مقبولية الدليل الرقمي في المحاكم الجنائية

أ.د. سالم محمد الأوجلي

إن التكنولوجيا الحديثة وما صاحبها من تطور في نظم الاتصالات أحدثت تقدماً كبيراً في تبادل المعلومات في كافة المجالات، المدنية والتجارية والعسكرية، وتزايداً عظيماً في خلق الوثائق الإلكترونية، فأغلب الوثائق التي ترسل في العالم أو تستخدم سواء من قبل الجهات العامة أو الأفراد هي وثائق الكترونية، وقلما يستعمل فيها الوسائل التقليدية.

ولهذا فإن الاستخدام المكثف للوسائل الالكترونية عبر البيئة الافتراضية ليست مستثناة من الاعتداءات و الممارسات غير المشروعة من غش واحتيال، وغيرها من الجرائم المرتكبة باستخدام وسائل الاتصال الحديثة مما ادى الى ظهور أنواع جديدة من الجرائم يجد الجناة والعصابات المنظمة في التكنولوجيا دعماً قوياً لارتكابها.

هذه الأنواع الجديدة من الجرائم والطرق الحديثة والأدوات المتطورة في ارتكابها، يتم إثباتها بالدليل الرقمي digital evidence فأصبحت هذه الوسيلة شيئاً فشيئاً جزءً مهماً في الإثبات الجنائي ، وتكتسب أهمية متزايدة أمام المحاكم، لدرجة يمكن معها القول بأن الدليل التقليدي traditional evidence بدأ يهجر النظم الإلكترونية والبيئة الافتراضية ذات العمليات المعقدة تاركاً المجال في ذلك للأدلة الرقمية (الالكترونية) التي تقتضي مقبوليتها في المحاكم الجنائية متطلبات وضوابط مختلفة عن الأدلة التقليدية. الأمر الذي يدعو معرفة مقبولية الدليل الرقمي في المحاكم الجنائية The admissibility of digital evidence in criminal courtsومتطلباته كوسيلة لكشف واثبات جرائم التكنولوجيا .لهذا الغرض تهدف الدراسة في هذه الورقة إلى الإجابة عن تساؤلات أساسية – ما هو الدليل الرقمي؟ كيفية تنظيم الدليل الرقمي في دول أوروبا وأمريكا باعتبارها من الدول الأكثر استخداماً للتكنولوجيا الحديثة، وما هي متطلبات مقبولية الدليل الرقمي أمام المحاكم الجنائية لهذه الدول؟ لا شك في أن الإجابة عن هذه التساؤلات تقودنا إلى الحقيقة التشريعية والقضائية لهذا الموضوع ، وعلى ذلك سنقسم هذه الورقة إلى ثلاثة مطالب.

- المطلب الأول – التعريف بمقبولية الدليل الرقمي.
- المطلب الثاني – مقبولية الدليل الرقمي في محاكم دول أوروبا.
- المطلب الثالث – متطلبات مقبولية الدليل الرقمي في المحاكم الأمريكية.

المطلب الأول

التعريف بمقبولية الدليل الرقمي

الفرع الأول

تعريف الدليل الرقمي

Definition of digital evidence

الدليل في المجال الجنائي هو الوسيلة التي يستعين بها القاضي للوصول إلى اليقين القضائي الذي يقيم عليه حكمه في ثبوت الاتهام المعروض عليه أو نفيه ، وتنقسم الأدلة الجنائية التقليدية إلى عديد من التقسيمات وفقاً لطبيعة كل منها ، فتوجد الأدلة المادية والأدلة القولية والأدلة الفنية، ولكن طبيعة الدليل الرقمي تجعله يختلف اختلافا جذرياً عن الدليل التقليدي الذي مصدره في الغالب هو التفتيش أو المعاينة التقليدية أو الاعتراف، وينتمي إلى بيئة مادية حقيقية.

أما الأدلة الرقمية فهي نتاج لاستخدام التقنية الحديثة من بيانات وأرقام وصور وغيرها في بيئة افتراضيه، وتستخدم في جمعها واستخلاص المعلومات المتعلقة بالجريمة والمجرم برامج خاصة، وتقنية عالية تعتمد على نوع الدليل ونوع الجهاز ونظام التشغيل .

ويمكن تعريف الدليل الرقمي في جرائم الكمبيوتر بأنه " أي بيانات مخزنة أو منقولة باستخدام الكمبيوتر التي تدعم أو تدحض نظرية كيفية وقوع الجريمة أو توضح عنصراً حاسماً في الجريمة [1] ".والبيانات المشار إليها في هذا التعريف هي مزيج أو خليط combination من الأرقام تمثل معلومات مختلفة و صور و أصوات، وهذه البيانات الرقمية المخزنة في الكمبيوتر أو المنقولة منه، يتمكن المحققون من خلالها كشف الجريمة

---

[1] Eogancasey digital Evidence and computer crimes third edition 2013 p 7.

وتحديد الفعل الإجرامي ونسبته إلى متهم معين أو نفيه عنه.[2] بمعنى ان أجهزة الكمبيوتر الموجودة في كل مكان، والبيانات الرقمية المخزنة بها أو المنقولة عبر الهواء أو من خلال الأسلاك تعد وسائل مهمة في التحقيق، إذ من خلال فحصها وتحليلها يتم الحصول على دليل الإدانة inculpatory evidence أو دليل البراءة exculpatory evidence ، وعند النظر إلى العديد من مصادر الأدلة الرقمية فإنه يمكن تصنيف أنظمة الكمبيوتر إلى ثلاث مجموعات :

أولاً– أنظمة الكمبيوتر المفتوح open computer systems

وهي أنظمة الكمبيوتر التي يستخدمها ويعلمها معظم الناس، وتتكون من القرص المرن، وأجهزة الكمبيوتر المحمولة والأجهزة المكتبية والخادم الذي ينفذ الأوامر ، هذه الأنظمة التي تتزايد من وقت لآخر سعتها التخزينية تعد مصدراً غنياً للأدلة الرقمية، فالملف البسيط يمكن أن يحتوي على معلومات متنوعة قد ترتبط بوقائع تفيد في التحقيق في جريمة ما.

ثانياً– أنظمة الاتصالات communication systems

أجهزة الاتصال التقليدية كالتليفون وأجهزة الاتصال الحديث كالأنترنت وشبكة المعلومات تعد مصدراً للدليل الرقمي مثال ذلك نظم الاتصالات عن بعد telecommunication systems التي تنقل الرسائل الإلكترونية في العالم مع تحديد الوقت الذي أرسلت فيه والمرسل ومحتوى الرسالة، كل هذه المعلومات يمكن أن تكون مهمة في التحقيق ، إذ عندما ترسل الرسالة فإنه يمكن فحصها من خلال دراسة ملفات وسيط الخادم intermediate server والموجهات التي تتعامل في إرسال الرسالة، و الحصول منها على معلومات تفيد في كشف الجريمة، ولهذا فإن العديد من أنظمة الاتصالات يمكن إعدادها وتهيئتها لضبط حركة المرور الإلكتروني للرسائل، وإعطاء المحققون إمكانية الدخول إلى كل أنواع الاتصالات "الرسائل، النصوص، المرفقات، المحادثات التليفونية " وكشف الجرائم وضبط أدلتها.

