مدي حجية الأدلة الإلكترونية الرقمية
في الإثبات في المواد الجنائية
دراسة تحليلة تطبيقيه مقارنة

د/ محمد عبد الحميد عرفة
مدرس القانون الجنائي
كلية الحقوق – جامعة الإسكندرية

المقدمة

تعتبر الجريمة الإلكترونية في الوقت المعاصر هي اكبر تحدي يواجه المشتغلين بالتشريع والقانون ليس في مصر فقط بل في العالم أجمع، إذ أن هذه الجريمة مرتبطة ارتباطاً وثيقاً بالتطور العلمي و التكنولوجي الهائل الذي تشهده علوم الكمبيوتر والحاسب الآلي في الأونة الأخيرة .

فضلاً عن ذلك ، نجد أن المجرم المعلوماتي يختلف اختلافاً جذرياً عن المجرم الطبيعي من حيث قدرات الذكاء والإحتيال التي تشرط أو تتطلب قدرات موازية ومماثلة لدي القائمين علي تشريع ووضع القوانين والتشريعات الخاصة بمكافحة الجريمة الإلكترونية ومعاقبة مرتكبها .[1]

هذا ويمكن القول بأن الأونة الأخيرة من القرن المنصرم شهدت ثورة معلوماتية ضخمة في مجال الاتصالات وتكتولوجيا المعلومات مما أدي لظهور أجيال جديدة من وسائل الاتصال عن بعد والتي كان لها دوراً في إعادة صياغة شكل العالم، فاصبح قرية صغيرة لا تعرف الحدود والفواصل وعليه، فتعقدت الجريمة وتنوعت أشكال ارتكابها مستعينة بهذا التطور العلمي الهائل، ومن هنا ظهر ما يعرف بالجريمة المعلوماتية أو الإلكترونية .[2]

هذا وقد أدي الإنتشار السريع و المتلاحق للإنترنت وكذا تطور أجيال جديدة وأنواع مختلفة من أجهزة الكمبيوتر إلي كثرة المخاطر ومضاعفة الإعتداء علي الملكية الخاصة والحقوق والحريات الشخصية ، بل اكثر من ذلك علي مصالح الدولة مما دعا بعض الدول الكبري للانتباه لهذه المسألة ، فبدأت الدول والحكومات في اقرار بعض الإتفاقيات الدولية التي تجرم بعض الأفعال أو السلوكيات الواقعة عبر الوسائل الإلكترونية أوبواسطتها كاتفاقية بودابست لعام ٢٠٠١.

"The Convention of Cyber Crime of the Council of Eurpoe (ccets. No 185)"

---

[1] انظر د/ نائلة عادل قورة، جرائم الحاسبات الإقتصادية: دراسة نظرية وتطبيقيه، دار النهضة العربية ،٢٠٠٤، ص٢١

[2] انظر د/ رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة والمواثيق الدولية، دار النهضة العربية، طبعة أولى ، ٢٠١١، ص٥٢ ومابعدها.

وكذا القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات و الاتصالات الذي تم في عام ٢٠٠٣ كتوصية ناتجة عن اجتماع مشترك لوزراء العدل العرب.

"Arab Model Law on Battling the Misuse of Technology and Cyber Crimes.[1]"

غير أن هذه التشريعات ليس لها أثراً فعلياً أو فعالاً في الأنظمة الجنائية في الدول العربية وبصفة خاصة مصر إذ أن هناك بعض التشريعات المتناثرة التي تحتويها قوانين تنظم موضوعات مختلفة فيما يتعلق ببعض صور التجريم الإلكتروني ومنها قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤ وقانون حماية الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢ وكذا قانون الأحوال المدنية المصري رقم ١٤٣ لعام ١٩٩٤ فضلاً عن قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ إلان هذه القوانين لم تشمل كافة صور الإجرام المعلوماتي وهو ما أثر بالسلب علي المجتمع انطلاقاً من عدم توفير الحماية القانونية اللازمة لافراده [٢] .

وانطلاقاً من المبدأ الدستوري الذي يحكم التجريم والعقاب في مصر والمعروف بمبدأ الشرعية الجنائية "Principle of Legality" المنصوص عليه في المادة ٩٥ من الدستور المصري ٢٠١٤ والذي يقضي بأن "العقوبة شخصية ولاعقوبة إلا بناء علي قانون ولا توقع عقوبة إلا بحكم قضائي ولاعقاب إلا علي الأفعال اللاحقة لتاريخ نفاذ القانون" فيصبح القاضي حائراً عندما يُعرض عليه فعل يشكل جرماً إلكترونياً وذلك في ظل غياب النص التشريعي رغم وجود المبدأ الدستوري، لا يجد نصاً صريحاً في قانون العقوبات فكيف يكون السبيل للحكم القضائي؟[٣]

---

[1] David Gray, Danielle K.Citron, &Liz C.Rinehart, Fighting Cyber Crime After United States v.Jones, 103 Journal of Criminal Law & Criminology 3 (2013).

[2] Susan W. Brenner, State Cyber Crime Legeslation in the United States of America:A Survey, 7 Richmond J. of Law & Technology 3 (2001).

[٣] الدستور المصري الحالي ٢٠١٤؛ مادة ٩٥.

ومن المسلم به أن الإثبات في المواد الجنائية هو نشاط إجرائي موجه مباشرة للوصول إلي الحقيقة واليقين القضائي طبقاً لمعيار الواقعية، وذلك فيما يتعلق بالإتهام أو تاكيده أو نفيه بمعني إقامة الدليل علي وقوع الجرم ونسبته لفاعل معين .[1] فيكون الهدف من الإثبات هو بيان مدي التطابق النموذجي بين الجريمة و الواقعة المعروضة أمام القاضي، فيكون له استخدام وسائل إثبات معينة – كي يصل للحقيقة : فهو عليه بذل المجهود في سبيل اكتشاف شخص أوحالة شئ مما يفيد في ايضاح عناصر الإثبات (الأدلة) المختلفة وترجمتها علي أرض الواقع الملموس.[2]

هذا وتثير مسألة الإثبات في النظم الإلكترونية والمعلوماتية صعوبات كبيرة أمام القائمين علي التحقيقات الجنائية، وذلك نتيجة لنظام التخزين الإلكتروني للمعطيات التي يجعل من شأنها غير مفهومة (غير مرئية) فيصعب ملاحظتها بالعين المجردة. [3] فإذا كان انعدام الدليل المرئي المفهوم يُشكل معضلة وعقبة قانونية كبيرة أمام كشف الجرائم ، وكذا تفسير البيانات المخزنة إلكترونياً وحتي – المنقولة عبر وسائل الاتصال عن بعد – فمن باب أولي أن محو الأدلة المعلوماتية وسهولته في زمن قصير قد لا يتجاوز بضع ثوانٍ – يعد من أهم المشاكل و الصعوبات التي تواجه عملية الإثبات الجنائي في مجال الإنترنت والحاسوب .[4]

وتزيد المشكلة تعقيداً عنما يتعلق الشأن ببيانات أو معلومات تم تخزينها في الخارج عبر شبكات الاتصال عن بُعد، إذ أن القواعد التقليدية الإثباتية لا تكون كافية بطبيعتها لضبط مثل هذه المعلومات بحثاً عن الأدلة وتحقيقها.

ولما كانت أدلة الإثبات المتحصلة من الإنترنت و الكمبيوتر تحتاج إلي خبرة فنية وإدارية عالية ومهارة فعالة، فإن نقص الخبرة في هذا المجال وخاصة من جانب سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدي – في بعض الأحيان – إلي ضياع

---

[1] د/ عبد العظيم مرسي وزير، شرح قانون العقوبات، دار النهضة العربية، ١٩٨٣، ص٣٣.
[2] د/ رامي القاضي، المرجع السابق، ص٥٤.
[3] راجع د/ أحمد فتحي سرور، القانون الجنائي الدستوري، دار الشروق، طبعة ثانية،٢٠٠٢، ص٣١.
[4] انظر د/ رمسيس بهنام،الإجراءات الجنائية تأصيلاً وتحليلاً، منشأة المعارف ،الإسكندرية،١٩٨٤.

الدليل بل تدميره. [1]كما أن صعوبة الدخول للحصول علي المعلومات المخزنة وذلك نتيجية لوجود نظام معلوماتي أمن وكذا تقاعس المجني عليه في الابلاغ عن الجرائم المعلوماتية إلي السلطة المختصة لاعتقاده – بعدم جدوي إبلاغه – بشكل صعوبات أخري في مجال الإثبات. [2]

ولما كانت الجريمة الإلكترونية أصحبت دافعاً ملموسًا لاريب فيه تواجه العالم أجمع وخاصة مصر في ظل القصوَر القانوني و التشريعي الجلي في مواجهة تلك الجرائم، فأنه يتعين علينا أن نخوض في الإجابة علي تساؤل هام يطرح نفسه وهو مدي حجية الدليل المعلوماتي (الإلكتروني) في مجال الإثبات الجنائي سواء من ناحية كونه دليل براءة أو إدانة ومدي تكييف ذلك من الناحية القانونية . بعبارة اخري ما هي حجية الدليل الرقمي أمام القضاء الجنائي المصري من حيث كونه دليل إثبات قائم بذاته ومدي إمكانية تعديل التشريعات المصرية المنظمة لحركة المعلومات والاتصالات وما يتوافق مع حقيقة وجود هذا الدليل واعتماده كدليل إثبات شأنه شأن كافة أدلة الإثبات الأخري المتعارف عليها في المواد الجنائية .

ولكن قبل الإجابة علي هذا التساؤل فأنه يتعين علينا أن نعرض في فصل تمهيدي لنبذة مختصرة – عن ماهية الجريمة الإلكترونية وأسبابها وخصائصها ونشأتها ووسائل مكافحتها في المواثيق الدولية وكذا الدستور و القانون فضلاً عن معرفة صفات المجرم المعلوماتي أو الإلكتروني .

---

[1] انظر بوجه عام، د/ جلال ثروت، نظم الإجراءات الجنائية ، دار الجامعة الجديدة ،الإسكندرية ، ٢٠٠٣.

[2] د/ رامي القاضي، مرجع سابق الإشارة إليه ، ص٥٧.

الفصل التمهيدي

الجريمة المعلوماتية (الإلكترونية)

تمهيد وتقسيم

أسهم دخول التكنولوجيا والتقنيات الحديثة في مجال الاتصالات وتكنولوجيا المعلومات وشبكة الإنترنت إلي انبثاق أنواع وأشكال مستخدمة من السلوكيات الإجرامية لم يكن للإنسانية سابق علم بها. فهذه النوعية من السلوكيات الجرمية تتصف بأنها معقدة في إمكانية ارتكابها ووسائل كشفها فضلاً عن اعتبارها ذات طبيعة دولية، فأصبحت خطراً داهماً يهدد العالم أجمع. وعليه سنتناول في هذا الفصل بعض ملامح الجريمة الإلكترونية وكذا خصائصها وطبيعتها القانونية وما يتميز به المجرم المعلوماتي عن المجرم التقليدي.

أولاً: في التعريف بالجريمة الإلكترونية والمعلوماتية وبيان خصائصها وطبيعتها القانونية

ذهب بعض الفقه للقول بأن الجريمة المعلوماتية "فعل غير مشروع يتورط في ارتكابه الحاسب الآلي أو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية" وكذا عرفها البعض بأنها كل عمل أو فعل أو نشاط غير مشروع هدفه (أوموجه) نسخ أو تغيير أو حذف أو الوصول للمعلومات المخزنة داخل الكمبيوتر وإلي تحويل طريقه.[1] أما مكتب تقييم التقنية الأمريكي "US Technical Assesement Office" وكذا معهد فلوريدا للتكنولوجيا قد توصل إلي تعريفها بأنها "الجرائم التي تلعب فيها البيانات الكمبيوتورية و البرامج المعلوماتية دوراً رئيسيًا[2]."

فيمكن القول – في ضوء التعريفات السابقة – إلي أن جريمة الحاسب تشمل استخدامه كأداة لارتكاب الجرم فضلاً عن الحالات الخاصة بالولوج غير القانوني لحاسب المجني عليه أو بياناته ، كما تمتد هذه الجريمة لتشمل الإعتداء المادي سواء علي بطاقات الإئتمان Credit Cards وانتهاك ماكينات الكمبيوتر بما تحويه من شبكات تحويل

---

[1] د/ على محمود حموده، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، اكاديمية شرطة دبي (٢٠٠٣).

[2] د/ حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة، دار النهضة العربية،(٢٠٠٩)، ص٥٣ ومابعدها.

الحسابات المصرفية بطريقة إلكترونية "Electronic Deposit" وكذا تزييف المحتويات المادية و المعنوية للحاسب بل وسرقته في ذاته وأي من مكوناته [1].

فقد يكون الإعتداء بهدف تحقيق الربح أو إلحاق خسارة بالمجني عليه، فالإتجاهات السابقة اهتمت إما بالناحية العضوية (الشكلية) في تعريف الجرم وإما بالناحية الموضوعية (الوظيفية) في تحديد مفهوم هذا السلوك.

وقيل أيضاً في مفهومها إنها عمل أو امتناع يحدثه الفرد إضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقوبة جنائية. كما أن الأمم المتحدة أشارت في مدونتها الصادرة بشأن الجريمة المعلوماتية إلي إنه لا يوجد اجماع في الفقه علي تعريف هذا السلوك إلا أن هناك اتفاق واجماع لا شك فيه حول وجود ظاهرة تتزايد بمعدلات عالمية لتلك الجرائم .[2]

وفي ضوء ذلك كله، يمكن القول بأنه من الصعوبة بمكان وضع تعريف أو مفهوم محدد لهذه الجريمة وإنما يمكن مراعاة اعتبارات عملية عند وضع تعريف لها، كأن يكون هذا التعريف مفهوم ومقبول دولياً وكذا أن يراعي التطورات المتزايدة في مجال تكنولوجيا المعلومات مع بيان طبيعة الدور الذي يقوم به الحاسب في إتمام النشاط الإجرامي فضلاً عن تمييز هذا التعريف بين الجريمة التقليدية و المعلوماتية [3]

وفي صدد الحديث عن المعلومات نجد أن أغلب التشريعات الوطنية جاءت خالية من وضع تعريف لها إلا أن المشرع الأمريكي قد عرفها في قانون المعاملات التجارية الإلكتروني لعام ١٩٩٩ (مادة ١٠/٢) بأنها "تشمل البيانات و الكلمات والصور والإجراءات و الوسائل وبرامج الكمبيوتر والبرامج المضغوطة الموضوعة علي الأقراص المرنة وقواعد بيانات أو ما شابه ذلك."[4]

---

[1] أنظر د/ هلال عبد الله أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة ٢٣ نوفمبر ٢٠٠١، دار النهضة العربية،٢٠٠٢، ص٦٧ ومابعدها.

[2] د/ رامي متولي القاضي، مرجع سابق الإشارة إليه ، ص٦١ ومابعدها.

[3] أنظر بوجه عام: د/ آمال عبد الرحيم عثمان، الإثبات الجنائي ووسائل التحقيق العلمية، دار النهضة العربية ١٩٧٥.

[4] د/ سعيد عبد اللطيف حسن ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت: الجرائم الواقعة في مجال تكنولوجيا المعلومات، طبعة أولى ، دار النهضة العربية،١٩٩٩، ص٧٥ ومابعدها.

كما عرفها المشرع الفرنسي في القانون رقم ٦٥٢/٨٢ لسنة ١٩٨٢ بأنها "صور أو مستندات أو معطيات أو خطابات أياً كانت طبيعتها."[١]

وفي قانون البحرين رقم ٨٣ لسنة ٢٠٠٢ بشأن المعاملات الإلكترونية فقد عرفت المعلومة (بأنها البيانات و النصوص والصور والأصوات والرموز وبرامج الحاسوب و البرمجيات ويمكن أن تكون قواعد البيانات و الكلام) ويمكن انطباق ذات التعريف السابق علي مفهوم المعلومة المنصوص عليه في قانون إمارة دبي بشأن المعاملات والتجارة الإلكترونية رقم ٢/ لسنة ٢٠٠٢. [٢] ويكمن معيار التمييز بين المعلومات والبيانات في كون الأخيرة تعبر عن مجموعة من الأرقام والرموز و الحقائق التي لاعلاقة بين بعضها البعض، أما الأولي فهي المعني الذي يستخلص منه هذه البيانات .[٣]

هذا وتتقسم المعلومات لعدة طوائف منها معلومات اسمية موضوعية كالمرتبطة بشخص المخاطب بها (كإسمه وموطنه و حالته الإجتماعية) وهي لا يجوز الإطلاع عليها إلا باذن وموافقة الشخص ذاته وهناك معلومات اسمية شخصية وهي المنسوبة لشخص آخر مما يستدعي ادلاء الغير برأي الشخص (كالمقالات الصحفية مثلاً). وهناك معلومات خاصة بالمصنفات الفكرية وهي محمية بحكم قوانين الملكية الفكرية (كالإختراعات و التسجيلات والمؤلفات وغيرها). وهناك المعلومات المتاحة للجميع، فلهم الحق في الحصول عليها، إذ إنها دون مالك فهي غير محمية بأي وسيلة من وسائل الحماية (كالنشرات الجوية وتقارير البورصة)[٤].

هذا ويشترط في المعلومات المتمتعة بالحماية القانونية أن يتوافر فيها الإبتكار و التحديد بمعني أن تكون المعلومة محددة تحديداً دقيقاً ، فإذا كانت المعلومة تفتقد التحديد

---

[١] د/ رامي القاضي، مرجع سابق الإشارة إليه، ص٦٤.

[٢] Okin S.Kerr, Cyber Crime's Scope: Intepreting "Acess" and "Authorization" in Computer Misuse Statutes,78 New York Univ.L. Rev.1596 (2003).

[٣] انظر د/ أحمد عوض بلال،الإجراءات الجنائية المقارنة والنظام الإجرائي في المملكة العربية السعودية، دار النهضة العربية، القاهرة، طبعة خمسة (٢٠١٣).

[٤] حسنين المحمدي البوادي، الوسائل العلمية الحديثة في الإثبات الجنائي، منشأة المعارف، الإسكندرية، طبعة أولى (٢٠٠٨)، ص ٧٢ ومابعدها.

فلا يمكن أن تكون معلومة حقيقية، ويتطلب ذلك في خصوص الإعتداء علي الأموال، إذ يشترط أن تكون الإعتداءات واقعة علي شئ مبتكر ومحدد أو (معين) إذ أن الشئ الشائع لا يتمتع بحماية قانونية .[1] ويشترط كذلك أن تكون المعلومة سرية، فالمعلومة العامة الشائعة تكون بمنأى عن أي حيازة فتكون سرية بالنظر لطبيعتها أو نظراً لإرادة الشخص أو الأمرين معاً (كالرقم السري Password).[2]

ثانياً: في أسباب الجريمة المعلوماتية وبيان خصائصها الرئيسية (طبيعتها القانونية) ونشأتها

من المسلم به أن فئات مرتكبي الجريمة الإلكترونية تختلف عن مرتكبي الأفعال الجريمة العادية، إذ أن من الطبيعي أن هذه الجرائم الأولي لها خصائص تختلف تماماً عن الأخيرة فضلاً عن السمات التي تميز الجاني في الجرم الأول عن شبيهه في الجرم الثاني .

ويأتي في مقدمة أسباب أو دوافع الجريمة الإلكترونية دافع التعلم المتمثل في الشغف في استخدام جهاز الكمبيوتر والإمكانيات الحديثة لنظم الاتصالات وتكنولوجيا المعلومات. ففيما يتعلق باخلاقيات قراصنة المعلومات، فهي مضمحلة لحد يمكن القول معه بأن هؤلاء القراصنة يرون أن جميع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة لآيه قيود، ومن هنا يتضح أن أخلاقهم ترتكز علي أن الدخول لأجهزة الحاسوب وأنظمته يمكن أن يعلمك كيف يدور العالم من حولك فضلاً عن عدم خضوع جميع المعلومات لأي عوائق، فبغرض التعلم يهدف هؤلاء القراصنة (Hackers) للوصول لمصادر المعلومات والحاسبات الإلكترونية و الشبكات.[3]

ويلاحظ أن هؤلاء الأشخاص لديهم اهتمام شديد بأجهزة الكمبيوتر، وبالتعلم يمكن دخولهم علي أنظمة تلك الأجهزة علي إنهم محترفين، فهم يرغبون في النهاية في البقاء مجهولين حتي يستطيعوا الإستمرار في التواجد داخل الأنظمة الإلكترونية لمدة طويلة فيكرس بعضهم وقته في تعلم كيفية اختراق الأنظمة والتقنيات الأمنية وكذا اختراق

---

[1] المرجع السابق، ص ٧٦.
[2] د/ أحمد بلال، مرجع سابق الإشارة إليه، ص٨١-٨٤.
[3] د/ رامي القاضي، مرجع سابق الإشارة إليه، ص٦٧-٧٠.

المواقع الممنوعة.[1] فكلما اكتشف قراصنة الأنظمة نقطة ضعف أو عيب أمني، فيقوموا بمحاولة استغلالها إذ إنها موجودة بهدف عدم سرقة المعلومات أوإتلافها (أو تخريبها).[2]

كما أن الرغبة في تحقيق الثراء تعتبر من العوامل الأساسية لارتكاب هذه الجرائم كما أشار بعض الفقه المختص في الأمن المعلوماتي"Information Security" . فيمكن القول بأن الدافع لارتكاب هذه الجرائم يكون سببه مجرد وجود مشاكل عائلية راجعة للنقود أو إدمان العاب القمار أو المخدرات أو حتي سداد الديون المستحقة، ولذلك فان بيع المعلومات المختلسة هو نشاط ممتع للغاية.[3]

هذا وتلعب الدوافع الشخصية دوراً اساسياً في ارتكاب مثل هذه السلوكيات، فغالباً ما يميل مرتكب تلك الجرائم إلي إظهار تفوقهم ومستوي ارتقاء براعتهم، فيكون الهدف هو الرغبة في قهر النظام القانوني وإثبات عجزه وفي محاولة لكسر حواجز الأمن لأجهزة الكمبيوتر.[4]

الأمرالذي قد دعا بعض فقهاء القانون الجنائي – وهو أمر يدعو للغرابة – إلي عدم مساءلة مرتكبي الجرائم الإلكترونية جنائياً إذ أن باعثهم – وفقاً لعامل الدوافع الشخصية يتمثل في إظهار التفوق التكنولوجي – إذ أن اعمالهم غير منطوية علي نوايا آثمة. وهوالأمرغير المقبول بطبيعة الحال، فقد تتوافر النية الإجرامية لدي الفاعل في الحاق الضرر بالمجني عليه فتقع الجريمة بناءاً علي هذا الأساس .[5] وعليه يمكن القول بأن البعض يرتكب تلك الأفعال لولوعه في الحصول علي المعلومات الجديدة كالقراصنة أو للإستيلاء علي المعلومات الموجودة على الحاسوب أو حتى حذفها أو تدميرها أو الغائها نهائياً، فيكون الغرض هو الآثارة و التحدي – وكذا أيضا تحقيق الشهرة وإثبات التفوق العلمي .

---

[1] راجع الدكتور/ هشام محمد رستم، الجوانب الإجرائية للجرائم المعلوماتية: دراسة مقارنة، مكتبة الآلات الحربية، أسيوط ،١٩٩٤، ص١٠-١٦.

[2] المرجع السابق، ص١٨.

[3] المرجع السابق، ص٢٠.

[4] انظر د/ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت: دراسة متعمقة في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة،٢٠٠٢، ص٤٤.

[5] المرجع السابق، ص٤٧.

أما فيما يتعلق بسمات هذه الجرائم وطبيعتها القانونية، فاننا نجد أن هذه الجرائم المرتكبة بواسطة الكمبيوتر كأداة وكهدف للجريمة تتميز بعده خصائص نعرضها فيما يلي:

١- سرعة تنفيذها: إذ أن تنفيذها لا يتطلب وقتاً طويلاً، فبضغطة واحدة علي لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات وهذا لايعني إنها لا تتطلب إعداداً جيداً ومسبقاً لتنفيذها (كاستخدام برامج ومعدات معينة) .[١]

٢- لا تعرف الحدود المكانية والزمانية : إذ إنها ترتكب عبر شبكات الإنترنت لا تحدها حدود جعرافية كحدود دولة بعينها، فيمكن أن يكون العالم مسرحاً للجرائم كما أن الزمن لا يعرقلها رغم اختلاف المواقيت بين الدول، فهي تحدث وتنفذ عن بُعد فلا يُتطلب وجود الفاعل في مكان الجرم (اللهم إلا كانت جريمة سرقة معدات الكمبيوتر تتطلب وجوده) فيرتكب الفاعل جريمته وهو في دول بعيدة، كالدخول على الشبكة المعنية أواعتراض عملية تحويل مالية مثلاً[٢].

٣- جريمة مخفية : إن الجرائم التي تقع علي الحاسوب أو بواسطته (كجرائم الإنترنت) تكون غالباً في الخفاء وإن كان يمكن ملاحظة آثارها والتنبوء بوقوعها. [٣]

٤- جرائم ناعمة : لا تتطلب استخدام الأدوات والعنف كما في الجرائم التقليدية كالسرقة والسطو المسلح، فنقل البيانات لا يحتاج ممارسة أي أعمال عنف أو الاشتباك مع رجال الامن .[٤]

٥- عابرة للدول: إذ أن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية و الفضائيات والإنترنت جعل الإنتشار الثقافي وعولمة الثقافة والجرم أمر شائع

---

[١] انظر محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة،الإسكندرية، ٢٠٠١، ص٤٢- ومابعدها.

[2] Janaletchumi Appuderai and Chita Ramalmgam, Computer Crimes:A Case Study of What Malysia Can Learn from Others? 2 Jounal of Digital Forensics Security, and Law 2 (2007).

[٣] د/ عبد الفتاح بيومي، المرجع السابق الإشارة إليه، ص٤٨.

[٤] المرجع السابق، ص٤٩.

وممكن الحدوث، لا يعترف بالحدود الإقليمية للدول ولا بالزمان ولا المكان، فقد يكون الضرر الواقع علي المجني عليه واقعاً في دولة غير دولة الجاني .[1]

٦- الصعوبة في الإثبات: ويكون ذلك راجعاً لافتقاد وجود الآثار التقليدية للجرم وغياب الدليل الفزيفي (كالبصمات وأفعال التخريب أوالشواهد المادية) وكذا بساطة محو وتدمير الدليل في مدة قصيرة فضلاً عن نقص خبرة الشرطة والنظام القانوني القائم وعدم كفايته .

٧- عالمية الجريمة والنظام العدلي الإجرائي: نظراً لارتباط المجتمع الدولي إلكترونياً، فقد أضحي العالم مساحة كبيرة لارتكاب الأفعال الإجرامية، الأمرالذي تطلب واستدعي الدول والحكومات و- خاصة الكبري والصناعية – لسن التشريعات وقوانين لمكافحة تلك الظاهرة مما أدي إلي اصطباغها بالصفة العالمية "Principle of Universality"[2]

هذا ويلاحظ إنه لا يتم الإبلاغ عن تلك الجرائم في معظم الأحيان وذلك لعدم اكتشاف الضحية، وإما لخوفه من التشهير والفضحية ، فمعظم هذه الجرائم غالباً ما تكتشف بمحض الصدفة وبعد مدة طويلة من ارتكابها .فهذه الجرائم تقع تحت ما يسمي بظاهرة الرقم المظلم أو الأسود Dark Figur of Crime فالفجوة بين عدد هذه الأفعال الخفية ومايتم اكتشافه كبيرة للغاية وذلك إذ إنه من السهل إخفاء معالمها وصعوبة تتبع مرتكبها.[3]

كما إنها لاتترك أثراً بعد ارتكابها، فمن غير الممكن أن تحتفظ باثارها الفنية بعد وقوعها – إلا فيما ندر – فليست هناك أموال أوغيرها مفقودة بل تلاعب وتغير في سجلات وبيانات ومعلومات كما أن الوصول للتحقيق بشأنها يستهدف الإستعانة بكفاءة قوية ومهارات عالية المستوي إذ إنها جرائم وأفعال تتسم بالغموض يصعب علي المحقق

---

[1] Jonathan Mayer, Cyber Crime Litgation, 164 Pennsylvaina L. Rev.145(2016).

[2] المرجع السابق، ص ١٤٦٠.

[3] المرجع السابق، ص ١٤٦٥.

العادي التعامل معها إذ أن ارتكابها يعتمد علي قمة الذكاء فيصعب متابعة هذه الجرائم وكشفها وإثباتها أى بإقامة الدليل عليها[1].

ويصعب المطالبة بالتعويض المدني بخصوص هذه الجرائم، إذ أن عولمة هذه الجرائم يؤدي إلي شلل جهود التحري والتعاون الدولي لتعقب مثل هذه الأفعال فيثار التساؤل حول القانون الواجب التطبيق علي هذه الجريمة فضلاً عن جهة الإختصاص القضائي.

في ضوء ما تقدم، يمكن القول بأن الجريمة المعلوماتية تثير صعوبات في مجال التحقيق الجنائي وكذا متطلبات الضبط والتفتيش والملاحقة الجنائية إذ إنها جرائم عابرة للحدود وتتسم بالخطورة الشديدة، فقد تكون الخسائر الناتجة عنها باهظة للغاية كما انها ترتكب من فئات إجرامية متعددة يجعل من الصعوبة بمكان معرفة الفاعل لانها تنطوي علي سلوكيات غير مألوفة.

ويبقي التساؤل في هذا الصدد حول المجرم المعلوماتي من هو؟ وما هى سماته ؟

كان لارتباط الجريمة الإلكترونية بأجهزة الكمبيوتر والحاسب الآلي أثره الرئيسي علي تمييزها عن غيرها من الجرائم المعتادة، خاصة جرائم الإعتداء علي الأموال بل وان كان آثره امتد لتمييز المجرم المعلوماتي – مرتكب هذا الجرم – عن غيره من المجرمين العاديين الذين قرورا الجنوح لارتكاب السلوك الإجرامي النمطي. وعليه، يمكن أن نستخلص مجموعة من الخصائص التي يتسم بها هذا المجرم والتي تساعد علي معرفة نوع شخصية هذا الجاني ومواجهه هذا النمط الحديث من المجرمين.

ذهب بعض الفقه المهتم بدراسة الجريمة الإلكترونية بصفة عامة والمجرم المعلوماتي بصفة خاصة وقالوا أن هذا المجرم يتميز بصفات معينة تختلف في جوهرها عن المجرم الكلاسيكي إلا انهم خلصوا إلي إنه لا يخرج عن كونه مرتكب لفعل إجرامي يستوجب توقيع العقاب عليه. هذا ويمكن إيجاز هذه السمات فيما يلي :

---

[1] المرجع السابق، ص ١٤٦٥- ١٤٨٦.

١- المجرم المعلوماتي هو مجرم ذكي ومحترف، إذ يتمتع باحترافية عالية في تنفيذ جرائمه إذ إنه يرتكبها عن طريق الحاسب،الأمرالذي يتطلب الكثير من الدقة والتخصص في هذا المجال كي يتغلب علي الصعوبات التي أوجدها المتخصصين بهذا الأمر كما في حالات البنوك والمؤسسات المالية الكبري .[١] كما يتميز هذا الجاني بأنه مُلم إلماماً تاماً بتقنية تكنولوجيا المعلومات والقدرة علي تبديل وتفسير برامج الكمبيوتر، فيكون ماهراً إما عن طريق الخبرة المكتسبة في المجال المعلوماتي والتكنولوجي وإما بمجرد التفاعل الاجتماعي مع الأخرين، فلا يشترط أن يكون هذا الجاني علي قدر معين من العلم إذ أن التجارب العملية أثبتت أن جزء كبير من انجح مجرمي هذه الجرائم لم يتلقوا المهارة المطلوبة لارتكاب هذا النوع من الإجرام .[٢]

٢- المجرم المعلوماتي هو مجرم غيرعنيف : فلا يلجأ للعنف أو القوة في أي صورة من صورها في تنفيذ سلوكياته الإجرامية إذ إنه ينتمي لنوع معين من الإجرام (إجرام الحيلة)، فهذا النوع لا يحتاج أي قدر من العناء أو المجهود للقيام به. كما إنه يتمتع بدرجة عالية من الثقافة، فيستطيع أن يضع تصور كامل لارتكاب فعله وذلك لأن مسرح جريمته هو نظام الحاسوب فيمكنه تطبيق جريمته علي أنظمة مشابهة مماثلة قبل تنفيذ فعله.[٣] كما إنه يلجأ في غالب الأحوال إلي وسائل بسيطة يحصل عليها من الحاسب ذاته وخاصة إذا كان النظام الذي يعمل به الكمبيوتر نظاماً معروفاً أو شائعاً إما إذا كان غير مألوف فيكون علي درجة عالية من التعقيد والصعوبة[٤].

---

[١] انظر د/ رمزي رياض عوض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها: دراسة تحليلية تاصيلية مقارنة ، دار النهضة العربية،١٩٩٧، ص٧٥-٧٨.

[٢] انظر د/ هشام محمد رستم، جرائم الحاسوب كصوره من صور الجرائم الأقتصادية المستحدثة، مجلة الدراسات القانونية، العدد ١٧، جامعة أسيوط،١٩٩٥.

[٣] انظر د/ فتوح الشاذلي ود/ عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون: دراسة مقارنة ، منشورات الحلبي الحقوقية، بيروت،٢٠٠٣ ، ص ٣٥-٤٠.

[٤] د/ رمزي عوض، المرجع السابق الإشارة إليه، ص ٧٩.

٣- المجرم المعلوماتي هو مجرم متخصص وعائد إلي الإجرام: فقد تبين في كثير من القضايا الواقعة في العمل أن عدد من هؤلاء المجرمين لا يرتكبون سوي جرائم الاتصال والمعلومات لانهم متخصصون فقط في هذا النوع دون أن يكون لهم علاقة أو دراية بالجرائم التقليدية الأخري .[١] كما يعود كثير من هولاء الجناة لارتكاب جرائم أخري في مجال الحاسب وذلك بدافع سد الفجوات أو التغيرات التي أدت للتعرف عليهم وتقديمهم للمحاكمة في المرة الأولى، فهذا يجعلهم عائدين للجرم وقد ينتهي كذلك بتقديمهم للمحاكمة من جديد.[٢] وغالباً ما يكون لهؤلاء الجناة سلطة مباشرة أوغير مباشرة في مواجهة المعلومات محل الجرم، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول للنظام المحتوي علي المعلومات وهو حتي في الدخول علي الحاسب وإجراء المعاملات ، فقد تكون هذه السلطة شرعية أو غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص معين.[٣]

هذا وقام بعض الفقه بتصنيف هؤلاء المجرمين إلي عدة أقسام منها طائفة يطلق عليها "Pran Kstres" وهم الذين يرتكبون هذه الأفعال بغرض المزاح مع الأخرين وعلي سبيل التسلية دون أن تتوافر لديهم نية احداث الضرر بالمجني عليهم (كالصغارمجرمي المعلوماتية)[٤]. وهناك طائفة أخري تسمي Hackers وهم يستهدفوا كسر الحواجز والصعوبات الأمنية من خلال الدخول علي انظمة الحاسبات الغير المصرح لهم بالدخول ويكون في الغالب بهدف إثبات القدرة علي خرق أنظمة الكمبيوتر وبدافع الفضول وكسب الخبرة.[٥]

---

[١] د/ رامي القاضي، المرجع السابق الإشارة إليه، ص ٧٣.

