليل:

إن إقامة الدليل على وقوع الجريمة ونسبتها إلى متهم معين تكتنفه إشكاليات وصعوبات لا تتعلق فقط بتقديم الأدلة غير المادية، ومدى حجيتها أمام القضاء، وهي من المسائل المهمة في مجال تطوير الإثبات الجنائي في هذه الجرائم، وإنما تتعلق أيضاً بصعوبات الحصول على هذا النوع من الأدلة، وهو ما نعنيه ونقتصر الإشارة إلى أهم هذه الصعوبات:

1- إخفاء الدليل:

نتيجة ضعف الأنظمة الرقابية يتمكن مرتكبو الجرائم الإلكترونية من التسلل والبعث في النبضات والذبذبات الإلكترونية التي تسجل عن طريقها المعلومات والبيانات بغرض إحداث تغيرات في البيانات والمعلومات والتلاعب في منظومة الحاسب الآلي ومحتوياته، ومن ثم إخفاء ما قاموا به أو محو الدليل عليه، بحيث يتعذر إعادة عرض أعمال التسلل والدخول، وهكذا يستطيع الجناة في الجرائم الإلكترونية إخفاء جرائمهم وطمس آثارها في وقت قياسي من القصر وقبل أن تصل إليه سلطة التحقيق الأمر الذي يؤدي إلى صعوبات تعيق إجراءات التحقيق الرامية إلى الوصول إلى دليل.[2]

([1]) عبدالفتاح بيومي حجازي، القانون الجنائي والتزوير في جرائم الإنترنت والكمبيوتر، دار الكتب القانونية، المحلة الكبرى، مصر، 2005م، ص24.

([2]) ومن أمثلة سهولة محو الدليل المعلوماتي في وقت قصير، أنه أثناء إجراء المحاكمة للمسؤولين عن أحد المشروعات بألمانيا طلبت سلطات التحقيق المساعدة القضائية من السلطات السويسرية وأثناء سير الإجراءات تمكن الجناة من محو البيانات التي كانت من الممكن أن تستخدم كدليل، ولكن لحسن الحظ بعد ضبط الدعامات والأقراص الصلبة وأسطوانات الليزر، تمكن الخبراء بطرق فنية من استعادة البيانات التي كانت مسجلة عليها.

انظر: د.هشام حمد فريد رستم، الجوانب الإجرامية للجرائم المعلوماتية، مكتبة الآلات الحديثة، 1994م، هامش رقم (1) ص19.

انظر: د.مفتاح أبوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-2012/9/25م، ص51.

2- غياب الدليل ضد متهم معين:

تختلف الجريمة الإلكترونية عن الجريمة التقليدية، بأن الجريمة الأولى لا تحتاج لارتكابها أي نوع من العنف إلا فيما نذر، وإنما هي معالجة بواسطة إدخال بيانات معلومات خاطئة أو محظورة ضمن البرامج، أو تعريف أو تعديل البيانات والمعلومات المخزنة أصلاً في الحاسب الآلي، أو إرسال برامج تخريبية أو التجسس على البيانات والمعلومات المخزنة ونسخها، وإذا ما صادف واكتشفت هذه الأفعال وجمعت الأدلة على وقوعها، فإن هذه الأدلة قد لا تفصح عن صلة شخص معين بالجريمة المرتكبة؛ نظراً لأن معظم نُظم الحاسب الآلي لا تسمح للمراجعين والفنيين بالتتابع العكسي لمسار مخرجاتها، علاوة على صعوبة تتبع الآثار الإلكترونية ومراجعة وفحص الكم الهائل من البيانات والمعلومات المدربة بالأنظمة، وتعمد الجناة إلى إخفاء هويتهم.[1]

3- إعاقة الوصول إلى الدليل:

يضع الجاني في بعض الحالات عقبات فنية لمنع كشف جريمة وضبط أدلتها باستخدام تقنيات التشفير[2]، أو كلمة السر، وذلك بصد حجب المعلومة عن التداول العام، ومنع الغير بما فيه أجهزة الرقابة من الوصول غير المشروع إلى البيانات والمعلومات المخزنة أو التلاعب فيها، وقد أثبتت التحقيقات في بعض الجرائم الإلكترونية بألمانيا وجود صعوبات تواجه البعض من هذه التحقيقات نتيجة استخدام مرتكبي هذه الجرائم لتقنيات خاصة كالتشفير والترميز لإعاقة الوصول إلى الأدلة التي تدينهم.[3]