ثالثاً – أنظمة الكمبيوتر التخزينية Embedded Computer systems

---

[2] Eoghancasey op cit p 7

أجهزة الموبايل والكروت الذكية smart cardsوالأنظمة الأخرى التي تشتمل على أدلة رقمية، فأجهزة الموبايل قد تحتوي على اتصالات وصور رقمية، وفيديو ، ومعلومات شخصية، وأنظمة الملاحة Navigation systems يمكن أن تستخدم لتحديد مكان المركبة، والاستشعار عن بعد sensing ووحدات التشخيص Diagnostic Modules في العديد من السيارات توجد بها معلومات مفيدة في فهم الحادث، إذ تبين سرعة السيارة وحالة الفرامل والموقف خلال خمس ثوان قبل الحادث، وكذلك الحال أجهزة Microwave ovens مزودة الآن بوحدات تنقل المعلومات من الإنترنت وبعض الأجهزة المنزلية التي تسمح للمستخدمين ببرمجتها عن طريق الشبكة أو الانترنت تفيد في تحقيقات الحريق إذ يمكن عن طريق البيانات المستخدمة data recovered في الأجهزة المنزلية تحديد سبب الحريق ووقت حدوثه[3] .

لذلك فإن كثرة الدليل الرقمي ووجوده في كل مكان ubiquity of digital evidence، يجعل من النادر وجود جريمة ليس لها بعض بيانات مخزنة أو منقولة في برنامج الكمبيوتر أو الاتصالات الحديثة، فهذه البيانات المخزنة أو المنقولة تعد دليلاً رقمياً مهماً لأي تحقيق، وتستخلص منها معلومات كثيرة حول الأفراد وأنشطتهم، إذ أن استخدام الكمبيوتر الشخصي وشبكات خدمات المعلومات وما تحتويه من بيانات ومعلومات محفوظة بشكل فعال، يمكن عن طريقها معرفة العديد من المعلومات عن أنشطة الأفراد وأصدقائهم المقربين وعائلتهم، فالمحققون المهرة يمكنهم الاستفادة من هذه المعلومات، والخوض في هذه المحفوظات السلوكية لاكتساب معرفة أعمق عن المجرم والضحية، ولكن على الرغم من أهمية الدليل الرقمي وانتشاره ،فإن قليل من الناس على درجة جيدة من المعرفة بالإثبات evidential والتقنية والمسائل القانونية المتعلقة بالأدلة الرقمية، لذلك فإن الدليل الرقمي غالبا ما يتم تجاهله overlooked أو يجمع بطريقة غير صحيحة incorrectly collected أو يحلل بطريقة غير فعالة analyzed ineffectively، ولهذا ينبغي أن يتزود القائمون بتطبيق القانون الجنائي بالمعرفة الأساسية بالدليل الرقمي، والمتطلبات المهارية لاستخدامه بشكل فعال في أي تحقيق، وكل ما يتعلق بجوانبه التقنية والقانونية.

---

[3] Eoghancasey op cit p 8

الفرع الثاني

تعريف مقبولية الدليل الرقمي في النظام الأنجلوسكسوني

إن عملية الإثبات الجنائي تقتضي قبول الدليل من ناحية، وتقدير قيمة الإثباتية من ناحية اخرى. وهذا يعني أنه ثمة فارق بين مقبولية الدليل admissibility of evidence والقيمة الإثباتية للدليلthe probative of value. سنحاول توضيح ذلك.

أولاً- مقبولية الدليل الرقمي :

المبدأ الذي يسود غالبية التشريعات المعاصرة في الأدلة التقليدية، هو كل دليل مقبول في الإثبات الجنائي، فلا يستطيع القاضي أن يستبعد أي دليل على أنه غير مقبول في الإثبات، هذه الحرية في قبول الأدلة تعد نتيجة حتمية لمبدأ أساسي في قوانين الإجراءات الجنائية ،هو حرية القاضي في تكوين عقيدته، كما أن القانون لا يتدخل في قبول الدليل وفي تقدير قيمته أو قوته الإثباتية، غير أن هذا المبدأ لا يعمل به على إطلاقه، إذ ثمة قيود ترد عليه، فقد يتدخل المشرع في قبول الدليل ويفرض شروطاً معينة لقبوله ، من أهمها مشروعية الدليل وحظر الالتجاء إلى أدلة معينة، و منع القاضي أن يحكم بعلمه، أو إلزامه بأدلة معينة في إثبات بعض الجرائم، كجرائم الحدود، أو المسائل التي وضع لها القانون تنظيماً فنياً معيناً؛ هذا ما نص عليه المشرع المغربي في المادة 288 من المسطرة الجنائية " يمكن إثبات الجرائم بأية وسيلة من وسائل الإثبات ما عدا الأحوال التي يقضي فيها القانون خلاف ذلك ".

وفكرة مقبولية الدليل الجنائي أمام المحكمة تقوم على تقييم assessment الدليل قبل تقديمه للمناقشة في الجلسة وتقدير مدى مقبوليته في الدعوى، بمعنى أن المقبولية تتعلق بمرحلة سابقة لجلسة المحاكمة ومناقشة الخصوم للدليل، تعرف بمرحلة مناقشة المقبولية discussion of admissibility تتم فيها دراسة وتقييم الدليل الرقمي، فيقبلadmit الدليل إذا كان موثوقاً فيه reliable وحائزاً لمتطلبات المقبولية ومقتضيات الدقة والأمانة

والمشروعية، أو غير مقبول inadmissible إذا لم تتوافر فيه متطلبات المقبولية بأن يكون على درجة من التقلب volatility أو عدم الصحة inauthentic[4]وغيرها من متطلبات المقبولية، بحيث لا يمكن الاعتماد عليه it will not be able to rely في بناء أي حكم.

وفي جرائم التكنولوجيا نجد المشرع في العديد من الدول لم يترك للقاضي سلطة مقبولية الدليل الرقمي، بل وضع له ضوابط محددة لمقبوليته يجب على القاضي مراعاتها ليكون الدليل مقبولاً أمامه وصالحاً لوضعه أمام المحلفين، ويوفر قاعدة صلبة في إصدار حكم في الدعوى[5]، ومن الناحية العملية فإن المقبولية عبارة عن مجموعة من الاختبارات الفنية التي يشرف عليها القاضي لتقييم عناصر الدليل ، وعملية التقييم هذه غالبا ما تكون معقدة خاصة عندما لا يتم التعامل مع الدليل بشكل صحيح أو أن له صفات أكثر موثوقية أو شروط أكثر رفضاً، لذلك تضع العديد من التشريعات قواعد لمقبولية الدليل يتعين مراعاتها عند تقييمه وتقرير مدى مقبوليته. وفي قضية Larraine . V. market American Insurance company تم التعرض لمقبولية الدليل الرقمي ووضعت مبادئ توجيهية عامة للوصول إلى قرار سليم بشأن مقبولية الدليل[6] .