[2] Eric J.Sinrod and William P.Reilly, Cyber-crimes:A Practical Approach to the Application of Federal Computer Crime Laws,16 Santa Clara High Technology Law Journal 2 (2000).

[3] Richard C.Hollinger and Lonn Lanza-Kaduce, The Process of Criminalization: The Case of Computer Crime Laws, 26 Criminology 101,116 (1988).

[4] 18 U.S.C.A. 1030 (west.supp.1999).

[5] United States V.Simons, 29 f.supp.2d 324 (E.D.va.1988).

وهناك ما يطلق عليهم MALICIOUS HACKERS ويكون هدفهم في الغالب إلحاق ضرر أو خسائر ليست مادية بالمجني عليه كمخترعي فيروسات الحاسب الآلية وموزيعيها وهؤلاء يختلفون عن الفئة الأكثر شيوعاً التي ترتكب هذه الجرائم بحيث يترتب عليها في غالبية الأحوال خسائر مادية وباهظة تلحق بالمجني علية ويطلق عليهم"Personal Problem Solvers". [1] وهناك فئة أخيرة يطلق عليها Carer Criminals وهم في الغالب يهدفون إلي تحقيق ربح مادي بطريقة غير مشروعة من وراء نشاطهم الإجرامي ويكونوا غالباً من مستخدموا الحاسب بالمنازل، أو الموظفون الساخطون علي منظمائهم، أوالمتسللون بقصد التسلية، أو المحترفون الذين يلجأون لمواقع معينة ويخرقون نظامها بإتلافه، أو العالمون في الجريمة المنظمة. [2]

ويتمتع هؤلاء الجناة الخاضعين لتلك الطائفة أن اعمارهم قد تتروح بين ١٨ إلي ٤٦ عام والمتوسط العمري لهم هو ٢٥ عاماً يملكون المعرفة والذكاء والقدرة الفنية الهائلة فضلاً عن حرصهم الشديد وخشية الضبط. كما يتميز هؤلاء الجناة بالتكيف مع المجتمع وعدم معادته كما يميلون نحوالتقليد والإفراط في النزعة الإجرامية .[3]

وهذا ومن الجدير بالذكر في هذا الصدد أن هناك شبه اجماع في الفقه الجنائي علي أن جرائم الحاسب تمثل تحدياً جديداً في عالم الجريمة، إذ إنه توجد صعوبة في التعرف علي هوية الجاني، فلا يترك أثراً لجريمته وإن ترك لا تدل عليه. [4]كما إنه في حالة اكتشاف هويته، إذا كان من بلد لا يعتبر ما قام به جرماً فهذا يمثل عقبة في محاكمته الجنائية فضلاً عن اتساع شرعية الجناة إذا تشمل صغار مستخدمي الإنترنت (الأطفال) فقد يستخدمونها في تخريب الأنظمة ولا يشترط توافر الخبرة العالية في

---

[1] د/ رامي القاضي،المرجع السابق الإشارة إليه، ص ٧٦. .

[2] د/ فتوح الشاذلي و د/ عفيفي كامل، المرجع السابق الإشارة إليه، ص ٨٥-٩٠.

[3] O'Hara E. Chevles, Fundemantels of Criminal Investigations,3rd Ed.(1973).

[4] المرجع السابق، ص١٠٧-١٠٨.

هذه الحالة إذ أن نقص الوعي بسلبية استخدام الإنترنت، قد يجعل البعض ينظر للأعمال التخريبية علي إنها أعمال بطولية (كاختراق المواقع مثلاً)[1].

هذا ويلاحظ أن الفقه الجنائي قد قام بتقسيم الجرائم المعلوماتية إلي عدة أنواع نذكر منها :

ا- **الجرائم المعلوماتية المتصلة بالكمبيوتر:** وهذه تتمثل في التزوير والغش والإحتيال المعلوماتي، ويقصد به الخداع القائم علي التلاعب في نظم المعالجة الآلية للمعلومات بهدف الحصول دون وجه حق علي خدمات أوأصول أموال معنية. ويقوم الجاني باستخدام التقنية الحديثة بغرض التلاعب في البيانات المصرفية والمستحقات المالية فيتم تحويل تلك الأموال في دقائق معدودة من حساب لآخر له وخطورة هذا الفعل تتمثل في كونه يتم عبر الحدود الإقليمية من دولة إلى دولة أو أكثر فيكون له أثراً كبيراً وسلبياً علي الاقتصاد القومي، فمثل هذا السلوك يؤدي إلي إفلاس بعض الشركات الكبرى أو البنوك في الدول .[2]

ب – الجرائم المتصلة بمحتوي الحاسب والإعتداءات الواقعة علي الملكية الفكرية : وهي تتعلق بجرائم إنتاج ونشر المواد الإباحية الخاصة بالأطفال والإتجار بهم والترويج لدعارة الأطفال وكذا الأفعال التي تستهدف الأعمال الأدبية والموسيقية وغيرها نظراً للسهولة التي يمكن من خلالها عمل نسخ غير مصرح بها عن طريق التكنولوجيا الرقمية مما تنعكس علي الحقوق المالية للمالكين والمنتجين بالضرر.[3]

ج- الجرائم ضد سرية وسلامة واتاحة البيانات والنظم الإلكترونية: وهذه الجرائم إما أن تأخذ شكل الإعتراض غير القانوني وهو سلوك يتعلق بانتهاك الحق في الخصوصية والتي تحدث عند اعتراض المراسلات والاتصالات الإلكترونية الخاصة بالغير فهي مرتبطة بكافة أشكال النقل الإلكتروني للبيانات سواء عن طريق التليفون أو الفاكس أو البريد الإلكتروني وغيرها. وهناك صورة الولوج الغير القانوني بمعني الدخول الغير

---

[1] المرجع السابق، ص١٠٩.

[2] Konn Parker, Fighting Computer Crime:A New Framework for Protecting Information,New York,John Wiely (1998).

[3] د/ أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية،القاهرة، ١٩٩٤، ص٤٣-٥٣.

المشروع للأنظمة المعلوماتية (القرصنة / Piracy) والتي يقوم بها القراصنة بهدف تدمير وإتلاف النظام المعلوماتي للغير أو الحصول علي معلومات أو بيانات سرية مملوكة للغير أو التدخل بتغيير البيانات المخترنة في النظام الإلكتروني المملوك للغير. كما أن هناك أشكال معتادة من هذه الجرائم كالإعتداء علي سلامة النظام الإلكتروني (كالإعتداء علي حسن تشغيل الجهاز أو نظام تشغيله) كاستخدام الفيروسات التى تودي لتوقف النظام عن العمل، أو الإعتداء علي سلامة البيانات وسرقة المعلومات وتكون بطريقة عمدية بهدف تعطيل أو شل حركة الجهاز المملوك الغير وطمس بيانات الحاسب فضلاً عن إساءة إستخدام أجهزة الحاسب من خلال كل فعل مجرم قانوناً.[1]

وهناك جانب من الفقه قسم هذه الجرائم من ناحية أخرى إلي نوعين بحسب الأداة المستخدمة في ارتكاب الجرم، فهناك Web Crime Computer وهي تتعلق بجرائم الإنترنت التي يستخدم الحاسب كوسيلة لإرتكاب جريمة مثل غسل الأموال والنصب والإحتيال وتشوية السمعة وكذا السب والقذف ويكون الحاسب في هذا النوع محتفظاً بأداة رقمية قد تساعد علي كشف الفاعل .[2] وهناك ما يسمي Crime Computer ويتعلق هذا النوع من جهة أخرى بالأفعال التى يكون فيها الحاسب محلاً للفعل الإجرامي كالأفعال المادية الجرمية الواقعة علي مكونات الحاسب المادية الملموسة أو المعنوية Software or Datebase أو المعلومات التي يتم الحصول عليها بطريقة غير مشروعة.[3]

كما يمكن القول بأن هذه الجرائم تشمل الجرائم التقليدية العادية التي ترتكب عبر استخدام الحاسب بالسرقة والنصب وخيانة الأمانة والإتلاف والتصنت وكذا التي تُمثل انتهاك للآداب العامة .[4]

---

[1] Hollinger and Kaduce، مرجع سابق الإشارة إليه، ص١١٤.

[2] Sinrod and Reilly، مرجع سابق الإشارة إليه، ص ٢.

[3] United States Sentencing Commission, Sentencing Guidlines for United States Courts, Part II,62 Fed.Reg.26616(1997).

[4] انظر بوجه عام، د/عبد الحافظ عبد الهادي عابد، الإثبات الجنائي بالقرائن: دراسة مقارنة، دار النهضة العربية، القاهرة،١٩٩٨.

هذا والجدير بالذكر أن دور الحاسب الآلي يختلف من جرم إلي آخر، إذ يكمن هذا الدور في كون النظام قد سهل أوساعد في ارتكاب الفعل وجهاز الحاسب الآلي في هذا المجال هو المكونات والمعلومات والبرامج التي تساعد في عملية المعالجة الآلية للمعلومات .

نشأة الجرائم في المعلوماتية بعض الأنظمة المقارنة

١. في الولايات المتحدة الأمريكية

تميزت الولايات المتحدة بسن تشريعات وقوانين خاصة متعلقة بكافة تقنية المعلومات وفي مجال الحوسبة وبالإنترنت وتكنولوجيا المعلومات والاتصالات سواء علي نحو مباشر أو غير مباشر فيما يتعلق باستخدام الإنترنت، وتتطورهذه القوانين والقواعد تبعاً لتطورالقطاع التقني والتكنولوجي .[١] فهذه الدولة وضعت قوانين فيدرالية وأخري محلية علي مستوي الولايات، فعلي المستوي الفدرالي كان لنشاط لجنة الكونجرس الخاصة بحماية استخدام الحاسب بتقديم مشروع قانون حماية الحاسوب ١٩٨٤ ولقي هذا القانون قبولاً حسناً بعد تعديله لاكثر من مرة فأصبح يطلق عليه قانون الإحتيال وسوء استخدام الحاسوب "Computer Fraud and Abuse Act".[٢]

وقد نص القانون المذكور علي تجريم مجرد الاتصال بنظام حاسوب وكذا الاتصال المصرح به الذي يستخدم فيه الجاني الكمبيوتر لأغراض أوأهداف غير قانونية (غير مصرح أو مسموح بها) كأفشاء أو تعديل أوإتلاف بيانات مخزنة بداخله. كما نص علي محاسبة من يرتكب فعلاً من شأنه منع الاستخدام القانوني المسموح به للحاسوب جنائياً.[٣]

ومن ناحية أخري صدر في عام ١٩٨٧ علي ذات المستوي الفيدرالي قانون أمن الحاسوب "Cyber and Computer Security" والذي ينص علي ان تتخذ جميع

---

[١] د/ أحمد حسام تمام، الجرائم الناشئة عن استخدام الحاسوب:الحماية للحاسوب- دراسة مقارنة، دار النهضة العربية، القاهرة ٢٠٠٠، ص٩٠-٩٥.

[٢] د/ فتوح الشاذلي و د/ عفيفي كامل، مرجع سابق الإشارة إليه، ص ٣٥-٣٨.

[٣] د/ محمد الأمين البشري، الأدلة الجنائية الرقمية: مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب- المجلد١٧- العدد٣٣- السنة ١٧ – الرياض، إبريل (٢٠٠٢).

الولايات الفيدرالية خطوات فعالة ملائمة لتأمين وحماية أنظمة أجهزتها المعلوماتية كما ينظم هذا القانون مستويات الرقابة والحماية بها والمسئولين، فنص القسم الثامن عشر (١٨) من القانون الرئيسي في مادته (٣٠) علي إنه يعتبر من قبيل الجريمة :

أ. الدخول غير المصرح به إلي أي كمبيوتر والتوصل إلي معلومات غير مسموح الإطلاع عليها؛

ب. الدخول إلي أحد أنظمة الكمبيوتر الحكومية وكشف المعلومات السرية ولذا كشفها غير مصرح به ؛

ج. الدخول الغير المسموح به إلي أي نظام معلوماتي (أو كمبيوتر) ومن ثم ارتكاب غش أو احتيال ؛

د. إلحاق اضرار من جراء الدخول غير المصرح به سواء للبرامج أو النظام أو المعلومات المخزنة فيها ؛

ه. بث أو تهديد بارتكاب ضرر لأي كمبيوترعبر الولايات أو للتجارة الأجنبية بغرض ابتزاز أموال أومنافع من أي شخص طبيعي أو معنوي .

كما يحظر ذات القانون في القسم ١٤٦٢ / فصل ١٨ استخدام الحاسوب لاستيراد مواد مخلة بالآداب العامة لداخل الولايات المتحدة كما يحظر نقل أي مواد فاحشة وكذا توظيف أي قاصر أو إغرائه في المشاركة في أنشطة جنسية بما فيها خلق أو تصوير مواد وبثها لجهات خارجية (قسم ١٤٦٣ أو ٢٢٥ فصل ١٨) كما يدخل في ذلك أيضاً استخدام الحاسوب الاخلال برعاية قاصر بقبوله استغلاله – مع العلم – في انتاج مواد تنطوي علي استغلال جنسي كما أن نقل وتبادل المواد الفاحشة ذات الصلة بالأطفال جريمة (قسم ٢٢٥٢،٢٢٥٢ / أ/ فصل ١٨).[1]

[1] أنظر على سبيل المثال: 18 U.S.C.A.Ss 1030 (a) (5) (A) &(B) (west supp.1999)

كما ان الإخلال بحق المؤلف جريمة فيدرالية فضلاً عن إنه يعتبر جريمة كل إنتاج أونقل أو إدارة جهاز يتضمن نظام كمبيوتر بقصد استخدام بتزوير الوثائق عن طريق التزوير.[1]

أما علي المستوي المحلي فإن كل ولاية تملك حرية التشريع وسن القوانين الخاصة بها، فليس هناك آلية محددة تتطلب تبني شكل محدد في إصدار قانون خاص بالجرم الإلكتروني بل هناك اتجاه حديث في الفقه الجنائي الأمريكي – ينادي بتوحيد التدابير التشريعية وذلك من خلال تبني النموذج الصادر من إحدي الهيئات الإكاديمية لقانون نموذجي يقسم الجرائم تقسيماً دقيقاً.[2]

٢- المملكة المتحدة (انجلترا)

سن المشرع البريطاني قانون استخدام إساءة الحاسوب عام ١٩٩٠ Computer Misuse Act حيث شمل هذا التشريع أنواع جديدة من الجرائم المعلوماتية لمحاربة جرائم الإختراق والتوصل غير المسموح به لتعديل معطيات الكمبيوتر وإتلافها بصفة عامة وجرائم زرع الفيروسات بصفة خاصة. فهذه الجرائم تشمل التحوير أو التعديل غير المسموح به لنظام الحاسب بقصد اضعاف نظامه أو تعطيله وكذا الدخول غير القانوني أي المحظور لنظام الحاسب لمجرد العبث أو التطفل بقصد ارتكاب أو تسهيل ارتكاب فعل آخر. هذا ويلاحظ أنه منذ عام ١٩٩٨، تميزت بريطانيا ليس فقط في مجال أمن المعلومات بل في مجال حماية البيانات الشخصية والخصوصية وتنظيم حرية المعلومات والبيانات في مختلف الفروع الأخري لقانون تقنين المعلومات.[3]

٣- فرنسا والمانيا

في المانيا بالتحديد في عام ١٩٨٦، صدر قانون مكافحة الجريمة الإقتصادية إذا جرم ذلك التشريع إتلاف أو محو أو تغيير أو تزوير البيانات المعالجة آلياً المسئولية

---

[1] راجع،د/ رامي متولى القاضي، مرجع سابق الإشارة إليه، ص٢٩.

[2] انظر بوجه عام، ممدوح عبد الحميد عبد المطلب،البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت- دار الكتب القانونية- القاهرة (٢٠٠٦).

[3] د/ أحمد بلال، مرجع سابق الإشارة إليه، ص٥٢.

والعقوبة الجنائية فيما يتعلق بالبيانات ذات الأهمية الخاصة بقطاع الأعمال البسيطة إلادارية (السجن والغرامة). كما جرم هذا القانون غش الحاسوب والإحتيال المعلوماتي بواسطته وكذا عاقب علي الحصول دون تصريح من جانب الفاعل لنفسه أو لغيره علي بيانات أو معلومات غيره أو مخصصة له ومحمية بوجه خاص ضد الدخول غير الشرعي.[1] وفي فرنسا قام المشرع الفرنسي بسن تشريع عام ١٩٨٨ خاص بالجرائم الإلكترونية في قانون العقوبات الفرنسي وحرم فيه مجرد الولوج إلي نظام المعالجة الآلية أو الإستمرار في الوجود فيه بطريق محظور كما جرم إتلاف المعطيات وتزوير المستندات وغيرها من الأفعال ذات الشأن وعاقب بعقوبات شديدة لتحقيق مزيد من الابعاد والردعية لخرقة هذه القوانين .[2]

٤- عُمان

صدر المرسوم السلطاني في عام ٢٠٠١ (رقم ٧٢) بتعديل أحكام القانون الجزائي وإضافة فصل يتعلق بجرائم الحاسب الآلي ونص علي عقوبات السجن والغرامة لكل من تعمد استخدام الحاسوب في الالتقاط الغير المشروع للمعلومات والدخول غير المشروع فى أنظمته والتجسس والتصنت وانتهاك خصوصية الأخرين (التعدي علي حقهم في الاحتفاظ باسرارهم) وكذا إتلاف البيانات وتزويرها وكذا كل من حصل أو استولي عمداً وبطريق غير مشروع على معطيات الحاسوب مع مضاعفة الجزاء الجنائي إذا قام الجاني بتقليد أو تزوير بطاقة الوفاء أو السحب أواستعمالها مع العلم بذلك أواستخدامها مع العلم بعدم وجود رصيد للسداد أو استخدامها بعد إلغائها (أو انتهاء صلاحيتها) أو استخدام بطاقة الغير.[3]

ثالثاً : الجريمة المعلوماتية تحت مظلة الشرعية الجنائية

---

[1] نفس المرجع السابق.
[2] د/ فتوح الشاذلي ود/ عفيفي كامل، مرجع سابق الإشارة إليه، ص٣٧.
[3] المرسوم السلطاني العماني رقم ٧٢ لعام ٢٠٠١.

لاريب في أن سياسة التجريم والعقاب تعد من أهم وأخطر الأمور التشريعية والقانونية المتصلة بحرية المواطنين العامة وحقوقهم الفردية وذلك بسبب خطورة الآثار المرتبة عليه، لذلك يتعين أن تصدر النصوص التشريعية الخاصة به وفقاً لمبدأ الشرعية الجنائية Legality Norm.

من المسلم به أن الدولة هى القاسم المشترك بين القانون الدستوري والقانون الجنائي، إذ أن الأول ينظم نشاط الدولة المتمثل في سلطاتها الثلاث سياسياً أما الثاني فينظم نشاطها جنائياً من خلال تنظيم علاقة الفرد بالدولة وعلاقتهم بعضهم البعض.

فثمة علاقة وثيقة بين هذين القانونين، فمبادىء الدستور تسهم في تحديد مضمون القانون الجنائي، إذ يتوقف تحديد الجرائم على تطوير المبادىء الدستورية، فيؤدي وظيفته في إطار الشرعية الدستورية على النحو الذي يحدده الدستور، فقد قام القانون الجنائي على عدد من تلك المبادىء أهمها – بل يعتبر حجر الزاوية للنظام الجنائي كله – مبدأ الشرعية الجنائية الذي تدور حوله كافة المبادىء الجنائية موضوعية كانت أو إجرائية. وهذا المبدأ يعني أن التشريع هو المصدر الأساسي للجريمة والعقاب وأن السلطة التشريعية وحدها هى المختصة بتحديد الجرائم والعقوبات دون القضائية والتنفيذية وأن مهمة القاضي تكمن في تطبيق النصوص الموضوعية من جانب المشرع.[1] هذا وقد أكدت المواثيق الدولية على هذا المبدأ (كإلاعلان العالمي لحقوق الإنسان ١٩٤٨ وكذا إعلان حقوق الإنسان والمواطن ١٧٨٩ فضلاً عن الإتفاقية الأوروبية لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية ١٩٦٦).[2]

وجدير بالذكر إنه كان للمحكمة الدستورية العليا في مصر دوراً بارزاً في تدعيم وترسيخ دعائم هذا المبدأ باعتباره أحد تطبيقات الأمن القانوني، فوضعت الضوابط الصحيحة لتفويض السلطة التنفيذية في بعض جوانب الجريمة والعقاب واستخلصت فكرة عدم جواز توقيع عقوبة إلا بناء على حكم قضائي، وكذا مفهوم الجريمة (وخاصة

---

[1] د/ عمر سالم، شرح قانون العقوبات المصري، دار النهضة العربية- القاهرة -٢٠١٠ ، ص٣٠.
[2] د/ أحمد فتحى سرور، مرجع سابق الإشارة إليه، ص٣١.

مفهومها الشرعي) من الناحية القانونية، ووضعت بموجبها المعايير التى بواسطتها تباشر رقابتها على دستورية النص الجنائي.[1]

ففي حكم شهير لها قضت :"بأن استقرار مبدأ شرعية الجرائم والعقوبات في الدول المتحضرة دعا إلى توكيده، ومن ثم وجد صداه في عديد المواثيق الدولية كما تردد في العديد من الدساتير".[2] فأصبح هذا المبدأ ضمانه دستورية ضد تعسف أو تحكم السلطة، فبعدما كان للسلطة دوراً في التشريع، عاد هذا الدور من جديد للمشرع، إذ يقرر للجرائم المرتكبة العقوبات المناسبة.[3]

كما أكدت في حكم لها أهمية هذا المبدأ في مجال السياسة الجنائية حيث قضت : " أن السياسة الجنائية الرشيدة يتعين أن تقوم على عناصر متجانسة، فإن كانت على عناصر متنافرة نتج عن ذلك افتقاد الصلة بين النصوص ومراميها ، بحيث لا تكون مؤدية إلى تحقيق الغاية المقصودة منها لانعدام الرابطة المنطقية بينهما إيماناً بأن الأصل في النصوص التشريعية – في الدولة القانونية – هو ارتباطها عقلاً باهدافها، ومن ثم يتعين دائماً استظهار ما إذا كان النص المطعون عليه يلزم إطاراً منطقياً للدائرة التى يعمل فيها، كافلاً تناغم الأغراض التي يستهدفها..... بالتالي لمبدأ خضوع الدولة للقانون....."[4]

هذا ويلاحظ أن المحكمة العليا قد أكدت على ارتباط ذلك المبدأ بالعدالة الجنائية للدولة حيث قضت بأن " العدالة الجنائية في جوهر ملامحها ، هي التى يتعين ضمانها من خلال قواعد محددة تحديداً دقيقاً، ومنصفاً يتقرر على صونها ما إذا كان المتهم مداناً أو بريئاً، ويفترض ذلك توازناً بين مصلحة الجماعة في استقرار أمنها، ومصلحة المتهم هى الا تُفرض عليه عقوبة ليس لها من صلة بفعل أتاه، أو تفتقر هذه الصلة إلى دليل يؤكدها، ولا يجوز النزول عنها أو التفريط فيها".[5] كما أكدت على ضمانات تطبيق هذا المبدأ

---

[1] د/ هدى حامد قشقوش، شرح قانون العقوبات – دار النهضة العربية- القاهرة-٢٠١٠،ص٣٠-٣١.
[2] حكم المحكمة الدستورية العليا المصرية في القضية رقم ٤٨ لسنة ١٧ قضاء دستوري جلسة ١٩٩٧/٢/٢٢.
[3] حكم المحكمة الدستورية العليا المصرية في القضية رقم ١١٤ لسنة ٢١ قضاء دستوري جلسة ٢٠٠١/٦/٢ .
[4] حكم المحكمة الدستورية العليا المصرية في القضية رقم ١١٤ لسنة ٢١ قضاء دستوري جلسة ٢٠٠١/٦/٢.
[5] حكم المحكمة الدستورية العليا المصرية في القضية رقم ٤٩ لسنة ١٧ قضاء دستوري جلسة ١٩٩٦/٦/١٥.

فقضت بأن " النطاق الحقيقي لمبدأ شرعية الجرائم والعقوبات إنما يتحدد على ضوء ضمانتين تكفلان الاغراض التى توخاها: أولهما: أن تصاغ النصوص العقابية بطريقة واضحة محددة لا خفاء فيها أو غموض ، فلا تكون هذه النصوص شباكاً أو شراكاً يلقيها المشرع متصيداً باتساعها أو بخفائها من يقعون تحتها أو يخطئون مواقعها وهى بعد ضمان غايتها أن يكون المخاطبين بالنصوص العقابية على بنية من حقيقتها، فلا يكون سلوكهم محاف لها بل متسقاً معها وثانيهما: أن المرحلة الزمنية التى تقع بين دخول القانون الجنائي حيز التنفيذ وإلغاء هذا القانون إنما تمثل تلك الفترة التى كان يحيا خلالها، فلا يطبق على أفعال اتاها جناتها قبل نفاذه، بل يتعين أن يكون هذا القانون سابقاً عليها فلا يكون رجعياً".[1] وكذا قالت "لايجوز إعمال نصوص عقابية يسيء تطبيقها إلى مركز قائم لمتهم، ولا كتفسيرها بما يخرجها عن معناها أو مقاصدها، ولا مد نطاق التجريم- وبطريق القياس إلى أفعال لم يؤثمها القاضي من بينها ما يكون أكثر ضماناً للحرية الشخصية في إطار علاقة منطقية يقيمها بين هذه النصوص وإرادة المشرع...".[2]

ويمكن القول بأن لهذا المبدأ مبرراته وخاصة في مجال الجريمة المعلوماتية، ، فمن ناحية تحقيق العدالة، فاحترام الإنسان يتطلب حصر الأفعال المجرمة إلكترونياً في صورة معلوماتية وأن تكون عقوبتها محددة تحديداً دقيقاً بحيث يواجها المشرع ويتم إعلام المجتمع بكل هذه الجرائم و عقوبتها.[3] كما يحقق هذا المبدأ، المساواة في العقاب بمعنى أن النصوص الخاصة بتجريم وعقاب الجرائم المعلوماتية تصاغ بشكل عام ومجرد، فتطبق على الكافة وعلى جميع الوقائع دون تمييز، وهذا يؤدي لتحقيق مساواة الجميع أمام القانون دون تمييز.[4] فضلاً عن ذلك، دور هذا المبدأ في تحقيق الردع العام العقابي،عن

---

[1] حكم المحكمة الدستورية العليا المصرية في القضية رقم ٥٩ لسنة ١٨ قضاء دستوري جلسة ١٩٩٧/٧/٥.
[2] د/ عمر سالم، مرجع سابق الإشارة إليه، ص٣٥-٣٦.
[3] د/ عمر سالم، مرجع سابق الإشارة إليه، ص٣٩.
[4] د/ هدى حامد قشقوش، مرجع سابق الإشارة إليه، ص٣٥-٣٦.

طريق إخبار المخاطبين بالقانون بالجرائم والعقوبات المعلوماتية فيحجمون عن ارتكاب مثل تلك السلوكيات، فيفكرون قبل الإقدام على ارتكابها خشية الحكم عليهم بعقوبتها.[1]

ويلاحظ أن هذا المبدأ يلعب دوراً هاماً في تحقيق مبدأ الفصل بين السلطات، فهناك سلطة ممثلة من الشعب (مجلس النواب) تتولى وضع النصوص التشريعية الخاصة بتجريم وعقاب هذه الجرائم وكذا سلطة قضائية تتولى تطبيق هذه النصوص وأخرى تنفيذية تقوم على تنفيذ ما يصدر عن القضاء من أحكام في هذا المجال.[2]

ولمبدأ شرعية الجرائم والعقوبات أهمية جلية بالنسبة للمشرع، إذ هو ملتزم وحده بمهمة التشريع الجنائي للجرائم المعلوماتية، وملتزم عند وضعه للنصوص الجنائية ألا يتعسف في استعمال حقه في التجريم، بحيث لا يحرم إلا الأفعال الإلكترونية التى تمثل اعتداء على المصالح الأساسية للأمة.[3]

كما أن النص على عدم سريان نصوص تجريم الجرائم المعلوماتية على الوقائع الحادثة قبل صدور نصوص التجريم بل يقتصر سريانها على المستقبل وهو ما يطلق عليه عدم رجعية النصوص الجنائية للجرم الإلكتروني، كما يلتزم المشرع بالوضوح التام دون لبس في صدور النصوص الجنائية، فلا يجوز له اللجوء لاسلوب النماذج الغامضة أو المفتوحة.[4] كما يتعين على القاضي الجنائي تطبيق النص الخاص بالجريمة المعلوماتية دون تعديل بإلاضافة أو الحذف – إذ أن ذلك محظور في المجال الجنائي. فيحدد ما إذا كان الجرم يندرج تحت أحد النماذج التي قررها المشرع من عدمه حتى يصل للتكييف القانوني السليم.[5] كما تلتزم سلطة التنفيذ بتنفيذ الحكم بذات الوضع الذي نص عليه القانون، فلا يجوز تطبيق عقوبة لم يحكم بها أو أن تحل نفسها محل القضاء في تطبيق العقوبة.[6]

---

[1] راجع د/ ابراهيم حامد طنطاوى و د/ على محمود حموده، شرح الأحكام العامة لقانون العقوبات –الجزء الأول، النظرية العامة للجريمة- دار النهضة العربية- القاهرة ،٢٠٠٧، ص١٧-١٨.

[2] د/ هدى حامد قشقوش، مرجع سابق الإشارة إليه، ص٣٧.

[3] د/عمر سالم، مرجع سابق الإشارة إليه، ص٤٠-٥٢.

[4] د/عبد العظيم وزير، مرجع سابق الإشارة إليه، ص٦٣.

[5] د/ ابراهيم طنطاوي ود/ على حموده ، مرجع سابق الإشارة إليه، ص٣٥.

[6] د/عمر سالم، مرجع سابق الإشارة إليه، ص٥٢-٥٣.

- **الجريمة المعلوماتية في مصر وشرعيتها الجنائية**

تنص المادة ٣١ من الدستور المصري الصادر عام ٢٠١٤ فيما يتعلق بالحفاظ على المعلومات والبيانات الإلكترونية على أن: " أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون".[١] ويلاحظ أن هناك عدة قوانين مصرية صدرت تتعلق ببعض العقوبات الخاصة بالجرائم المعلوماتية كقانون الأحوال المدنية المصري رقم ١٤٣ لسنة ١٩٩٤ الذي جرم تعديل بيانات الأحوال الشخصية للمواطنين المسجلة على الحاسوب أو الوسائط الإلكترونية الموجودة بالمصالح الحكومية بالتزوير أو الإتلاف أوالإطلاع عليها دون وجه حق (المواد ٧٢- ٧٤-٧٥-٧٦) وتراوحت العقوبات طبقاً لهذا القانون ما بين السجن والغرامة.

هذا ومن ناحية أخرى، نص قانون حماية الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢ على حماية السرقات الأدبية عبر شبكة الإنترنت وتراوحت العقوبات بين الحبس والغرامة (مواد ١٤٠- ١٨١) ، كما نظم قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ بعض جرائم الإنترنت فيما يتعلق باذاعة أو نشر أو تسجيل لمضمون الرسائل الخاصة بالاتصال والإمتناع عمداً عن إرسالها وغيرها من الأفعال (المواد ٧٣-٧٥) فضلاً عن إنشاء أو اذاعة أسرارغير مصرح بالبوح بها وتتراوح العقوبات أيضاً ما بين الحبس والغرامة.[٢] هذا ويلاحظ إنه قد صدر القانون رقم ١٥ لسنة ٢٠٠٤ في شأن التوقيع الإلكتروني لتنظيم بعض صور الجرائم الإلكترونية، كأصدار شهادات تصديق إلكترونية دون ترخيص، أو إتلاف أو تزوير توقيعاً أو محرراً إلكترونياً مع العلم بذلك، فتكون العقوبات الحبس والغرامة (مواد ٢٣-١٣).[٣] وكذلك قانون الطفل المعدل بالقانون من ١٢٦ لسنة ٢٠٠٨ الذي جرم استغلال الأطفال جنسياً عبر شبكات الإنترنت وغيرها من الأفعال غير المشروعة المنافية للآداب، فيعاقب بالحبس والغرامة أيضاً (مادة ١١٦).[٤]

---

[١] نفس المرجع السابق والمادة (٣١) من دستور جمهورية مصر العربية.
[٢] المواد ١٤٠-١٨١ من قانون حماية الملكية الفكرية المصري رقم ٨٢ لسنة ٢٠٠٢.
[٣] المواد ١٣-٢٣ من قانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤.
[٤] المواد ١١٥- ١١٦ من قانون الطفل المعدل رقم ٢٦ لسنة ٢٠٠٨.

كما نص الدستور الحالي في المادة ٥٧ منه على أن "للحياة الخاصة حرمه، وهى مصونة لا تمس وللمراسلات البريدية والبرقية والإلكترونية والمجادثات الهاتفية وغيرها من وسائل الاتصال حرمه، وسريتها مكفولة، ولا تجوز مصادرتها أوالإطلاع عليها أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة ، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي.....".[١]

في ضوء كل ما تقدم، يمكن القول بأن أعظم وأهم ما يقع على عاتق القاضي الجنائي عند نظر الدعوى الجنائية هو تقدير أدلة الإثبات والتحقق منها والأقتناع بها، وذلك حتى لا يُدان برىء ولا يفلت مجرم من الجزاء "Beyond Reasonable Doubt". إذ أن الهدف الرئيسي لقانون الإجراءات الجنائية هو البحث عن الحقيقة عبر الدعوى الجنائية، إذ تقوم النيابة العامة بوصفها ممثلة عن المجتمع، بجمع الأدلة وتمحيصها بهدف اسناد الجرم للفاعل، ومن ثم تطبيق الجزاء الجنائي المنصوص عليه في قانون العقوبات وإعلاء تلك الحقيقة في الحكم القضائي الذي ما يكون هو عنوانها، فالإدعاء العام هو خصم شريف في الدعوى، أمين عليها يهدف إلى حماية حقوق المجتمع وحرياته، فيسعى دائماً من خلال السلطة المخولة له إلى إرساء الضمانات القانونية التى تساعد على كشف وإظهار الحقيقة.[٢]

ولا شك في أن نظرية الإثبات هى القاعدة التى ترتكز عليها القواعد الجنائية الجزائية منذ لحظة وقوع الجرم لحين صدور حكم قضائي، فالإثبات تأكيداً للحق بالبينة، فالدليل هو قوام حياة الحق وينزل منزلة السلاح في معركة الخصومة بين المتنازعين ولذا يستوي حق له وجود له مع حق لا دليل عليه.[٣]

ومن الجدير بالذكر أن أدلة الإثبات في قانون الإجراءات الجنائية المصري وتعديلاته هى متعددة منها الأعتراف، شهادة الشهود، القرائن، الأدلة الكتابية وكذا أى دليل تطمئن له المحكمة من

---

[١] المادة (٥٧) من دستور جمهورية مصر العربية ٢٠١٤.

[٢] انظر بوجه عام، د/مأمون محمد سلامه،الإجراءات الجنائية في التشريع المصري- دار الفكر العربي، القاهرة (١٩٨٨).

[٣] د/أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية،دار النهضة العربية، القاهرة، الطبعة السابعة (١٩٩٦).

خلال سلطاتها التقديرية طالما وجدت إنه لازم وهام في إظهار الحقيقة، ومايهمنا في هذه الدراسة هو الإثبات بالدليل الإلكتروني في المجال الجنائي.