ثانياً : صعوبات تتعلق بالجانب الفني:

من المسائل التي تعوق عمليات البحث والتحقيق في الجرائم الإلكترونية نقص في المعرفة التقنية الحديثة والمتعددة لدى القائمين بالبحث والتحقيق في هذه الجرائم، مما يجعل منهم غير قادرين على أداء واجبهم على الوجه المطلوب؛ إذ نقص الخبرة والكفاءة، سواء في أجهزة الشرطة أو الادعاء يعد من الأسباب الرئيسية عن الإخفاق في كشف الجرائم الإلكترونية وجمع أدلتها، ويظهر ذلك بشكل واضح في الدول التي لا تزال تتعامل مع هذه الجرائم بإجراءات البحث والتحقيق التقليدية وتفتقر سلطاتها الضبطية والقضائية للأجهزة التقنية المتطورة في متابعة الجرائم الإلكترونية وضبط أدلتها، وبديهياً أنه في حالة عدم توافر التأهيل والخبرة وشح الإمكانيات التقنية على وجه الخصوص، فلا يمكن أن نتصور أي وجه للتعامل مع هذه الجرائم، وبالتالي ستكون النتائج سلبية لا محالة، ما لم تضع الدول برنامج تدريب وتأهيل لرجال

([1]) المرجع نفسه، ص52.

([2]) التشفير يعني: مناهج لحفظ البيانات من خلال لوغاريتمات أو خوارزميات بحيث لا يمكن لشخص ثالث قراءتها.

([3]) حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نائف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، 2000م، ص233-234.

الشرطة على أساليب الوقاية من جرائم الحاسب الآلي ووضع التدابير المانعة لوقوعها، والقيام بالتحري عما ارتكب منها وكشفها، وأيضاً كيفية التعامل مع الأدلة وضبطها، والاستعانة بدوي التخصصات الدقيقة المتعمقة في أنظمة الحاسب الآلي والإنترنت وشبكات الاتصال الخارجي.

المطلب الرابع

تفعيل التعاون الدولي ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية المتبادلة

أدركت الدول أهمية التعاون الدولي وأحست بأنه أمر مهم لتجاوز تحديات الجرائم الإلكترونية، فعمدت الكثير منها إلى عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في هذا النوع من الجرائم[1] ، وسوف نعرض فيما يلى الدور الذي لعبته كل من الامم المتحدة والاتحاد الاوربي ومجلس وزراء العدل العرب في هده المجال .

اولاً : دور الامم المتحدة

ففي عام 1983م أجرت منظمة التعاون والإنماء الاقتصادي دراسة حول إمكان تطبيق القوانين الجنائية الوطنية وتكييف نصوصها لمواجهة تحديات الجرائم الإلكترونية وسوء استخدامه، وفي عام 1985م أصدرت هذه المنظمة تقريراً على تضمن قائمة بالحد الأدنى لعدد أفعال سوء استخدام الحاسب الآلي التي يجب على الدول أن تجرمها وتفرض لها عقوبات في قوانينها ومن أمثلة هذه الأفعال : الغش أو التزوير في الحاسب الآلي، تغيير برامج الحاسب الآلي أو المعلومات المخزنة فيه، سرقة الأسرار المدعمة في قواعد الحاسب الآلي، تفعيل التعاون الدولي في مجال مكافحة الجريمة كما عالجت اتفاقية فيينا لسنة 1988م الموضوع ذاته وحثت الكثير من الدول على عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في هذه الجرائم، وكذلك لفت اللقاء التمهيدي الإقليمي لاسيا والباسفيك المنعقد 1989م الممهد للمؤتمر الثامن للأمم المتحدة المنعقد في كوريا 1990م النظر إلى نتائج التطور والتقدم التكنولوجي فيما يتعلق بالجريمة الإلكترونية واقتراح تشجيع اتخاذ إجراء دولي حيال هذه الجريمة.[2]

([1]) د.حمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في الفترة من 1-3 مايو 2000م، بكلية الشريعة والقانون بدولة الإمارات العربية، ص1028.

([2]) انظر في ذلك: د.محمد محيي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة 25-28 أكتوبر 1993م، ص362.