ثانياً – تقدير القيمة الإثباتية للدليل :

عرفنا مما سبق بأن القاعدة التي تحكم مقبولية الأدلة، هي أن القاضي يقبل جميع الأدلة التي يقدمها الخصوم في الدعوى، فلا يوجد أدلة يحظر القانون مقدماً قبولها، على أن يمارس القاضي السلطة التقديرية الكاملة في تقدير قيمة الدليل، وبناء حكمه عليه وفقاً لقاعدة " يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته ..." المادة 275 إجراءات جنائية ليبي.

إلا أنه بعد تقديم الخصوم للأدلة وتقرير مقبوليتها يأتي دور القاضي في فحص الأدلة التي قدمت إليه وتقدير قيمتها الإثباتية و بناء حكمه عليها، أي تقييم حجيتها وتقدير قيمتها الإقناعية، فله أن يقتنع بدليل معين أو يهمله وفقاً لضوابط الاقتناع القضائي، ويختلف هذا الدور الذي يقوم به القاضي في هذه المرحلة عن مرحلة مقبولية الدليل، إذ أنه يأتي لاحقاً

---

(4) prof – Murdoch watney- Admissibility of electronic evidence in criminal proceedings An outing of South Africa Legal position 2009 p5.
(5) keiko. L. Sugiska Admissibility of evidence in Minnesota p.1456
(6) Ibid., P. 1458.

لمرحلة مقبولية الدليل، بمعنى أن موضع الاختلاف بين مقبولية الدليل وتقدير قيمته الإثباتية، هي إطلاق الأولى بحيث يقبل أي دليل كقاعدة في الأدلة المادية (الملموسة) tangible evidence وإخضاع الأدلة الرقمية لمعايير المقبولية المقررة النظام الأنجلوسكسوني، وفي الثانية يمنح القاضي سلطة تقديرية واسعة في تقدير قوة الدليل في الاقتناع بعد طرحه في جلسات المحاكمة، وإتاحة الفرصة لأطراف الدعوى لمناقشته، ومن خلال ذلك يؤسس القاضي قناعته من هذه الأدلة، أي أن الأدلة التي طرحت في الجلسة وأبدى فيها الخصوم كافة الدفوع والملاحظات التي يؤسس عليها القاضي حكمه تسبقها في العديد من التشريعات السائدة في النظام الأنجلوسكسوني ما يعرف بمقبولية الدليل، بحيث لا يطرح الدليل الرقمي في الجلسة إلا بعد أن تتوافر فيه متطلبات المقبولية باعتبار ذلك ضمانة أساسية لإقامة عدالة صحيحة.

المطلب الثاني

مقبولية الدليل الرقمي في محاكم دول أوروبا

إن التعاون بين دول الاتحاد الأوروبي وكذلك الدول المرشحة للانضمام إلى هذا الاتحاد في تبادل المعلومات والخبرات في كافة المجالات، يعد وسيلة مهمة لتطوير التعاون التشريعي والقضائي، وإعداد رؤية أوروبية موحدة تهدف إلى العمل كفريق واحد من المحققين الأوروبيين من مختلف التخصصات في مجال مكافحة جرائم التكنولوجيا.

ومن أجل الوقوف على درجة التطور والتجانس القانوني Legal homogeneity الذي تحقق في أوروبا، ينبغي مراجعة التشريعات السائدة الآن في أوروبا بشأن الأدلة الرقمية، وتحليل موقف هذه التشريعات منها والنهج المتبع في متطلبات مقبوليتها أمام القضاء الجنائي والنظرة العامة للأدلة الرقمية ، وعليه سنقسم هذا المبحث إلى ثلاثة مطالب.

الفرع الأول: استعراض التشريعات الأوروبية المتعلقة بالأدلة الرقمية.

الفرع الثاني : تحديد موقف التشريعات الأوروبية من الأدلة الرقمية.

الفرع الثالث : تقدير الأدلة الرقمية.

الفرع الأول

استعراض التشريعات الأوروبية المتعلقة بالأدلة الرقمية

من خلال مراجعة التشريعات الأوروبية التي تمكننا من الاطلاع عليها، لاحظنا اهتمامها بالأدلة الرقمية في المسائل الجنائية ،مع انها لم تضع تعريفا محدداً لها، ففي غالبية تشريعات الدول الأوربية توجد نصوص خاصة بالدليل الرقمي، فقانون الإجراءات الجنائية الألماني يشتمل على مواد للأدلة الرقمية، كالمواد المتعلقة بحماية المعلومات خلال التحقيقات، وحالات تدمير المعلومات، وهذه المواد توضح الإجراءات والتدابير التي تتبع لحماية المعلومات المتحصل عليها من التحقيقات، ومن قواعد بيانات الشرطة[7]، وقانون الإجراءات الجنائية الأسترالي يشتمل هو الآخر على سلسلة من الإجراءات، والمتطلبات التي يجب أن تتخذ في حالة القيام بتدابير مراقبة الاتصالات الالكترونية، وفي بلجيكا يوجد قانون لجرائم الكمبيوتر يتضمن الإجراءات المتبعة في جمع الأدلة الرقمية، وفي إسبانيا تناول قانون الإجراءات الجنائية موضوع الأدلة ووسائل استنساخ الكلمات والأصوات والصور، وجمع المعلومات والبيانات وغيرها و الحفاظ عليها. وكذلك القانون الإجرائي الفنلندي أشار عند حديثه عن عبء الإثبات burden of proof إلى الأفعال التي تدعم الإجراءات التي تتخذ في الأدلة الرقمية علي غرار ما هو متبع في الأدلة التقليدية[8] .

في إيطاليا تم تحديث القانون الجنائي وفقاً للتشريعات الأوروبية، إذ نص القانون على تعريف الوثائق الرقميـــة، مثل أدوات الكمبيوتر التي تحتوي على معلومات لها قيمة اثباتية evidentiary والبرامج التي توجد بهـــا هذه المعلومات، لذلك فإن مدونة الحكومـــــة الإلكترونيـــة code of electronic Government تشتمل على المعنى الدقيق للوثائق الإلكترونية electronic documents والأصل التوثيقي الإلكتـــروني

---

[7] cybexintellegnce on e-evidence – about the admissibility of electronic evidence in court p27.
[8] The same reference p-27.

electronic authentication وغيرها من المفاهيم التي تقرر بأن الوثيقة الإلكترونية هي تمثيل الكتروني للأعمال والأفعال والمعلومات بطريقة قانونية[9] .

وفي بريطانيا توجد أكثر من إشارة مباشرة في قانون الشرطة ومدونة الأدلة الجنائية – إلى الأدلة الرقمية وجمع المعلومات التي تحتويها أجهزة الكمبيوتر، والى تعريفات للمصطلحات الإلكترونية.

وفي رومانيا عرف قانون الإجراءات الجنائية الدليل كأي عنصر واقعي factual element يستخدم لكشف و ضبط جريمة جنائية و نسبتها الى الفاعل [10] .