لقد تطورت وسائل التحقيق الجنائي في عصر العولمة والمعلوماتية تطوراً سريعاً وملموساً مع تطور السلوك الإجرامي وتطور أسلوب ارتكابه، فاصبحت المرحلة العلمية والعملية الحديثة قائمة على الإستعانة بالأساليب العلمية واستخدام شبكة الإنترنت هي الصفة الطاغية والمميزة.

فالمجرم والجريمة في تقدم مستمر لا ينتهي فجريمة الامس ليست كجريمة اليوم ومجرم الماضي ليس كمجرم الحاضر أو المستقبل، فالطبيعة التقنية والفنية للجرائم المعلوماتية نتج عنها في مجال الإثبات في المواد الجنائية، شكلاً جديداً من أشكال الأدلة وهو الدليل الإلكتروني الذي اعتدت به المحاكم في الأنظمة القانونية المقارنة سواء من حيث حجيته في الإثبات وقيمته القانونية، إذ هى ساوت في الإثبات الجنائي بين هذا الدليل والدليل التقليدي.[1]

هذا ويعد الدليل الإلكتروني في وقتنا المعاصر الراهن من الأدلة القانونية المقبولة في مجال الإثبات الجنائي فهو يقوم على عدة إفكار هامة هى:

(أ) فكرة المحرر (السند) كتابياً كان أو إلكترونياً: فبعد أن كان محل الإثبات ينحصر في وقائع الجرم ومسئولية الجاني وانعدام الدفوع القانونية، أى كان المحل متمثل فقط في المستند الورقي، فأصبح الدليل الكتابي الإلكتروني المتمثل في المستندات (تسجيلات إلكترونية) هى محل الإثبات في المواد الجنائية.[2]

(ب) مبدأ الكتابة: جعل المشرع المصري الكتابة وسيلة قانونية صالحة للإثبات في بعض المسائل الجنائية، إذ اعترف لها بقوة إثبات يمكن من خلالها إثبات وقائع الجرم. ولكن لا يوجد ما يمنع أن تكون الكتابة موجودة على دعامات وسائل الاتصال المستحدثة كالإنترنت، فتكون كتابة إلكترونية لا تتسم بالطابع التقليدي، ومن ثم يصلح الدليل الكتابي الإلكتروني وسيلة للإثبات الجنائي.

---

[1] Robert Richardson, Hackers:Devils or Saints?Network,June 1997,at 62.

[2] نفس المرجع السابق.

(ج) فكرة التوقيع : من المسلم به إنه كي يصلح المحرر (السند) دليلاً كاملاً في الإثبات الجنائي، لابد أن يحتوي على توقيع من صدر منه، فيكون منسوب له. فمن الملاحظ أن التوقيع تطور بتطور الزمن من مفهومه التقليدي (الإمضاء الكتابي) وهو التوقيع العادي أو بالبصمة أو الختم أو الرمز وغيرها إلى ما يسمى بالتوقيع الإلكتروني "Electronic Signature" لمواكبة النقلة الهائلة في مجال تكنولوجيا المعلومات.

في ضوء هذه العناصر الثلاثة للدليل الإلكتروني في الإثبات، يتطلب من المشرع المصري ضرورة اعتناق هذا النوع من الأدلة وابتكار وسائل حديثة لمسايرة العصر من خلال اختراع أو خلق وسائل حديثة وفق ضوابط علمية للاستدلال على الجرم ومعرفة الجاني وادانته في إطار الشرعية القانونية.

فالإثبات بالدليل المعلوماتي أضحى أساساً متيناً وملحاً في الوقت الحاضر لمعظم المسائل الجنائية. فتطور الجريمة دفع لتطوير الأجهزة الأمنية بفروعها ومنها الأدلة الجنائية واستخلاصها وجمعها، فالكتابة بصورتها الإلكترونية أصبحت عنصراً أساسياً لحفظ الحقوق وتأكيدها، فعملياً، يفقد الحق قيمته إذا لم يستطيع صاحبه أن يقيم الدليل عليه.

وبناء على ما تقدم، نلاحظ أن المشرع المصري لم ينظم مسألة الإثبات بالدليل الإلكتروني سواء من الناحية الموضوعية أو الإجرائية للقانون الجنائي. فمن خلال هذه الدراسة يمكن معرفة مدى ملائمة تطبيق هذه الأحكام العادية التقليدية على الإثبات الإلكتروني الجنائي. فهذه الدراسة تسلط الضوء على إشكالية هامة تثور يومياً في الحياة العملية القانونية وهى إثبات الجريمة بالدليل الإلكتروني بكل ما يعتريه من مشكلات سواء فيما يتعلق بصحته ومدى صلاحيته في الإثبات. فضلاً عن ذلك، هناك سؤال يتعلق بمدى السلطة التقديرية المخولة للقاضي الجنائي في تقدير هذا الدليل ومدى اقتناعه به في ظل مبدأ " القناعة الوجدانية للقاضي الجنائي" إذ له الحرية في اللجوء إلى ما يؤدي لكشف حقيقة الجرم في إطار القانون، فله قبول هذا الدليل أو دحضه وخاصة في مجال تقدير المحررات المستخرجة إلكترونياً فضلاً عن المشكلات الأخرى التي تثور بشأن الطبيعة

الخاصة للأدلة الإلكترونية المتحصلة من الجرائم المعلوماتية وخاصة في مجال التفتيش والضبط ومدى مراعاه حق الخصوصية والقواعد الدستورية لضمانات المتهم الإلكتروني.

- **أهداف الدراسة وأهميتها**

تهدف هذه الدراسة إلى بيان ماهية ومعنى الدليل الإلكتروني ومدى قبوله في الإثبات الجنائي وإلقاء الضوء على شروط قبوله وأنواعه وبيان حجيته القانونية في الإثبات ومدى إمكانية العمل به خاصة لدى المحاكم الجنائية المصرية فضلاً عن بيان كيفية المنازعة في صحته وبيان الحدود القانونية الممنوحة لسلطة القاضي الجنائي في تقديره.

وعليه، تتمحور أهمية دراسة ذلك الموضوع في اعتبار نظرية الإثبات هى أهم النظريات القانونية والأكثر تطبيقاً وشيوعاً وتعقيداً في العمل، فهى النظرية التى لا تنقطع المحاكم الجنائية عن استخدامها و تطبيقها يومياً. فقد يعتمد القاضي على هذا الدليل كليةً. ومن هذا المنطلق يبنى عليه حكمه، فالإثبات الجنائي بالدليل الإلكتروني له دور فعال في خلق قواعد قانونية موضوعية جديدة وخاصة قواعد إعداد الدليل، وهذا يعطيه أهمية في حل المشكلات وإثبات الجرائم المادية وكذا تحديد المسئولية الجنائية. هذا وان وسائل الإثبات الجنائي التقليدية كالخبرة والمعاينة والشهادة غالباً ما تحتاج إلى إثباتها إلكترونياً باعتبار أن المحررات الإلكترونية أداة من أدوات حفظ الأدلة الجنائية بصورة إلكترونية، فالإثبات إلكترونياً له دور كبير في إدانه المتهم من عدمه. هذا ويلاحظ أن الدليل يقوم بدور محوري جوهري في ضبط واحضار واستجواب الأشخاص.

خطة الدراسة

نتناول في هذه الدراسة النطاق الموضوعي للإثبات بالدليل الإلكتروني في المسائل الجنائية من حيث تعريفه وأنواعه وحجيته ومدى قبول القاضي له واقتناعه من عدمه وذلك على النحو التالي في بابين مستقلين.

الباب الأول: في ماهية الدليل الإلكتروني وأهميته وأنواعه وشروطه فى الإثبات الجنائي

الباب الثاني: القيمة القانونية وحجية الدليل الإلكتروني في الإثبات في المواد الجنائية

الباب الأول

ماهية الدليل الإلكتروني في الإثبات الجنائي

تمهيد وتقسم

إن بيان مفهوم الدليل الإلكتروني يتطلب الوقوف على تعريفه من خلال بيان مفهومه وأهميته وخصائصه وتقسيماته، ومن ثم بيان مكانته من أدلة الإثبات الجنائي وبيان شروط صحة قبوله في إثبات المواد الجنائية. وعليه، نقسم هذا الباب إلى فصلين على النحو التالي

الفصل الأول : التعريف بالدليل الإلكتروني وبيان أهميتة وخصائصه و أنواعه

الفصل الثاني: مكانته من أدلة الإثبات وشروط صحة قبوله

الفصل الأول

ماهية الدليل الإلكتروني وخصائصه

تمهيد وتقسيم

يلزم التعريف بالدليل المعلوماتي (الإلكتروني) كوسيلة للإثبات في المسائل الجنائية أن نتعرض لتحديده فقهاً وقانوناً مشيرين إلى خصائصه في مبحثين على النحو التالي:

المبحث الأول: ماهية الدليل الإلكتروني وأهميته وخصائصه

المبحث الثاني: شروط الأخذ بالدليل الإلكتروني في المسائل الجنائية

المبحث الأول

ماهية الدليل الإلكتروني وبيان أهميته

أولاً : في التعريف بالدليل الالكتروني

من المسلم به قانوناً أن طلبات ودفوع الخصوم في الدعوى الجنائية لابد لها من الإثبات عبر الدليل وهذا الدليل قد يكون تقليدياً أو إلكترونياً. فالإثبات الجنائي بوجه عام هو نشاط إجرائي موجه مباشرة للوصول لليقين القضائي والحقيقة طبقاً لمعيارها الواقعي الخاص (تحديد الجرم) وذلك بشأن الإتهام سواء بتأكيده أو نفيه.[1] كما أن الدليل الجنائي هو وسيلة القاضي في تحديد فاعل الجريمة (أو حتى الشريك فيها)، فهو كل وسيلة

[1] د/متولي القاضي، مرجع سابق الإشارة إليه، ص٥٦-٥٩.

مسموح به قانوناً يلجأ لها القاضي لإثبات وجود أو عدم وجود الواقعة المرتكبة أو صحة أو كذب الواقعة، فالدليل هو قوام حكم القاضي وله أن يقدر أهميته وملائمته كي يكون ثمة فصل في الدعوى العمومية إما بالبراءة أو الإدانة.[1]

هذا ولم يعرف المشرع المصري- وكذا غيره – الدليل الإلكتروني في مجال الإثبات الجنائي. الدليل الإلكتروني في الإثبات الجنائي هو مكون رقمي لتقديم معلومات في أشكال متنوعة كالحروف والأشكال والرموز والارقام والصور والأصوات.

هذا وقد ذهب جانب من الفقه الجنائي للقول بأنه" الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل نبضات مغناطيسية أو كهربائية، ممكن تجميعها أو تحليلها 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 إنفاذ وتطبيق القانون".[2]

كما قيل إنه " معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها و شبكات الإتصال، ويمكن استخدامها في أى مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جانٍ أو مجني عليه".[3] فهو له أساس في العالم الافتراضي ويؤدي لوقوع الجرم. فيمكن القول بأنه دليل مشتق (أو بواسطة) النظم المعلوماتية الحاسوبية البرامجية، وأجهزة ومعدات وأدوات الحاسوب أو شبكات الإتصال من خلال إجراءات قانونية، يتم تقديمها للقضاء لإثبات وقوع الجريمة وتقرير البراءة أو الإدانة.[4]

---

[1] انظر محمد محمد شتات، فكرة الحماية الجنائية لبرامج الحاسب الآلي – دار الجامعة الجديدة- الإسكندرية (٢٠٠١)، ص ٧٩ ومابعدها.

[2] د/ نائلة قورة ، مرجع سابق الإشارة إليه، ص٢٥.

[3] راجع بصفة عامة، د/ هلالي عبد اللاه أحمد – حجية المخرجات الكمبيوترية في الإثبات الجنائي، طبعة أولى ، دار النهضة العربية، القاهرة،١٩٩٧.

[4] انظر تفصيلاً في هذا الشأن، د/ جميل عبد الباقي الصغير- أدلة الإثبات الجنائي والتكنولوجيا الحديثة (أجهزة الرادار – الحاسبات الإلية – البصمة الوراثية): دراسة مقارنة – دار النهضة العربية ، القاهرة،٢٠٠١.

الحاسوب أو شبكات الإتصال من خلال إجراءات قانونية، يتم تقديمها للقضاء لإثبات وقوع الجريمة وتقرير البراءة أو الإدانة.[1]

يتضح مما تقدم، أن المفاهيم السابقة اشتملت على الأدلة التي يتم استخراجها من جهاز الكمبيوتر وهذا معيار ضيق يقصر الأدلة المعلوماتية على تلك التى تخرج من الحاسب الآلي فقط وهذا أمر غير مقبول عقلاً ومنطقاً، إذ يجوز استخراج الدليل المعلوماتي من أى آلة أخرى غير الحاسوب، فهناك من الأجهزة – في وقتنا المعاصر– التى تعتمد على التقنية الفنية العالية في تشغيلها فيمكن أن تكون مصدراً لهذا الدليل. كما أن هذه التعريفات خلطت بين الدليل في ذاته وأمر استخلاصه، بمعنى أن هذا الدليل لا تثبت له هذه الصفة إلا إذا تم استخلاصه من مصدره– وهو أمر لا يمكن التسليم به– إذ أن هذه الموجات والنبضات الكهربائية لا تصلح أن توصف بوصف الدليل في مجال الإثبات قبل فصلها عن مصدرها بواسطة الوسائل التقنية.[2]

وبناء على ذلك، يمكن تعريف الدليل الإلكتروني في المجال الجنائي وخصوصاً الإثبات، بأنه مجموعة الموجات المغناطيسية أو النبضات الكهربائية التى يمكن تجميعها وفحصها باستخدام تطبيقات وبرامج معينة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية. وعليه يمكن القول بأن الدليل الإلكتروني قد يكون هو الوسيلة الوحيدة والرئيسية لإثبات الفعل غير المشروع الواقع عبر أجهزة الحاسوب والنظم الإلكترونية والشبكة المعلوماتية.

وتبدو للدليل الإلكتروني أهمية كبيرة إذ هو أساس الإثبات في الجريمة المعلوماتية وهو الوسيلة التي يستفيد بها القاضي الجنائي للوصول للحقيقة الواقعية لإثبات وقوع الجرم من الناحية الفعلية (بمعنى تحقيق ركنيها المادي والمعنوي) ونسبتها إلى المتهم (فاعلاً كان أو شريكاً) لاعمال حكم القانون.[3]

---

[1] انظر تفصيلاً في هذا الشأن، د/ جميل عبد الباقي الصغير- أدلة الإثبات الجنائي والتكنولوجيا الحديثة (أجهزة الرادار – الحاسبات إلإلية – البصمة الوراثية): دراسة مقارنة – دار النهضة العربية ، القاهرة،٢٠٠١.

[2] راجع د/ خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي،الإسكندرية، ٢٠٠٩، ص٧٤.

[3] د/ رامي القاضي، مرجع سابق الإشارة إليه، ص٥٤-٥٥.

ووفقاً للسياسة الجنائية الحديثة التى هدفها تفريد العقاب الجنائي لشخصية المتهم ومبدأ فردية المسئولية الجنائية، يكون الدليل الإلكتروني ذو أهمية عظيمة، من ناحية، التقدير القانوني للجرم من حيث ارتكابه ونسبته للمتهم لتوقيع الجزاء الجنائي ومن ناحية أخرى، تقدير ظروف المتهم الشخصية ومدى خطورته على المجتمع (التقدير الاجتماعي).١ كما تبدو أهمية هذا الدليل من حيث تقديم أسلوباً قانونياً علمياً جديداً يمكن الإستعانة به في إثبات السلوك الإجرامي الذي يتم في الجرائم المعلوماتية فضلاً عن الفائدة السريعة التى يقدمها لأجهزة إنفاذ القانون وكذا دعمه حجية المخرجات المعلوماتية، (الإلكترونية) في المواد الجنائية.٢

وتطبيقاً للقاعدة العامة في الإثبات وخاصة إثبات الدعوى الجنائية وهى جواز الإثبات بكافة طرق الإثبات القانونية، فتظهر أهميته ويتعين أن يكون الدليل من الأدلة التي يمكن قبولها قانوناً، ولذلك يجب أن يعترف القانون بالأدلة ذات الطبيعة الإلكترونية، وخاصة مع تطور الأنشطة الجرمية وخاصة ما ينتشر منها في بيئة الأعمال والتجارة والبنوك الإلكترونية، فمحتوى الأدلة العادي يكون مادياً في معظم الحالات التى لا يمكن أن تنطبق أو تستخرج في الحالات السابقة إذ اتسم الإجرام بالحداثة وخاصة إذا كان إلكترونياً فكان البحث والتنقيب من قبل الدول الغربية بوجه خاص للاعتراف بالحجة القانونية التي يقدمها ذلك الدليل ذو المحتوى المعلوماتي ليس بالضرورة الموضوعية في إطار أو وعاء مادي.٣

وعلى الرغم من تلك الأهمية لهذا الدليل، فإن المشرع المصري لم يتطرق له لا من الناحية الموضوعية في شأن العقوبات ولا الإجرائية في شأن الإجراءات وأصول المحاكمات بل اكتفى بذكر الأدلة التقليدية في مجال الإثبات الجنائي كالشهادة والمحررات والقرائن والأعتراف والخبرة والمعاينة، وهذا يشكل بدوره عيباً تشريعياً وقانوناً – وحتى فقهياً– ينبغي معالجته لمواجهة صعوبات إثبات الجرائم المعلوماتية التي تنتشر يوم بعد

---

[1] Mark L. Krotoski, Effectively Using Electronic Evidence Before and After aTrial,59 Bulletin of United States Attorney 6 (2011).

[٢] المرجع السابق، ص٥٥-٥٧.

[٣] المرجع السابق، ص٥٨.

يوم في حياتنا المعاصرة العملية والتي يقف القاضي عاجزاً عن الحكم فيها ما لم يأخذ القاضي بمبدأ الإقناع وما تطمئن له عقيدته.[1]

وبناء على ماتقدم، فأن الدليل الإلكتروني يصلح لإثبات الجرائم الواقعة بواسطة الآلة، إذ تستخدم الحاسبات والإنترنت في هذا النوع من الجرائم كوسيلة لمساعدة مرتكبيها، كجرائم الغش والإحتيال أو لتهريب المخدرات، وهذا النوع من السلوكيات الإجرامية لاصلة له بالوسط الافتراضي إلا من حيث الوسيلة (فالجريمة عادية تقليدية في هذا الغرض استخدمت في وقوعها أداة رقمية) بالرغم من عدم اتصال هذه الجريمة بالنظام المعلوماتي.[2] كما يصلح ذلك الدليل في إثبات جرائم الإنترنت والآلة الرقمية، إذ يكون محل هذه الجرائم هو الحاسب الآلي أو الآلة بوجه عام، حيث يكون الإعتداء واقعاً إما على الكيان المادي للآلة ذاتها أو على الكيان المعنوي للحاسب (قاعدة البيانات أو المعلومات) كجرائم القرصنة لانتهاك الملكية الفكرية.[3]

وتكمن أهمية هذا الدليل في إنه يكون متضمناً إثبات الجرم ومرتكبه معاً، فيكون عادة جسم هذه الجريمة هو الدليل الإلكتروني ذاته، فقد يكون مشتملاً على ما يفيد نسبة الجرم لشخص ما، كما لو ارسل شخص لآخر رسالة عبر البريد الإلكتروني (e-mail) محتويه على فيروس أدى لإتلاف الحساب الخاص بذلك الشخص، فتعد هذه الرسالة في ذاتها دليلاً على وقوع الجرم.[4] كما يصلح هذا الدليل لإثبات بعض الجرائم الأخرى، إذا استعملت الآلة المعلوماتية للتمهيد لارتكاب الجرم أو لإخفاء معالمها.

ثانياً: في خصائص الدليل الإلكتروني

يتميز الدليل الإلكتروني في مجال الإثبات الجنائي بعده خصائص تجعله ذو طبيعة وأهمية خاصة بالمقارنة مع الدليل الكلاسيكي التقليدي. فيعتبر الدليل المعلوماتي دليلاً غير ملموس، فهو دليل مادي بالمعنى التقليدي، فترجمة هذا الدليل وإخراجه في شكل

---

[1] المرجع السابق، ص٥٩.
[2] د/ جميل عبد الباقي، مرجع سابق الإشارة إليه.
[3] د/ نائلة قورة، مرجع سابق الإشارة إليه، ص٣٠-٣٢.
[4] د/ هلالي أحمد ،مرجع سابق الإشارة إليه.

ملموس أو مادي لا يعني أن هذا التجميع هو الدليل – بل هى مجرد عملية لنقل تلك الموجات أو النبضات الإلكترونية إلى الشكل الذى يمكن الاستدلالال به على المعلومات.[1]

إذ أن هذا الدليل يعتبر دليلاً علمياً وفنياً في ذات الوقت وخاصة إذا كان مستخرجاً من الآلة، ولذا فأن فهم مضمونه يعتمد على استخدام أجهزة فنية ووثيقة ودقيقة تختص بفحص وتحليل ما يتضمنه من محتوى، وعلى ذلك، فكل ما لا يمكن تحليله أو تحديد مضمونه لا يعد دليلاً إلكترونياً لعدم امكانية الاستدلال به على معلومات معينة قد تعدم قيمته أو حجيته التدليلية في إثبات الجرم ونسبته على المتهم.[2]

كما يتميز هذا الدليل بأنه ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الأتصال متعدية الحدود الزمنية والإقليمية (المكانية) فضلاً عن امتياز سعته التخزينية العالمية، فيمكن تخزين ملايين المستندات أو غيرها على دسك أو اسطوانة صغيرة (USB Drive) – (CD-Desk). ٣هذا ويلاحظ أن الإتساع العالمي لمسرح الدليل المعلوماتي، يساعد مستغلي هذا الدليل من تبادل المعرفة الرقمية في مناطق مختلفة من العالم بسرعة فائقة مما يكون له الفائدة في معرفة الجناة أو الاستدلال عليهم أو سلوكياتهم بسرعة أقل نسبياً.٤

هذا ويلاحظ انه ممكن من خلال هذا الدليل رصد وجمع المعلومات عن المتهم وفحصها في ذات الوقت، فيستطيع هذا الدليل تسجيل حركات الفرد، وسلوكياته وبعض أموره الخاصة ، ولذلك فقد يجد البحث الجنائي سهولة في استخدامه عن الدليل الكلاسيكي المادي.[5] كما يمكن استخراج نسخ من الأدلة الجنائية المعلوماتية طبق الأصل فتكون لها نفس الحجية القانونية والقيمة الأساسية في الإثبات، إذ أن هذا قد لا يتوافر – في بعض الأحيان– في الأدلة المادية الأخرى، مما يُشكل ضمانة كبيرة وفعالة للحفاظ على الدليل

---

[1]David L.Gripman, The Doors are Locked but the Thieves and Vandarls are Still Getting in:A Proposal in Tort to Alleviate Corporate America's Cyber-crime Problem,16 J. Marshell J.Computer & Info.L.167,169-70 (1997).

[2]راجع Krotoski، مرجع السابق الإشارة إليه، ص٦٠.

[3]المرجع السابق ، ص٦١.

[4]المرجع السابق ، ص٦٢.

[5]راجع في هذا الشأن: هلال بن محمد البوسعيدي- الحماية القانونية والفنية لقواعد المعلومات المحوسبة: دراسة قانونية فنية مقارنة – دار النهضة العربية، القاهرة، ٢٠٠٩ ، ص١٣٩.

بعض الأحيان- في الأدلة المادية الأخرى، مما يُشكل ضمانة كبيرة وفعالة للحفاظ على الدليل ضد أى تلف أو تغيير أو تدمير (ضياع).[1] ومن هذا المنطلق يمكن القول بأنه يجوز لمأموري الضبط القضائي ضبط الأجهزة والبرامج والأدوات المستخدمة لإرتكاب الأفعال المعلوماتية المجرمة والتحفظ على البيانات والمعلومات المتعلقة بارتكاب أى منها.[2]

ومن الجدير بالذكر أن الأدلة الإلكترونية يمكن استرجعها بعد محوها وإظهارها بعد طمسها وإصلاحها بعد إتلافها، مما يعنى صعوبة التخلص منها بالمقارنة بالدليل المادي العادي فهناك الكثير من البرامج الآلية التي تكون وظيفتها استعادة المعلومات وارجاع البيانات التى تم إلغائها أو حذفها سواء تم ذلك بأمر (delete) أو (format) ، إذ أن ذلك يعنى صعوبة تستر أو تخفي المتهم أو اخفاءه لجريمته عن أعين العدالة والامن طالما علم رجال البحث الجنائي بوقوع الجرم.[3]

ثالثاً: في أنواع وتقسيمات (تصنيفات) الأدلة المعلوماتية

الدليل المعلوماتي ليس له صورة واحدة ، بل له عدة أشكال وصور مختلفة منها الأدلة الرقمية خاصة بشبكات وأجهزة الحاسوب وكذا أدلة رقمية خاصة بشبكة الإنترنت العالمية، فضلاً عن الأدلة الرقمية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة المعلوماتية.[4]

ولهذا التنوع أهميته في إنه ليس هناك وسيلة وحيدة للحصول على الدليل، إنما هناك صور ووسائل عدة يمكن أن توصل إليه. وعلى ذلك، يمكن القول بأن الأدلة الإلكترونية تتخذ صورتين رئيسيتين إما أدلة أعُدت لكي تكون وسيلة إثبات، كالسجلات التى تم خلقها

---

[1] د/ رمزي عوض، مرجع سابق الإشارة إليه.

[2] John Nikell and John Fisher, Crime, Science, and Methods of Forensic Detection, Lexington,Univi.of Kentuchky (1999).

[3] Ronald L. Mendle, Investigating Computer Crimes:A Primer for Security Manger, New York (Charles Thomas 1998).

[4] انظر:سامي حمدان الواشدة، قاعدة استبعاد الأدلة غير المشروعة في الإجراءات الجزائية، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة، الأردن، المجلد ٣، العدد٢،٢٠١١،٣.

بواسطة الآلة اتومتيكياً (تلقائياً)، إذ تعتبر من مخرجاتها التى لا دخل للفرد في إنشائها مثل قوانين الحاسب الآلي وسجلات الهواتف، وإما السجلات التى تم حفظ جزء منها بالإدخال وتم إنشاء جزء منه بواسطة الآلة (كإجراء العمليات الحسابية على بيانات تم معالجتها من خلال برنامج خاص).[1]

وهناك أدلة لم تكن معده لكي تكون وسيلة إثبات، إذ إنها نشأت دون إراده فرد، فهى مجرد آثر يتركه المتهم دون أن يكون راغباً في وجوده، (البصمة الإلكترونية أو الآثار المعلوماتية الإلكترونية) وهى المتبلورة في الآثار التى يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه وكذا التى يستقبلها.[2] ويلاحظ أن هذا النوع لم يعد من الأساس للحفظ من جهة من صدر عنه بل إن الوسائل التكنولوجية الفنية تساعد في ضبط هذه الأدلة ولو بعد فترة طويلة من نشوئها، إذ يمكن ضبط المراسلات والإتصالات التى تتم عبر الإنترنت بواسطة تقنية خاصة بذلك.[3]

وبناء على ما تقدم، يتخذ الدليل الإلكتروني في الإثبات الجنائي أشكالاً رئيسية باستخدام الشاشة المرئية وهى تمثل بديل عن الصورة الفوتوغرافية العادية فهى أفضل منها وأكثر تطوراً عنها وكذا التسجيلات الصوتية التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية (كالمحادثات الصوتية الهاتفية أوعبر الإنترنت وغيرها).[4] وهناك النصوص المكتوبة بواسطة الآلة الرقمية كالرسائل عبر البريد الإلكتروني أو الهاتف المحمول وكذلك وسائل التواصل الاجتماعي المعروفة حالياً في وقتنا الراهن مثل "Face Book" "Twitter" "Whats App". فلا ريب في أن هذا الدليل يتطور بتطور وسائل الحصول عليه، فعلمياً هناك دليل البصمة الوراثية واثره في التعرف على المجرمين عن

---

[1] انظر على سبيل المثال:(18 U.S.C.A. Ss 1029(a)(7) (west sup.1999

[2] انظر مثلا: United States V.Sablan, 92f, 3d867(9thcir.1996)

[3] أنظر شمسان ناجي الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت: دراسة مقارنة ، دار النهضة العربية،القاهرة،٢٠٠٩، ص٤٤.

[4] المرجع السابق ، ص٤٥.

المبحث الثاني

شروط صحة قبول الدليل الإلكتروني في الإثبات الجنائي

يتمتع الدليل المعلوماتي بصفة الحداثة والتطور السريع، حيث إنه من الأدلة الجديدة التى انتجها التطور العلمي والتقني الهائل في مجال الاتصالات وتكنولوجيا المعلومات. كما إنه ذو طبيعة خاصة من حيث الوسط الذي نشأ فيه وكذا طبيعته الفنية التى تميزه عن الدليل التقليدي، ولذلك يثور التساؤل حول مشروعية (مدى قانونية) الأخذ والعمل به، إذ إنه ـــــ طبقاً للقواعد العامة في الإجراءات الجنائية – يشترط في الدليل أن يكون مشروعاً من حيث وجوده والحصول عليه التي تتم باتباع الإجراءات المقررة قانوناً. لذلك فيثير الوسط الذي نشأ فيه هذا الدليل عدة تساؤلات منها إمكانية البحث عنه في العالم الافتراضي وضبطه وفقاً لقواعد التفتيش وكذا صفة الشخص القائم على جمع هذا الدليل وكذا شروط صحة قبوله. وعلى ذلك، كان الفقه قد بحث هذه المسالة وثارت عده خلافات ينبغي التعرض لها فضلاً عن بيان موقف التشريعات من مكانه هذا الدليل وشروط صحته في الإثبات.

أولاً– موقف الفقه الجنائي والتشريعات من الدليل المعلوماتي كوسيلة إثبات في المسائل والمواد الجنائية

بادىء ذى بدء، تجدر الإشارة إلى أن الأدلة المتحصلة من الوسائل المعلوماتية (الإلكترونية) تخضع للسلطة التقديرية للقاضي الجنائي، فإذا اطمئن إليه وتكونت عقيدته واستراح ضميره لها ووجدها قوية ومنطقية وكافية واستمد اقتناعه الكامل منها، فله أن يعول ويستند عليها في الحكم الذي يصدره وينتهي إليه.

فاتساع دائرة استخدام الشبكات الدولية للمعلومات في العصر الراهن أدى إلى استخدامها المتزايد وما نتج عن هذا الاستخدام من مخاطر، كافراز نوع جديد من الإجرام و هو الإجرام المعلوماتي الذي افرز بعض الجرائم الإلكترونية كالتزوير والإختلاس والذي يتم عبر الوسائل الإلكترونية وكذا سرقة المعلومات والجرائم الماسة بالأخلاق والآداب العامة وغيرها، فنجد أن النصوص العادية للقوانين لا تسعف مجابهة تلك السلوكيات الحديثة.

انطلاقاً من ذلك، وحماية لحريات الأشخاص وسمعتهم وكذا درء العدوان على الممتلكات العامة والخاصة وفي سياق توجيهات المجتمع الدولي، أصدرت بعض الدول التشريعات الخاصة بالجرائم الإلكترونية ومكافحتها وذلك أيضاً في ضوء الإلتزام بأحكام المواثيق الدولية كالإتفاقية العربية لمكافحة جرائم تقنية المعلومات، فصدر في مصر على سبيل المثال- لا الحصر كما أسلفنا الإشارة من قبل - قانون التوقيع الإلكتروني وكذا تنظيم الإتصالات وكذا تشريعات حماية الملكية الفكرية.[1]

هذا ويمكن القول بأن التشريعات السالف الإشارة إليها تضمنت جرائم وعقوبات مشددة على بعض الجرائم الإلكترونية التى تقع سواء على المعلومات أو الأنظمة المعلوماتية أو حتى باستخدام الوسائل الإلكترونية وكذا أفعال التزوير والغش والتلاعب في البيانات أو المحررات الحكومية وغيرها أو حتى التعطيل أو الوقوف العمدي للوصول للمواقع الإلكترونية.

إلا أن المشرع المصري وكذا غيره وخاصة في الدول العربية لم يتعرض لمعالجة مسألة الإثبات بالدليل الإلكتروني في المواد الجنائية وخاصة في قانون الإجراءات الجنائية.

من المعروف إنه لا يوجد نص صريح في قانون الإجراءات الجنائية المصري بقبول الدليل الإلكتروني في الإثبات الجنائي، ولكن يمكن القول بأنه يجوز للمحاكم الجنائية في مصر- وغيرها من الدول- أن تأخذ بهذا الدليل كحجه في الدعوى الجنائية في ضوء القواعد والأحكام العامة الواردة بشأن الإثبات الجنائي.

فالدليل الإلكتروني قد يكون في شكل نص مكتوب على دعامة (قرص مدمج) ويختلف عن المستند (المحرر) التقليدي، وبالرجوع لأحكام قانون الإجراءات الجنائية، نجد أن هناك نصوص تتحدث عن الاوراق والمستندات كدليل إثبات وقبول المشرع لها، فاذا كان ذلك كذلك، فالمستند الإلكتروني لا يختلف عن المحرر العادي إلا من حيث شكله (الدعامة المكتوب عليها) ولذا فأن هذا الدليل إذا اتخذ شكل النص المكتوب، فأنه يكون مشروعاً ويأخذ حكم المستندات والاوراق التي يقبلها القانون كدليل إثبات.٢

---

[1] راجع في هذا الصدد، التشريعات المصرية الخاصة بالحماية الإلكترونية ومنها- قانون التوقيع الإلكتروني ٢٠٠٤، وكذا قانون حماية الملكية الفكرية٢٠٠٢ وكذا قانون تنظيم الاتصالات رقم١٠ لسنة ٢٠٠٣.

[2] أنظر في هذا الشأن على سبيل المثال: United States v. Czubinski,106 F.3d 1069,1078 (1st cir.1997).

هذا ومن المسلم به أن المشرع الإجرائي وكذا المشرع الدستوري قد نص على حماية الحق في حرمه الحياة الخاصة، فلا يجوز الإعتداء عليها بأى وسيلة كانت، ويعتبر جريمة كل إعتداء يمس بحرمه هذه الحياة ويدخل في ذلك، الإعتداء على هذا الحق باستعمال وسائل إلكترونية وفي مجال الإجراءات وخاصة ما يتعلق بالضبط والتفتيش، فيجوز لمأموري الضبط القضائي القيام بهذه الأعمال وكذا مراقبة المحادثات الهاتفية ولكن بعد الحصول على إذن (أمر) قضائي مسبب لتلك الإجراء حتى تكون متفقة وصحيح القانون متى كان لذلك فائدة في إظهار الحقيقة وكشف الجريمة.[1]

ولذلك فلوسائل الإثبات العلمية قيمة قانونية لإثبات الجرم، ومن ثم يعد الدليل الإلكتروني بوصفه من الأدلة العلمية كوسيلة إثبات بشرط الحصول عليه بما يتفق وحكم القانون، إذ يشترط مشروعية الحصول على الدليل وخصوصاً مراعاة حرمة الحياة الخاصة.[2] هذا ويلاحظ أن الأدلة التى تُكفل وتكون حجة في إثبات بعض الجرائم (كالزنا مثلاً) إذ وقع الضبط في حالة تلبس قائم بالفعل أو بوجود وثائق قاطعة بوقوع الفعل أو حتى الأعتراف القضائي، فقد تكون هذه الوثائق، رسائل أو مكاتبات، فتصلح أن تكون دليلاً إلكترونياً لإثبات الواقعة متى تم الحصول عليها بطريق مشروع يراعي الخصوصية.[3]

هذا ومن المعروف أن العرف قد جرى على الأخذ بكافة طرق الإثبات في المسائل المدنية والتجارية بما في ذلك البيانات الإلكترونية، فلا يوجد ما يمنع إن يشمل الإثبات في المسائل الجنائية ، فإثبات المعاملات المادية والمصرفية قد يصلح كدليل لإثبات واقعة جنائية (إجرامية) ، فالتشابك والتداخل في الوقائع موضوع الإثبات هو ما يمكن الإستناد إليه، كإثبات جرائم غسل الأموال التى ترتكبها البنوك مثلاً.[4]

---

[1] National Information Infrastructutre Protection Act of 1996: Hearings on S.982,104 th Cong.90 (1996).