أما المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين والمنعقد في القاهرة عام 1995 فقد أوصى بوجوب حماية الإنسان في حياته الخاصة وفي ملكيته الفكرية من تزايد مخاطر التكنولوجيا ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الإجراءات المناسبة.[1]

وقد أوصى المؤتمر العاشر المنعقد في بودابست بالمجر عام 2000م بوجوب العمل الجاد على الحد من جرائم الحاسب الآلي المتزايدة والمعتبرة نمطاً من أنماط الجرائم المستحدثة والعمل على اتخاذ تدابير مناسبة للحد من أعمال القرصنة.[2]

ثانياً: دور المجلس الأوروبي:

لقد بدل وما زال المجلس الأوروبي يبدل جهوداً كبيرة في مواجهة جرائم المعطيات والحاسب الآلي عموماً ، وفي 28 يناير 1981م تم توقيع اتفاقية تحت إشرافه، تعلقت بحماية الأشخاص في مواجهة المعالجة الإلكترونية للمعطيات الطبيعية الشخصية.[3]

ولقد أصدر المجلس العديد من القواعد التوجيهية في هذا المجال، تضمنت وجوب تجريم العديد من السلوكيات كالغش المعلوماتي وتزوير المعلومات وسرقة الأسرار المخزنة والتوصل غير المصرح به وسرقة منفذ الحاسب، كما تضمنت العديد من الإجراءات الفنية لتجنب الحصول غير المرخص به إلى المعلومات المخزنة كحماية كلمة السر المستخدمة في النهايات الطرفية وحماية الأوامر الخاصة بالتشغيل وترميز المعلومات الشخصية وأسماء من تتعلق بهم.[4]

وأهم ما قام به المجلس في هذا المجال هو إشرافه على اتفاقية بودابست الموقعة في 23 نوفمبر 2001م.

ثالثاً: الدور العربي:

يعتبر اعتماد مجلس وزراء العدل العرب للقانون الجزائي العدلي الموحد كقانون نموذجي بموجب قرار رقم 229 لسنة 1996م يعتبر الأهم عربياً في مجال مواجهة جرائم المعطيات والحاسب الآلي عموماً، وبالرجوع الي الباب السابع من القانون ، والخاص بالجرائم ضد الاشخاص، نجد قد حوى فصلاً خاصاً بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية، فعاقبت على الدخول بطريق الغش

([1]) محمود أحمد عبانيه، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005م، ص158.

([2]) المرجع السابق، ص159.

([3]) د.أسامة عبدالله قايد، الحماية الجنائية الخاصة وبنوك المعلومات، دار النهضة، القاهرة، ص83.

([4]) أسامة عبدالله قايد، مرجع سابق، ص84.

إلى كامل أو جزء من نظام المعالجة لآلية المعلومات، وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتاد، وتغير المعلومات داخل النظام، وتزوير وثائق المعالجة الآلية، وسرقة المعلومات.[1]

وللجمعية المصرية للقانون الجنائي دوراً في هذا المجال، فقد عقدت مؤتمرها السادس بالقاهرة عام 1993م حول جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات والذي أكد على عالمية هذه الجرائم وضرورة تكاثف الجهود لمكافحتها، ووجوب تعديل نصوص قانون العقوبات التقليدية أو إضافة نصوص جديدة، نظراً لعجز النصوص القائمة عن مواجهة هذه الجرائم واوصى المؤتمر بالتعاون الدولي في هذا المجال لاسيما في مجال الإنابة القضائية وتسليم المجرمين وتنفيذ الأحكام، كما أوصى بوجوب تدريب رجال الضبطية القضائية والنيابة العامة والقضاة على طرق وكيفية استخدام أجهزة المعلومات وطرق الاستدلال والتحقيق وجمع الأدلة في الجرائم المتعلقة بها.[2]

الخاتمة

أولاً : النتائج:

توصلنا من خلال هذه الورقة إلى عدة نتاج أهمها:

1- الدليل الرقمي مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة تظهر في شكل صور أو تسجيلات صوتية أو مرئية.

2- يتميز الدليل الرقمي بصعوبة محوه أو تحطيمه، ويمكن كشف محاولة الجاني محو هذا الدليل لتتخذ بذاتها دليلاً ضده.