الفرع الثاني

تحديد موقف التشريعات الأوروبية من متطلبات المقبولية

من خلال قراءة العديد من التشريعات الأوروبية يتبين بأن الدليل الرقمي مساوياً equivalent للدليل التقليدي traditional evidence في هذه التشريعات، علاوة على ذلك توجد ثلاثة أنواع من المساواة أو التكافؤ بين الدليلين: الدليل الرقمي و الدليل التقليدي، **النوع الأول** وهو الأكثر شيوعاً يشير إلى معادلة (مساواة) بين الوثيقة الإلكترونية والوثيقة العادية، ففي بعض القوانين يتم تحديد نوع المستند وعلى ضوئه يقارن الأصل الإلكتروني بالورقي. **النوع الثاني**، يشير إلى معادلة التوقيع الإلكتروني بالتوقيع اليدوي، وأعمال التوثيق الإلكتروني electronic notarial deeds بأعمال التوثيق العادية. **النوع الثالث** يعادل البريد الإلكتروني بالبريد العادي، وهنا يشار إلى القانون البرتغالي الذي يعادل البريد الإلكتروني بالمحادثات التليفونية[11] .

ومن الناحية الواقعية توجد مجموعة من الدول الأوروبية تسعى من أجل استيعاب assimilate الوثائق الإلكترونية ومعادلتها بالوثائق الورقية، وإعطائها ذات القيمة للأدلة الوثائقية documentary evidence في المحاكمة، وتوجد مجموعة أخرى تعمل على معادلة التوقيع الإلكتروني بالتوقيع العادي، وأن يكون لكليهما نفس القيمة الإثباتية أمام المحاكم[12] .

---

[9] cyber intellegnce op cit p 28.
[10] Ibid ., p 28.
[11] cyber intellegnce op cit p 28.
[12] Ibid., p 29.

ومن وجهة نظر الممارسة القانونية، فإن غالبية القضاة الأوربيين ينظرون إلى الدليل الرقمي معادلاً للدليل التقليدي، ويميل الممثلون للقضاء الأوروبي إلى معادلة الأدلة الرقمية بالأدلة الوثائقية التقليدية، مع أن البعض يرى بأن الأدلة الرقمية نوعا من الدعم وليست من وسائل الإثبات، وتذهب الغالبية العظمى من المحامين في أوروبا إلى إمكانية وجود نوع من التنظيم للدليل الرقمي، وتتنوع الحجج و تنقسم الآراء في ذلك .

فمثلا الإطار الأوروبي المنظم للأدلة الرقمية يعتبره كثيرون أمراً ضرورياً بسبب آثار وأبعاد الجرائم العابرة للحدود، إذ يسهم بقدر كبير في إثبات هذه الجرائم ويسهل التعاون الدولي بشأنها، ويعمل علي توحيد وتطوير الإجراءات اللازمة للحصول على البيانات والمعلومات وحمايتها وجمع الأدلة الرقمية، بينما عدداً قليلاً من القانونيينjurists يعتبر أن تنظيم الأدلة ينبغي أن يظل خاصا بكل دولة، والممثلون عن استراليا والدنمارك وفنلندا يروا إن التشريعات الداخلية في كل دولة تغطي كل جوانب الأدلة بما في ذلك الرقمية، ولا ينكرون الآراء التي تشير إلى أنه بدون التنظيم الأوروبي المشترك للأدلة فإن تطبيق التشريعات على جرائم التكنولوجيا العابرة للحدود سيثير العديد من الاشكاليات القانونية بين الدول.

ولذلك فإن الإطار الأوروبي المنظم للأدلة هو السبل لتنظيم الأدلة الرقمية (الإلكترونية) وأنه عنصراً ايجابيا للتطوير التشريعي the legislative evolution في هذه المسألة[13]، و السؤال الذي يطرح هنا، ما هي المتطلبات التي يجب الوفاء بها في الأدلة الرقمية لكي تكون مقبولة في المحاكم الأوروبية ؟ للإجابة عن ذلك نقول أنه طبقاً للنصوص القانونية توجد مجموعتان من الدول فيما يتعلق بالمتطلبات التي يجب الوفاء بها في الدليل الرقمي لقبوله في المحكمة : المجموعة الأولى من الدول التي لها قواسم مشتركة من التقاليد القانونية وضعت معياراً واسعاًbroad criteriaلمقبولية الأدلة تستند فيه إلى النظرة الحرة للقاضي free consideration of the judge،ومن هذه الدول استراليا، الدنمارك، السويد، وفنلندا، والمجموعة الثانية من الدول نظمت تشريعاتها بطريقة أكثر تقييداً لمقبولية الأدلة وفقاً لسلسلة من المتطلبات اللازمة للأدلة أو طرق الإثبات.

ويعد مطلب مشروعية الدليل legality of evidence هو الأكثر ذكراً في قوانين بعض الدول مثل ألمانيا، و ايرلندا و المملكة المتحدة .[14]

---

[13] cyber intellegnce op cit p 38.
[14] Ibid. ,p 36.

وكذلك مطلب احترام الحقوق الأساسية الذي غالبا ما تشير إليه قواعد حماية المعلومات الشخصية، ويعد أيضاً موثوقية الدليل The reliability evidence من أهم المتطلبات الأساسية التي يفحصها القاضي من أجل تقرير مقبولية الدليل، وتوجد متطلبات أخرى تنص عليها بعض التشريعات تحدد مدى مقبولية الدليل الذي استخرج ومدى فعاليته في إثبات أي أدعاء[15] .

وخلاصة القول بأن القاسم المشترك في القوانين الأوربية أنها تشترط في متطلبات مقبولية الأدلة بأن يكون الدليل أصليا original كلما كان ذلك ممكناً وليس نسخة، ويجب أن يكون مباشراً وليس شهادة سماعية أو قولاً مرسلاً، و تعرف هذه المتطلبات بقواعد الاستبعاد rules of exclusion التي تحكم مقبولية الأدلة الرقمية في العديد من دول أوروبا، وعلى وجه الخصوص المملكة المتحدة وايرلندا.

وعلى الرغم من أن المتطلبات السابق ذكرها واضحة في النصوص القانونية، إلا أنه في الممارسة يظهر الحقوقيون اهتماما اكثر بالقواعد الأساسية المتعلقة بحق حماية المعلومات التي إذا اخترقت صار الدليل مرفوضاً، والقواعد اللازمة لفحص الدليل للتأكد بأنه أصلي authenticity ولم يتم تغييره inalterability.[16].