[2] راجع شمسان الخيلي، مرجع سابق الإشارة إليه، ص٤٧.

[3] المرجع السابق، ص٤٩-٥٠.

[4] المرجع السابق ، ص٥٦ومابعدها.

طبقاً للمبادىء المستقر عليها في قانون الإجراءات الجنائية في غالبية الدول هو أن الأدلة الجنائية غير محددة على سبيل الحصر في القانون، إذ أن ذلك يتطلب حرية القاضي في تكوين عقيدته وقناعته، وعدم حصر الأدلة على سبيل الحصر معناه أن الأدلة الجنائية تستقر في ضمير القاضي وعقيدته من كل شيء ويتخذ من كل ظرف دليلاً على براءة أو إدانه الجاني طالما تم طرح الدليل للمناقشة في الجلسة وكان الخصوم على علم به، وإن كان من المحظور على القاضي الجنائي تكوين عقيدته من معلومات شخصية أو اهواء فردية قد يستقيها من مصادر خارج الدعوى الجنائية.[1]

والسبب وراء عدم حصر المشرع الجنائي الإجرائي للأدلة الجنائية بنصوص تفترض شكلية خاصة كما هو الحال في الأدلة المدنية، كالإقرار أو توفر الكتابة لإثبات بعض التصرفات القانونية، حيث أن المجرم يتخذ كل الوسائل ويبذل قصارى جهده من أجل طمس الأدلة التى من شأنها إدانته، كما أن الجرم ليس معروف أو معلوم كيف ومتى وبأى أسلوب يقع، فمن الأفضل ترك وسائل الإثبات دون تحديد، فهى وسائل غير محددة.[2]

وبناء على ماتقدم، تنقسم الأدلة إلى أدلة مادية وهو كل ما له كيان مادي ملموس و يمكن إدراكه والكشف عنه سواء بالحواس مباشرة، كالرؤية واللمس كضبط الجاني حاملاً سلاحاً استعمله في تنفيذ الجرم وكذا وجود الشيء المسروق في حيازة المتهم أو حتى بأحد الأجهزة العلمية (أى بصورة غير مباشرة) إذ لا يشترط كشف الآثار المادية للأدلة مباشرة كما أسلفنا من قبل، فلا مانع من اللجوء للوسائل التقنية الحديثة كبصمة اليد أو الأشعة مثلاً.[3] وهناك الأدلة المعنوية (القولية) التى تصل لعلم المحقق – غالباً– على لسان الغير كالأعتراف والشهادة.

---

[1] انظر د/ ابراهيم طنطاوي ود/ على حموده، مرجع سابق الإشارة إليه، ص٣٣-٣٤.
[2] المرجع السابق،ص ٣٥-٣٦.
[3] المرجع السابق،ص٣٨ ومابعدها.

هذا ويمكن القول بأن الأدلة الجنائية المباشرة، هى أدلة قاطعة لا لبس فيها فيما يتعلق بإثبات الجرم وكذا الوقائع التى ارتكبها الجاني، فالقاضي هنا يكون عقيدته عبر إثبات الوقائع ولا يحتاج لأدلة أخرى، كالشهادة والأعتراف.[1]

فهى أدلة إثبات سهلة ومباشرة ومؤكدة، فغالباً لا تحتاج لتعليقات أو مناقشات، فمعاينة سكين ملوث بالدم في محل الواقعة، قرينة قوية على أن ذلك السكين هو سلاح (أداة) الجرم. أما الأدلة غير المباشرة لا تنصب على الواقعة المراد إثباتها مباشرة وإنما بشكل غير مباشر، فهى تنصب على واقعة أخرى لها صلة منطقية بالواقعة المرتكبة، ودور المحقق هنا أن يستنبط ذلك عبر إحكام عقله، فيستنبط من الواقعة التى ارتكز الدليل عليها الواقعة الأخرى المراد إثباتها، ومثال ذلك إذا أراد مأمور الضبط القضائي (أو المحقق) إثبات وجود الجاني على مسرح الجريمة، فعليه إثبات واقعة وجود بصمة اصابعه.[2]

وتجدر الإشارة في هذا الصدد إلى أن بعض الفقه قد ذهب لاعتبار الأدلة الإلكترونية مرحلة متقدمة من الأدلة المادية والممكن إدراكها بالحواس الطبيعية، فاما أن تكون مخرجات مستندية ورقية يتم إخراجها عبر الطابعات (printers) وإما مخرجات غير ورقية (إلكترونية) كالأقراص و الأشرطة المدمجة والأسطوانات الممغنطة وغيرها وإما مخرجات مرئية تتمثل في عرض مخرجات المعالجة بواسطة الحاسب على الشاشة أو الإنترنت عن طريق وحدة العرض المرئي .[3] بينما ذهب اتجاه آخر في الفقه يرى أن الدليل الإلكتروني له طبيعة خاصة تميزه عن غيره من الأدلة، فهو إضافة جديدة لأنواع الأدلة الجنائية الأخرى. وعلى آية حال، فيجب اعتبار واعتماد تلك الأدلة الجديدة التى تتفق مع طبيعة البيئة (الوسط) المرتكب فيه الجريمة.

---

[1] انظر بوجه عام في هذا الإطار، أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، مكتبة الجامعة، الطبعة الأولى،الشارقة،٢٠١٢.

[2] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى ،٢٠٠٧، ص١٠-١٨.

[3] د/ جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة: دراسة في الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة،٢٠١٢ ، ص ٤٥-٤٨.

ثانياً: في شروط صحة قبول الدليل الإلكتروني في الإثبات الجنائي

هذه الشروط تنقسم إلى نوعين ، منها ما هو متعلق بالشروط القانونية اللازمة لصحة هذا الدليل، ومنها شروط فنية تقنية لازمة لصحة هذا الدليل. وفي ضوء ذلك، يمكن القول بأن الدليل الإلكتروني عبارة عن مستند (محرر) مكتوب وموقع إلكترونياً، يوضع على وسيط مادي (الدعامة الإلكترونية). فالكتابة والتوقيع هما الشرطان القانونيان اللازمان لصحة قبول هذا الدليل. ونبين فيما يلي شرطي الكتابة والتوقيع كوسيلة من وسائل الإثبات.

١. الكتابة كوسيلة إثبات معتمدة قانوناً

الكتابة إجرائياً، هى الخط الذي يُعتمد عليه في توثيق الحقوق، فهى كل كتابة تصدر من المجني عليه في الدعوى الجنائية هدفها تحديد الجاني أو على الأقل تجعل وجوده قريب الاحتمال. ولا شك في أن الكتابة أصبحت من الأدلة القوية التى يُأخذ بها في الدعوى الجنائية ويتعين على القاضي الأخذ بها وعدم تجاهلها كدليل أساسي في الدعوى إذ كانت تؤدي لاظهار الحقيقة.[١]

فتطورت الكتابة مع تطور الجريمة، فتطورت أجهزة العدالة الجنائية بفروعها ومنها الأدلة الجنائية والطب الشرعي المختص باستخلاص جمع الأدلة ومضاهاة الخطوط وغيرها، فاصبحت الكتابة الإلكترونية عاملاً فعالاً لحفظ الحقوق وتأكيدها.[٢]

هذا والكتابة المستخدمة في الإثبات الجنائي إما رسمية وإما عرفية، فالكتابة الرسمية هى الصادرة عن موظف عام مختص في حدود سلطته وأثناء قيامه بمهام عمله وطبقاً للأوضاع المقررة قانوناً، وتعد المحررات الرسمية حجة على جميع الأشخاص بما دُون فيها من أمور قام بها محررها أو مُصدرها ما لم يتبين تزويرها بالطرق المحددة قانوناً.[٣]

---

[١] المرجع السابق،ص٤٩-٥٠.

[2] Brent Schneider, High- Technology Crime: Investigating Cases Involving Computers,(San Jose:KSK Publications 1999), at 100-105.

[3] Howard W.Cox, Recent Develpomats and Trends in Searching and Seizing Electronic Evidence,59 The United States Attorney Bulletin 6 (2011), at 75-79.

فإذا تخلف أحد الشروط المقررة قانوناً، فلم يكتسب المحرر صفة الرسمية وبالتالي كان بمثابة معلومات عادية غالباً ما لا يحتج بها أمام المحاكم.[1]

أما الكتابة العرفية (المحرر العرفي)، هى الصادرة عن الأشخاص بهدف حسم ما قد يثور من نزاع حول أمر معين، وتكون موقعة ممن يحتج عليه بها وهذا المحرر لا يصدر من موظف عام مختص كالمحرر الرسمي.[2]

وجدير بالذكر، إنه قبل ظهور الكتابة الإلكترونية، لا يشترط شكلاً معيناً في الكتابة و هناك اجماع في الفقه الجنائي على إنه إذا ما اشتمل أو تضمن المحرر كتابة تثبت ما تم الإتفاق عليه، فلا يشترط بعد ذلك شكلاً خاصاً لصياغة هذه الكتابة، فقد تكون خطية أو مطبوعة أو بأى مادة كانت بل يجوز أن تكون برموز خاصة طالما احتفظ الأطراف بمفاتيح هذه الرموز.[3]

وبعد أن أصبحت المحررات الإلكترونية حقيقة واقعية ملموسة، حدثت فجوة بين العمل و القواعد المستقرة في الإثبات الجنائي والتي لا تقبل سوى المحررات الورقية. لذا اعترف المشرع المصري- وخاصة في قانون التوقيع الإلكتروني ٢٠٠٤- بحجية المحررات الإلكترونية في الإثبات بوجه عام مما أدى لظهور مفهوم قانوني جديد للكتابة المطلوبة للإثبات، فاضحت الكتابة الإلكترونية دليلاً كتابياً ملزماً للقاضي كالكتابة التقليدية.[4]

والكتابة الإلكترونية هى كل حروف أو أرقام أو رموز أو أى علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أى وسيلة مشابهة وتعطي دلالة قابلة للإدراك كما أن المحرر الإلكتروني هو رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو تستقبل أو ترسل، كلياً أو جزئياً بوسيلة إلكترونية أو رقمية أو ضوئية أو آية

---

[1] راجع د/ ممدوح عبد المطلب،مرجع سابق الإشارة إليه، ص٧٣.

[2] د/ محمود محمود مصطفى، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، طبعة ١٩٧٦،١١، ص١٠٠-١٠٥.

[3] John Paradel, Droit Penal General, CuJus (2002-2003) No.181,at p.175.

[4] د/أحمد فتحي سرور، مرجع سابق الإشارة إليه، ص٩٧.

وسيلة أخرى، وعليه، فالكتابة تقليدية كانت أو إلكترونية ما هى إلا وسيلة يتم إعمالها لإظهار الدليل، مما يمكن أطراف النزاع من الرجوع إليه أوإطلاع القاضي عليه.[1]

ويشترط في الكتابة بوجه عام أن تكون مقروءة، بمعنى لكى تحوز الكتابة الحجية في الإثبات يجب أن تكتب بحروف أو رموز أو إشارات تدل على معناها (المقصود منها، بحيث يستطيع الغير فهمها).

وهذا ما أوضحه المشرع المصري في قانون التوقيع الإلكتروني وكذا قانون الإثبات.[2] وعلى الرغم من أن الكتابة الإلكترونية مرئية الشكل، ورقمية- إلا إنها في نهاية المطاف – تأخذ على شاشة الجهاز صورة الكتابة التقليدية وبالتالي يمكن قراءتها وفهم محتواها (مضمونها) بصورة جلية.[3]

كما يجب أن تكون هذه الكتابة باقية، إذ أن دوامها يتطلب تدويتها على دعامة تسمح ببقائها وثباتها (فتكون المادة التى دونت بها صالحة للبقاء والإستمرار) كي يمكن الرجوع إليها إن لزم . هذا وعلى الرغم من أن الكتابة الإلكترونية دائماً ما تكتب على أقراص أو شرائط ممغنطة، وهى أدوات حساسة يمكن تعرضها للتلف السريع إلا أن الدراسات الحديثة والتقنيات السريعة المتطورة أثبتت إمكانية تلاشي هذا العيب الفني، بحيث يمكن الاحتفاظ بتلك الكتابة مدد زمنية تفوق قدرة الدعامات الورقية.[4]

هذا ويلاحظ أنه يشترط عدم قابلية الكتابة للتعديل، بمعنى أن الدليل الكتابي قد يعتريه عيوب مادية كالإضافة أو الحذف أو التحشير أو المحو، وبالتالي هذه العيوب تُضعف من قيمته أو تفقده كل قيمته في بعض الأحيان فلا تكون ملزمة للقاضي .[5] وإذا كان من السهل التعرف على تلك العيوب التى يمكن أن تدخل على الكتاب التقليدية عن طريق

---

[1] المرجع السابق، ص٩٥.

[2] Richard Power and Rik Farrow,Electronic Commerce Crime,Includes Related Article on Exerpt from a Hacker's Email, Internet/Web/Online Service Information,Network,Dec.1997.

[3] انظر هلال البوسعيدي، سابق الإشارة إليه، ص٥٠-٥٥.

[4] انظر د/خالد ابراهيم، سابق الإشارة إليه، ص٧٦-٧٧.

[5] انظرد/ حسين بن سعيد الغافري،السياسة الجنائية في مواجهة جرائم الإنترنت:دراسة مقارنة،دار النهضة العربية،القاهرة،٢٠٠٩،ص٥٣ ومابعدها.

الإستعانة بالخبرة الفنية، إلا إنه قد يبدو من السهل التلاعب في الكتابة الإلكترونية، ولكن أثبتت الدراسات التقنية الحديثة التغلب على هذه العقبة عن طريق استخدام برامج إلية تسمح بتحويل النص الذي يمكن تعديلة "Document War Processing " بصورة ثابتة لا يمكن تحويلها " Document Image Processing " .[1]

٢- التوقيع كوسيلة إثبات:

تجدر الإشارة إلى أن الكتابة وحدها لاتعد دليلاً كاملاً في الإثبات الجنائي إلا إذا كانت موقعة، فالتوقيع هوالعنصر الأساسي الثاني من عناصر الدليل المعلوماتي، وغيابه يفقده حجيته، بل طبيعته كدليل، فالتوقيع هو الذي ينسب الكتابة لمن وقعها حتى لو كانت بخط غيره.[2]

هذا وقد تولى بعض الفقه مهمة تحديد مفهوم للتوقيع، فعرفه بأنه" علامة مميزه وخاصة بالشخص الموقع، تسمح بتحديد شخصيته والتعرف عليه بسهوله، على نحو يظهر إرادته الصريحه". وبعبارة أخرى، هو علامة خطية مميزة يصفها الموقع بأى وسيلة على مستند لإقراره.[3] هذا وقد حددت المواثيق والتشريعات الدولية والوطنية تعريفات مختلفة لشكل التوقيع، فقد عرفته المادة(٢) من قانون اليونيسترال "Model of UNICETRAL" بأنه عبارة عن "بيانات مدرجة في شكل إلكتروني مدرجة في رسالة البيانات أومضافة إليها أو مرتبطة بها منطقياً، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة لرسالة البيانات ولبيان موافقته على المعلومات الواردة في هذه الرسالة."[4]

ويمكن القول كذلك بأنه بيان أو معلومة معالجة إلكترونياً تلتصق أو ترتبط منطقياً بمعلومات أو بيانات إلكترونية أخرى (كمحرر أو رسالة) وتصبح وسيلة لتوثيقها أو إقرارها وهذا حسب تعريف أحكام التوجيه الأوروبي بشأن التوقيع الإلكتروني.[5]

---

[1] Richard Raysman & Peter Brown,Virsues,Worms, and Other Destructive Forces, N.Y.L.J., July 13,1999.

[2] أنظر مثلاً: 18 U.S.C.A.Ss 1030 (e) (2) (B) (west sup.1999).

[3] أنظر مثلاً: 18 U.S.C.A.Ss 1030 (e) (2) (A).

[4] أنظر مثلاً: 18 U.S.C.A.Ss 1030 (e) (2) (8).

[5] أنظر قانون اليونيسترالUNICITRAL Model Law on Electronic Commerce Guide to

في ضوء ما تقدم، يمكن القول بأن التوقيع الإلكتروني يتعين أن يؤدي ذات وظائف التوقيع التقليدي ، بأن يكون محدداً لشخص الموقع، وكذا معبراً عن رضائه بالإلتزام بمحتوى المحرر و مضمونه الذي وقع عليه، عبر وسيلة آمنة تضمن سرية وأمان التوقيع وصحة نسبته لصاحبه.[1]

هذا وقد يتم هذا التوقيع عن طريق قيام الموقع بكتابة توقيعه الشخصي- بخط إليد- باستخدام قلم إلكتروني ضوئي خاص تمكنه من الكتابة على شاشة الحاسوب، عبر برنامج خاص بالتقاط التوقيع والتحقق من صحته، بالإستناد وكحركة القلم على الشاشة.[2] ويتم ذلك في الغالب عن طريق التصوير بالماسح الضوئي"scanner" ثم نقل هذه الصورة الملتقطة للتوقيع للملف المعني عبر الشبكة المعلوماتية.[3]

وتتسم هذه الصورة من صور التوقيع الإلكتروني بسهولتها ومرونتها التى تتم بمجرد تحويل التوقيع العادى لإلكترونى ولكن تكون غير آمنة – فى بعض الأحيان – بصعوبة إثبات الصلة بين التوقيع ورسالة البيانات أو المحرر، وبالتالى لا يجوز الأخذ بهذه الصورة فى الإثبات الجنائى .[4] ويمكن التوقيع باستخدام البطاقة الممغنطة المقترنة بالرقم السرى وهى الطريقة الأكثر شيوعاً فى العمل – وخاصة فى المعاملات البنكية والمصرفية، إذ إنها لا تشترط أن يمتلك الشخص حاسباً إلياً (أو أن يكون جهازه متصلاً بالإنترنت)، فاستخدامها لا يتطلب خبرة معينة، فأى شخص له استخدام هذه الصورة .[5]

وغالباً ما تقوم المؤسسات المالية والإئتمانية إصدار تلك البطاقات حاملة بيانات العميل والرقم السرى الخاص به والتى تُمكن حاملها من استخدامها فى السحب النقدى والدفع غير النقدى (كالوفاء بثمن المشتريات من المحال التجارية التى تقبل التعامل بها

Enactment (1996), arts. (6) &(7) .

[1] د/ رمسيس بهنام، مرجع سابق الإشارة إليه، ص٨٠- ٨٥.

[2] د/ جلال ثروت، مرجع سابق الإشارة إليه، ص١٦٠-١٦٥ .

[3] على حمودة، مرجع سابق الإشارة إليه (بصفة عامة).

[4] Haeji Hong, Hacking through the Computer Fraud and Abuse Act,31 U.C.Davis L.Rev.283,296(1997).

[5] Wendy Davis, ProsecutorsWatching the Web Street Crime is Down but that May Just Mean its Moving Online,158 N.L.J.935 (1999).

بموجب اتفاق مع البنك مُصدر البطاقة).[1] هذا جدير بالذكر أن القضاء الفرنسى قد أقر ذلك النوع من التوقيعات واعترف بحجيته فى مجال الإثبات الجنائى في كثير من أحكامه.

وقد يأخذ التوقيع صورة التوقيع "باستخدام الخواص الذاتية "Biometrix" وذلك عبر التحقق من شخصية المتعامل بالإعتماد على الخواص الذاتية، والصفات الفيزيائية والطبيعية للأشخاص، كبصمة الشفاه ونبرة الصوت وقزحية العينين وغيرها، فيقوم الحاسوب بأخذ صورة دقيقة لشكل التوقيع ثم تخزينيها بطريقة مشفرة فى ذاكرته، ويتم فك هذا التشفير للتأكد من صحة التوقيع بمطابقة بصمة العميل بالبصمة المخزنة وهذه الطريقة آمنة للغاية إلا إنها تحتاج لتكليفات عالية وباهظة لوضع نظام مُحكم أو آمن لاستخدام هذا التوقيع.[2]

كما أن هناك صورة حديثة للتوقيع الرقمى قائمة على استخدام أو شفرة المفاتيح الخاصة بانشاء التوقيع وكتابة الرسالة والأخرى خاصة بفتح الرسالة وتسمى مفاتيح عامة وخاصة.[3] لا شك أن التوقيع أى كان شكله ولكى ينتج أثره الفعال فى الإثبات الجنائى، يشترط أن يُستخدم فى تحديد هوية الموقع بالنسبة لرسالة البيانات كما يشترط أن يتسم ذلك التوقيع بالدوام والإستمرار وأن يكون مرتبطاً بصاحبه ومتصلاً بالمحرر المعلوماتى.[4]

هنا ويلاحظ إنه يكون الدليل باطلاً إذ تم التحصل عليه بطريق غير مشروع أي بالمخالفة للقانون وقد تبطل كافة الآثار المترتبة على بطلان الدليل، فإذا كان الدليل الباطل هو الدليل الوحيد فى الدعوى فلا يجوز الإستناد إليه فى إدانة الجانى.[5] هذا ويقع عبء الإثبات فى الجرائم المعلوماتية – طبقاً للقواعد العامة – على عاتق النيابة العامة بوصفها ممثلة سلطة الإدعاء العام للدعوى العمومية ولكن يجوز الخروج على هذه القاعدة –

---

[1] د/ جميل عبد الباقي الصغير،المواجهة الجنائية لقرصنة البرامج التلفيزيونية المدفوعة: دراسة مقارنة، دار النهضة العربية، القاهرة،٢٠٠١.

[2] انظر على سبيل المثال: United States V.Colterman, 637F.3d 1068 (9th cir.2011).

[3] د/ رمسيس بهنام، مرجع سابق الإشارة إليه.

[4] انظر مثلاً: United States V.Abbouchi,502 F.3d 850,855 C 9th Cir

[5] د/ آمال عثمان، مرجع سابق الإشارة إليه، ص٣٠٣.

إستثناءاً – فينتقل عبء الإثبات إلى المجنى عليه.[1] فطبقاً للقواعد العامة فى الإجراءات الجنائية، تقوم النيابة العامة بالتحرى وجمع الأدلة والتحقق لاستقصاء الجريمة وكشف مرتكبيها، وللمحقق فعل ذلك بأي وسيلة مادامت غير ماسة بحقوق وحريات الأفراد.

وبناءاً على ذلك، يمكن القول بأنه لكى يكون الدليل الإلكتروني مقبولاً ومشروعاً فى المواد الجنائية فانه يجب الحصول عليه بطريقة مشروعة وقانونية غير مخالفة لأحكام الدستور والقانون وبخاصة قانون العقوبات، فمن المهم تنظيم ذلك الشرط فى ضوء وجود نص قانونى يحمي الحماية الخاصة المخزنة فى أنظمة المعلومات كالإنترنت والحاسبات.[2]

ويعد غير مشروعاً التصنت للبحث عن هذا الدليل وكذا الإكراه مادياً كان أو معنوياً أو التحريض على ارتكاب الجريمة الإلكترونية من قبل إعطاء مأمور الضبط القضائى أو حتى التحريض على الغش أو التزوير الإلكتروني أو التجسس المعلوماتى والمراقبة المعلوماتية عن بُعد وغيرها.[3] فضلاً عن ذلك، استخدام التدليس والخداع والغش فى الحصول على الأدلة المعلوماتية. هذا وقد نصت المواثيق الدولية على حماية الأشخاص فى مواجهة مخاطر المعالجة الإلكترونية البيانات الشخصية، فقد أكدت الاتفاقيات الدولية الخاصة ذلك الأمر، فيجب أن تكون البيانات المضبوطة مجتمعة وكاملة ومستمدة بطرق محددة ومدة حفظها محددة زمنياً وعدم إفشائها فى غير الأغراض المخصصة لها وحق الشخص فى الإطلاع عليها وتعديلها وتصحيحها ومحوها لو كانت باطلة.[4]

كما يجب أن تكون الأدلة المعلوماتية يقينية (غير قابلة للشك) حتى يمكن الحكم بالأوراق، فلا مجال لجحد قرينة البراءة وافتراض عكسها إلا عندما تصل عقيدة القاضى لحد اليقين والجزم، فيستطيع القاضى من خلال ما يُعرض عليه من مخرجات إلكترونية أن يحدد القوة الاستدلالية على صدق نسبة الجرم المعلوماتى لشخص معين بذاته دون غيره.[5]

---

[1] د/ هلالي عبد اللاه أحمد، إلتزام الشاهد بالاعلام في الجرائم المعلوماتية: دراسة مقارنة، النسر الذهبي، القاهرة، ٢٠٠٠.
[2] د/ هشام رستم ، مرجع سابق الإشارة إليه.
[3] د/ محمد البشري، مرجع سابق الإشارة إليه.
[4] د/ فتوح الشاذلي ود/عفيفي كامل، مرجع سابق الإشارة إليه.
[5] أنظر في هذا الشأن على سبيل المثال: United States V.Morris,928 F.2d 504,505 (2nd cir.1991)

وعلى ذلك، يجب اعتبار نظام المعالجة الإلكترونية مؤهلاً لإثبات تحويل حق مما يجعل مهمة النيابة العامة سهلة فى ضبط الدليل الإلكتروني. ويشترط من جهة أخرى، إمكانية مناقشة الأدلة المعلوماتية المستخرجة من الحاسبات والإنترنت وهو ما يعنى مبدأ وجوب مناقشة الدليل الجنائى بوجه عام، إذ أن القاضى لا يمكن أن يبنى اقتناعه أو عقيدته إلا على العناصر الإثباتية التى طرحت فى أثناء جلسات المحاكمة، وخضعت لحرية مناقشة طرفى الدعوى، فكافة الأدلة المتحصلة من جرائم الإنترنت والحاسب يجب أن تكون محلاً للنقاش – أى كان شكلها – ويتعين على المحكمة أن تأخذ بها كأدلة إثبات إذا كانت مفيدة فى إظهار الحقيقة، فيجب مناقشة هذه الأدلة أمام القاضى فى المحكمة فلا يجب عرض الدليل من خلال ملف الدعوى فى التحقيق الإبتدائي، فيجب أن تناقش مباشرة أمام القضاء وكذا الشهود فى تلك الجرائم حتى ولو كانت قد سُمعت أقوالهم فى التحقيقات، فيجب إدلائها مباشرة أمام المحكمة من جديد وكذا يجب إستدعاء الخبراء فى تلك الجرائم – على اختلاف اختصاصهم – لمناقشتهم وبحث وتمحيص تقاريرهم الفنية التى خلصوا إليها لكشف الحقيقة وإظهار الحق.[1]

ومن الجدير بالذكر فى هذا الصدد، بأن المشرع المصرى قد أكد على أهمية تفادى المشاكل التقنية والفنية التى قد تُثار فى مجال التوقيع والإثبات الإلكتروني. فقد قرر فى ضوء أحكام قانون التوقيع الإلكتروني عام ٢٠٠٤، إنه لذلك التوقيع فى نطاق كافة المعاملات المدنية والتجارية والادارية والجنائية نفس أو ذات الحجية المقررة للتوقيعات فى أحكام قانون الإثبات فى المواد المدنية والتجارية إذا روعى فى إنشائه وإتمامه النصوص المقررة فى هذا القانون وكذا الضوابط العلمية والفنية التى حددتها اللائحة التنفيذية لهذا القانون (مادة ١٤).[2] كما أكد القانون السالف الذكر، على أن للكتابة الإلكترونية والمحررات المعلوماتية فى كافة المعاملات بما فيها المسائل الجنائية ذات

---

[1] انظر مثلاً: 18 U.S.C.A.Ss1030(a) (4) (west sup.1999)

[2] Robyn E. Bumner, Government Want to Bore Web Pee- phole, St. Petersburg Times, March 12,2000,at 4D.

الحجية المقررة للكتابة والمحررات الرسمية والعرفية – متى استوفيت الشروط المقررة – فى قانون الإثبات (مادة ١٥).[١]

وهذا ويمكن القول بأن ذات القانون، قد أجمل شروط تمتع التوقيع والمحرر الإلكتروني وكذا الكتابة الإلكترونية وحجتها فى الإثبات فى كون ذلك التوقيع مرتبطاً بالموقع وحده دون غيره؛ وكذا سيطرته وحده دون غيره على الوسيط الإلكتروني فضلاً عن إمكانية كشف أي تعديل أو تبديل فى بيانات المحرر أو التوقيع الإلكتروني (مادة ١٨).[٢]

هذا وقد بينت اللائحة التنفيذية لذلك القانون بعض الضوابط الفنية لإعتماد الدليل الإلكتروني ذات الحجية فى الإثبات، منها مثلاً أن يكون هذا التوقيع مرتبط بشهادة تصديق إلكترونى معتمدة وسارية المفعول صادرة عن جهة تصديق إلكترونى معتمدة أو مرخصة، وكذا سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني عبر حيازة الموقع لإدارة حفظ المفتاح الشفوى الخاص، متضمن البطاقة الذكية الآمنة وكودها السرى المقترن بها (مواد ٩ و ١٠ من اللائحة التنفيذية). هذا ويلاحظ إنه فى حالة فقد الموقع سيطرته على الوسيط الإلكتروني وأصبحت بيانات إنشاء التوقيع غير سرية (مكشوفة) يعلمها الأخرين، فإن هذا التوقيع لا يكون له قيمة أو حجة في الإثبات الجنائى، حيث أن تحديد الموقع وذاتيته أصبح مشكوك فيه.[٣]

وبناءاً على ما تقدم، وفى ضوء اللائحة التنفيذية لقانون التوقيع الإلكتروني المصرى يتضح أن المحرر وكذا التوقيع الإلكتروني يتمتعان بحجية وقيمة فى مجال الإثبات الجنائى بشرط توافر إمكانية كشف أي تعديل أو تبديل فى بيانات المحرر والتوقيع المعلوماتى، إما عن طريق مضاهاة شهادة التصديق الإلكتروني وكذا بيانات إنشاء التوقيع الإلكتروني بأصل هذه الشهادة وتلك البيانات أو باستخدام تقنية شفرة المفتاح العام والمفتاح الخاص وبأية وسيلة أخرى مشابهة (مادة ١١).[٤]

---

[١] راجع المادة (١٥) من قانون الإثبات في المواد المدنية والتجارية المصري.
[٢] راجع المادة (١٨) من قانون الإثبات في المواد المدنية والتجارية المصري.
[٣] راجع المواد (٩) و(١٠) من اللائحة التنفيذية لقانون الإثبات في المواد المدنية والتجارية المصري.
[٤] راجع المادة (١١) من قانون الإثبات في المواد المدنية والتجارية المصري.

وتجدر الإشارة إلى أن أسهل وأقرب طريق إلى هاتين الوسيلتين سالفتى الذكر، هو استخدام نظام الارشيف الإلكتروني "Electronic Archive"، حيث إنه نظام تتولاه جهة أو هيئة متخصصة تسمح بحفظ البيانات الإلكترونية طوال مدة محددة، بما يضمن صحتها ويحافظ على سلامتها وأمنها، حتى يمكن الرجوع إليها إن لزم الأمر.[1] وبناء على ذلك ، فإن هذا النموذج أو النظام يُعد ويعتبر من الوسائل التى تساهم فى كشف أي تعديل أو تبديل (أو تلاعب) فى كل من بيانات المحرر الإلكتروني أو حتى التوقيع الإلكتروني ذاته.[2] فإذا تحققت الشروط القانونية وكذا الفنية سابقة الذكر، يمكن القول بأن الدليل الإلكتروني فى هذه الحالة يتمتع بالحجية والقيمة القانونية المعقولة والمقبولة فى الإثبات فى المواد الجنائية.

وبناءاً على ما تقدم، يمكن القول بأن قواعد الإثبات تمثل أهمية خاصة للقاضى الجنائى، إذ أن الحق موضوع التقاضى يتجرد من كل قيمة إذا لم يقم الدليل على الواقعة التى يستند إليها، فالدليل هو عصب الواقعة، أو هو النتيجة التى تحققت (إنتاج الدليل) باستخدام وسائل الإثبات المختلفة.

صفوة القول هو إن التطور العلمى والفنى والتقنى فى وسائل الاتصال وتكنولوجيا المعلومات أدى دون أدنى شك إلى تغيير جذرى كبير وخاصة فى المفاهيم السائدة حول الدليل الجنائى، وذلك يقود للقول بإمكانية انضمام الخبرة التقنية إلى علم الخبرة المتميزة بتصنيف التعامل فى موضوع الدعوى الجنائية، وكذا من حيث ضرورة الاستفادة بالمختصين والإستعانة بهم فى مجال المنزاعات وخاصة ذى الطبيعة الجنائية الحساسة.

---

[1] Carlos Albert O Rohrmann, Legal Aspects of Electronic Criminal Evidence in Brazil, 20 International Rev.of Law,Computers, & Technology Journal 182 (2007), at 77-93.

[2] د/ فتوح الشاذلي ود/عفيفي كامل، مرجع سابق الإشارة إليه. وأنظر أيضا:

- Francis Lim,Is Electronic Evidence Admissible in Criminal Case? Inquirer.Net, March13, 2018.
-

الباب الثانى

القيمة القانونية وحجية الدليل الإلكتروني فى الإثبات الجنائى

تمهيد وتقسيم

بما إن الإثبات الجنائى هو مجموعة القواعد القانونية المتعلقة بالبحث عن الأدلة ووصفها وإقامتها أمام القضاء وخاصة المحاكم الجنائية المختصة وكذا تقديرها من جانب القاضى الجنائى. فيمكن القول بأن الإثبات هو مجموع الاسباب المنتجة أو الكاشفة للحقيقة الواقعية أو اليقين، وعليه فالإثبات الجنائى ما هو إلا كافة الأدلة التى تؤكد وقوع الجرم، وكذا تحقيق يقيين القاضى ، سواء قرر إدانته أو براءته – فى حالة شكه وعدم تأكده – إذ يجب ثبوت ارتكاب الواقعة الجنائية فى ذاتها وإن المتهم هو الذى ارتكابها (وقوع الجرم بوجه عام و نسبته للمتهم بوجه خاص).

فى ضوء ذلك، لابد من بيان دور الدليل الإلكتروني كوسيلة إثبات فى مسائل الإجراءات الجنائية وكذا حجيته والفروض العملية أي المشاكل المثارة فى صحته. وعليه نقسم هذا الباب إلى الفصلين التاليين:

الفصل الأول: الحجية القانونية ودور الدليل الإلكتروني فى الإثبات الجنائى

الفصل الثانى: الفروض العملية والمشاكل المثارة فى صحة الدليل الإلكتروني

الفصل الأول

الحجية القانونية ودور الدليل الإلكتروني فى الإثبات الجنائى

تمهيد وتقسيم

تمثل قواعد الإثبات أهمية بالغة، وحتى يتحقق الدليل الإلكتروني اللازم للإثبات، فإنه يلزم من جمع عناصر التحقيق والدعوى – وكذا تقديم هذه العناصر إلى سلطة التحقيق الإبتدائي، فإذا انبثق عن هذا التحقيق أدلة ترجح معها إدانة المتهم، وجب تقديمها للمحكمة

، إذ أن مرحلة المحاكمة هى أهم مراحل الدعوى الجنائية، فهى مرحلة القطع والجزم بتوافر أدلة يقتنع بها القاضى فى إدانة المتهم وإلا وجب عليه الحكم ببراءته.