3- يتوقف مشروعية وجود الدليل الرقمي على طبيعة نظام الإثبات، ما إذا كان نظاماً مقيداً أم حراً ويتبنى القانون الليبي نظاماً مختلطاً بأخذ الأدلة القانونية مع إعطاء القاضي سلطة واسعة لتقدير القيمة.

4- لا يقتصر دور الدليل الرقمي في الإثبات على الجريمة المعلوماتية بالمفهوم الضيق فهو يصلح لإثبات أية جريمة قد تضمن معلومات عنها بأية طريقة.

5- وفقاً للقواعد العامة في القانون الليبي لا يوجد نص صريح بقبول الأدلة الرقمية، ومع ذلك يمكن العمل بها، حيث تستمد الأدلة الرقمية في شكل نصوص مشروعيتها باعتبارها تأخذ حكم

([1]) محمود أحمد عبانية، مرجع سابق، ص170.

([2]) المرجع السابق، ص172

المحررات التي يقبل بها القانون الليبي كأدلة إثبات، وتستمد الصور والتسجيلات مشروعيتها بوصفها قرائن قضائية.

6- يعتبر التفتيش عن الدليل الرقمي في الوسط الافتراضي وضبط محتوياته مشروعا.

7- هناك تطبيقان خاصان لقبول الدليل الرقمي في القانون الليبي، وهما ما نص عليه في قانون المصارف من حيث الاعتراف بحجية المستندات الرقمية في المعاملات المصرفية وما يتصل بها طبقاً للمادة 97 ، وما ورد في قانون حد الزنى بشأن جواز إثبات الجريمة الزنى بالوسائل العلمية، فتدخل في ذلك الأدلة الرقمية بوصفها أدلة علمية.

8- لا يجوز امتداد التفتيش في الوسط الافتراضي خارج حدود الدولة احتراماً لمبدأ السيادة ومع ذلك يجوز الحصول على الأدلة الموجودة في وسط افتراضي خارج حدود الدولة تطبيقاً لاتفاقات الإنابة القضائية، أو وفق لنظام تبادل المساعدات، ولا يجوز تفتيش النظام المعلوماتي الممتد لمنزل غير المتهم إلا في الأحوال التي يجوز فيها تفتيش منزل غير المتهم.

9- تتمتع الأدلة الرقمية بحجية قاطعة في الدلالة على الوقائع التي تتضمنها، ويمكن التغلب على مشكلة الشك في مصداقيتها من خلال إخضاعها لاختبارات تمكن من التأكد من صحتها.

ثانياً: التوصيات:

1- الدعوة الملحة للمشرع الليبي بسن تشريعات خاصة للجرائم الافتراضية والدليل الرقمي وحجيته في مجال الإثبات الجنائي ومنح الإذن بالتفتيش الممتد في الجرائم الافتراضية من النيابة العامة.

2- الاهتمام بتأهيل العناصر البشرية العاملة في جهاز الضبطية ودعمهم مادياً ومعنوياً وكيفية التعامل مع النظام المعلوماتي بما يمكنهم من تفتيش الوسط الافتراضي وضبط محتوياته.

3- دعوة المؤسسات الأكاديمية المتخصصة في مجال تقنية المعلومات إلى التعاون والتنسيق وعقد الاتفاقيات الثنائية مع الأجهزة الضبطية المماثلة لها في التخصص.

4- التوسع في عقد الاتفاقيات الدولية للاستفادة من نظام الإنابة القضائية وتبادل المعلومات في المجال المعلوماتي لتفادي مشكلة البحث عن الدليل الرقمي خارج حدود الدولة، وإنشاء المعامل الرقمية.

5- المشاركة بحضور المؤتمرات والندوات وورش العمل المحلية الإقليمية والعالمية المتعلقة بجوانب الجرائم المعلوماتية للاستفادة منها وتبادل الخبرات والمعلومات بين هذه المؤسسات.

6- توفير المعامل الرقمية وأحدث البرمجيات والأجهزة والمعدات الحاسوبية والتي تساهم وبشكل تقني في استخراج واسترداد الأدلة الرقمية وإعادة بناء الأدلة الرقمية من جديد وذلك وفقاً للمعايير الدولية والسعي للحصول على شهادة الجودة العالمية (الأيزو).

أسأل الله – تعالى – أن يجد فيه من يطلع عليه الفائدة (وآخر دعوانا أن الحمد لله رب العالمين).