الفرع الثالث

تقدير الأدلة الرقمية

في إطار تحليل الدليل الرقمي والعناصر المؤثرة في متطلبات مقبولية الدليل الرقمي في المحاكم وفهم ما يواجه ذلك من مشاكل، وتحديد أفضل الممارسات لحماية الضحايا ومراعاة الحقوق الأساسية، وإمكانية تطوير الدليل الرقمي ومتطلبات مقبوليته كأداة مفيدة لمكافحة جرائم التكنولوجيا، أجريت في أوروبا العديد من المقابلات مع الفنيين والقانونيين والقضاة والممثلين للسلطات القضائية والشرطة و خبراء الطب الشرعي ورجال الأعمال، خلصت نتائج تلك المقابلات إلي بيان مزايا advantages وعدم ملاءمة inconvenience استخدام الدليل الرقمي إلى الآتي :

أولاً– مزايا الدليل الرقمي :

---

[15] cyber intellegnce op cit p 35.
Ibid., p 37.

1- إن الأدلة الرقمية تعرض المعلومات بشكل كامل وواضح ودقيق وموضوعي ومحايد، لأنه يأتي من عنصر الكتروني ،فلا توجد فيها الجوانب الشخصية على الإطلاق عند مقارنتها بأدلة أخري، مثال ذلك التصريحات التي يدلي بها الشهود يمكن أن تتناقض، علاوة على ذلك فإنها تتيح الحصول على المعلومات التي غالبا ما يستحيل الحصول عليها بالوسائل العادية وإثباتها بالأدلة التقليدية، ولذا يكون الدليل الرقمي هو أداة لجمع المعلومات واستظهار الحقيقة في الجرائم الالكترونية[17]

2- في العديد من الوقائع يعتبر الدليل الرقمي أداة أساسية لكشف وضبط الجرائم، لأنه قد يكون هو دليل الإثبات الوحيد الموجود في الواقعة ولا يمكن الاستغناء عنه

3- سهولة وسرعة جمع الأدلة الرقمية واستخدامها وحفظها conservation وتخزينها Storage.

4- هناك اتفاق كبير بين المحترفين professionals يدعو إلى استخدام الوثائق الإلكترونية والعمل على تطوير استخدام التكنولوجيا في التجارة الدولية وإثباتها بوسائل التقنية الحديثة[18].

ثانياً- عدم ملاءمة الدليل الرقمي :

إن الخلاف حول استخدام الدليل الرقمي ومقبوليته أمام المحاكم يتعلق بالموثوقية reliability، ومع أن الكثيرين يثقون في موضوعية ودقة الأدلة الرقمية ويعتبرونها أكثر موثوقية، وينادون باستخدامها، يرى آخرون أن عدم وجود وسائل للتحقق من أنها أصلية authenticity يجعلها أكثر عرضه للرفض، لذلك فإنها أقل موثوقية من الأدلة التقليدية، ومن غير الملائم استخدامها وقبولها للأسباب الآتية :

1- إن إعطاء قيمة قانونية لهذا النوع من الدليل أمر صعب بسبب الجهل بإجراءات معالجة البيانات، وترجم العاملون في مجال القانون هذه الصعوبة في عدم وجود لوائح ومنهجية محددة، وكذلك عدم وجود تجانس قضائي بين الأجهزة القضائية في أوروبا، لذلك فإن العاملين في مجال تقنية المعلومات أبدوا تخوفهم من ضعف الرقابة وسهولة التلاعب manipulated في هذه الأدلة مما يؤدي إلى وجود

---

[17] cyber intellegnce op cit p 29

[18] cyber intellegnce op cit p 29.

درجة عالية من التقلب وعدم التيقن من صحة الأدلة، الامر الذي يصعب معه قبولها كدليل إثبات .[19]

2- يرى البعض أن الأدلة ذات التقنية العالية تبدو غير مفهومة للقضاة وأعضاء النيابة العامة وصعبة في الشرح، إضافة إلى ذلك صعوبة الحفاظ علي البيانات والمسح الضوئي للمعلومات، وتخزينها بشكل صحيح لحفظها وبالتالي فإن الخروج من هذه المشكلة هو رفض استخدام الأدلة الرقمية في المحاكم، ([3]).

3- يرى العديد من خبراء الكمبيوتر بأن عدم وجود الدعم القانوني للأدلة الرقمية يجعل من الصعب قبولها كأدلة في المحكمة، فضلاً عن مطالبة القضاة بمزيد من الضوابط والضمانات لهذه الأدلة أكثر مما هو مطلوب في الأدلة التقليدية، ويفسر العديد من الخبراء بأن عدم الفهم الذي أبدته بعض الهيئات القضائية في أوروبا يعد عقبة أمام اللجان التي تقوم بتطوير آلية الحصول على الأدلة الرقمية، لذلك فإن هؤلاء الخبراء ينظرون إلى عملية الحصول علي المعلومات التي توفرها الأجهزة الالكترونية وتحليلها من أجل تحويلها إلى أدلة رقمية تستغرق وقتاً طويلاً، وتكلف مبالغ كثيرة وهذا يعوق عملية استخدامها[20] ،

4- إن تأمين المعلومات التي تقدمها الأدلة الرقمية بحيث تكون كاملة وحقيقية يعد أمراً صعباً في الوقت الحاضر، إذ أن الحفاظ على الأدلة إلى حين تقديمها للمحكمة بالنظر الى الوقت الطويل الذي تستغرقه المحاكمة يعد أمراً صعباً، إضافة الى ما تتطلبه من معرفة تقنية وتخصص دقيق والألمام بأحدث التقنيات [21] .

المطلب الثالث

متطلبات مقبولية الدليل الرقمي في المحاكم الأمريكية

في عام 2006 أجريت تعديلات جوهرية علي القواعد الفيدرالية للإجراءات في امريكا، وأصبحت هذه القواعد هي المتبعة في مسائل المعلومات الإلكترونية وكيفية استخدام الأدلة الرقمية ومقبوليتها في المحاكم، و قد نصت هذه القواعد على شروط

---

[19] Ibid., p 29.
[20] cyber intellegnce op cit p 30
[21] Ibid ., p .....

لمقبولية الدليل الرقمي ،و على ذلك فإن أي دليل يمكن أن يقبل، ويمكن أن يرفض ولو كان متصلاً بالقضية لأسباب تتعلق بطبيعة الدليل أو موثوقيته أو أن الدليل غير ذي صلة بالواقعةnot be relevantأو فقد قيمة الاثباتية عند استلامه، أو يحتوي على قول مرسل أو شهادة سماعية، إذ أن اكتشاف المعلومات المتعلقة بالجريمة لا يؤدي إلى افتراض قبولها، فربما يحدث العكس بأن ترفض إذا لم تتوافر فيها معايير مقبولية الأدلة الرقمية التي نصت عليها القواعد الفيدرالية للإثبات Federal Rules of Evidence. وقررتها المحكمة في القضية الشهيرة بين شركة Lorrinace و شركة Markel American Insurance التي وضعت خمسة مبادئ أساسية لمقبولية الدليل الرقمي أياً كان نوعه : أن يكون له صلة بالواقعة relevant–أن يكون أصلي authenticموثوقا فيه- reliable – الدليل الأفضل The best evidence – ليس شهادة سماعية not hearsay – .[22]

و يعد هذا الحكم سابقة قضائية مهمة لأنه يتناول بشكل مفصل متطلبات مقبولية الأدلة المستخرجة من الأجهزة الإلكترونية المختلفة كالبريد الإلكتروني ومواقع الإنترنت ومحتويات غرف الدردشة والتسجيلات المخزنة والمنقولة، وسنتناول في هذا المطلب دراسة هذه المتطلبات :

الفرع الأول

علاقة الدليل بالواقعة

يشترط في الدليل الذي تثبت به الجريمة وتنسب إلى المتهم أن يكون وثيق الصلة relevantly بالواقعة المراد إثباتها بطريقة مباشرة أو غير مباشرة، فكلاهما يؤدي إلى كشف الحقيقة، وإن كان في الأدلة غير المباشرة يتطلب من القاضي القيام بعملية ذهنية لاستنباط الحقيقة لأنها تنصب على غير الواقعة المراد إثباتها.