هذا ويلاحظ أن كل من الشهادة والضبط والتفتيش والمعاينة أحد وسائل جمع الأدلة، حيث أن لكل منها قواعده الخاصة التى تحكمه والتى يتم اتباعها وفقاً للقانون. كما أن خصوصية الجرائم الإلكترونية تعكس هذه الطبيعة الخاصة على الإجراءات الجنائية المطبقة عليها ومنها مثلاً إجراءات ملاحقة الجناة وتتبعهم. فى ضوء ذلك، ينقسم هذا الفصل إلى ثلاثة مباحث على النحو التإلى:

المبحث الأول: الدليل الإلكتروني فى إطار الإجراءات الجنائية

المبحث الثانى: سلطة القاضى الجنائى فى استخلاص الدليل المعلوماتى

المبحث الثالث: حجية (قيمة) وشروط الدليل الإلكتروني الناشئ عن التفتيش الجنائى

المبحث الأول

الدليل الإلكتروني فى إطار الإجراءات الجنائية

طبقاً للقواعد العامة فى الإجراءات الجنائية، يكون الدليل – أي كان نوعه – باطلاً إذا كان متحصلاً بطريق غير مشروع (أي بالمخالفة للقانون)، ولهذا الأمرأهميته البالغة لما يترتب على بطلان الدليل من آثار إجرائية، فلا يصح الإستناد على دليل باطل حتى ولو كان الدليل الوحيد فى الدعوى فى إدانة الجانى، إذ يعتبر الدليل فى هذه الحالة باطلاً بطلاناً مطلقاً والبطلان هنا متعلق بالنظام العام، فلا يجوز التمسك بما ورد فى محاضر جمع الاستدلالات أو حتى محاضر التحقيق كما لا يجوز للمحكمة الأخذ بهذا الدليل والإعتماد عليه فى حكمها بل عليها انكاره. والواقع أن هناك دوراً كبيراً وهاماً تلعبه وسائل الإتصال المعلوماتية فى مجال ارتكاب واكتشاف الجرائم الإلكترونية.

أولاً: فى مرحلة التتبع والملاحقة الجنائية

يلاحظ فى هذه المرحلة أن الشبكة المعلوماتية (الإنترنت) قد تكون هدفاً للجرم ذاته – كما فى حالات الدخول المحظور لأنظمة البيانات فى مواقع معلوماتية معينة لتدمير تلك البيانات أو إتلاف المعطيات الخاصة بها (مخزنة كانت أو منقولة عبر النظم الآلية) أو

حتى فى حالة إخفاء الجانى نشاطه بإعادة إنتاج ذات البيانات عبر نفس الشبكة.[1] وقد تكون الشبكة ذاتها هى سلاح أو أداة الجريمة ذاتها لارتكاب جرائم معلوماتية من خلالها، كما فى حالة استخدام التقنيات الحديثة فى عمليات التزييف والتزوير أو فى الإستيلاء على الأموال عبر تحويلات مالية غير مشروعة (وهمية) .[2] وفى هذا المجال يمكن القول بأن أنشطة غسل الأموال هى المجال الرئيسى والمنتشر فى هذا الإطار الإجرامى التى غالباً ما تتم عبر الإنترنت وما يرتبط بها من عمليات جمة متشابكة ومعقدة تأخذ فى مظهرها شكل التجارة الإلكترونية (e-commerce) والتعاقد من الباطن الذى يكون ورائه إخفاء المصادر الحقيقية غير المشروعة للأموال القذرة.[3]

وفضلاً عن ذلك، قد تكون الشبكة المعلوماتية (الإنترنت) هى بيئة نمو الجريمة، ومثال ذلك إبرام اتفاقات لترويج إلانشطة إلاباحية وكذا الأعمال الإرهابية وغيرها، ولكن قد يكون لهذه الشبكة دوراً فعالاً فى كشف تلك الجريمة وتتبعها لمحاولة الوصول لمرتكبيها وذلك أن أجهزة إنقاذ القانون – فى إطر التعاون الدولى – بدأت تعتمد على النظم التقنية فى إدارة المهمات من خلال بناء قواعد بيانية خاصة بكشف تلك الجرائم مع تزايد حجم ارتكابها واستخدام مرتكبيها للوسائل فائقة التقنية، فيتضح دور هذه الشبكة الهام فى كشف فاعلى تلك الأفعال والقدرة على إبطال آثارها.[4]

هذا ولا يجب الخلط بين دور الوسيلة الإلكترونية فى الجرم (كوسيلة إعتداء أو بهدف الإعتداء) أو تكون بيئة للسلوك الإجرامى وبين محل الجرم (المعلومات والأجهزة وكذا الأشخاص). ولعل أهم عناصر تلك الجريمة هو مكان وقوعها (أي مسرحها)، فهذا

---

[1] انظر د/ رميس بهنام، مرجع سابق الإشارة إليه.

[2] انظر د/ جميل عبد الباقي، مرجع سابق الإشارة إليه.

[3] انظر في هذا الشأن تفصيلاً:
- د/ رمزي عوض، مرجع سابق الإشارة إليه، ص٨٠-٨٣.
- د/رامي القاضي، مرجع سابق الإشارة إليه، ص٥٨-٦٠.

[4] انظر في هذا الشأن:
- د/ محمد ذكي أبو عامر،الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية،٢٠١٦ .
- د/ أحمد فتحى سرور، مرجع سابق الإشارة إليه.
-

العنصر يمثل أهم مفاتيح ضبط وتحرى الجريمة وملاحقة فاعليها.[1] فإذا كان مسرح تلك الجريمة هو الشبكة المعلوماتية التى هى تختلف عن مسرح الجريمة التقليدية، فإن ترك الجانى لآثاره وبصماته المعنوية الآلية فى الموقع الذى يزوره أو يتصفحه، هو علامة بارزة فى تحديد عنوانه الإلكتروني (الذى قد يكون دائماً) وكذا تحديد نوع الجهاز المستخدم والمكان الذى يتم التصفح أو التجول منه.[2]

وعملية التتبع هذه، هى عملية قد تتم فى بعض الأحيان بوسائل بسيطة يمكن للمستخدمين العاديين كشف معلومات المستخدم إذن – الهدف هو تتبع حركات الجانى وغالباً ما يقوم بذلك هم المختصون الفنيون لتوافر المهارة العالية لديهم.[3]

ولكن هذا معقداً وليس بهذه السهولة، إذ تكون عملية الملاحقة والتتبع بسيطة وناجحة بالنسبة للمجرمين المبتدئيين، أما المحترفين (المتخصصين) فيقوموا فى الغالب بمحو آثارهم كمسح الملفات والعناوين والمواقع الإلكترونية باجهزتهم بطرق شتى، مما يجعل تلك العملية غاية فى الصعوبة كما أن طبيعة المجرم المعلوماتى حيث تميزه بالذكاء الشديد والخبرة العالية تزيد من تعقيد تلك العملية.

ويلاحظ أن ضبط الجرم وإثباته يعتمد أساساً على جمع الأدلة التى حدد المشرع الإجرائي وسائل وطرق إثباتها حصراً وذلك لحماية حقوق الأفراد العامة وحرياتهم الأساسية، ومن ثم يصعب فى كثير من الأحيان – على السلطات المعنية– ملاحقة الجانى وتتبع أنشطته الجرمية، إذ أحياناً يدخل الجانى على الحاسوب والشبكة المعلوماتية باسم غير حقيقى أى مستعار، فيكون إثبات هذا الفعل فى غاية الصعوبة.[4]

---

[1] D.Glenn Baker,Trespassers Will be Prosecuted: Computer Crime in the 1990's,12 Computer Law Journal 1 (1993),at 68.

[2] انظر على سبيل المثال: Computer Fraud and Abuse Act,(1986),at Ss1030 &Atomic energy Act of 1954& Senate Judiciary Committee Report No.99-432 , at p.6-7 (1986).

[3] انظر د/ على حسن الطوالبة، التفتيش الجنائي على نظام الحاسوب والإنترنت: دراسة مقارنة، طبعة أولى،عالم الكتب الحديث، اربد،٢٠٠٤.

[4] راجع على حموده، مرجع سابق الإشارة إليه.

وفى هذا الصدد، من المعروف أن لمأمور الضبط القضائى ذو الإختصاص العام بحسب القانون، الحق فى استقصاء وتحرى تلك الجرائم وجمع تحريات عنها فى إطار ذلك الإختصاص ودون تخطيه، فهم المختصون بتحرى تلك الجرائم الواقعة فى المحيط الإلكتروني ما لم ينص القانون على غير ذلك، ولهم فى ذلك الإستعانة بالخبرة فى المجال الإلكتروني.[1] فى ضوء ذلك، يمكن القول بأن الدليل الإلكتروني كوسيلة إثبات فى هذه الجرائم دور فى مرحلة التتبع والملاحقة.

فمن المعروف أن النظام المعلوماتى يتولى المعالجة الآلية للبيانات والمعلومات والمعطيات، فهو يسمح بتنظيم عدد كبير من المعلومات التى يمكن من خلالها ملاحقة أحد الجناة طوال حياته اجتماعياً ومكانياً ومهنياً وذلك ما يتم عن طريق الرقم القومى المستخدم فى تحديد هوية الأشخاص.[2] فبعد التقدم العلمى والتكنولوجى، أصبح من السهل تحديد مكان الشخص المرتكب الجرم، حيث أن النظام الإلكتروني غالباً ما يحتفظ بآثار العمليات التى تتم بواسطته، فتسمح المعالجة الإلكترونية للمعلومات باتساع مجال البحث والتحرى وملاحقة الجناة عبر تحديد هويتهم إما عن طريق ميكنة بصمة الاصابع، فالكشف عن البصمات من الوسائل الهامة فى معرفة أشخاص الجناة، ويتم ذلك هنا، عن طريق التسجيل والمقارنة (تسجيل البصمات المأخوذة المرفوعة فى قسم الشرطة) أو حتى من مسرح الجرم ومضاهتها بالبصمات المخزنة إلكترونياً وخصائص البصمات موضوع الدعوى (التحقيق) ويتم التأكد من ذلك فنياً لاحقاً.[3]

هذا ويمكن أن تتم الملاحقة والتتبع عن طريق إنشاء ملفات أبجدية للمجرمين، فيلعب الدليل الإلكتروني هنا دوراً كبيراً، إذ يمكن استخدام النظام المعلوماتي فى تخزين ملفات الكترونية تحتوى على أوصاف الأشخاص الذى يجرى البحث عنهم إما بمعرفة سلطة

---

[1] انظر بوجه عام:المستشار ادوارد غالي الذهبي،الإجراءات الجنائية في التشريع المصري والمقارن، مكتبة غريب، القاهرة،(طبعة منقحة ومزيدة) طبعة خمسة،٢٠١٠.

[2] انظر :د/ ثروت عبد الحميد، التوقيع الإلكتروني: ماهيته، مخاطره، وكيفيه مواجهته، مدى حجيته في الإثبات، الجلاء الجديدة، المنصورة،٢٠٠١.

[3] انظر بوجه عام:د/ طارق سرور، ذاتية جرائم الإعلان الإلكتروني: دراسة مقارنة ، دار النهضة العربية، الطبعة الأولى، القاهرة،٢٠٠١.

التحقيق أو الاستدلال أو حتى المحاكمة. فيكون لهذه الملفات دور فى تسهيل مهمة مأمورى الضبط القضائى فى سرعة الوصول للجانى الجارى البحث عنه خاصة بالنسبة للمجرمين الخطريين فضلاً عن قيام رجال البحث الجنائى (المباحث أو الشرطة) بعرض نماذج مختلفة عبر تقنية وجه الروبوت (Robot Face) على الشهود أو المجنى عليه كى تساعدهم فى التعرف على المجرم من خلال الإنتقال من مقطع إلى مقطع فى ملامح وجه الشخص، فقد تصل فى النهاية إلى تطابق تلك المقاطع مع صورة الجانى.[1] ويجب أن تتضمن البطاقات (الملفات) معلومات عن هوية الجناة وأوصافهم والمهنة والعنوان وغيرها إذ أن ذلك يساعد فى سهولة كشفهم.

ثانياً: شهادة الشهود

تثير الشهادة – فى مجال الإجراءات الجنائية – عدة إشكاليات فى مجال الدعوى الجنائية للجريمة الإلكترونية وخاصة فيما يتعلق بنطاق إنشاء المعلومات أو التى يجوز للشاهد البوح بها. فالأصل طبقاً للقواعد العامة أن الشاهد يُدلى بما يشهده بذاته أو حكم به، أما فى الدعاوى الجنائية المتعلقة بالجرم المعلوماتى، فإن الأمرمختلف، فهناك بعض الأمور والأعمال المتصلة بالشاهد ذاته أو معلومات تكون متصلة بنظام الكترونى وليست – متصلة بشخص طبيعى – فلا يجوز له البوح بها فى إطار الإلتزام بالخصوصية والسرية.[2]

فالتنظيم القانونى لقواعد الإثبات المتعلقة بالأدلة المعلوماتية يجب أن يُعاد تنظيمه حتى لا يتم وضع الشاهد موضع المساءلة القانونية ولا يفوت الفرصة على القاضى من الإستفادة من شهادته كى يصل لحقيقة الجرم. فقد ذهب جانب من الفقه للقول بأن الشهادة

---

[1] انظر على سبيل المثال:
- Electronic Communications Privacy Act, Communication Assistance for Law &Cyber Security Enhancment Act. Enforcement Act,

[2] انظر أيضاً في هذا الشأن: د/ هلالي عبد اللاه أحمد، التزام الشاهد بالاعلام في الجرائم المعلوماتية، مرجع سابق الإشارة إليه.
National Stolen Property Act,Economic Espionage Act of 1996, and 17 U.S.C.A.Ss506 - (a) (1).The Fraudlent Online Identity Sancations Act.

فى الجريمة المعلوماتية لا تختلف عن مفهومها وإجراءاتها فى الجريمة التقليدية، إذ أن أمر سماعهم (الشهود) متروك للسلطة التقديرية لجهات التحقيق وكذا المحكمة.[1]

والأصل أنه يجوز للخصوم سماع من يرون من شهود وللمحقق استدعاء من يرى فى شهادته إفادة فى التحقيق وله أن يسمع شهادة أى شاهد تقدم من تلقاء نفسه.[2] والشاهد المعلوماتى هو الشخص التقنى الفنى صاحب الخبرة والمهارة العالية فى مجال تكنولوجيا المعلومات والعلوم الإلكترونية حيث يتوافر لديه معلومات محورية وجوهرية لازمة للدخول فى نظام المعالجة الآلية للمعلومات إذا اقتضت مصلحة التحقيق ذلك بمعنى الدخول والتنقيب والبحث بداخل أنظمة الحاسوب وشبكته المعلوماتية.[3]

وهم على أنواع، فمنهم المحللون الذين يقومون بتحليل الخطوات وتجميع البيانات الخاصة بنظم معينة إلى وحدات منفصلة واستنتاج علاقة بعضها البعض فضلاً عن تتبع البيانات داخل الأنظمة ومنهم مديرو النظم الموكول لهم أعمال الإدارة فى النظم الإلكترونية وكذا مهندسوا الصيانة، المسئولون عن أعمال صيانة تقنيات الحاسب وشبكات الإتصال المتعلقة به وكذلك منهم مشغلوا الحاسبات المهتمون بتشغيل الحاسب ومعداته وهم الخبراء المتسمين بالدراية الكاملة بنظم التشغيل وقواعد كتابة البرامج وأخيراً منهم المبرمجون كمخططوا برامج التطبيقات للحصول على خصائص الأنظمة وكذلك مخططوا برامج النظم المختصون بتعديل وتصحيح البرامج.[4]

ثالثاً: الإنتقال للمعاينة والخبرة

ذهب بعض الفقه الجنائى للقول بأن الإنتقال للمعاينة ليس بالأهمية القصوى فى مجال الجريمة المعلوماتية وخاصة فيما يتعلق بإثباتها، إذ من النادر أن يترك الجانى آثار مادية

---

[1] د/ محمد السيد عرفه، التجارة الإلكترونية عبر الإنترنت: مفهومها، القاعدة القانونية التى تحكمها، ومدى حجية المخرجات في الإثبات، دراسة مقدمة إلى المؤتمرالمنعقد بكلية الشريعة والقانون بجامعة الإمارات العربية المتحدة (في موضوع القانون والكمبيوتر والإنترنت) من ١-٣ مايو ٢٠٠٠.

[2] د/ غنام محمد غنام،عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، دراسة مقدمة لذات المؤتمر السالف ذكره أعلاه (هامش١).

[3] د/ محمد سامى الشوا، ثورة المعلومات وانعكاستها على قانون العقوبات، دار النهضة العربية، القاهرة- ١٩٩٤.

[4] انظر تفصيلاً في هذا الصدد بوجه عام: د/ مدحت عبد الحليم رمضان، جرائم الإعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة(٢٠٠٠)؛ وكذلك لذات المؤلف الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية،(٢٠٠١).

عند ارتكابها فضلاً عن طول الفترة بين وقوع الجرم (ارتكابها) وكشفها، فقد تزول الآثار الناجمة عنها بالمحو أو العبث أو التدمير (التلف).[1]

وعلى آية حال، أنه فى حالة تلقى بلاغ عن وقوع جريمة معلوماتية، يتم الإنتقال لمسرحها لمعيانته، فهذه الجريمة غالباً ما تكون مستمرة كما هو الحال فى بعض جرائم الإعتداء على الأموال (كالسرقة والإحتيال) والجرائم الإقتصادية الأخرى وقد يكون مسرحها كالجرائم الأخرى كالتزوير، ففى الحالة الأولى يكون غرض المعاينة، المداهمة والتحفظ على الأدلة، أما فى الحالة الثانية- بعد وقوع الجرم – فيتوقف الأمرعلى اعتراف الجناة إذا كان قد تم القبض عليهم وكذا القرائن والشهود.[2]

هذا وينبغى عند إجراء المعاينة مراعاة بعض الضوابط منها مثلاً إخطار وإعادة الفريق الذى سيقوم بإجرائها فنياً وعلمياً لوضع استراتيجية مناسبة لضبط الأدلة بوقت كافٍ، وكذا تطوير الكمبيوتر وما يتصل به من أجهزة أخرى وإعداد خطة المعاينة ومراجعتها لاتمامها بشكل جيد، ملاحظة وإثبات حالة التوصيلات (الكابلات) لإجراء المقارنة عند عرض الأمرعلى القاضى؛ إجراء اختبارات قبل نقل أي مادة إلكترونية من محل الجرم للتأكد من عدم محو أى بيانات أو معلومات مخزنة وكذا التحفظ على جميع المعلومات والمستندات وقواعد الإدخال والمخرجات وغيرها، فضلاً عن قيام المختصين فى هذا المجال بإجرائها وفق مبدأ المشروعية وفي إطار ما تنص عليه التشريعات الجنائية .[3] هذا وقد عالج المشرع المصري إجراءات الإنتقال للمعاينة فى قانون الإجراءات الجنائية المصرى بالنسبة للجرائم العادية أو تصوير ما حدث وجمع الآثار والأدلة المادية وغير ذلك وهوالأمرغير الموجود كثيراً في الجرائم المعلوماتية.[4]

---

[1] Orin S.Kerr, ExAnte Regulation of Computer Search and Seizure, 96 Va. L. Rev. 1241(2010).

[2] د/طارق سرور، مرجع سابق الإشارة إليه.

[3] د/على عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، دراسات مقدمة لذات المؤتمر المشار إليه سلفاً(هامش ١).

[4] المرجع السابق .

أما الخبرة فلها دوراً كبير فى العصر الحالى فى عملية الإثبات القضائى نظراً لما يشهده العالم من تطور علمى وتكنولوجى وما يمكن وصفه بعصر المعلومات. والخبرة هى إجراء يرتبط بإجراء موضوع يحتاج الإلمام والدراية بمعلومات فنية لإمكان استخلاص الدليل منه، فهى غالباً ما تكون استشارة فنية يستفيد بها المحقق والقاضى لمساعدته فى تقدير إثبات المسائل الفنية التى لا تتوافر لدى عضو السلطة القضائية نظراً لاحتياج تقديرها لمساعدة فنية أو إدارية.[1]

والخبير هو كل شخص له دراية خاصة بمسألة من المسائل قد يحتاج فحصها لكفاءة علمية وخبرة فنية معينة قد لا تتوافر – أو فى الغالب هى غير متوافرة – لدى المحقق، كالطبيب الشرعى الذى يُستدعى لمضاهاة الخطوط المدعى تزويرها وكذا كتابة تقرير الصفة التشريحية فى جرائم القتل مثلاً.[2]

وطبقاً للقانون، يجوز الإستعانة بخبير أو أكثر إذا توقف تمييز الجرم فى طبيعته وظروفه على معرفة بعض المهام التى يقوم بها المختصون كل حسب وظيفته. هذا وقد نظم المشرع المصرى هذه الوسيلة فى إطار الجريمة العادية متجاهلاً أهميتها فى إثبات الجريمة المعلوماتية، فهى وسيلة أساسية من وسائل الوصول للدليل الإلكتروني الهادفة لكشف بعض الدلائل، وتحديد معناها عبر الإستعانة بالمعلومات العلمية.[3]

هذا وقد تظهر أهمية الإستعانة بخبير فى الجرائم المعلوماتية عند عجز الشرطة عن كشف الغموض حول الجرم أو عجز أجهزة التحقيق والاستدلال عن جمع الأدلة حول الواقعة أو توفير الأدلة أو محواها نتيجة لنقص الكفاءة الفنية أو الإهمال أو الجهل عند التعامل مع الأدلة.[4] ويمكن القول بأنه نتيجة للتطور العلمى، قد ظهرت أنشطة جديدة تتم عن طريق النظم الآلية، كالأعمال المالية أو المصرفية الإلكترونية، التجارة الإلكترونية والحقوق الإلكترونية

---

[1] انظر بوجه عام، د/هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن – دار النهضة العربية، القاهرة، ١٩٩٢.

[2] انظر تفصيلاً في هذا الصدد: د/هشام فريد رستم، الحماية الجنائية لسرية السوابق القضائية، مكتبة الالات الحديثة،أسيوط ،١٩٩٥.

[3] An Act concerning the Connection Uniform Electronic Transactions Act, Bill No.561,Feb,session,2002.

[4] انظر د/ محمد السعيد رشدي، حجية وسائل الإتصال الحديثة في الإثبات، دار النهضة العربية-القاهرة-١٩٩٩، ص٥٠-٨٥.

الإلكترونية وغيرها وهذه الأعمال قد تتعرض لبعض الجرائم، كالتزوير والتلاعب فى البيانات والمستندات المدخلة على الأنظمة الآلية وغيرها، مما أدى إلى ظهور صعوبات يواجهها الخبير الجنائى فى سبيل جمع هذه الأدلة من الحاسبات، فمنها على سبيل المثال، تهيئة المتهم جهاز الحاسب للتدمير أو التفجير بمجرد تشغيله، أو إخفاء هويته عمداً عبر قيامه بالإجراءات التى تؤدى لطمس شخصيته، أو إخفاء المعلومات بخلق أنظمة معينة يستحيل معها إرجاع هذه المعلومات وكذا فى حالة توزيع مسرح الجرم بين أكثر من دولة نتيجة تحقيق الإجراءات للحصول على دليل رقمى وغير ذلك من المعوقات التى غالباً ما تعوق عمل الخبير وتؤدى إلى عرقلته فى الوصول لحقيقة الجرم.[1]

لذلك تظهر أهمية الخبرة كوسيلة إثبات فى مجال الجرائم المعلوماتية فى كون الخبير ملماً بتركيب الحاسبات وصناعته ونظم تشغيله (إلخ....) وكذا قدرته – الخبير – على إتقان وظيفته دون تدمير الأدلة فضلاً عن تمكنه من نقل أدلة الإثبات غير المرئية لأدلة مقروئة، والمحافظة على دعامتها الإسطوانية دون تلف.[2] وبناء على ذلك، يشترط فى الخبير أن يكون عالماً وعلى دراية بنظم أجهزة الحاسب الآلي وبمكوناته المادية والبرامجية وكذا برامج فحصه واسترجاع البيانات وإصلاح التالف منها وفك الشفرات.[3] وكذلك يشترط أن يكون قادراً على تفسير الملاحظات والربط بين الإشياء واستخلاص دلالات علمية وفنية وكذا الربط بين الدليل المادى والرقمى فى الواقعة محل البحث.[4]

رابعاً: إجراءات الضبط والتفتيش

بادئ ذى بدء، يمكن القول بأن الضبط والتفتيش هو الغور والبحث فى مستودع ومكنون أسرار المتهم فهو إجراء من إجراءات التحقيق الذى يتطلب إذن أو أمر قضائى مسبب لإمكانية

---

[1] وفي الشأن المدني،انظر بوجه عام: د/ حسن عبد الباسط جميعي،إثبات التصرفات القانونية التى يتم إبرامها عن طريق الإنترنت – دار النهضة العربية-القاهرة-٢٠٠٠، ص٦٣.

[2] د/ محمد رشدي، المرجع السابق الإشارة إليه، ص٨٦.

[3] د/ثروت عبد الحميد، المرجع السابق الإشارة إليه، ص٩٠-١٠٠ ومابعدها.

[4] د/أشرف توفيق شمس الدين، الصحافة والحماية الجنائية للحق في الخصوصية : دراسة مقارنة (ورقة مقدمة للمؤتمر العلمي الثاني لكلية الحقوق جامعة حلوان في موضوع الاعلام والقانون ١٤-١٥ مارس ١٩٩٩).

مباشرته، وعلى النيابة العامة المبادرة بإجراء التفتيش قبل قيام المجرم بإخفاء معالم جريمته وطمسها، فهو يقوم بذلك إذا ما سمحت له الفرصة وكان لديه متسع من الوقت.

ويلاحظ أن التفتيش فى مفهومه القانونى الإجرائي فيما يتعلق بالجرائم المعلوماتية لا يختلف عن معناه السائد فى فقه وقضاء الإجراءات الجنائية، إذ أنه إجراء من إجراءات التحقيق تتولاه سلطة مختصة بهدف الدخول لنظم المعالجة الآلية للمعطيات والبيانات بما تحتويه من مدخلات وتخزين مخرجات بغرض البحث عن سلوكيات غير مشروعة تكون مُرتكبة تشكل جناية أو جنحة والوصول من خلال ذلك لأدلة تفيد فى إثبات الجرم ونسبتها لفاعلها.[1]

فتفتيش مسرح ومحل الجريمة وما يتصل به من أماكن وضبط الأحراز المتعلقة بالجريمة، هى مسائل نظمتها التشريعات الجنائية الإجرائية، فيثور السؤال حول مدى إمكانية انطباق القواعد القائمة الخاصة بالتفتيش على تفتيش الحاسبات ونظم المعلومات، إذ قرر بعض الفقه الأمريكى بأن "الخطأ فى ضبط وتفتيش الدليل قد يؤدى لفوات فرصة كشف المجرم أو حتى فوات فرصة الإدانة على الرغم من معرفة الجانى".[2]

فتفتيش أنظمة الكمبيوتر وما تحتويه من بيانات ومعلومات ومعطيات هو بمثابة تفتيش للفضاء الإفتراضي وكذا أجهزة التخزين هو أمر متعلق بالقدرة على تحديد المطلوب مسبقاً ليس مجرد التدخل والإطلاع على ما بداخل الأجهزة والأنظمة المعلوماتية، إذ أن ذلك قد يرتب عوائق إجرائية يكون أهمها بطلان الإجراءات والآثار المترتبة على التفتيش، إذ أنه قد يكون تم خارج نطاق الإذن المسبب الصادر به (فضلاً عن أمر الضبط) أو نتيجة للإطلاع على خصوصية البيانات المخزنة.[3]

هذا ويلاحظ وجود بعض العوائق الإجرائية التى تعوق خضوع المعطيات المحفوظة إلياً لقواعد التفتيش المتعارف عليها والتى منها مثلاً، تعدد الإماكن التى يوجد بها النظام

---

[1] انظر :على حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، بحث منشور عبر موقع كلية الحقوق بجامعة العلوم التطبيقية، مملكة البحرين (٢٠٠٩).

[2] المرجع السابق.

[3] د/ محمد الشوا، مرجع سابق الإشارة إليه، ص١٦١.

الإلكتروني داخل أو خارج إقليم الدولة، وكذا عدم اكتمال المعرفة والخبرة الإلكترونية بالشئ المراد ضبطه وتفتيشه أو حتى بالتقنية المتطلبة لإتمام عملية التفتيش على الوجه الأكمل.[1]

هذا وقد نظم المشرع المصرى إجراءات التفتيش والضبط تفصيلاً فى تشريع الإجراءات الجنائية الخاصة بالجريمة المادية دون الإلكترونية لكى يمكن إثباتها بالدليل الإلكتروني ولهذا تخضع إجراءات تفتيش النظم المعلوماتية والإنترنت لمجموعة القواعد العامة المنصوص عليها في قوانين الإجراءات فى ظل غياب النصوص الخاصة التى يجب وأن تنظم هذا الأمرعلى حده.[2]

وفى هذا الصدد، يمكن القول أن بعض المواد المراد تفتيشها يكون مادياً كالأجهزة والمعدات أو معنوياً كالبيانات والبرمجيات أو شبكات (ملفات مشفرة)، فيخضع التفتيش فى هذه الحالة لبعض القواعد الشكلية الخاصة بالأشخاص الواجب حضورها إجراء التفتيش وكذا من يقوم بإعداد محضر التفتيش، فيجب أن يقوم بإجراءه أشخاص متخصصة وذلك عبر تحديد النظام المراد تفتيشه بقدر من الدقة حتى يتم تلاشى تلف الكيان المراد تفتيشه.[3]

وطبقاً للقواعد العامة، يجوز لمأمورى الضبط القضائى – بعد الحصول على إذن مسبب من النيابة العامة – الدخول للأماكن التى تشير الدلائل إلى استخدامها فى إرتكاب الجرم كما يجوز تفتيش الأجهزة والأدوات والبرامج والوسائل وغيرها التى ترشد الدلائل فى استعمالها فى ارتكاب الجرم، وعلى مأمورى الضبط تحرير محضر بذلك ورفعه للنيابة العامة.[4]

وعلى ذلك، فالتفتيش فى الجرائم الإلكترونية يكون محله كل مكونات النظام الآلي سواء مادية أو معنوية، وكذا شبكات الإتصال المعلوماتية فضلاً عن الأفراد الذين يستخدمون محل التفتيش بجميع عناصره ومكوناته المادية والمعنوية (كبرامج التطبيقات

---

[1] د/أحمد بلال، مرجع سابق الإشارة إليه، ص٤٨-٤٩.

[2] انظر د/ محمد الأمين،العدالة الجنائية ومنع الجريمة: دراسة مقارنة ، طبعة أولى، اكاديمية نايف العربية للعلوم الأمنية، الرياض ١٩٩٧.

[3] د/غنام محمد، مرجع سابق الإشارة إليه، ص٣٤.

[4] د/ مدحت رمضان، مرجع سابق الإشارة إليه، ص٣١.

والنظم سابقة التجهيزبحسب احتياجات أو طلبات العميل) إذ يتطلب تفتيش هذا النظام مجموعة من الخبراء الفنيين .[1]

هذا ويشترط موضوعياً كي يكون هذا التفتيش منتجاً لآثاره الإجرائية، أن يكون له محل سواء كان متمثل في شخص أو مكان ويشترط أن يكون هذا المحل محدداً أو معيناً بالذات أو قابلاً للتحديد وأن يكون مشروعاً (جائز للتعامل فيه قانوناً)، فلا يجوز مثلاً تفتيش أعضاء البعثات الدبلوماسية ولا منازلهم وكذا محامي المتهم أو الخبير الإستشاري لضبط مستندات إذ إنهم يؤدوا مهامهم الدفاعية طبقاً لمقضيات حق الدفاع المحمي دستورياً.[2] كما يشترط أن يكون هناك جرم واقع بالفعل وهو سبب التفتيش سواء تمثل هذا الجرم في شكل جناية أو جنحة. هذا فيما يتعلق بالشروط الموضوعية للتفتيش.

أما فيما يتعلق بشروطه الشكلية، لا يملك القيام به- طبقاً للقواعد العامة- إلا سلطة التحقيق أو الإتهام (أى النيابة العامة)، فهو يخضع لخصائص التحقيق الإبتدائي كوجوب كتابته أو تدوينه من قبل المختص بذلك وكذا سريته عن الجمهور وحضور الخصوم أو وكلائهم إذ أمكن ذلك كما يشترط أن يكون إذن أوامر التفتيش مسبباً وذلك لضمان وجود سبب قانوني للتفتيش، إذ يجب أن يصدر الإذن وفقاً لما قرره القانون، بمعنى إمكانية تقدير جديته لصدوره من عدمه وهو أمر يقدره المحقق تحت رقابة محكمة الموضوع فضلاً عن حق الدفاع في مراقبة ذلك انطلاقاً من كفالة حق الدفاع "Due Process".[3]

ولكى يمكن أن تنجح عملية التفتيش في الجرائم الإلكترونية يجب تجميع أشخاص أو فريقاً متخصصاً فنياً وتقنياً من مأموري الضبط القضائي للقيام به، وكذا التعرف على النظام المراد تفتيشه ووضع خطته وكذا خطة بديلة في حال فشل الخطة الأساسية، وكذا وضع مسوده الأمرأو الإذن الصادر به محتوياً على وصف المحل المراد تفتيشه بدقة وتفصيل.[4]

---

[1] انظر على سبيل المثال، قانون التوقيع والتسجيلات الإلكترونية لولاية نيويورك الذي يعهد لمكتب تقنيات الولاية بالحق في اختيار وسيلة التوقيع الإلكتروني بالنسبة للأجهزة الحكومية.

[2] انظر د/ لؤي عبد الله نوح، مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي وانظر له أيضاً، حجية مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي:دراسة مقارنة ،مركز الدراسات العربية للنشر والتوزيع- القاهرة -٢٠١٨.

[3] انظر على سبيل المثال المادة (١٠٥) (٦) من قانون التوقيع الإلكتروني الإتحادي الإمريكي لعام ٢٠٠٠.

[4] د/ طارق سرور،مرجع سابق الإشارة إليه، رقم ١ ص٢.