المصادر والمراجع

(1) أسامة عبدالله قايد، الحماية الجنائية الخاصة وبنوك المعلومات، دار النهضة، القاهرة ، بدون طبعة ، وبدون سنة طبع.

(2) خالد ممدوح إبراهيم، الدليل الإلكتروني في جرائم المعلوماتية، بحث منشور على الإنترنت http://www.f-law.net

(3) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، ج1، 2011م .

(4) حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نائف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، 2000م.

(5) حمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في الفترة من 1-3 مايو 2000م، بكلية الشريعة والقانون بدولة الإمارات العربية .

(6) رشيد بوكر، الدليل الإلكتروني ومدى حجيته في الإثبات الجنائي، رسالة ماجستير منشورة في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 27 العدد الأول.

(7) راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، بحث مقدم للمؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الإنترنت، الفترة 2-4 يوليو 2008م، منشور على الإنترنت، http://www.f-law.net

(8) سهى إبراهيم داود عريقات، الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي، رسالة ماجستير، قسم القانون الجنائي، كلية الحقوق، جامعة د.ن .

(9) طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، كلية القانون، جامعة قاريونس، بحث منشور على الإنترنت.

(10) عبدالحافظ عبدالهادي عابد، الإثبات الجنائي بالقرائن، أطروحة دكتوراه، 1989م

(11) عبدالناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007/11/1214م .

(12) عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الإنترنت، ندوة الدليل الرقمي عبر جامعة الدول العربية، مصر، في الفترة 5-8 مارس 2006م .

(13) علي محمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مقدم ضمن أعمال المؤتمر العلمي حول الجوانب القانونية والأمنية للعمليات الإلكترونية ونظمه، أكاديمية شرطة دبي في الفترة من 26-2003/4/28م، منشور على الإنترنت - http://www.f-law.net.

(14) علي حسن الطوالبة، مشروعية الدليل الرقمي المستمد من التفتيش الجنائي، دراسة مقارنة، جامعة العلوم التطبيقية، البحرين، كلية الحقوق، بحث منشور على الإنترنت من قبل مركز الإعلام الأمني، - http://www.policemc.gov

(15) عبدالفتاح بيومي حجازي، الدليل الرقمي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة معمقة في جرائم الحاسب الآلي والإنترنت، بهجات للطباعة والتجليد، مصر، 2009م .

(16) عبدالفتاح بيومي حجازي، القانون الجنائي والتزوير في جرائم الإنترنت والكمبيوتر، دار الكتب القانونية، المحلة الكبرى، مصر، 2005م.

(17) محمد عبيد سعيد يوسف، مشروعية الدليل في المجالين الجنائي والتأديبي، دراسة مقارنة بالتطبيق على تشريعات دولة الإمارات العربية المتحدة، أطروحة دكتوراه في علوم الشرطة، أكاديمية مبارك للأمن، كلية الدراسات العليا، مصر.

(18) محمد عبدالحميد عبدالمطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، مصر، 2006م .

(19) محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض، 2004م .

(20) محمد نافع فالح رشدان العدواني، حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، تشرين الثاني، 2015م.

(21) محمود أحمد عبانيه، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005م.

(22) ممدوح عبدالحميد عبدالمطلب، استخدام بروتوكول TCP IP في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات ، رقم العدد 4 ، المحور الأمني والإداري، تاريخ الانعقاد 26 أبريل 2003م، والانتهاء 28 أبريل 2003م دبي ، الإمارات العربية المتحدة .

(23) ممدوح عبدالحميد عبدالمطلب، زبيدة محمد قاسم، عبدالله عبدالعزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر الأعمال المصرفية والإلكترونية، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة التجارة والصناعة دبي في الفترة من 10-2003/5/12م .

(24) محمد محيي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة 25-28 أكتوبر 1993م .

(25) مفتاح أبوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-2012/9/25م.

(26) ناصر إبراهيم محمد زكي، سلطة القاضي الجنائي في تقدير الأدلة ودراسة مقارنة، أطروحة دكتوراه، جامعة الأزهر، كلية الشريعة والقانون، 1987م .

(27) هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، مصر، 1994م .

(28) هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية دراسة مقارنة، د.ط، د.ن، 1999م .