ويشترط لمقبولية الدليل الرقمي فيما يتعلق بعلاقته بالواقعة المراد إثباتها ما يشترط في غيره من الأدلة التقليدية ومن أهمها المشروعية، فلا يصح الاستناد عليه إذا تم الحصول عليه أو ضبطه بطريقة غير مشروعة .

والقاعدة العامة أن أمر التفتيش Search Warrant مطلوب للبحث عن الدليل وضبطه، فيلزم الحصول عليه قبل قيام المكلف بإجراء التفتيش سواء كان التفتيش متعلقا بشخص المتهم أم أوراقه أم متاعه أم منزله، ويتعين لإصدار أمر التفتيش أن يحدد القائم

---

[22]keilko. L. sugisak opcit p 1458.

به مبرر التفتيش، وبيان المكان أو الأشياء المراد تفتيشها والأشخاص المطلوب تفتيشهم، موضحا ظروف وملابسات الجريمة المرتكبة والدليل المراد ضبطه[23] ، إلا أنه يمكن في حالات معينة قبول الدليل الرقمي إذا تم الحصول عليه بدون أذن أو تفويض، فأوامر التفتيش في بريطانيا والعديد من الدول الأوروبية أكثر مرونة مما عليه في الولايات المتحدة إذ توجد في بريطانيا أنواعاً عديدة من الأوامر، مثل مذكرة تفتيش أماكن محددة، وغير محددة، وأوامر الدخول المتعددة للأماكن[24]، ولا يشترط في بعض الحالات لصحة التفتيش حصوله بناءً على إذن، إذ توجد في غالبية التشريعات استثناءات تسمح بالتفتيش بدون أمر، ومثال ذلك، المشاهدة (الرؤية الواضحة)plain view الرضا consent،والحاجة الماسة أو حالة الضرورة exigency ،ففي المشاهدة أو ما يعرف بالتلبس يستطيع المحقق ضبط الدليل، وهذه الصلاحية تخوله دخول المكان الذي يوجد به الدليل، وكذلك في حالة الرضا بالتفتيش يستطيع المحقق إجراء التفتيش دون الحصول على أمر التفتيش، إلا أنه يجب عليه أن يجري التفتيش بطريقة صحيحة للحد من الطعن فيه بالبطلان أثناء المحاكمة، والتفتيش بدون أذن warrantless search يمكن أن يتم أيضاً في أي حادث طارئ emergency يهدد الحياة أو سلامة البدن أو يهدد الدليل الرقمي بالتغيير أو التدمير،ففي الحالة الأخيرة يكون من الضروري ضبط جهاز الحوسبة computing device حالاً للتقليل من احتمال تدمير الدليل To reduce The potential of destruction of evidence على أن يتم التحفظ على الدليل بشكل جيد[25] .

ومن المسلم بهً أن التفتيش عن الأدلة الرقمية وضبطها سواء تم عملاً بالقاعدة العامة من وجوب الحصول على أذن للتفتيش عن الأدلة الرقمية وضبطها أو وفقاً للاستثناءات سالفة الذكر، توجد أربع مسائل يجب على المحققين مراعاتها عند تفتيش وضبط الأدلة الرقمية[26]، وهي :

أ- قانون سرية الاتصالات الإلكترونية (ACPA).

ب- تنفيذ متطلبات سرية الاتصالات الإلكترونية.

ج-الوقت الذي يبقى فيه المحققون في مسرح الجريمة.

---

[23]Eoghan cases op cit p 57.
[24]Ibid ., p 57.
[25]Eoghan cases op cit p55.
[26]Ibid,. p59.

د- احتياج المحققين لإعادة إدخال المعلومات.

كما يجب على القائمين بالتفتيش عن الأدلة الرقمية التركيز على أدلة الجريمة المرتكبة دون غيرها، ففي قضية (Carey سنة 1998) في أمريكا عثر المحققون على صور إباحية pornography على الآلة المراد تفتيشها بحثاً عن دليل لنشاط متعلق بالمخدرات، فهذه الصور لم تقبل في المحكمة باعتبارها خارج نطاق أذن التفتيش، إذ الطريقة الوحيدة للتعامل مع هذه المسألة هي الحصول على إذن تفتيش خاص بهذه الجريمة.

وفي عام 2009 – وضعت المحاكم الأمريكية ضوابط أكثر صرامةً للتفتيش عن الدليل الرقمي في حالة المشاهدة عن بعد(البعد الرقمية) digital dimension واقترحت طرق لتجنب المخاطر المرتبطة بانتهاكات السرية[27] .

الفرع الثاني

أصلية الدليل الرقمي

Authenticity of digital Evidence

في المحاكم عموماً عند البحث في مقبولية الدليل يتم السؤال عما إذا كان الدليل المستخرج recovered evidence هو نفس أصل البيانات التي ضبطت، ذلك أن التحقق من أن الدليل الرقمي هو دليل أصلي **Authentic** وأنه استخرج أو تم ضبطه من كمبيوتر أومن موقع معين، وإنه نسخة مطابقة للبيانات التي وجدت بجهاز الكمبيوتر دون أن يلحقه أي تغيير منذ ضبطه وتجميعه[28]، يعد أمرا ضروريا لمقبوليته .

ولاشك في أن إجراءات الحفاظ على البيانات والوثائق وسلامتها أو ما يعرف Chain custody and integrity، يعد أمراً مهماً لإثبات أصلية الدليل الرقمي[29]، ويتم إثبات الحفاظ على البيانات وسلامتها من خلال التأكد بأنها استخرجت من جهاز أو موقع معين، وأن هذه البيانات والأدلة المستمدة منها ظلت تحت المراقبة منذ لحظة تجميعها ولم ينالها

---

[27] Ibid,. p59.
[28] Robert.M.Redis. Amissibity of electronic evidence p2.
[29] Eoghan cases op cit p60.

أي تغيير أو تدمير، ذلك أنه من خلال الحفاظ على الوثائق والبيانات يمكن الربط بين الدليل الرقمي المستمد من تلك الوثائق أو البيانات والجريمة المرتكبة، فإذا كانت هذه الوثائق والبيانات أو المعلومات لم يحافظ عليها وعلى سلامتها بشكل صحيح، فإن ذلك يؤدي إلى نتيجة مربكة وتظهر الشك في موثوقية الدليل المتحصل عليه من خلالها[30] .