ومن المعروف أن هدف التفتيش هو ضبط الأدلة المادية لكشف الحقيقة الخاصة بالجرم وذلك في حالة ضبط الأدلة المادية لمكونات الكمبيوتر وهذا أمر سهل، أما الصعوبة تنبثق عن ضبط البيانات والبرمجيات، إذ أن الراجح فقهاً هو عدم إمكانية توقيع إجراء الضبط على الكيانات المعنوية إلا بعد تحويلها لكيانات مادية (ورق أو أقراص مدمجة) أو أى وسيلة أخرى تصلح لذات الهدف حتى يتم ضبطها بعد ذلك، إذ أن الكيانات المعنوية هى عبارة عن خلاصة فكر المبرمج الآلي (نتاج فكري) الذي يهدف للحصول على البرنامج أو النظام النهائي.[1]

هذا ويجوز لمأمور الضبط القضائي- في إطار اختصاصهم العام المقرر قانوناً- ضبط الأجهزة والأدوات والوسائل المستخدمة في ارتكاب الجرائم الإلكترونية وكذا الأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكابها مع الأخذ في الإعتبار بمراعاة حقوق الغير حسن النية- إذا تبين عدم إشتراكهم في الجرائم- فيكون للضبط آثاره الجنائية الإجرائية.[2]

هذا وفيما يتعلق بضبط البريد الإلكتروني والمراسلات وخاصة في مجال الجرائم المعلوماتية، فيجوز مراقبة المحادثات الهاتفية وعبر الإنترنت وشبكات الكمبيوتر وتسجيلها ولكن ذلك بعد اتباع الإجراءات المقررة قانوناً المتعلقة بآلية مراقبة المحادثات والتصنت عليها وهى الحصول على إذن (أمر) قضائي مسبب يُجيز ذلك وكذا يمكن تفتيش حساب الإنترنت من خلال أمر التفتيش المسبب الخاص بالمستخدم المشكوك فيه ارتكابه الجرم.[3] وفي جميع الأحوال، مع مراعاة الإجراءات المقررة قانوناً، يجوز ضبط ومصادرة الأجهزة والوسائل والمعلومات المستعملة في وقوع الجرم وكذا تعطيل أو وقف عمل المواقع المعلوماتية التى يرتكب بها أى من الجرائم.[4]

---

[1] د/ على القهوجي، مرجع سابق الإشارة إليه، ص ٦.
[2] د/ طارق سرور،مرجع سابق الإشارة إليه، ص ٣٦ رقم ١٤ و ص٨٥ رقم ٤٩.
[3] د/ مدحت رمضان، مرجع سابق الإشارة إليه، ص٣٠ و٧٢.
[4] انظر في هذا الشأن ما يلي:
- د/ جميل الصغير، مرجع سابق الإشارة إليه،(الإنترنت والقانون الجنائي)، ص٦٣.
- د/ على القهوجي، مرجع سابق الإشارة إليه، ص٤٧-٥٩.

المبحث الثاني

سلطة القاضي الجنائي في استخلاص الدليل المعلوماتي

مما لا شك فيه أن للتطور العلمي الحالي آثارة وانعكاسته على قانون العقوبات وكذا قانون الإجراءات الجنائية، إذ يجب تعديل وتطويع تلك القوانين مع تلك الإنعكاسات وبصفة خاصة في مجال الإثبات الجنائي، إذ إنه قد تأثر بالتطور الضخم الذي لحق مجال الأدلة الجنائية انبثاقاً من تطور أساليب ارتكاب الجريمة، الأمرالذي استوجب معه تغيير وجهة النظر لطرق الإثبات الجنائي كي تصبح الحقيقة العلمية الفنية مقترنة في واقعها من الحقيقة القضائية.

فإثبات الأفعال الإجرامية والخاصة بالجرائم المعلوماتية قد تأثر بطبيعة هذه الجرائم وكذا بوسائل ارتكابها مما قد يؤدي لاحتمال عدم كشفها في بعض الأحيان أو عدم الوصول للمجرمين أو العجز عن إقامة الدليل على إثباتها مما يلحق الضرر بافراد المجتمع. هذا ونتيجة لما يتميز به الدليل الإلكتروني من طابع خاص كوسيلة إثبات في المواد الجنائية، مما أدي لوجود بعض الصعوبات على المحققين في القيام بمهامهم، منها مثلاً التخزين الإلكتروني وسهولة محو الدليل في زمن قصير، فقد نادى البعض من الفقه بعدم الأخذ به كدليل إثبات في المجال الجنائي.[1]

ويتعقد الأمرإذا تم التخزين عن بُعد، فلا تكفي القواعد الإجرائية التقليدية في الإثبات، فمن الصعوبة بمكان إجراء ضبط وتفتيش لمعلومات أو معطيات للحصول على أدلة تفيد في كشف حقيقة الجرم، وخاصة إذا كانت هذه المعطيات في دولة أجنبية، إذ أن هذا الإجراء يتعارض و سيادتها التى لا يجوز المساس بها طبقاً لقواعد القانون الدولي العام.[2]

- Criminal Evidence Act of 1992 •
- "An Electronic Record shall have the same force and effect as those records not produced by electronic means."
- Report to the Governonr & Legislature on New York State's Electronic Signatures and Records Act, p.8 &14.
-

[1] انظر د/ محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص- الطبعة الثانية، دار النهضة العربية، القاهرة ١٩٩٤، ص٢٤٨.

[2] انظر د/ فوزية عبد الستار، قانون العقوبات- القسم الخاص – الطبعة الثانية- دار النهضة العربية، القاهرة، ٢٠٠٠، ص٢٧.

هذا ويلاحظ أن الأدلة القولية تختلف عن الفنية، إذ أن الأولى يسهل فهمها وإدراك مضمونها، أما الأخيرة فينصب مضمونها في الغالب على مسائل لا تكفي لتحقيق قبولها أو الأقناع بها ، فمن الصعب التحصل عليها إلا من خلال عمليات تقنية معقدة، فالوصول إلى فهم مضمونها قد يكون أمر بالغ في التعقيد. فقد يكون من المستعصي على رجال البحث الجنائي كشف الغش والتدليس الواقع على أنظمة المعالجة الآلية، وذلك نتيجة للطبيعة غير المادية للبيانات المخزنة وكذا طبيعتها المعنوية لوسائل نقلها، إذ أن ذلك الأمرقد يتطلب إعادة جميع العمليات الآلية من جديد لكشف التلاعب فضلاً عن سهولة اختراق البرامج والأنظمة المعلوماتية.[1]

في ضوء ذلك، يتعين وضع برامج تدريبية متخصصة لجهات التحقيق الجنائي والضبط القضائي في استيعاب وفهم طبيعة المعطيات الواقعة على الجرائم الإلكترونية وكيفية التعامل مع لغة ونظم الحاسبات بالقدر الكافي لكشف الجرم، وهذا ما أوصى به المجلس الأوروبي في عام ١٩٩٥ من وضرورة استحداث وخلق دوائر جديدة تتولى مواجهة الجرائم المعلوماتية.

صفوة القول هنا، أن الدليل الناتج من الوسائل الإلكترونية يستمد طبيعته من العمليات المعلوماتية التى نتج منها في حالة الإعتداء غير المشروع (كتقليد أو تزوير التوقيع الإلكتروني) فلا يمكن كشفه بالطرق التقليدية المتبعة وإنما يتم معرفه ذلك بالوسائل الإلكترونية. فإن الطبيعة الخاصة لهذا الدليل ستنعكس بالضرورة على الطرق التى من خلالها يتم الوصول إليها، إذ لم تعد الطرق العادية صالحة أو كافية في البحث عن الأدلة المتحصلة من الجرائم أو الوسائل الإلكترونية، إذ يلزم اتباع طرق جديدة تتناسب مع هذه الأدلة لإثبات الأفعال غير المشروعة الخاصة بالجرائم المعلوماتية.

---

[1] راجع تفصيلاً في هذا الشأن:

- د/ عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية: دراسة تحليلية نقدية لنصوص التشريع المصري مقارناً بالتشريع الفرنسي- دار النهضة العربية- القاهرة، الطبعة الثانية ١٩٩٥،رقم ٤٥، ص٧٩.

- د/ محمود نجيب حسني، مرجع سابق الإشارة إليه، ص٢٩٥.

Electronic Signaturees Approvals, Policy Manual University of North Texas.

ففيما يتعلق بالسلطة التقديرية للقاضي الجنائي في استخلاص الدليل الإلكتروني، يجب التسليم بأن مشروعية الحصول على هذا الدليل أمر أساسي لاغنى عنه. ففي المواد الجنائية، يجب أن يتم الحصول على هذا الدليل بطريق مشروع كما يجب أن يكون الأطلاع على البيانات أو المعلومات أو الأدلة المأخوذة من الأنظمة الإلكترونية، من شخص مختص أى أن يكون القانون قد منحه حق الأطلاع كمأموري الضبط القضائي وأعضاء النيابة العامة فضلاً عن القضاة وذلك في إطار تحقيق جنائي، حماية للحقوق والحريات الشخصية.[1] فيجب قصرالإطلاع على هذه المعلومات أو الأدلة على أشخاص معينين ومختصين طبقاً للقانون وهو شرط أساسي لقبول هذه الأدلة المتحصلة بطريقة مباشرة أو غير مباشرة فضلاً عن إخضاع الأطلاع لرقابة وإشراف السلطة القضائية.[2]

وبناء على ذلك، فكل الطرق غير المشروعة للحصول على تلك الأدلة كالإكراه المعنوي أو المادي أو حتى التحريض على إرتكاب الجرائم من قبل رجال البحث الجنائي دون مسوغ قانوني يؤدي في نهاية المطاف لجحد ودحض هذه الأدلة.[3] وعلى ذلك، فهناك طرق مشروعة وقانونية للحصول على تلك الأدلة و كي تكون مقبولة لدى القضاء إما عبر فحص نظام الإتصال بالإنترنت أوفحص مكونات الكمبيوتر المادية والمعنوية (البرامج). وهذه العملية- الحصول- تتسم بالتعقيد لما تحتاجه من خبرة ومهارة كبيرة في مجال الإتصال وتكنولوجيا المعلومات وذلك نظراً لتعدد صور الجريمة المعلوماتية (كتدمير المعلومات غير مهاجمتها أو الإستيلاء عليها أو إختراق كلمات السر ومفاتيح الشفرة وغيره)[4] .

هذا ويمكن تجميع الأدلة الإلكترونية – طبقاً لما يراه بعض المتخصصين- إما عن طريق تجميع المعلومات المخزنة لدى الشخص مُقدم الخدمة وإما عن طريق المراقبة، فقد يعود المجرم لمسرح الجرم و يحوم حول جريمته.[5] ويمكن مراقبة الأجهزة الإلكترونية عبر استخدام برامج وكاميرات مراقبة وغيرها من الوسائل عالية التقنية وهذا ويمكن

---

[1] انظر على سبيل المثال: United States v.Braks,842 F.2d 509,512 (1st cir.1988)

[2] د/ محمود نجيب حسني، مرجع سابق الإشارة إليه، ص٢٤٧.

[3] انظر:الجريدة الرسمية العدد ٢٣ (تابع) في ٩ يونيو سنة ١٩٩٤.

[4] د/ محمد السيد عرفه، مرجع سابق الإشارة إليه، ص٩.

[5] انظر على سبيل المثال في القانون المصري، المادة ٣٦١ من قانون العقوبات.

ضبط الأجهزة الإلكترونية المشتبه فيها وفحصها فحصاً فنياً دقيقاً ومشروعاً- طبقاً للقواعد القانونية المعتبرة – ولكافة ملحقاتها – المادية والمعنوية (البرامج و المعطيات) للحصول على الدليل المادي وتقديمه لجهة التحقيق أو الحكم لتقرير مدى وقوع الجرم من عدمه وعليه إدانه أو براءة الجاني وذلك طبقاً لما هو معروف ومتبع في حقل الخبرة المعلوماتية.[1]

وجدير بالذكر، أن وزارة العدل الأمريكية "US Department of Justice" قد وضعت تصوراً عملياً يحدد خطوات أساسية لجمع الأدلة المعلوماتية وفحصها وتحليلها وكتابة تقرير بها وبنتائجها، ويتميز هذا النموذج بأنه يوضح أنواع الأدلة والمعلومات المستخلصة منها ويربطها بنوع محدد من الجرائم الإلكترونية.

فالتعرف على المعلومات المقيدة (رقم الضمان الإجتماعي "Social Security Number" وأرقام الهوية وغيرها) يفيد في عملية التحري والبحث، فهى بمثابة خطوة إيجابية تساعد في تقديم أدلة قانونية للقضاء عند تقديم المجرمين للمحاكمة الجنائية.[2]

ويثور التساؤل في هذا المجال، حول مدى قبول وتقدير القاضي للدليل المعلوماتي في الإثبات الجنائي، إذ لم يتعرض المشرع لهذه المسألة على الإطلاق ومدى إمكانية تطبيق القواعد العامة المتعارف عليها.

غنى عن البيان، أن الإثبات الجنائي حر وغير مقيد ولكنها قاعدة ليست على إطلاقها، فلا يمكن تصور عدم اخضاع الدليل للنصوص القانونية، إذ أن حرية الإثبات لابد وأن تتسق مع مشروعية الدليل. وطبقاً للقواعد العامة، يجوز إثبات الجريمة ونسبتها لمرتكبها بكافة طرق للإثبات إلا إذا نص القانون على غير ذلك، إذ أن المحكمة تعتمد في اقتناعها على الأدلة المستمدة من التحقيق الذي اجرته في الدعوى أو حتى من التحقيقات السابقة على المحاكمة، فلها كامل الحرية (المطلقة) في ترجيح دليل على آخر وتكوين عقيدتها

---

[1] د/ مدحت رمضان، مرجع سابق الإشارة إليه، ص٤٦.
[2] المرجع السابق، ص٥٥.

طبقاً لما يستقر في وجدانها وضميرها ولكن لا يجوز للقاضي – مطلقاً- أن يحكم بناء على معلومات أو أهواء شخصية.[1]

وجدير بالذكر أن أساس حرية الإثبات تكمن في قبول جميع الأدلة في الإثبات، بمعنى أن هناك حظر أو قيد فيما يتعلق بفرض أدلة معينة وتقييد الإثبات بهذه الأدلة، غير أن هذا الحظر خاص بالقاضي (أى منع له) ولكنه لا يقيد المشرع.[2]

فيجوز للمشرع الخروج على ذلك إذا قرر إثبات بعض السلوكيات الإجرامية بطرق معينة، إذ انه في بعض الأحوال يتوقف تحريك الدعوى الجنائية على تقديم شكوى من المجني عليه كما هو الحال في جرائم السب والقذف مثلاً وهذا ما استقر عليه قضاء محكمة النقض المصرية.[3] فلمحكمة الموضوع مطلق الحرية في الأقناع بالأدلة الموضوعة أمامها إذا كانت تتفق مع العقل والمنطق وكانت كاشفة في إظهار حقيقة الجريمة المرفوعة بشأنها الدعوى الجنائية دون رقابة عليها من محكمة النقض فهى مسألة موضوعية بحتة لا تحتاج معقب عليها.[4]

فحرية الإثبات تعنى قبول كل دليل يُحتمل أن يساهم في إثبات الجرم وكشف من ارتكبها، فيجب طرح جميع الأدلة أمام القاضي الجنائي وليس له أن يستبعد أى دليل مسبق قبل فحصه، ما دام كان هذا الدليل قد يكون له أهمية في إثبات الدعوى.[5] هذا وحظر استبعاد القاضي لما يُعرض أمامه من أدله قد يمس بحقوق الافراد إذ قد يشوب ذلك الاستبعاد عدم النزاهة والحيادية، وإنما يتعين عليه تقدير القيمة القانونية (الحجية القانونية) لهذه الأدلة.[6]

---

[1] د/ جميل الصغير، مرجع سابق ، ص١٥٠.

[2] انظر كل من أ. محمد رفيق البطوطي و أ. محمد أحمد حسن، قانون العقوبات في ضوء أحكام محكمة النقض،طبعة نادي القضاة- المجلد الأول-٢٠٠٣، ص٧١٤-٧١٥ .

[3] د/ محمد حسام لطفي، الاطار القانوني للمعاملات الإلكترونية:دراسة في قواعد الإثبات في المواد المدنية والتجارية مع إشارة خاصة لبعض قوانين البلدان العربية، القاهرة٢٠٠٢ ، ص٢٨- ٣٥.

[4] المرجع السابق ، ص٣٩.

[5] Guide to Electronic Commerce Regulations,2002,op.cit

[6] أنظر مثلاً: United States V.Ickes,393 f.3d 501-06 (4thcir.2005)

فنظام الإثبات الجنائي تحكمه قرينة البراءة "Presumption of Innocence" التى طبقاً لها، يتعين الحكم بالبراءة كلما شاب الأدلة الشك وعدم اليقين والجزم. فمجرد الحصول على الدليل الإلكتروني وتقديمه للقاضي الجنائي يُعد غير كافياً لإدانة الجاني، إذ أن هذا الدليل قابل للعبث فيه وفقاً لطبيعته الفنية، إذ يمكن تحريف الحقائق التى يصعب لمن يدركها غير المتخصص، فمشكلة إثارة الشك ومدى مصداقية هذا الدليل من عدمه مازالت محل خلاف في الفقه والعمل.[1]

وبناء على ما تقدم، فيمكن القول بأنه في النظام القانوني اللاتينى وخاصة ما يتعلق بمسائل الإثبات ومنها النظام القانوني المصري، فالقاضٍ يملك سلطة تقديرية واسعة في تقييم وتقدير الدليل من حيث حجيته وقيمته القانونية، فله قبوله أو رفضه بحسب اقتناعه الشخصي وتكوين عقيدته، وهذا ما أكده النظام الإجرائي القانوني المصري.[2] فالدليل الإلكتروني يتمتع من حيث قوته بقوة في الإثبات قد تصل لحد الجزم واليقين، إلا أن ذلك لا يتناقض مع ما قد يشوب هذا الدليل من حيث سلامته من حيث العبث به من ناحية وصحة الإجراءات المتبعه في الحصول عليه من جهة أخرى .

أما في الأنظمة القانونية الإنجلوسكسونية التى تأخذ بنظام الإثبات المقيد (القانوني)، إذ أن القانون قيد حرية القاضي بقائمة أو مجموعة من الأدلة التى حُددت قيمتها في الإثبات، فلا يكون للقاضي أى دور في تقدير حجية الدليل. فالمشرع هو الذي يحصر الأدلة ويحدد ما يجوز وما لا يجوز أن يلجأ له القاضي في الإثبات، فيكون دورهذا الأخير قاصراً على مجرد فحص الدليل للتأكد من توافر الشروط المقررة قانوناً، فلا مناص للاستناد لأى دليل لم ينص عليه القانون صراحةً.[3]

ففي ظل هذا النظام الإجرائي الذي تتبعه مثلاً الولايات المتحدة وبريطانيا، لا يعترف للدليل الإلكتروني بحجية في الإثبات ما لم ينص القانون عليه بلغة صريحة ضمن قائمة

---

[1] انظر على سبيل المثال: Kansas Statute No.16-1602.(2000-2002)

[2] د/ ثروت عبد الحميد،، مرجع سابق الإشارة إليه ، ص٩٦-٩٨.

[3] انظر على سبيل المثال: The American Bar Association (ABA) creates First Digital Signature Guidlines to Aid in Security of the Internet (1996).

الأدلة، وعليه فخلو نص القانون من ذكره، يهدر ما يتمتع به من حجية حتى لو كان يقينياً، فلا يجوز للقاضي أن يستند إليه في تكوين عقيدته.[1]

فسلطة القاضي الجنائي في تقدير وقبول الأدلة الإلكترونية في الإثبات ليست مطلقة – كما يظن البعض– بل تخضع لقواعد معينة، فهو يتقيد بالأدلة اليقينية المقتربة نحو الحقيقة الواقعية ، بعيداً عن الظن والشك والتخمين، ويناقشها طبقاً لمبدأ شفافية المرافعة، كما يجب أن تكون مشروعة ومتفقة مع مقتضيات العقل والمنطق.

المبحث الثالث

حجية وشروط الدليل الإلكتروني الناشىءعن التفتيش الجنائي

خصصنا هذا المبحث لمعرفة الشروط التي يجب أن تتوافر في الدليل الإلكتروني الناتج عن عملية التفتيش بما للتفتيش من أهمية بالغة في مجالات الإجراءات وخاصة المجال الإجرائي الجنائي. وعلى ذلك، فالدليل المتحصل من تفتيش نظام الحاسب الآلي و الإنترنت لا يكون مشروعاً ويعتبر باطلاً بطلاناً مطلقاً وكذا ما يترتب عليه من آثار إجرائية إذا لم تتوافر فيه عدة شروط قانونية معينة.

أولاً: في شروط الدليل المتحصل من تفتيش النظم المعلوماتية (الآلية)

الشرط الأول – الحصول على الدليل بطريق مشروع غير مخالف لأحكام الدستور والقانون (قانون العقوبات)

فهدف المواثيق الدستورية هو صيانة كرامة الأشخاص والحفاظ على حريتهم وحقوقهم العامة، لذا فإن معظم الدساتير الحديثة – بما فيها الدستور المصري الحالي ٢٠١٤– تتضمن قواعد ونصوص تنظم ضوابط بعض الإجراءات وخاصة الإستجواب والإستيقاف والحبس والقبض والتفتيش وغيرها وهذا ما قيد المشرع الإجرائي في مصر وغيرها عند وضع قانون الإجراءات الجنائية.[2] فعلى سبيل المثال، نص المشرع

---

[1] Thomas A.o'Malley, Using Historical Cell Sit Analysis Evidence in Crimnal Trials, 59 The United States's Attoney 3 Bulliten 6 (2011).

د/ ثروت عبد الحميد ، مرجع سابق، ص٩٩- ١٠٠ .

[2] انظر في هذا الصدد مثلاً:

الدستوري على حرمه المساكن والأماكن الخاصة إذ لا يجوز دخولها ولا تفتيشها إلا في الأحوال المقررة قانوناً وبالكيفية التى نظمها القانون، وكذا كفل سرية المراسلات البريدية والمحادثات الهاتفية وغيرها، فلا يجوز مراقبتها أو التصنت عليه إلا في الأحوال التى حددها القانون وبأذن (أمر) قضائي مسبب.[1]

وعلى ذلك، فإجراءات الحصول على الأدلة الجنائية، يجب أن يكون من خلال الإطار العام الذي حدده الدستور، فالدليل المتحصل عليه بالمخالفة لاحكامه يُعد باطلاً بطلاناً مطلقاً والبطلان هنا متعلق بالنظام العام، ولكل صاحب مصلحة التمسك به وللمحكمة أن تقضي به من تلقاء نفسها.[2] أما اذا تم الحصول على الأدلة بالمخالفة لاحكام القانون، فجزاء ذلك يكون جنائياً أو إدارياً فضلاً عن الجزاء المدني المتمثل في الحكم بالتعويض. وما يهمنا في هذا المجال هو الجزاء الإجرائي، إذ أن الدليل الناتج عن افتعال جريمة يكون باطلاً بطلاناً مطلقاً متعلقاً بالنظام العام.[3]

هذا ولم يقتصر المشرع الإجرائي في حمايته لأسرار الأشخاص على الإطلاع عليها بطرق عادية بل شمل كافة الأسرار داخل المراسلات البريدية والبرقيات وغيرها، فقرر عقوبات الحبس والغرامة في حالة مخالفة ذلك. وفي جميع الأحوال، يرتب العمل المخالف للقانون لمن وقع عليه الضرر، الحق في التعويض المدني مع وجوب بطلان هذا

State of Connecticut v. Swinton, 847 A.2d 921 (S.Ct.couu.2004) (requiring an adequate foundation for enhancements of photographs has been presented).

[1] انظر في هذا الصدد مثلاً:

Williams v.Long,2008 WL 4848362 (D.md., April 7,2008) (case search results printed from official government websites admitted on the basis that they are self-auth enticating).

[2] هذا وقد نص قانون التخلص من الأوراق الحكومية الأمريكي "Government Paperwork Elimination Act 1998" على أن الهيئات الحكومية عليها إلتزام بحفظ المعلومات الإلكترونية أو تسليمها أو حتى الكشف عنها، كلما كان ذلك ممكناً كان بديل للمستندات الورقية وكذا وجوب اتخاذ الإجراءات الكفيلة باستخدام وقبول التوقيعات الإلكترونية كلما كان ذلك ممكناً.

[3] الدكتور/ محمد حسام الدين لطفي،استخدام وسائل الإتصال الحديثة في التفاوض على العقود وابرامها- دراسة مقدمة إلى ندوة وسائل حسم المنازعات في "عمليات المصرفية "(مركز القاهرة للتحكيم التجاري الدولىCIRICA) (يونيو ١٩٩٨)،ص٨.

العمل كونه نتاج عمل إجرامي، ولذا بطلان الدليل، إذ أن ما بنى على باطل فهو باطل، طبقاً للقواعد العامة.[1]

وعلى آية حال، يمكن تطبيق القواعد العامة التقليدية على ما قد يقوم به رجال البحث الجنائي وغيرهم، ممن خول له القانون في نطاق اختصاصه كشف الجرائم- في حالة إطلاعهم (بحكم مهامهم) على أسرار المواطنين عبر أجهزة الحاسوب أو الإنترنت، ولكن اختلف الفقه المقارن حول الشهود في الجريمة المعلوماتية، فهل هم ملزمون بالإفصاح عن شفرات أو كلمات مسربة أو طبع ملفات أو غير ذلك؟

ذهب رأى في الفقه إلى إنه ليس من واجب الشاهد أن يقوم بذلك، فلا يجب إجباره على التعاون في كل ما يعرفه عند سؤاله أمام القاضي الجنائي، فالإلتزام بأداء الشهادة لا يتضمن القيام بذلك الواجب طبقاً للقواعد التقليدية العامة في الشهادة، وهذا ما ذهب إليه كل من لوكسبورج والمانيا فضلاً عن عدم جواز اكراه الشاهد للإفصاح عن بيانات أو كلمات سرية أو غيرها.[2]

وذهب رأى آخر في الفقه للقول بجواز قيام الشاهد بذلك، ففي فرنسا مثلاً، يكون الشاهد مكلفاً بالكف عن كلمات المرور السرية والشفرات فيما عدا ما يتعلق بالمحافظة على أسرار المهنة. وفي هولندا، يتيح قانون الحاسبات الإلكترونية إصدار أمر للقائم بالتشغيل بتقديم المعطيات اللازمة لاختراقه ودخوله.[3] فاستقر معظم الفقه والقضاء الفرنسيين على جواز استخدام وسائل في كشف الجرائم المعلوماتية، فيجوز لرجال الضبط القضائي اللجوء لطرق إلكترونية في التصنت على المحادثات التليفونية وذلك على الرغم من خلو بعض نصوص القانون المتعلقة بالنزاهة والأمانة في البحث عن الحقيقة، والبعض في فرنسا قد نادى بالبحث عن هذه الجرائم والحصول على أدلتها بطرق مشروعة ونزيهة وهو المعمول به في بلجيكا وسويسرا وكذا انجلترا واليابان.[4]

---

[1] المرجع السابق ، ص٤١.

[2] انظر في هذا الشأن: Bank v.Eurich,831N.E 2d 909 (S.J.c mass.,)August 3.2005)(computer printouts admitted; bank routinely accessed and relied upon the accuracy of information).

[3] د/رمزي عوض، مرجع سابق الإشارة إليه، ص٨٥، د/أحمد بلال، مرجع سابق الإشارة إليه، ص١٦ ومابعدها.

[4] راجع في هذا الصدد:د/على الطوالبة، مرجع سابق الإشارة إليه، ص١٧٩.

هذا وقد تضمن قانون الشرطة والإثبات الجنائي البريطاني ١٩٨٤ الشروط الأساسية الواجب توافرها فيما يخرج من الكمبيوتر لكي يُقبل أمام القضاء (كظروف تقييم البيانات أو وجود دافع إخفاء أو تشويه البيانات لدى شخص معين مثلاً).[١] وعلى ذلك، يشترط أن يوجد أساس معقول للإعتقاد بأن البيان أو المعطى خاطىء وغير دقيق نتيجة للإستعمال الخاطىء أو غير الملائم، وكذا يجب أن تكون جميع مكونات الحاسوب المادية تعمل بدقة فضلاً عن خضوع تقدير تلك الشروط للقاضي الجنائي وهذا ما قد أكدت عليه أحكام القضاء الانجليزي، ففي حكم لمحكمة الاستئناف في انجلترا، قضى بأنه " لايجوز إنكار أو رفض أية صلاحيات أو مميزات مقررة وفقاً لقانون الإثبات، يمكن من خلالها- عن طريق التقنيات الحديثة- الوصول للحقيقة الخاصة بالجرم، ولكن لابد من خضوع أى تقنيات للتمحيص والفحص الدقيق وذلك في ضوء جميع ظروف كل حاله على حدة".[٢]

الشرط الثاني- إمكانية مناقشة الأدلة المعلوماتية (الإنترنت أو الحاسوب)

لايمكن للقاضي الجنائي بوجه عام أن يبنى اقتناعة إلاعلى العناصر الجوهرية التى طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى، فالأدلة المتحصلة من الجرائم المعلوماتية سواء كانت بيانات معروضة على شاشات الحاسب أو مطبوعة أو مختزنة على أقراص مدمجة أو غير ذلك من الأشكال، فكل ذلك يجب أن يخضع للمناقشة التفصيلية أمام المحكمة.[٣]

وطبقاً للقواعد العامة المستقرة في فقه الإجراءات الجنائية، أنه لا يجوز قبول الشهادة السماعية أمام المحاكم الجنائية، إلا إذ نص القانون على غير ذلك بشروط وضوابط معينة، وهذا قد يؤدي في بعض الأحيان لاستحالة مناقشة واستجواب الشاهد الأصلى من

---

[١] د/ هلالي أحمد، مرجع سابق الإشارة إليه، ص٥٢-٥٦ وص١٢١-١٢٢؛ د/هشام رستم، مرجع سابق الإشارة إليه، ص١١٧.

[٢] د/ هلالي أحمد، مرجع سابق الإشارة إليه، ص١٣٢؛ د/جميل عبد الباقي- أدلة الإثبات الجنائي، مرجع سابق، ص١١١-١١٢ وانظر كذلك: د/أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات: دراسة مقارنة، دار النهضة العربية- القاهرة (طبعة ثانية)،١٩٨٩، ص٩٣-٩٤.

[٣] انظر: Police and Criminal Evidence Act 1984,op-cit-p.25&28

قبل المحكمة والدفاع.[1] ولكن استثناءاً من ذلك، فقد تضمنت بعض القواعد الفيدرالية الأمريكية نصاً يعتبر البيانات والسجلات بدقة وسيلة إثبات مقبولة أمام القضاء الجنائي، وعلى ذلك، يجوز اعتبار البيانات والتقارير والمعلومات وغيرها المحفوظة في أى شكل كان وحتى الأراء ونتائج التحاليل المنقولة بواسطة الخبراء والمختصين وسلية إثبات مقبولة أمام القاضي الجنائي كونها بيانات أكثر دقة ومحمية بأسلوب علمي يختلف عن غيرها من الأدلة السماعية، وعلى ذلك، فالأدلة الإلكترونية من هذا القبيل كونها معدة بهذا الأسلوب العلمي الدقيق لا يشوبها الشك.[2]

هذا وفي بعض الأنظمة القانونية المقارنة كالقانون الهولندي، يجوز للقائم بالتفتيش سلطة تسجيل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام الإلكتروني دون التقيد بالحصول على أمر (إذن) مسبق بذلك من المحقق المختص ولكن هذه القاعدة غير مطلقة، فهى مقيدة بأن لا تكون النهاية الطرفية للكمبيوتر موجودة ضمن إقليم دولة أخرى، إذ قد يؤدي الاتصال بها لانتهاك سيادتها الإقليمية وهو مخالف لاعراف القانون الدولي والمواثيق الدولية، وكذا احتواء هذه النهاية الطرفية على بيانات هامة وضرورية تكفي لظهور الحقيقة، فضلاً عن حلول قاضي التحقيق محل الشخص صاحب المكان الذي يتعين تفتيشه بصورة مؤقتة.[3]

ولكن على سبيل الإستثناء استناداً للإتفاقيات الدولية المتعلقة بالتعاون القضائي والأمني في هذا المجال، يجوز الحصول على الأدلة المعلوماتية في إقليم دولة أخرى، كما أن متحصلات هذه الجريمة، يجب عرضها على القاضي الجنائي المختص بكافة عناصرها، إلا أن حيادية القاضي تلزمه بأن لا يقيم قضاءه أو حكمه إلا على ما عرض وطرح عليه (أو أمامه) وكان موضوعاً للمناقشة، فلا يجوز له أن يقضي بناء على علمه

---

[1] Naughan Bevan and Ken Lidstone, A Guide to the Police and Criminal Evidence Act 1984.(Bulterworth,London,1985),at 497.

[2] راجع د/هلالي أحمد، مرجع سابق،حجية المخرجات الإلكترونية ، ص٩٦.

[3] انظر في هذا الشأن: حكم (قرار) محكمة النقض المصرية رقم ١٧٩ في ١٩٨٦/١١/٢٠- المبادىء القانونية- ص٩٤٣.

الشخصي كما يجب تأهيل القضاة فنياً وتقنياً لمواكبة المناقشات العلمية للأدلة المعلوماتية بشكل يتماشى ويتواكب مع روح عصر تكنولوجيا الإتصالات والمعلومات.[1]

الشرط الثالث- عدم قابلية الدليل الإلكتروني للشك (يقينه الدليل المعلوماتي)

يلزم في الأدلة المستخرجة من أجهزة الحاسوب وكذلك الشبكة المعلوماتية أن تكون يقينية غير قابلة للشك، أى مبنية على الجزم حتى يتمكن القاضي من الحكم بأدانة المتهم، فلا مجال لجحد قرينة البراءة وافتراض عكسها إلا عندما يتحقق اقتناع القاضي المبني على الجزم واليقين.[2]

ويشترط قانون البوليس والإثبات في انجلترا "Police and Evidence Act " حتى تتحقق يقينة الأدلة المعلوماتية أن تكون المعطيات والبيانات دقيقة وخارجة عن الحاسب بشكل سليم. وفي كندا، فالسائد فقهاً وعملاً هو اعتبار كل ما يخرج عن الحاسوب من مخرجات من أفضل الأدلة، فيتحقق الجزم واليقين المتطلب في الأحكام الجنائية.[3]

هذا وقد نصت بعض القوانين المحلية في بعض الولايات في أمريكا، على أن النسخ المستخرجة من بيانات الكمبيوتر تعتبر من أفضل الأدلة المتاحة للإثبات ، وبالتالي تحقق الجزم واليقين.[4] وجدير بالذكر في هذا الصدد أن القواعد الفيدرالية الأمريكية تنص على" أن الشرط الرئيسي للتوثيق أو التحقق من صدقه وصحة الدليل، كشرط مسبق لقبوله، هو أن يفي بدلالة أو أمارة أو بينة كافية إذ إنها تدع اكتشاف أو الوصول للأمور التى تتصل بالموضوع بما يؤيد الإدعاءات أو المطالبة المدعى بها".[5]

---

[1] د/ هلالي أحمد، مرجع سابق الإشارة إليه، ص٢٣ ومابعدها (الالتزام الشاهد).

[2] د/ عفيفي كامل ود/ فتوح الشاذلي، مرجع سابق الإشارة إليه، ص٣٤٧؛ د/محمد البشري، مرجع سابق الإشارة إليه، ص١٢٨-١٢٩.

[3] د/ هلالي أحمد، تفتيش نظم الحاسب، مرجع سابق الإشارة إليه، ص١٣٩ ومابعدها.

[4] انظر: ABA Standing Committee on Ethics and Professional Responsibility formal opinion 06-442,Review and Use of Metadata (August 5,2006).

[5] انظر على سبيل المثال: Vinhnee v.American Express Travel Related Service Company,Inc,336 B.R.437(9th cir.BAP 2005) (computerized Business records not admitted due to lack of foundation).

هذا وذهب الفقه الياباني لقبول الأدلة المستخرجة من الحاسب الآلي التى تم تحويلها لصور مرئية سواء كانت أصلية أو نسخاً مستخرجة عن هذا الأصل، فيتحقق اليقين المتطلب الذي يُبنى عليه الحكم الجنائي ويدخل في ذلك التقارير المعتمدة من الخبراء وهذا ما أخذت به بعض دول أمريكا اللاتينية فيما يتعلق بقوانين الحاسوب كتشيلي والأرجنتين.[1] هذا ويلاحظ أن المشرع الأردني قد اعتبر نظام المعالجة المعلوماتي صالحاً لإثبات تحويل الحق مما يسهل مهمة المحقق في ضبط الأدلة المعلوماتية، وذلك إذا كانت النسخة المعتمدة من السند القابل للتعديل (للتحويل) محددة بصورة غير قابلة للتعديل أو اذا كانت هذه النسخة تدل على اسم الشخص الذي تم سحب السند لصالحه، فيجوز استخدام كل من هذه الوسائل في تفتيش أجهزة وأنظمة الحاسوب والإنترنت.[2]

ثانياُ: الحجية القانونية للدليل المعلوماتي الناشىء عن التفتيش الجنائي

من المسلم به إن القيمة القانونية (حجية) المخرجات الناتجة عن الحاسب الآلي وشبكاته، هى التى تتمثل في القوة الاستدلالية والقيمة الإثباتية على صدق نسبة الفعل الجرمي إلى شخص بعينه أو كذبه. بعبارة أخرى، هى قيمة ما يتمتع به المعطى أو المخرج المتحصل من الحاسوب أى كان نوعها ورقية أو إلكترونية أو غيرها من قيمة وحجة استدلالية في كشف الحقيقة.[3]

هذا وقد اختلفت أنظمة الإثبات المتعددة في تقدير حجية الأدلة الإلكترونية (مخرجات الحاسوب).ففي الأنظمة الإنجلوسكسونية، التى يحدد فيها المشرع أدلة الإثبات وكذا حجيتها القانونية أو قوتها الإقناعية، ففي بريطانيا– التى تعد في مقدمة الدول التي تعتمد على هذا النظام– بعد أن أصدرت قانون سوء استخدام الحاسوب عام ١٩٩٠ الذي لم يتعرض لا من قريب ولا من بعيد للأدلة الإلكترونية وحجيتها في الإثبات الجنائي وإن

---

[1] د/ محمد فهمي طلبة (وآخرون)،دائرة معارف الحاسب الإلكتروني- مجموعة كتب دلتا- مطابع المكتب المصري الحديث، القاهرة،١٩٩١، ص ٣١ ومابعدها.

[2] أنظر على سبيل المثال: (المواد ١٥٧،١٥٦-١٦٢) من قانون أصول المحاكمات الجزائية الأردني، وانظر على سبيل المثال:

- People v.Rivera,537 N.E 2d 924 (App.ct. Illinois, April 4,4.1989) (enunciated standards for the admissibility of computer records).

[3] انظر د/ هلالي أحمد، حجية المخرجات الكمبيوترية، مرجع سابق الإشارة إليه، ص٢٢.

كان قانون البوليس والإثبات الجنائي ١٩٤٨ قد تناول هذه المسألة تفصيلاً مبيناً قواعد قبول هذه الأدلة في الإثبات في المسائل الجنائية- والتى أسلفنا لها الإشارة من قبل.[١]

أما في الولايات المتحدة الأمريكية، فقد تعرضت بعض القوانين لقيمة الأدلة المعلوماتية في الإثبات، ومثال ذلك، ما نص عليه قانون الحاسب الآلي ١٩٨٤ الصادر في "Iowa" من أن مخرجاته ومعطياته تكون مقبولة ولها قيمة قانونية بوصفها أدلة إثبات (مادة ٧١٦/أ/١٦) فضلاً عن قانون الإثبات الصادر في California الذي نص على أن النسخ المستخرجة من البيانات التى يتضمنها الحاسوب تكون معتمدة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات.[٢] هذا وينص قانون الإثبات الكندي في المادة ٢٩ على مجموعة من الضوابط التى يلزم توافرها قبل عمل صور (copies) من السجلات التى تضاف إلى الأدلة. ومن هذه القواعد مثلاً، أن تكون الصورة حقيقية من المدخل الأصلي (أى طبق الأصل).[٣] وفي حكم شهير في قضية (McMullan)، قضت محكمة استئناف Ontarieo الكندية بأنه "يشترط كي تعتبر سجلات الحاسوب معتمدة بوصفها نسخاً حقيقياً من السجلات المعلوماتية وأن تكون متضمنة على توصيف كامل لنظام حفظ السجلات السائد في المؤسسات المصرفية والمالية وكذا وصفاً تفصيلياً للإجراءات والعمليات الخاصة بإدخال البيانات وتخزينها واسترجاعها حتى يتضح أن المخرج المستخرج من الكمبيوتر موثوق به بشكل محدد وكافٍ".[٤]

وتجدر الإشارة إلى أن الضوابط الفيدرالية الإمريكية فيما يتعلق بالإثبات، قررات أن النسخ طبق الأصل – أى كانت وسيلة النسخ – كالطابعة والتصوير والتسجيل الإلكتروني والميكانيكي لها نفس القيمة القانونية التى تكون للأصل وهذا ما استقر عليه القضاء الأمريكي من حيث قبول دليل السجلات المحتفظ بها على الحاسب.[٥]

---

[١] المرجع السابق، ص٤٢.
[٢] المرجع السابق، ص٤٣.
[٣] المرجع السابق، ص٤٤-٤٥.
[٤] المرجع السابق، ص٤٦.
[٥] المرجع السابق، ص٥٥-٥٧.

أما فيما يتعلق بالنظم القانونية اللاتينية ومنها القانون الفرنسي والقانون المصري، فأن حجية الأدلة لإثبات الجرائم المعلوماتية ولا حتى ما يتمتع به القاضي الجنائي من حرية في تقييم هذه الأدلة.[1]

هذا وقد قضت محكمة النقض الفرنسية في هذا الصدد بأن " أشرطة التسجيل الممغنطة و المدمجة التى تكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي".[2]

هذا ما صارت عليه معظم الدول الأوروبية كاليونان والمانيا وكذا دول أمريكا اللاتينية كتشيلي والبرازيل، إذ أن هذه الدول تخضع الأدلة المعلوماتية لسلطان القاضي في الأقناع الذاتي، فله قبولها أو جحدها – رغم قوتها وقطعيتها علمياً– وذلك في حالة ما إذا وجد هذا الدليل غير متسق مع مقتضيات العقل والمنطق وكذا ظروف وملابسات الواقعة.[3]

هذا وجدير بالذكر أن قانون الإجراءات الجنائية التشيلي يعتبر استخدام الأفلام السينيمائية وكذا نظم انتاج الصورة والصوت وغيرها من الوسائل التى تكون ملائمة ووثيقة الصلة وتؤدي لاستخلاص الحقيقة والمصداقية ويمكن قبولها كأداة إثبات (مادة ١١٣).[4] واستقر الفقه التشيلي على أن الدليل المستخرج من الحاسوب الآلي والإنترنت، يمكن قبوله أمام القاضي الجنائي كدليل كتابي (أو مستندي)، وحجته في ذلك، هو توسيع شبكة ومظلة الوسائل العلمية و التقنية الحديثة في الإثبات الجنائي، لتغطي العناصر الإثباتية عن الجرائم الإلكترونية.[5]

أما فيما يتعلق بالقوانين ذات الإتجاه المختلط في الإثبات (وهى الجامعة بين النظام اللاتيني وإلانجلوسكسوني)، فيقوم على أن يحدد القانون أدلة معينة لإثبات بعض الوقائع

---

[1] انظر مثلاً:
McDaniel v.United States, 343 F.2d 789 (5th cir), cert.denied,382 U.S. 826 (1965);people v.McHugh,124 mis.2d 559,560,476 N.Y.S.2d 721,722 (1984).

[2] د/ هلالي أحمد، المرجع السابق، ص٦٢.

[3] د/ فتوح الشاذلي ود/عفيفي كامل، مرجع سابق الإشارة إليه، ص٣٧٣-٣٧٤.

[4] د/ هلالي أحمد، المرجع السابق، ص٦٤-٦٦.

[5] راجع في هذا الصدد:د/ عبد الحافظ عبد الهادي عابد،الإثبات الجنائي بالقرائن: دراسة مقارنة،دار النهضة العربية، القاهرة،١٩٩٨، ص ٥٦٣ ومابعدها.

دون البعض الآخر، أو يضع ضوابط معينة في دليل معين في بعض الأحوال، أو حتى يمنح القاضي الحرية في تقدير الأدلة الإلكترونية.[1]

فعلى سبيل المثال، حصر المشرع الإجرائي في اليابان طرق الإثبات المعتمدة جنائياً في القرائن وأعمال الخبرة وكذا أقوال الشهود والمتهم، أما فيما يتعلق بالأدلة الإلكترونية، فاستقر الفقه الجنائي الياباني على أن السجلات الالكترومغناطيسية تكون غير ملموسة أو مرئية في ذاتها، فلا يجوز استخدامها كدليل يستند إليه القاضي إلا إذا أصبحت مقروءة ومرئية بعد تحويلها، فيمكن فهمها وقرائتها واستعيبها، فتعتمد في هذا الغرض سواء كانت هى الأصل أو نسخ طبق الأصل (كمخرجات الطباعة لسجلات البيانات مثلاً).[2]

أما عن الحجية القانونية أو القيمة الإثباتية للتسجيلات الصوتية المسجلة إلكترونياً "Electronic Recording"، فهى لا تحتمل الخطأ عن تسجيلها معلوماتياً، إذ أن من الصعوبة التلاعب فيها ويمكن للخبراء كشف التلاعب إن حدث حتى ولو بكفاءة وتقنية عالية، وعلى ذلك، يمكن القول بأن التسجيل الصوتي الممغنط له حجة قوية ودامغة في الإثبات الجنائي.[3]

وعبر استخدام وسائل الإتصال وتكنولوجيا المعلومات الحديثة والسريعة، يمكن استخدام تسجيلات القيديو لإثبات جرائم القوة والتعذيب وإساءة استعمال السلطة الواقعة من مأموري الضبط القضائي وغيرهم من الموظفون العموميون المخول لهم اختصاص كشف الجرائم وكذا يمكن استعمالها لتسجيل عمليات القبض والتفتيش وضبط الآثار والأدلة الناجمة عن الجرم تسجيلاً قوياً ودقيقاً وكذا عمليات المعاينة المتطلبة لمسرح الجرم.[4]

هذا وقد اشترط الفقه الجنائي لمشروعية الدليل المستمد من التسجيل والمراقبة ما يلي من شروط:

---

[1] د/ هدى قشقوش،الحماية الجنائية، مرجع سابق الإشارة إليه، ص٧١.

[2] د/ عبد الفتاح حجازي، مرجع سابق الإشارة إليه، ص٤٦.

[3] Karl J. Flusche, Computer Crime and Analysis of Computer Evidence it Ain't Just Hackers And Phreakers Anymore! 7 Journal of Information Systems Security 1 (1998),at1-6.

[4] د/ أحمد تمام، مرجع سابق الإشارة إليه، ص٢٧٤-٢٧٥.

١. تحديد دقيق لشخصية وهوية الفرد المراد تسجيل مكالمته أو أحاديثه أو حتى بريده الإلكتروني إذا كان ذلك ممكناً في حالة الإنابة للتفتيش؛
٢. تحديد نوع الحديث المراد ضبطه أو التقاطه، والجرم المتعلق به، والجهد المسموح لها بذلك، وكذا المدة الجائز خلالها التقاط أو تسجيل الحديث؛
٣. إذا لم يكن التسجيل منطوياً أو متضمناً أى إعتداء على حق يحميه القانون، فيكون مشروعاً الدليل في هذا الغرض ويجوز للمحكمة أن تستند عليه في حكمها بالبراءة أو الإدانة.[١]

هذا واعتبر بعض الفقه انه يمكن استخدام حاسوب الجيب"IPAD" على إنه" أداة تبرئة"، حيث أن تكون التوقيعات المشفرة من خلال دليل غير قابل للانكسار في مواجهة آية إتهامات باطلة، فلو أن شخص معين قد الصقت به عدة اتهامات باطلة أو اتهم بجرم معين، فله أن يدافع عن نفسه من خلال ما هومسجل من أفعال وأقوال في أى وقت.[٢]

وهذا ينطبق أيضاً على البريد الإلكتروني، وذلك عند غرسال رسالة من خلاله، فيكون لدى الشخص المستقبل توقيعاً معلوماتياً فهو وحده القادر على استخدامه، فيمكن استخدام المعلومات الموجودة داخل الرسالة (سواء كانت صوت، فيديو أو تحويلات بنكية أو غيرها) كحجية في الإثبات الجنائي من خلال معرفة شخص مرسل الرسالة، تحديد وقت إرسالها بالضبط وأنه لم يتم التلاعب فيها أو فك شفرتها.[٣]

وتجدر الإشارة إلي انه يستخدم التوقيع الإلكتروني في تأمين المعلومات من خلال إدخال شفرات رقمية معينة، فيُسهل كشف أى تلاعب تم عبر تزوير أو خداع (تلفيق) حيث أن علم التصوير في مجال الإثبات الجنائي قد اضاف الكثير من القيمات العلمية بما له من قدرة وأثر في نقل صورة صادقة للأدلة الإلكترونية.[٤]

---

[١] انظر د/ محمد الأمين البشري، مرجع سابق الإشارة إليه، ص١٢٧-١٢٨.
[٢] د/ محمد الأمين، مرجع سابق الإشارة إليه، ص٣٠٣ ومابعدها.
[٣] نفس المرجع السابق.
[٤] انظر على سبيل المثال:د/ محمد المرسي الزهرة، مدى حجية التوقيع الإلكتروني في الإثبات في المواد المدنية والتجارية، ورقة عمل مقدمة لمؤتمر الحاسب والقانون، جامعة الكويت ١٩٨٩، ص٩.

ومن الجدير بالذكر، أن حجية التوقيع الإلكتروني وقيمته القانونية في الإثبات في المواد المدنية يختلف عنه في المسائل الجنائية، إذ إنه يخضع لقواعد شكلية في الإثبات المدني ويخضع لحرية وسلطة قاضي الموضوع واقتناعه بصحته وقوته في الإثبات الجنائي.[1] فقد أصبح التوقيع الإلكتروني بديلاً عن التوقيع التقليدي إذ يؤدي ذات الوظيفة فيما يخص الرسائل والوثائق الإلكترونية، إذ تبرز أهميته في كونه يحدد شخصية الموقع ويعبر عن إرادته في الإلتزام بمضمونه وإقراره لها وكذا يعتبر دليل على حضور أطراف التصرف أو من يمثلهم قانوناً أو اتفاقاً وقت التوقيع.[2]

هذا ويلاحظ أن وجود نظام تسجيل الدخول على الشبكة المعلوماتية (الإنترنت) يسمح بتحديد الأفراد الذين أو حاولوا (شرعوا) في الدخول بعد ارتكاب السلوك الإجرامي. ومن النادر ضبط الفاعل متلبساً، وقد يرجع ذلك إما لخطأ في نظام الكمبيوتر أو الشبكة أو حتى الأجهزة الأخرى أو حتى عبر مراقبة الشرطة بعد اكتشاف أو ملاحظة وجود انتهاكات واعتداءات غير قانونية.[3]

هذا وقد اعتبر الفقه الفرنسي إعتداء أو إنتهاك الأنظمة الأمنية لبعض المواقع المحمية دليلاً قطعياً وحتمياً وكذا قرينة قاطعة على وجود القصد الجنائي لإرتكاب الجرم وكذا سوء نية مرتكب الفعل- وهى المشكلة للركن المعنوي بطبيعة الحال- ، فيمكن القول باعتبارها دليلاً جنائياً إلكترونياً.[4]

هذا واعتبر الفقه الجنائي الأمريكي- حديثاً- الماسحات الضوئية وطابعات الليزر أدوات يمكن استخدامها في ارتكاب الجرائم المعلوماتية. ففي مدينة Dallas في Texas عام ١٩٩٤، قام أحد الأفراد بتزوير وتلاعب في إجازات قيادة سيارات التاكسي عبر

---

[1] انظر عباس العبودي، التعاقد عن طريق وسائل الإتصال الفوري وحجيتها في الإثبات المدني، دار الثقافة للنشر، عمان،طبعة ١٩٩٧، ص٦٠ ومابعدها.

[2] وبصفة عامة في الإثبات المدني، انظر د/ اسماعيل غانم، أحكام الالتزام والإثبات، الجزء الثاني، مكتبة عبد الله وهبه،١٩٦٧، ف٣٢٣،ص٤٩٢؛ حسن جميعي،مرجع سابق الإشارة إليه،ص ٥٨-٥٦.

[3] - SinisiVincenzo, Digital Signature Legeslation in Europe, op.cit, p.489.
- Chris Reed,What is a Signature? 3 Journal of Information,Law,and Technology (J I LT) (2000).

[4] د/ عبد الحافظ ، مرجع سابق الإشارة إليه، ص٥٦٤ ومابعدها.

الماسحات الضوئية وطابعات الليزر وكذا استخدام ذات الوسيلة في إصدار بطاقات التأمين (Insurance Cards) و بعض أنواع الصكوك وأوامر الصرف المالية وغيرها عبر استعمال برمجيات الرسوم المتطورة الحديثة، فتم تقديم جميع هؤلاء الأشخاص للمحاكمة الجنائية واعتبار الأدوات المستخدمة في الأعمال سالفة الذكر سلاح الجرم وتم تقرير مسئوليتهم الجنائية وحُكم عليهم بعقوبات جنائية تنوعت ما بين الحبس والغرامة.

الفصل الثاني

إشكاليات صحة الدليل المعلوماتي في الإثبات الجنائي

تمهيد وتقسيم

من المعروف أن الدليل المعلوماتي (الإلكتروني) عبارة عن سند أو محرر مستخرج من أجهزة الحاسوب وشبكاته المعلوماتية (الإنترنت) ويكون إما في شكل نبضات كهربائية أو موجات ومجالات مغناطيسية يمكن تجميعها وفحصها وتحليلها عبر استخدام برامج وتطبيقات برمجية وتكنولوجيا معينة، حيث إنه مكون رقمي لتقديم معلومات في صور وأشكال مختلفة، كالنصوص المكتوبة أو الأشكال أو الصور أو الرسوم أو الأصوات وغيرها. وعلى ذلك، فأن ما يتم تقديمه للمحكمة وعرضه على القاضي الجنائي هو عبارة عن صورة من صور تلك الدعامات أو صورة مطبوعة أو منسوخة على الورق من السند أو المحرر الإلكتروني، وعلى ذلك، في حالة نشوب أى نزاع حول صحة هذا الدليل كوسيلة إثبات، وجب على القاضي التحري والتأكد من توافر عناصر وشروط صحته ومدى قبوله، كما أسلفنا تفصيلاً من قبل.

ومما تجدر الإشارة إليه، أن المشرع الإجرائي، وخاصة المشرع المصري لم يتعرض لهذه المسألة الهامة المتعلقة بكيفية إثبات صحة الدليل المعلوماتي في الإثبات، واكتفى في هذا الصدد بالرجوع للقواعد العامة التقليدية التى- وبطبيعة الحال- قد لا تتناسب والطبيعة الخاصة لهذا الدليل.

وبناء على ما قدم، نعرض في هذا الفصل للقواعد العامة القانونية التى تسمح بالمنازعة في صحة الدليل بوجه عام ومدى انطباقها على الدليل المعلوماتي بوجه خاص وهى المتمثلة في إحدى الصورتين إما الإدعاء بالتزوير أو إنكار (جحد) التوقيع وذلك في المبحثين التاليين.

المبحث الأول : التزوير الإلكتروني والإدعاء به

المبحث الثاني: التوقيع الإلكتروني وإنكاره (جحده)

المبحث الأول

الإدعاء بتزوير الدليل المعلوماتي

نعرض فيما يلي لمفهوم التزوير ونطاقه وأشكاله ووسائله (طرقه) وإجراءاته فضلاً عن التحقق منه والحكم فيه وأثره فيما يتعلق بالدليل المعلوماتي (الإلكتروني)

أولاً: في مفهوم التزوير ونطاقه ووسائله

طبقاً للقواعد العامة في قانون العقوبات، يقصد بالتزوير هو تغيير الحقيقة في محرر أو سند (رسمي أو عرفي) بأحدى الطرق التى حددها القانون تغييراً من شأنه أن يحدث ضرراً للغير، وهو يعد جرماً يعاقب عليه القانون الجنائي إذا توافرت اركانه.[1]

هذا والإدعاء بالتزوير أمام المحكمة يعتبر من الطرق القانونية المتاحة لإهدار حجية و قوة المحررات في الإثبات، وكذا هو الوسيلة الوحيدة قانوناً للطعن في صحة المحررات والسندات الرسمية.[2]

فالإدعاء بالتزوير – طبقاً لهذا المفهوم – يرد على المحررات الإلكترونية كما يرد على المحررات العادية التقليدية في حالات معينة، فهو يُعد من أهم الوسائل للطعن في

---

[1] د/ محمود نجيب حسني، شرح قانون العقوبات- القسم الخاص، دار النهضة العربية، القاهرة، طبعة أولى (١٩٨٨)، ص٢٠١٥.

[2] مرجع سابق، الطبعة الثانية (١٩٩٤)، ص ٢٤٧-٢٤٨؛ د/ فوزية عبد الستار، مرجع سابق الإشارة إليه، ص٢٧٠. انظر: أ/ أحمد أمين- شرح قانون العقوبات الإهلى- القسم الخاص- الطبعة الثانية،١٩٢٤،ص١٨٧.انظر على سبيل المثال في تعريف التزوير وجرائمه في القانون الجنائي المصري، المواد (٢٠٦-٢١٠) من قانون العقوبات المصري.

صحة المحررات الإلكترونية رسمية كانت أو عرفية، وعلى ذلك فلا مجال لإنكار التوقيع الإلكتروني وهذا ما أكده قانون التوقيع الإلكتروني المصري لعام ٢٠٠٤ .[١]

وبالرغم من أن المشرع الفرنسي قد عدل قواعد الإثبات واستحدث نصوص جديدة بها لتستوعب المحررات و السندات الإلكترونية فضلاً عن الورقية العادية إلا إنه لم يضع تصوراً محدداً لطرق وأشكال التزوير المعلوماتي الذي يتم عبر الوسائل الإلكترونية. وبناء على ذلك، يمكن القول بأن أى تعديل أو تغيير في أى من بيانات المحرر أو التوقيع أياً كان شكلة تقليدياً (عادياً) أو إلكترونياً، يكون محلاً للطعن عليه بالتزوير.[٢]

وما يجري عليه العمل طبقاً لنص المادة (٢٣) من قانون التوقيع الإلكتروني المصري التى أوردت صوراً وأشكالاً للتزوير الإلكتروني التى تكون محلاً للمسألة الجنائية وبالتالي للعقوبة الجنائية، بعد إمكانية الإدعاء بها أمام المحكمة الجنائية، فهذه الصور هى:

ا. إتلاف أو تعييب المحرر أو التوقيع الإلكتروني أو الوسيط الإلكتروني المستخدم في إنشائه.
ب. اصطناع أو تعديل أو تحوير المحرر أو الوسيط الإلكتروني.
ج. اختراق الوسيط الإلكتروني أو اعتراضه أو تعطيله عن أداء وظيفته.
د. التوصل بأى وسيلة إلى الحصول – بغير حق– على توقيع أو محرر أو وسيط إلكتروني.
ه. وضع التوقيع الإلكتروني على المحرر الإلكتروني دون علم أو رضاء صاحبه.
و. وضع توقيع إلكتروني على المحرر الإلكتروني وإسناده إلى الشخص المحتج عليه بالمحرر دون أن يكون هذا التوقيع خاصاً به.[٣]

وعلى ذلك، إذا توافرت إحدى هذه الحالات، أمكن وجاز الإدعاء بتزوير المحرر أو التوقيع الإلكتروني على أن تطبق في شأن هذا الإدعاء الأحكام المقررة والمنصوص

---

[1] Sharon Hatch Hodge, Satellite Data and Environmental Law:Technology: Ripe for Litigation Application,14 Pace Envitl.L.Rev.691-718 (1997).

[٢] أنظر :عمر محمد يونس،الإجراءات الجزائية عبر الإنترنت في القانون الامريكي، دار النهضة العربية- القاهرة- طبعة أولى (٢٠٠٢)،ص٥٩٢.

[٣] انظر في هذا الصدد: محمد أحمد المنشاوي- سلطة القاضي الجنائي في تقدير الدليل الإلكتروني- بحث منشور في مجلة الحقوق،الكويت،جامعة الكويت،العدد ٢،السنة ٣٦،ص٥١٥-٥٦٣.

عليها في قانون الإثبات في المواد المدنية والتجارية المتعلقة بالإدعاء بالتزوير وذلك طبقاً للإحالة الواردة في المادة (١٧) من قانون التوقيع الإلكتروني المصري.[١]

ويتم الإدعاء بالتزوير سواء كان محله محرراً ورقياً أو إلكترونياً رسمياً أو عرفياً إما بتقديم طلب عارض يُقدم أثناء سير الدعوى وهو مايطلق عليه "دعوى التزوير الفرعية" وإما بتقديم طلب أصلي يرفع بدعوى مبتدأة تسمى "بدعوى التزوير الأصلية".[٢]

هذا ويلاحظ إنه في شأن إجراءات الإدعاء بالتزوير الإلكتروني، تقضي القواعد العامة المنصوص عليها في قانون الإثبات وكذا قانون التوقيع الإلكتروني بأنه يجب تحرير أو تنظيم محضر بالمحرر المزور ويكون مفصلاً وموقعاً إما من أحد أعضاء النيابة العامة أو القاضي (أو رئيس المحكمة) والشخص الذي اظهره أو ادعى بوجوده وخصمه في الدعوى إن وجد، هذا ويجب أن يتضمن هذا المحضر بياناً يفيد ما إذا كان التزوير واقعاً على المحرر الإلكتروني أو التوقيع المعلوماتي أو حتى الوسيط الإلكتروني المستخدم في ارتكاب الجرم.[٣]

ويلزم إبلاغ الخصم بإجراءات الإدعاء بالتزوير، إذا كان هذا الإدعاء بطلب عارض مقدم أثناء سير الدعوى الجنائية وكذا وجوب ايداع المحرر المزور قلم كُتاب المحكمة (أو حتى لدى النيابة العامة) بحسب الأحوال.[٤] فاذا كان الإدعاء بالتزوير المعلوماتي بطلب عارض، وانتهت مرحلة الإدعاء بقبوله "Acceptance" تبدأ مرحلة التحقيق "Investigation". وإجراءات تحقيق الإدعاء الفرعي بالتزوير، تنطبق كذلك على الدعوى الأصلية للتزوير.[٥]

---

[١] د/ جميل الصغير، مرجع سابق الإشارة إليه، ص١٠١-١٠٢.

[٢] د/ عبد الفتاح حجازي، مرجع سابق الإشارة إليه، ص٢٤.

[٣] انظر في هذا الصدد:

- د/ مأمون محمد سلامه،الإجراءات الجنائية في التشريع المصري، الجزء الأول، دار النهضة العربية ،القاهرة،٢٠٠١، ص٦٤٥.

- د/ فوزية عبد الستار، مرجع سابق الإشارة إليه، ص٣٣٢.

[٤] د/ عبد الله على محمود، إجراءات جمع الأدلة في مجال الجرائم المعلوماتية، دار الفكر العربي، القاهرة، طبعة أولى،(٢٠١٣)، ص٦١٦.

[٥] رأفت عبد الفتاح حلاوه، الإثبات الجنائي وقواعده وأدلته، دار النهضة العربية، القاهرة، طبعة أولى،(٢٠١٣)،ص٥.

وفي ضوء ذلك، يشترط لكى تأمر المحكمة بإجراء التحقيق، أن يكون الإدعاء بالتزوير منتجاً في الدعوى الجنائية، بمعنى أن يكون الفصل في صحة أو تزوير المحرر لازماً وضرورياً للفصل في موضوع المنازعة. وهذا يرجع للسلطة التقديرية للمحكمة، إذا رأت عدم جدية أو مصداقية هذا الإدعاء، قضت برفض طلب الأمر باجراء التحقيق، بل أكثر من ذلك، فتحكم بصحة المحرر (المستند) إذا اكتشفت عدم جدية الإدعاء وكان هدفه المماطلة فقط. [1]

وكذا يشترط أن يكون إجراء التحقيق ذاته منتجاً في الدعوى الجنائية، بمعنى أن ترى المحكمة أن في الإدعاء بالتزوير الذي قدمه مدعيه، إذا أثبت صحته ما يؤدي للفصل في صحة تزوير المحرر، فإذا تبين أن هذا الإدعاء وأدلته غير متعلقة بالدعوى (أى بعيدة عن موضوعها) أو أن هذه الأدلة غير جائزة القبول أو غير منتجة أو حتى غير مُصدقة، قضت برفض طلب الأمربعمل التحقيق. [2]

وكذلك يشترط لإجراء التحقيق، أن تكون وقائع ومستندات الدعوى غير كافية لتكوين عقيدة المحكمة وقوتها الإقناعية في شأن صحة المحرر أو تزويره، فلها إنكار طلب الأمر بإجراء التحقيق إذا رأت ما يكفي لاقناع ضميرها وما يجب أن يستقرفي وجدانها. [3]

هذا فضلاً عن كون التحقيق جائزاً، بمعنى إنه لا يجوز إجراء التحقيق الذي يكون هدفه نفى أو دحض قرينة قانونية قاطعة، ومثالها التي تهدف لإثبات عدم صحة محرر سبق للمحكمة أن قضت بصحته وقوته في الإثبات، إذ في هذه الحالة يكون غرض التحقيق متعارضاً مع حجية الأمرالمقضي. [4] وفي جميع الأحوال، تخضع سلطة القاضي الجنائي فيما يتعلق في الأمر بمدى جدية (تحقق) الإدعاء بالتزوير إلى مبدأ حرية القاضي في تقدير الدليل. [5]

---

[1] انظر: عبد الحميد الشواربي-الإثبات الجنائي في ضوء الفقه والقضاء، منشأة المعارف،الإسكندرية-(١٩٩٨)، ص١٤.

[2] المرجع السابق، ص٦٥٨.

[3] المرجع السابق، ص٦٩٣.

[4] John L. Roberts, Admissibility of Digital Image Data and Animations: Courtroom Concerne,Advanced Imaging 102 (August 1995).

[5] انظر في هذا الشأن:

United States Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2001).

هذا ويلاحظ أن القاضي الجنائي ملتزم- عند الإدعاء بتزوير التوقيع أو المحرر الإلكتروني- بالتحقق من شروطه وضوابط صحة المحرر أو التوقيع المعلوماتي المحددة طبقاً للقانون، وعلى ذلك، فهو غير قادر أو لا يملك أن يحكم أو يقضِ- على الرغم بحالة من حرية في تقييم الأدلة- بصحة أو برد أو بطلان المحرر أو حتى يرفض إنكار (جحد) التوقيع؛ إذ أن القول بذلك يتطلب التحقق والتأكد من مدى توافر الضوابط والقواعد (أو القيود) الفنية و التقنية العلمية التى قررها القانون وهو ما لا يتحقق – بطبيعة الحال- إلا باللجوء للتحقيق، إذ أن هذا الدليل المعلوماتي هو دليل تقنى علمي يصل لحد الجزم واليقين.[1]

بالإضافة إلى ذلك، يلتزم القاضي الجنائي بالقرينة القانونية المحددة في القانون والمتعلقة بصحة المستند (المحرر) وكذا التوقيع الإلكتروني، وهى استناده إلى شهادة تصديق إلكتروني (شهادة إلكترونية معتمدة) ولا يجوز أن يحكم بعكسها إلا بناء على عناصر وأدلة قدمت في الدعوى الجنائية تكفي لانكارها أو دحضها.[2]

فالقاضي مقيد في القول بصحة الدليل المعلوماتي أو بعدم صحته بحسب توافر الشروط والقرائن القانونية من عدمه والتى لا يمكن التحقق منها إلا بالتحقيق، وبناء على ذلك إذا إدعى أمام القاضي الجنائي بالتزوير المعلوماتي (أو حتى بأحد عناصره)، فلا يملك – أمام هذا الإدعاء- سوى إحالته للتحقيق بالوسائل والآليات التى يحددها القانون.[3] كما أنه لا يجوز للقاضي في أى مسائل قضائية مدنية كانت أو جنائية (أوغيرها) أن يحكم معتمداً (بناءاً على) معلوماته وأهوائه الشخصية.

---

[1] انظر على سبيل المثال:
United States v. Evans,892 F.supp.2d 949 N.D.Ill.(2012), United States v.Wurie,728 F.3d 1,1st cir.(2013).

[2] انظر :جميل الشرقاوي،الإثبات في المواد المدنية والتجارية والجنائية، دار النهضة العربية، القاهرة، طبعة أولى، ص ٩٧ (١٩٨٢).

[3] هذا ويلاحظ أن التوقيع الإلكتروني لولاية Kansas يعني صوتاً أو رمزاً أو معالجة إلكترونية مرفقه بسجل أو متحدة به ويتم إجرائها أو إقرارها من شخص مصحوبة بنية التوقيع على السجل.
Electronic record "means a record created, sent, reciened or communicated,or stored by electronic means." Kansas Statute no.16-1602,2001-2002, United v.Wlliams,592 F3.d 511,515-17, ath cir.(2010).

ومن الجدير بالذكر في هذا المقام، إنه ليس للقاضي الجنائي أن يقضي ببطلان أو رد الدليل الإلكتروني إذا كان مستخرجاً من جهاز الحاسوب على ورق (حتى لو اعتقد من حالتها) وإنما يجب عليه في هذه الحالة أن يطبق القواعد المتعارف عليها والمعمول بها عند تعارض صورة المحرر مع أصله، إذ أن هذه الورقة منسوخة من المحرر الإلكتروني وتعد صورة لهذا المحرر المكتوب على الدعامة المعلوماتية.[1]

هذا وقد نصت المادة (١٦) من قانون التوقيع المعلوماتي المصري على أن: "الصورة المنسوخة على الورق من المحرر الإلكتروني الرسمي حجة على الكافة بالقدر الذي تكون فيه مطابقة لأصل هذا المحرر، وذلك ما دام المحرر الإلكتروني الرسمي والتوقيع الإلكتروني موجودين على الدعامة الإلكترونية".[2] ويجرى تحقيق الإدعاء بالتزوير سواء بدعوى أصلية أو بطلب عارض عبر المضاهاة.

هذا ومن الناحية الفنية، يستطيع القاضي الجنائي أن يتأكد ويتحقق من أى تعديل أو تبديل في بيانات ومعطيات الدليل الإلكتروني أو التوقيع المعلوماتي عبر الإستعانة بأهل الخبرة الفنية، حيث أن الإستعانة بخبير فني في تحقيق الإدعاء بالتزوير الإلكتروني هو أمر وجوبي وإلزامي على القاضي، إذا رأى أن الفصل في الدعوى كان متوقفاً على الفصل في صحة المحرر أو التوقيع الإلكتروني.[3]

وجدير بالذكر، إنه طبقاً للقواعد العامة في الإثبات وفي فقه الإجراءات الجنائية أن المحكمة هى الخبير الأعلى في الدعوى وإن رأى الخبير ليس إلا عنصراً من عناصر الإثبات في الدعوى يخضع لتقدير المحكمة – شأنه شأن غيره من الأدلة – دون معقب عليها ، فرأى الخبير في الدعوى لا يفيد أو يلزم المحكمة فلها أن تأخذ به كله أو أن تأخذ ببعضه أو تستبعد البعض الأخر أو أن تدحضه كله وتحكم (أو تقضي) وفقاً لما تطمئن

---

[1] انظر أمثلة أخرى في هذا المجال في كل من قوانين: California and Pennsylvnia as California is the first state in the Nation to adopt Electronic contracting-law,cap-cit.p.4.