كما أن سلامة integrity الوثائق تساعد في إثبات أن الدليل الرقمي لم يتغير منذ تجميعه، ففي الحالات التي يكون فيها جزء من الدليل الرقمي يختلف عن الأصل، فإنه من الممكن عزل الأجزاء التي تختلف عن الأصل بحسب تغييرها والتأكد من سلامة ما تبقى منها، فعلى سبيل المثال إن الجزء السيئ الموجود على القرص الصلب الذي يحدث بسبب التكرار أو التغير في محرك الأقراص الذي يدخل ضمن الوثائق المستخرجة يتم استبعاده، فتحديد الأجزاء السيئة وتوثيقها يساعد المحققون على معرفة وتخصيص الملفات والبيانات المهمة في القضية، إضافة إلى أن الملفات الممتزجة بأجزاء سيئة يمكن أن تكون مفيدة في القضية من خلال مقارنتها بالأصل الموجود على القرص الصلب للتأكد من أن البيانات والأدلة المستمدة منها لم تتأثر بالأجزاء السيئة، وعندما تكون هناك مخاوف Concerns من أن الدليل الرقمي قد أسيء استعماله mishandledمما يحتمل أن تكون معلومات البراءة exculpatory information قد دمرت، فإن ذلك لا يمنع المحكمة من قبول الدليل طالما أنها رأت أن الأدلة مازالت محل ثقة[31] .

وفي بعض القضايا يحاول الطرف المعارض أن يلقى الشك في أي نوع من الأدلة، مثل التسجيلات والوثائق وجلسات الدردشة، وتعد قضية Tank في الولايات المتحدة أول قضية مهمة في التعامل مع أصلية تسجيلات الدردشة، ولكن البعض يرى أنه ماتزال هناك شكوك حول أصلية وموثوقية سجلات دردشة الانترنت، مع أنه قد توجد بها معلومات مهمة، فالمحققون يعتمدون اعتماداً كبيراً على السجلات وما يرد بها ،إذ أنهم قادرون على تعويض أي نقص في وجود الوثائق التي تثبت بأن الأدلة التي قدمت أصلية وموثوقة [32].

---

[30] Murdoch Watney-Admissibility of electronic evidence in criminal proceedings An outline of the south Africa – Legal position p.7.

[31] Eoghan cases op cit p60.

[32] Rebert. M. Redis op cit ….

الفرع الثالث

موثوقية الدليل الرقمي

Reliability of digital evidence

يتطلب تقييم موثوقيةReliability الدليل الرقمي أن يكون الدليل أصليا(حقيقياً)، ويتبع أحد النهجين في تقييم to assessing ما إذا كان الدليل الرقمي يمكن الاعتماد عليه في المحكمة: النهج الأول The first approach يقوم على التأكد من أن الكمبيوتر الذي أنتج generated الدليل يعمل بصورة عادية، والنهج الثانيThe second يقوم على فحص الدليل الرقمي الحقيقي The actual digital evidence لمعرفة الأدلة الناشئة عن العبث وغيرها من الافعال[33] .

في الماضي كانت غالبية التشريعات في الولايات المتحدة الأمريكية والمملكة المتحدة تتبع النهج الأول الذي يعطي المحاكم سلطة تقييم البيانات المستخرجة من الكمبيوتر على أسس موثوقية نظام الكمبيوتر وعملية استخراج البيانات، فعلى سبيل المثال المادة 9/6/901 من القواعد الفيدرالية للإثبات بعنوان متطلبات أصلية authentication والتطابق أو التماثل identification تقضي بأن الدليل يصف العملية أو النظام المستخدم في إحداث النتيجة، ويبين أن العملية أو النظام أحدث أو أنتج نتيجة دقيقة، وفي بريطانيا فإن الجزء رقم 69 يشتمل علي شرط شكلي للتأكد الايجابي positive assertion بأن الكمبيوتر المنتج للدليل يعمل بصورة صحيحة[34].

ومن المعلوم بأن موثوقية نظام أو عملية كمبيوتر معين أمر صعب في التقييم، فمن الناحية العملية المحاكم ليست مجهزة بشكل جيد لتقييم موثوقية أنظمة الكمبيوتر أو عملياتها، كما أن زيادة التنوع والتعقيد في أنظمة الكمبيوتر جعل من الصعب فحص كل

---

[33] Eoghan cases op cit p61.
[34] Ibid,. p62.

الأجهزة والوقوف على كل تعقيدات تشغيلها، إضافة إلى ما يبديه المبرمجون ومصممو البرامج من تحفظ على موثوقية الدليل، في أنه لا يمكن أن يؤسس على أدنى مستوى من فحص أجهزة الكمبيوتر والتعرف على دقتها، ولهذا نجد أعباء كثيرة على المحاكم وازدحام العديد منها بشهود التقنية[35]، كما أن صعوبة تصديق الكمبيوتر أو حتى عملية معينة في عمومها يمكن أن يعطل الموثوقية في ظروف معينة، علي اعتبار ان أنظمة الكمبيوتر توجد بها أخطاء تشغيل غير متوقعة تؤدي في بعض الأحيان إلى تلف البيانات، أو قد يحدث تعطل كارثيCatastrophic crash، لذلك فإن أجهزة الكمبيوتر ليست آمنة لكي نفترض ان الأدوات الميكانيكية منضبطة وقت العمل[36] .

ولهذا فإن مسألة موثوقية الدليل وفقاً للنهج الأول مسألة معقدة، فعندما يكون هناك شك يتعلق بموثوقية الدليل الرقمي، فلا يجعله غير مقبول، ولكنه يخفض من قيمته الإثباتية لدى المحكمة، وبالتالي إذا ما جادل الخصم في الدليل الرقمي على أنه غير موثوق فيه، لوجود شك بأنه تم التلاعب فيه أو تعديله altered أو تلفيقه Fabricated قبل ضبطه وجمعه أو بعد ذلك، فإن هذا التشكيك في الدليل قد يقلل من قيمته أو وزنه، وفي هذه المسألة بالذات أصبح القضاة أكثر دراية familiar بالدليل الرقمي، ويشترطون أدلة لدعم الادعاءات غير الموثوقة[37] .

وخلاصة القول أن تقييم موثوقية الدليل الرقمي الأكثر فاعلية هي التركيز على الدليل الرقمي ذاته أكثر من التركيز على العملية التي أنتجت الدليل، فهي أفضل من التأكد من كمبيوتر معين أو عملية معينة في عمومها موثوقة، وأكثر فاعلية للتعرف على التلاعب الكيدي أو تدمير عنصر معين من الدليل الرقمي، وعلاوة عن ذلك فإن عملية تطوير برامج الكمبيوتر وتعديل وظائفها لإصلاح الخلل ليست آمنة لكي نفترض أن عملية معينة في النظام الحالي قد تمت بنفس الطريقة وقت وقوع الجريمة[38] .

وهذا النهج لا يمكن العمل به عندما يكون الكمبيوتر تحت سيطرة الجاني، فليس من الملائم وضع تصنيف جامد لأنواع الأدلة بشكل عام بأنها صحيحة ويستطيع المدعي أن يتمسك بموثوقيتها، إذ أن البيانات الموجودة بأجهزة الكمبيوتر والأدلة المستمدة منها يمكن

---

[35] Eoghan cases op cit p62.
[36] Ibid ,. p62.
[37] Ibid,. p63.
[38] Eoghan cases op cit p62.

التلاعب tampered فيها، ولهذا التلاعب علامات مثل إلغاء سجل الدخول أو التسلل للكمبيوتر، وحتى اذا تم التأكد من موثوقية نظام وعملية الكمبيوتر، فإن ذلك لا يعني بالضرورة بأنه عندما كان في متناول يد الغير لم يتم العبث فيه لإخفاء الجريمة أو تضليل المحققين[39] ، في عام 1997م اوصت لجنة القانون law commission في بريطانيا بإلغاء الجزء 69 إذ لاحظت صعوبة تقييم موثوقية أنظمة الكمبيوتر واعتبرت ذلك نقداً مهماً لهذا الجزء (69)، لأن موثوقية أجهزة الكمبيوتر تتطلب شروط معقدة في أنظمة الكمبيوتر ذاتها حتى ولو لم يشترط في الدليل المستخرج أن يكون موثوقاً، لأنها قد تفشل في تحديد الأسباب الرئيسية لعدم دقة inaccuracy الدليل الرقمي[40] .

الفرع الرابع

الدليل الأفضل The best evidence

تقوم فكرة الدليل الأفضل على المطالبة بالدليل الأصلي original evidence عند التعامل مع محتويات الكتابة أو التسجيلات أو الصور، لضمان أن الأحكام والقرارات التي تصدرها المحاكم تستند إلى أفضل البيانات والمعلومات والأدلة المتاحة، ذلك أن ظهور التصوير والماسحات الضوئية Scanners والأجهزة الالكترونية الأخرى التي يمكن أن تصنع على نحو فعال نسخ مطابقة ومكررة identical duplicated للتسجيلات والصور وغيرها، ونسخ مقبولة بدلاً من الأصل، ولذلك عادة ما يثار سؤال حول صحة النسخة ودقتها مما يبعث الشك والريبة في هذه النسخة واعتمادها كدليل إثبات في الدعوى، وفي هذه الحالة فإن تقديم أصل الدليل الإلكتروني غالباً ما يكون مرغوباً desirableلأنه يزيل الشك أو الخطر بأن النسخة معدلة أو أن الأصل ذاته تم تغييره و نسخ منه شكل مطابق له تماما بعد تغييره والتلاعب فيه[41] ، لذلك فإنه وفقاً لقاعدة الدليل الأفضل المقررة بالمادة 1002 من القواعد الفيدرالية للإثبات في أمريكا لا تقبل نسخ الدليل الرقمي، إذ تقضى هذه المادة بأن الأصل يكون مطلوباً عند اثبات محتوي الرسائل أو السجلات أو الصور، وتقضى المادة 3/1003 بأنه إذا كانت المعلومات مخزنة في الكمبيوتر أو جهاز مماثل،

---

(39) ibid,. p62.
(40) Ibid,. p62.
(41) Ibid,. p64.

فإن أي مطبوع منها أو مستخرج output منها مقروء بالبصر readable by sight يظهر البيانات بدقة يعد نسخة أصلية[42] .

الفرع الخامس

الشهادة السماعيةhearsay

الدليل الرقمي لا يمكن قبوله إذا كان قولاً مرسلاً أو مجرد إشاعة (شهادة سماعية hearsay) لأن المتكلم أو مؤلف الدليل author of the evidence غير موجود في المحكمة للتحقق من صدقه، إذ أن الدليل هو بيان أو قول داخل المحكمة يكرر فيه الشخص ما أدلى به خارج المحكمة، وكذلك الأدلة الواردة في وثيقة هي مجرد قول مكتوب في وثيقة، فإذا لم تقدم هذه الوثيقة للمحكمة لإثبات أن التصريحات الواردة بها صحيحة، فإن الدليل المستمد منها يستبعد، باعتبار أن ما احتوته هذه الوثيقة تم خارج المحكمة، فعلى سبيل المثال ان الرسالة البريدية يمكن أن تستخدم لإثبات أن أحد الأفراد أرسل رسالة، ولكن لا يمكن أن تستخدم هذه الرسالة في إثبات حقيقة البيان الذي تحتويه الرسالة، ولذلك فاذا أرسل (أ) رسالة بريدية إلى آخر يشير فيها بأنه قتل أخاه، فإن المحققين يحتاجون إلى اعتراف confession أو دليل آخر لإثبات هذه الواقعة[43]، وفي أحدى القضايا نقض قاضي محكمة الاستئناف تهمة التوزيع مشيراً إلى أن البيان الصادر عن نشرة الإعلانات بأن البضاعة تم تحميلها من قبل شركة recent Zephyr مصحوبا بتسجيل في أغسطس أو أكتوبر 1993، هو مجرد أقاويل [44] ، إذ لا يوجد أي دليل على التحميل أو التاريخ المحدد، وإذا كانت القاعدة العامة في القواعد الفيدرالية للإثبات هي عدم قبول الشهادة السماعية، فإن المادة 803 قررت العديد من الاستثناءاتexceptions على هذه القاعدة [45]، باستيعابAccommodate الدليل الذي يصور الأحداث بدقة

---

[42]Robert M. Redis op cit p24.
[43]Eoghan cases op cit p65.
[44]ibid ,. p65.
[45]keiko.L.sugisak op cit p1460.

تامة ويسهل التحقق منها، كما أن القواعد الفيدرالية للإثبات في أمريكا التي تحدد السجلات المنظمة للأنشطة لم تستبعد إثبات هذه السجلات بقاعدة الشهادة السماعية[46] .

وكذلك البيانات الإلكترونية في الأعمال التجارية، فإن الكثيرين يحاولون التغلب علي اعتراضات الشهادة السماعية بإثبات عنصر العمل التجاري في هذه السجلات لاستثنائها أيضا من قاعدة عدم قبول الشهادة السماعية[47] .

أ.د. سالم الأوجلي
عضو هيأة التدريس بقسم القانون الجنائي
كلية الحقوق – جامعة بنغازي

[46]Robert . M. Redis op cit p20.
[47]Rebert . M. Redis op cit p20.

المـــراجع

1- EoghanCassey Digital evidence an computer crime third edithion 2011.
2- Keiko. L. Sugisaka Admissibility of evidence in Minnesota: New problems or evidence as usual.
3- Murdoch watney – Admissibility of electronic evidence in criminal proceedings: An outline of the south Africa Legal position journal of information, Low and Technology 2009.
4- Rebert. M. medis Admissibility of electronic evidence.
5- Cybex intelligence on evidence . The Admissibility of electronic evidence in court www. Cybex.
6- Stephon mason international electronic evidence British institute of international and comparative law.