[2] انظر: المادة الثانية من اتفاقية برن المعقودة في ٢٣ ديسمبر ١٩٩٦.

[3] د/ على القهوجي، مرجع سابق الإشارة إليه، ص٣٩ .

إليه في عقيدتها وما يستقر في وجدانها كذلك على أن تبين في حكمها الأسباب الكافية والمبررات المعقولة التى جعلتها تطرح أو ترفض رأى الخبير.[1]

ولكن يمكن القول بأنه إذا تعلق الأمر بالخبرة وما تثيره من بعض الأمور أحياناً حيث إنه لا يستطيع أن يفصل في صحته إذا كان هو الدليل الوحيد في الدعوى المقامة عن الجرم الإلكتروني كما إنه لا يستطيع أن يحكم بعلمه الشخصي أو الخاص، فله أن يأخذ برأى الخبير أو أكثر حتى يستقر ضميره وتتكون قناعته وذلك إذا كان الدليل الإلكتروني لازماً في الفصل في الدعوى الجنائية.[2]

وبعد إنتهاء إجراءات التحقيق، تُصدر المحكمة وتقضي بحكمها في الإدعاء بالتزوير، ويجب عليها أن تفصل في الإدعاء بالتزوير قبل الفصل في موضوع الدعوى، فلا يجوز لها أن تفصل فيهما معاً (أى في ذات الوقت)، فاذا انتهت لعدم ثبوت التزوير أو التلاعب، قضت بصحة الدليل المعلوماتي (أو التوقيع الإلكتروني) وإلا حكمت على مُرتكب التزوير (فاعلاً كان أو شريكاً) بالعقوبة المنصوص عليها في قانون العقوبات و التى هى في الغالب تكون (السجن أو الحبس) فضلاً عن الغرامة.[3]

ويمكن القول بأن التزوير الإلكتروني (المعلوماتي) هو أحد اعتداءات العالم الإلكتروني التى تستلزم العناية والأخذ في الإعتبار لكي يتسنى ضبط الجناة والمجرمين

---

[1] انظر تفصيلاً: US.Code,Title 18,Crimes and Criminal Procedures, Part,I Crimes,Chapter119,Wire & Electronic Communication Interception and Interception of Oral Communications, March,2015.

[2] انظر: Valsamis Mitsilegas, EU Criminal Law, Oxford & Port Land, Hart, 2009.

[3] انظر:

- Council of Europe, The European Convention on Mutual Assistance in Criminal Matters, Strasboung, April 20, 1959.
- Council Framework Decsion 2003/577/JMA of July 26, 2003 on the Execution in the European Union of Orders Freezing Property or Evidence .
-Kenneth J .Markowitz , Legal Challenges and Market Rewards to the Use and Acceptance of Remote Sensing and Digital Information As Evidience,12 Duke Environmental L. & Policy Forum (2002), at 219-264.

وكذا توفير الحماية للثقة العامة في المحررات الإلكترونية التى تعد أخطر بمراحل ومرات من التزوير العادي أو التقليدي المتعارف عليه.

المبحث الثاني

التوقيع الإلكتروني وإنكاره في الإثبات الجنائي

التوقيع بصورته العادية أو التقليدية المتعارف عليها يتخذ شكل إمضاء أو بصمة أو ختم أو بصمة أصبع، ويوضع على دعامة ورقية (أو مستند أو محرر) في حين إنه في قانون التوقيع الإلكتروني – يأخذ شكل أرقام أو إشارات أو حروف أو رموز أو غيرها من العلامات العلمية التقنية الحديثة، ويوضع على محرر معلوماتي (إلكتروني) يحفظ ويُخزن على دعامة إلكترونية اتوماتيكياً (تلقائياً). وفي ضوء ذلك، نسلط الضوء في هذا المبحث على مدى جواز رفض أو جحد (إنكار) التوقيع الإلكتروني كدليل إثبات عبر استعراض موقف القوانين والتشريعات المقارنة في هذا الصدد.

أولاً: هل يجوز إنكار (دحض) التوقيع الإلكتروني؟

على الرغم من الأشكال والصور المختلفة للتوقيع الإلكتروني ومدى اختلافها الجذري عن التوقيع العادي، إلا أن هذه الصور في النهاية هى أشكال قانونية ومعتمدة للتوقيع (تقليدية كانت أو إلكترونية)، فاعترف المشرع وخاصة الإجرائي لهذه الأشكال بالقيمة والحجية القانونية في الإثبات إذ إنها تقوم بوظيفة التوقيع التى هى تتمثل في التعرف على شخص الموقع وتحديد هويته وتميزه عن غيره.[1]

هذا ويلاحظ أن إنكار التوقيع الإلكتروني لايرد إلا على المحررات العرفية العادية، فهذا الإنكار يفترض أن يكون المستند أو المحرر عرفياً (عادياً) لايكتسب الصفة الرسمية أى يكون صادر من موظف عام مختص وكذا أن يكون صريحاً وليس ضمنياً يستدل عليه من ظروف الحال أو ملابسات الدعوى وأن يكون قبل مناقشة موضوع المحررفضلاً عن كون المحرر منتجاً في الدعوى (له سبب).[2]

---

[1] د/محمد حسين منصور –المسئولية الإلكترونية ، دار المعارف –الإسكندرية ٢٠١٠ ، ص ١٤٦-١٤٧.

[2] .عبد الحميد الشواربى ،مرجع سابق الإشارة إليه ، ص ٦٨٥

هذا وذهب بعض الفقه إلى إضافة تحقيق الخطوط والتأكد منها وكذا انتفاء التصديق على التوقيع (أو الإمضاء)، وعلى ذلك فيتوقف القول بقبول أو إنكار التوقيع المعلوماتي على مدى توافر هذه العناصر من عدمه.[1] وانطلاقاً من ذلك، يمكن القول بأن هذه القواعد ، فكما تسري على التوقيع الخطى، فكذلك يجوز سريانها على التوقيع الإلكتروني، فلا يرد الإنكار إلا على التوقيع منها .[2]

وعلى ذلك، فليس كافياً أن يكون إنكار أو رفض التوقيع صريحاً وقبل مناقشة موضوع المحرر، بل يجب أن ترى المحكمة أن الفصل في موضوع المنازعة يكون متوقفاً على إثبات صحته، ولكن ليس في مستندات ووقائع وظروف (ملابسات) الدعوى ما هو لازم أو كافٍ لتكوين عقيدتها .[3] أما إذا تبين للمحكمة أن وقائع الدعوى وأوراقها كافية لتكوين قناعتها فيما يتعلق بصحة التوقيع من عدمه، فلا تطالب بالمحرر، فيجوز لها دحض هذا الإنكار وعدم الإعتداد به وكذا اعتباره منازعة غير جدية (ليس لها اهمية)، ملتزمة ببيان ذلك الإنكار في حكمها.[4]

ولا يفوتنا أن نشير في هذا المقام إلى أن صراحة إنكار الإمضاء أو التوقيع قبل مناقشة الموضوع تُعد دفعاً من الدفوع الإجرائية التى تسري على المحررات التقليدية (العرفية) ورقية كانت أو معلوماتية علماً بأن هذا الإنكار يجب أن يكون منصباً على التوقيع أو الختم أو البصمة في ذاته .[5] فيسري هذا القيد على المحررات العادية والإلكترونية ولا يمنع من سريانه على المحرر الإلكتروني إلا ماجاء به نص أو تحديد لأشكال التوقيع التي ينصب عليها الإنكار والتى هى البصمة الخاصة بالأصبع والأمضاء والختم وليس من بينها الصورة الإلكترونية.

---

[1] مرجع سابق ، ص ٦٦١ .

[2] انظر : عبد الله عبد الكريم ، مرجع سابق الإشارة إليه، ص١٦٨-١٦٩.

[3] عمر يونس ،مرجع سابق الإشارة إليه ،ص ١٩٣.

JonathanE.Stern,The Electronic Signatures in Global and National Commerce Act ,16 Berkely Technology Law Journale (2001),at 391-411.

C-Bradford Biddle ,Misplaced Priorities :The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure ,33San Diego L.Rev.1146 (1996).

وعليه، إذا انتهت المحكمة وخاصة المحكمة الجنائية لعدم كفاية مستندات الدعوى ووقائع النزاع كي تكون عقيدتها فيما يخص الخط أو التوقيع أوغيره، فلها أن تقضي بإجراء تحقيق إما بالمقارنة أو ما يطلق عليه (المضاهاه) أو حتى سماع الشهود بشأن التوقيع أو بهما معاً إذا ارتئت ذلك في تحقيق مصلحة الدعوى وهنا يتعين تحرير محضر بحالة المحرر وأوصافه الكاملة ويتم توقيع هذا المحضر والتأشير عليه من مصدره وكاتب الجلسة وكذا الخصوم.[1]

هذا ويلاحظ أن القضاء بإجراء التحقيق يلزم أن يتضمن تعيين أو ندب خبير أو أكثر فضلاً عن ندوب أحد القضاة لمباشرة ذلك التحقيق في وقت محدد علماً بأن المحرريجب وأن يودع في قلم كُتاب المحكمة.[2]

هذا ويقصد بالمضاهاه أوالمقارنة في مجال الإثبات، هى مقارنة الخط أو التوقيع أو بصمة الأصبع التى حصل إنكارها أو جحدها بتوقيع أو خط أو بصمة ثابتة صحيحة لمن انكر صدورها من الإثبات نتيجة الإختلاف أو التشابه (التطابق) بينهما.[3] هذا ولا يشترط توثيق التوقيع في المحررات العرفية إلا أن المصلحة العامة (مصلحة الأطراف) تقضي بتوثيقه تفادياً لأى إنكار للتوقيع إذا ما نشب نزاع مستقبلاً، فمن مصلحة من يتعامل بالمحرر العرفي العادي أن يطلب من الطرف الأخر تصديقه أو توثيقه قانوناً، فيكون توثيق (تصديق) التوقيع وسيلة حمايته لتجنب أى خلافات قد ينشب مستقبلاً فيما يتعلق بصحة الإمضاء (التوقيع) من عدمه.[4]

وهذا ومن الجدير بالذكر، أنه إذا كان المحرر العرفي مصدقاً على التوقيع الذي يشمله، فلا يكفي لجحد قيمته أو حجيته في الإثبات إنكاره بل يلزم في هذا الفرض الإدعاء بالتزوير – كما أسلفنا من قبل – إذ أن المحرر على الرغم من كونه عرفياً، إلا

---

[1] د/ محمد حسام لطفى ، مرجع سابق الإشارة إليه ، ص ٣٢ومابعدها.
[2] د/طارق سرور، مرجع سابق الإشاره إليه ، ص ٣٧ ومابعدها.
[3] Benjamin Beard ,Removing Barriers to E-Commerce :The Unifom Electronic Transactions Act ,Sf06 Al l-ABA B7 -139(2000)
[4] د/ محمد حسين منصور، مرجع سابق الإشاره إليه، ص١٤٨ ومابعدها.

أنه بتصديق وتوثيق توقيعه، أصبح رسمياً كون التصديق صادر عن موظف عام مختص طبقاً للقواعد المعمول بها في هذا الشأن.[1]

وفي هذا المقام، عرف جانب من الفقه الإجرائي بأن جهة التوثيق الإلكتروني هى تلك الجهة المعتمدة أو المرخص لها قانوناً بأصدار شهادات أو مستندات التوثيق (التصديق) وكذا كافة الخدمات المتعلقة بهذه الشهادات وفقاً للقواعد المقررة قانوناً والأنظمة والتعليمات الإدارية الصادرة من الجهات (الهيئات) المختصة.

وهذه الجهات قد تكون مصلحة الشهر العقاري، المكاتب التابعة لوزارات التنمية المحلية (أو الإدارية) أو حتى وزارة الاتصالات وتكنولوجيا المعلومات.[2]

ويمكن تعريف التوثيق الإلكتروني (المعلوماتي) بأنه التأكد من ذاتية أو هوية الشخص مستخدم شهادة وصلاحيتها وصحتها والتى هى الشهادة الصادرة (المستند الصادر) عن جهه التصديق أو التوثيق المختصة بذلك قانوناً بهدف إثبات نسبة التوقيع (أو الإمضاء) الإلكتروني لشخص ما طبقاً لقواعد التوثيق الإجرائية المعتمدة قانوناً.[3] فهذه الشهادة لها أهمية خاصة في إثبات الإرتباط بين الموقع وبيانات إنشاء التوقيع طبقاً لإجراءات معتمدة، وعلى ذلك، فالجهة المختصة بذلك التصديق غالباً ما تكون جهه رسمية (كالهيئات والمكاتب التابعة للوزارات وغيرها من الجهات الحكومية) واما أن تكون اشخاص أو شركات محلية أو أجنبية تقوم بممارسة نشاط مهني خاص في مجال تكنولوجيا المعلومات والمعاملات المعلوماتية (الإلكترونية) بناء على ترخيص صادر من الدولة ممثلة في وزارة أو هيئة الاتصالات وتكنولوجيا المعلومات أو حتى وزارة التنمية المحلية.[4]

---

[1] د/ عبد الحافظ عابد، مرجع سابق الإشاره إليه، ص٧ ومابعدها.

[2] انظر مثلا: Elec .Transactions ACT SS 6(8) , 7AU.L.A. 2015(Supp .2000) Unif.

[3] David W.Carstens,Contracts Have a New Look Thanks to E- Signature Act,Texas Law , 54. July 31, 2000, at

[4] راجع دكتور مدحت رمضان، مرجع سابق الإشارة إليه، ص ٥٢ وما بعدها.

هذا ويلاحظ أن التوثيق الإلكتروني – كما ذهب بعض الفقه– للقول بأنه لا يُعد عملاً صادراً عن موظف عام مختص بل أن جهته هى مجرد طرف ثالث محايد موضوعي في المعاملة الإلكترونية يشترط وجودها أحياناً لتحقيق الأمان والثقة في المعاملات.[1]

كما أن شهادة التوثيق المعلوماتي– طبقاً لهذا الفقه أيضاً – لا تصبغ الشكل الرسمي على التوقيع المعلوماتي إذ إنها ليست رسمية، فلا يكون هذا التوقيع رسمياً على الرغم من تصديقه أو توثيقه رسمياً.[2]

وطبقاً للقانون والقواعد الإجرائية المتعارف عليها، يجب على الموقع أن يبذل قدراً من العناية وأن يتخذ قدر من الحيطة والحذر كي يتجنب استخدام أشخاص آخرين (الغير) بيانات وأداة توقيعه الإلكتروني استعمالاً غير مشروع، والتوجه في الحال لإبلاغ السلطات المختصة إذا توافرت لدية شكوكاً ودلائل قوية وكافية على أن توقيعه الإلكتروني قد تعرض للتلاعب أو الإستخدام المحظور. وعليه أيضاً أن يبذل عناية الرجل العادي في استخدام الشهادة المصدقة إلكترونياً وخاصة فيما يتعلق بدقة ومعقولية واكتمال المعطيات والبيانات الجوهرية المتعلقة بهذا المستند طوال صلاحية أو فترة سريانه.[3]

هذا وقد حدد القانون الجهة التى تتولى تنظيم خدمات التوثيق الإلكتروني والتى منها على سبيل المثال – لا الحصر– إصدار وتجديد التراخيص اللازمة لممارسة أنشطة خدمات هذا التصديق، ومراقبة هذه المزاولة، وكذا تحديد ضوابط وشروط هذا التصديق بما يتفق وطبيعته الفنية فضلاً عن تلقي الشكوى التى يقدمها المواطنين المتعلقة بمستوى الخدمات وأنشطة الجهة المزاولة وغيرها.[4]

---

[1] انظر د/ علي القهوجي، مرجع سابق الإشارة إليه، ص ٥٥ وما بعدها.

[2] Richard Raysmans and Peter Brown, The Impact of the New Federal E- sign Act on [New York Law , 224 N.Y.L.J. 3(August 8,2000)" Shared secret method"]

[3] Benjamin Wright, Eggs In Baskets : Distrbuting the Risks of Electronic Signatures , 452 PL /I, pat 63.69-70(1996) "security and biometric technology ".

[4] انظر علي سبيل المثال : 15U.S.C.A.S7002(a)(1)8(west supp. 2001)

وعلى ذلك، لا يجوز مزاولة نشاط إصدار شهادات التوثيق المعلوماتي إلا بعد الحصول على ترخيص من الجهة المختصة قانوناً ويكون في هذه الحالة المرخص له مسئولاً عن صحة تنفيذ تلك القواعد الملزمة.[1]

وطبقاً للقواعد القانونية المقررة، يجوز للجهة المختصة في حالة اكتشاف أى مخالفات أو انتهاكات، أن تصدر قرارها بسحب أو إلغاء الترخيص الخاص بإصدار شهادات موثقة أو غيرها من الخدمات بهذا الشأن حتى إزالة المخالفة وخاصة في حالة ما تم مخالفة شروط الترخيص أو حتى زوال الضمانات التى صدر الترخيص على أساسها.[2]

ثانياً : التوقيع الإلكتروني وإنكاره في الأنظمة القانونية المقارنة ووضعه في الإثبات الجنائي

ففيما يتعلق بالتوقيعات الإلكترونية وحجيتها في الإثبات في أحكام التوجيه الأوروبي، فقد قرر هذا الميثاق إنه على الدول مرعاة أن هذا التوقيع المبني على شهادة توثيق إلكترونية بوسيلة آمنة أن يحقق الشروط التى حددها القانون للتوقيع فيما يتعلق بالمعلومات المكتوبة إلكترونياً بنفس (ذات) الحجة (القيمة) القانونية التى يحققها التوقيع إليدوي بالنسبة للمعلومات (المعطيات) المكتوبة يدوياً وكونه مقبولاً كدليل إثبات أمام المحكمة (مادة ٥).[3]

هذا ويلاحظ أن هذا التوجيه قد قرر إنه لا يجب أن يفقد التوقيع الإلكتروني قيمته القانونية (حجيته) في الإثبات لكونه جاء في شكل إلكتروني (معلوماتي) أو لم يستند لشهادة توثيق إلكترونية أو أن تكون صادرة من جهة غير مرخص لها بذلك (غير معتمدة) أو لم يكن قد تم إصداره أو إنشائه من خلال تقنيات تجعله توقيعاً إلكترونياً آمناً (مادة٥/٢). [4]

وفي ضوء ما تقدم، يتضح أن المشرع الأوروبي قد وضع معيار التفرقة بين التوقيع الإلكتروني المنشأ بوسيلة آمنة ومبني على شهادة توثيق إلكترونية و التوقيع الإلكتروني الذي لا يستند لمثل هذه الشهادة المُصدقة ولم يكن آمناً في انشاءه عبر وسائل علمية، ولذا

---

[1] د/جميل عبد الباقي الصغير، الإنترنت والقانون، مرجع سابق الإشارة إليه، ص ٦٤ وما بعدها .

[2] د / هشام رستم ، مرجع سابق الإشارة إليه ، ص٣١٥ وما بعدها؛ د/ غنام محمد ، مرجع سابق الإشارة إليه، ص ١٥ وما بعدها.

[3] انظر المادة (٥) من أحكام التوجية الأوربي بشأن التوقيعات الإلكترونية .

[4] انظر المادة (٢/٥) من أحكام التوجية الأوربي بشأن التوقيعات الإلكترونية

يحوز النوع الأول الحجية والقيمة القانونية في الإثبات تلقائياً (بقوة القانون)، ويكون ملزماً للقاضي كالتوقيع اليدوي العادي لتحقيق القوة الإلزامية ولتمتعه بقرينة قانونية بسيطة على صحته، فلا يمكن إنكاره وعلى من يدعي العكس عبء إثبات هذه القرينة. [1]

أما فيما يتعلق بالنوع الثاني فلا يتمتع بذات المرتبة القانونية المخوله للنوع الأول إلا أن حجيته و قيمته القانونية في الإثبات لا ترفض أو تجحد علي إطلاقها، أما إذا انكر الشخص المنسوب إليه هذا التوقيع فعلي الطرف الآخر الذي يدعي نسبته أو وجوده وسيلة إنشاءه.[2] وعلي ذلك، فالشهادة الإلكترونية (التوتيق المعلوماتي) ينحصر آثارها ونتائجها في نقل عب الإثبات عند إنكار التوقيع المعلوماتي وذلك من وجهة نظر المشرع الأوروبي.

هذا ومن ناحية أخري، فقد نصت المادة (٦) من قانون الأونسيترال النموذجي UNICETRAL علي أنه "حينما يشترط القانون وجود توقيع إلكتروني من شخص، يُعد ذلك الشرط مستوفياً في رسالة البيانات إذا استخدم توقيع إلكتروني موثوق به بالقدر المناسب للغرض الذي إنشات أو أبلغت من أجله رسالة البيانات وفي ضوء الظروف بما في ذلك أي اتفاق ذي صلة و يعتبر التوقيع الإلكتروني موثوقاً به أي صحيحاً ومعتمداً لغرض الوفاء إذا كانت بيانات إنشانه مرتبطة في السياق الذي يستخدم فيه بالموقع دون أي شخص أخر وإذا كان أي تغيير في التوقيع يجري بعد حدوث التوقيع قابلاً للإكتشاف. هذا ويجوز للشخص القيام بأي طريقة أخرى بإثبات صحة موثوقية التوقيع الإلكتروني فضلاً عن تقديم دليل في حالة عدم صحة أو موثوقية هذا التوقيع" .[3]

هذا وينص ذات القانون النموذجي علي إنه "يجوز لأي شخص أو جهاز أو سلطة تحددها الدولة – عامة كانت أو خاصة – بتحديد التوقيعات المعلوماتية ومدي قبولها وتمتع حجيتها في الإثبات وخاصة المجال الجنائي". (مادة ٧)[4]. هذا وعرف القانون الشخص الذي يتولي تقديم خدمات التوثيق أو التصديق الإلكتروني بأنه شخص يصدر شهادات إلكترونية تؤكد الارتباط

---

[1] انظر علي سبيل المثال: 15U.S.C.A.S7003(b)(1)(a)(3).7005(a)- (b)(west supp 2001)

[2] Maria Angela Biasiottii, A Proposed Electronic Evidence Exchange Across the European Union, 14 Digital Evidence and Electronic Signatuene L. Rev. (2017).

[3] انظر بوجه عام: د/ أحمد أبو الوفا، التعليق علي نصوص قانون الإثبات، منشأة المعارف،الإسكندرية (2003).

[4] ممدوح منير الجهيني، قوانين اليونسترال النموذجي في مجال التجارة الإلكترونية، دار الفكر الجامعي للنشر،الإسكندرية (٢٠٠٦).

بين الموقع وبيانات (معطيات) إنشاء التوقيع ويجوز أن يقدم خدمات أخري ذات صلة بالتوقيعات المعلوماتية (الإلكترونية) (مادة ٢/ب و / هـ)[١].

وعلي ضوء ما تقدم يمكن القول بأن قانون UNICETRAL لم يلزم أطراف المعاملة المعلوماتية (الإلكترونية) بتوثيق تلك المعاملات أو الممارسات ولم يربط اعتماد أو اعتراف القيمة أو الحجية القانونية للتوقيع الإلكتروني في الإثبات بأصدار شهادة توثيق إلكترونية من جهة أو هيئة رسمية مرخص لها بذلك، وإنما قرر إقامة قرينة قانونية بسيطة حيث افترض صحة التوقيع الموثق إلكترونياً وأجاز إثبات عكس هذه القرينة ويكون عبء هذا الإثبات على من يدعي العكس طبقاً للمبدأ العام المعمول به والذي يقضي بأن (البينة علي من ادعي واليمين علي من أنكر).[٢]

وفي ضوء ذلك كله، يمكن القول بأنه إذا كان الدليل المعلوماتي أو الإلكتروني كوسيلة إثبات في المواد الجنائية هو من نتائج التقدم العلمي والتكنولوجي الهائل في مجال الإتصالات و تكنولوجيا المعلومات كان له أثر كبير في نظرية الإثبات الجنائي بوجه عام إذ أن هذا الدليل في نهاية المطاف هو الوسيلة الأصلية والأساسية في إثبات الجرائم المعلوماتية أو حتي التي تقع علي هذه الوسائل. فقد تبين واتضح جلياً عجز النصوص القانونية والتشريعات الإجرائية وخاصة في مجال الإجراءات الجنائية التقليدية عن مواكبة الإثبات بالدليل المعلوماتي أو الإلكتروني ومكافحة الجرائم المعلوماتية ومواجهة مرتكبيها وردعهم .[٣]

---

[١] راجع في هذا الشأن بوجه عام :
د/ محمد حسين منصور،الإثبات التقليدي والإلكتروني – دار الفكر الجامعي،الإسكندرية (٢٠٠٦).
د/ محمد حسين منصور، مباديءالإثبات وطرقه – دار الفكر الجامعي،الإسكندرية (٢٠٠٦).

[٢] انظر : أميرفرج يوسف، التوقيع الإلكتروني – دار المطبوعات الجامعية –الإسكندرية ٢٠٠٨ وكذلك راجع د/ أشرف توفيق شمس الدين : الحماية الجنائية للنشر الإلكتروني : دراسة مقارنة دار النهضة العربية، القاهرة، الطبعة الأولي ، ٢٠٠٦.

[٣] انظر علي سبيل المثال بوجه عام :
د/ أيمن سعد سليم، التوقيع الإلكتروني : دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٤.
Uniform Commercial Code Sections 1-207 and Article 2 and 2 A are also exempted from the electronic record provisions – Ss 7003(a)(3).
Jane Kufman Winn Open Systems, Free Markets and Regulations of Internet Commerce, 72 Tul .L. Rev. 1177, 1232 (1998).
د / عبد الرازق السنهوري ، الوسيط في شرح القانون المدني ، الجزء الثاني – الإثبات، آثار الإلتزام، دار إحياء التراث العربي (١٩٨٢).

الخاتمة

من خلال ما تم استعراضه من تعريف لمفهوم الجريمة المعلوماتية وأنواعها وصورها وكذلك مرتكبيها وكذا الدليل المعلوماتي (الرقمي) وحجيته وقيمته القانونية في الإثبات، يمكن القول بأن هناك تقصيراً شديداً ليس فقط في النظام القانوني المصري بل في الأنظمة القانونية العربية وكذا الدولية لمكافحة تلك الظاهرة الإجرامية التي تتزايد بشكل سريع ومتطور ومخيف تزامناً مع التطور الفني والعلمي الهائل في مجال الإتصالات وتكنولوجيا المعلومات في العالم التي من شأنها تهديد استقرار الدولة وسلامة وحرية أفرادها .

هذا ويلاحظ أن القانون المصري قد أعطي للقاضي الجنائي سلطة تقديرية واسعة في تقدير وتقييم الأدلة في الأحكام الجنائية ولما كان هناك قصورا في النصوص – التشريعية في تنظيم الأدلة الرقمية كدليل إثبات، فأن السلطة التقديرية للقضاة – في الغالب الأعم – تكون هي المعيار الأساسي في اعتبار الدليل المعلوماتي دليل قوي في الإثبات من عدمه أو حتي علي سبيل الإسترشاد أو الاستدلال. فهذا الدليل هو المتحصل من أجهزة الحاسوب دليل غير ملموس وكذا أن فهمه يعتمد علي استعمال أجهزة تقنية خاصة بتجميع وتحليل محتواه فكل ما لا يمكن تحديد وفحص محتواه لا يمكن اعتباره دليلاً رقمياً لعدم إمكانية الاستدلال به علي معلومات معينة مما يضعف أو يعدم قيمته التدليلية في إثبات الجرم ونسبته للمتهم .

كما أن هذا الدليل يتسم بصعوبة تحطيمه أو محوه حتي ولو في حالة إعطاء أمر بازالته، فمن الممكن استرجاعه ببرامج آلية متخصصة، إذ أن محاولة المتهم في محوه تُعد في ذاتها دليلاً علي ارتكابه الجرم. كما أن الطبيعة الفنية تجعل من اخضاعه لبعض التطبيقات البرمجية في معرفة ما إذا كان قد تعرض للعبث والتلاعب من عدمه. وهذا الدليل يأخذ أشكالاً وصوراً متعددة، فمنها علي سبيل المثال ما يعتبر أدلة أعدت لتكون وسيلة تم إنشأوه بواسطتها وهناك أدلة لم تكن معدة كوسيلة إثبات والمتمثلة في آثار يتكبدها الجاني دون رغبته أو إرادته في ذلك وهو ما يطلق عليه "الآثار الرقمية

المعلوماتية". وهذا الدليل إما أن يأخذ هذه الصورة الرقمية أو النصوص المكتوبة أو حتي التسجيلات الصوتية .

وجدير بالذكر أن القانون يجيز للقاضي الإستناد للدليل الرقمي و يعترف له بالمشروعية لتكوين عقيدته للحكم بالإدانة وخاصة في نظام الإثبات الحر في ظل الأنظمة اللاتينية التي يتمتع فيها القاضي الجنائي بحرية مطلقة بصدد إثبات الوقائع المعروضة أمامه، فله بناء عقيدته ووجدانه بناءاً على أى دليل يطمئن إليه، إذ طبقاً لهذا النظام، كل الأدلة تتساوى قيمتها في الإثبات فلا يتدخل المشرع في تحديد حجيتها القانونية، فحتي إذا توافرت شروط حجية الدليل، فللقاضي جحده إذا لم يقتنع به في الوصول للحقيقة. فتحت مظلة هذا النظام، لا تثور مشكلة مشروعية الدليل الرقمي من حيث وجوده، فمسألة قبوله متوقفة علي إقناع القاضي فقط، فيكون الدليل المعلوماتي مشروع من حيث وجوده وذلك قياساً علي الأصل العام في الإثبات .

ولكن علي النقيض، لا يكون للقاضي أي دور في تقدير حجيته أو قيمته القانونية في الإثبات في ظل النظام المقيد أوالقانوني حيث أن القانون قيد القاضي بقائمة من الأدلة محدداً قيمتها التدليلية، فلا يكون لهذا الدليل أي قيمة إلا في حالة النص عليه صراحة ضمن القائمة، فخلو نص القانون يهدر كل قيمة اثباتية علي الرغم من توافر شروط صحته ويقينيته في إثبات الجرم والوصول للحقيقة .

وتجدر الإشارة إلي أن مجرد الحصول علي هذا الدليل وتقديمه للقضاء لا يكفي لاعتباره دليل إدانة، فلا يستطيع غير المختص إدراك العبث فيه وفقا لطبيعته الخاصة التي قد تسمح بذلك التلاعب كما أن نسبة الخطأ في إجراءات الحصول علي دليل صادق للوصول للحقيقة قد تبدو عالية في هذا النوع من الأدلة. ففكرة الشك في الأدلة المعلوماتية لا تتعلق بمضمونه كدليل وإنما بعوامل مستقلة عنه ولكنها بطبيعة الحال تؤثر في مصداقيته فيخضع هذا الدليل المعلوماتي (الرقمي) لقواعد معينة تحكم وسائل الحصول عليه، كما إنه يخضع لقواعد أخري للحكم علي قميته وحجيته القانونية، فهناك

وسائل فنية تقنية تمكن من فحصه والتأكد من سلامته وصحة إجراءات الحصول عليه بطريقة مشروعة.

هذا ويمكن القول بأنه يجوز التأكد من سلامة وصحة الدليل المعلوماتي (الرقمي) وحمايته من التلاعب بعدة وسائل، منها أن علم الحاسبات والكمبيوتر يلعب دوراً رئيسياً في تقديم المعلومات والمعطيات الفنية التي تساعد علي فهم وتحليل هذا الدليل كما إنها تساعد علي كشف أي نوع من أنواع الغش والتلاعب منه، وهذا ما يتم في الغالب عن طريق ما يعرف باسم (التحليل التناظري الرقمي) والذي من خلاله تتم مقارنة الدليل المعلوماتي المقدم للقاضي بالأصل الموجود في الأدلة، فتكون مهمة هذه الطريقة هي الكشف عن مصداقية الدليل والتأكد من مدي حصول عبث من عدمه. كما أن العمليات الحسابية (الخورازميات) تساعد علي التأكد من سلامته من التحريف والتبديل. هذا فضلاً عن أن هناك نوعاً من الأدلة المعلوماتية يسمي بالأدلة المحايدة وهي لا علاقة لها من قريب أو بعيد بموضوع الجرم وإنما تساهم في التأكد من مدي سلامة الدليل الرقمي المقصود من حيث عدم تغيير أو تعديل في النظام المعلوماتي .

ويمكن الوقوف علي انه اذا توافرت الشروط العامة للدليل الإلكتروني، فأنه من غير الجائز أن يجحده القاضي إذ كونه بوصفه دليلاً علمياً، فأن دلالالته قاطعة بشأن الواقعة المستشهد بها، فأذا كان خالصاً دون عبث أو خطأ، فلا يمكن رده استناداً لفكرة الشك، إذ أن القاضي يلجأ لذلك في حالة ما إذا كان هناك ما يرقي لمستوي التشكيك في الدليل وهو ما لا يمكن إعماله إذا توافرت شروط صحته، فيكون دوره متقصراً علي بحث صلته بالجرم المرتكب. هذا ويلاحظ أن الخبرة الفنية تحتل دورا ليس بالهين في التأكد والتثبت من صلاحيته كدعامة لعقيدة ووجدان القاضي، فبحث مصدقيته وصحته الفنية هي من صميم عمل الخبير وليس القاضي .

هذا ولا يجوز الخلط بين الشك الذي يعتري الدليل المعلوماتي نتيجة العبث أو لوجود خطأ وبين القيمة القانونية (أو الحجية الإثباتية) له إذ انه في الفرض الأول لا يملك القاضي الفصل فيها، حيث انها مسألة فنية فيكون القول الفصل فيها لأهل الخبرة، فأذا

ثبت صحة الدليل من التلاعب فليس للقاضي غير الأخذ به أو قبوله فلا يمكنه التشكيك في حجيته القانونية أو قيمته في الإثبات، إذ إنه- بحكم طبيعته التقنية الفنية – يمثل إنعاكساً حقيقاً للواقع مالم يثبت عكس ذلك (عدم صلته بالجرم المرتكب).

ومن الجدير بالذكر في هذا الصدد، أن تناول الجريمة المعلوماتية وكذا الدليل الإلكتروني الناتج من منظور المبدأ الدستوري المستقر في غالبية الدول وهو مبدأ الشرعية الجنائية له أهميته القصوي ودلالته القوية، إذ يقرر أن لا جريمة ولاعقوبة إلا بنص أو بناءاً علي قانون. هذا ومع التقدم الهائل في عصر المعلوماتية، واجهت بعض الدول المتقدمة هذه الظاهرة بتشريعات حددت هذه الأفعال بأركانها المادية أو المعنوية وكذا عقوبتها .

هذا ويمكن القول بأنه لا يوجد ما يمنع من أن تأخذ المحاكم الجنائية بالأدلة المعلوماتية حيث أن القضاء الجنائي في الغالب الأعم لا يواجه مشاكل عكس ما هو مزعوم – في التعامل مع الأدلة المعلوماتية الرقمية وذلك لعدة أسباب منها:

١- وضوح تلك الأدلة ودقتها في إثبات العلاقة بين الجاني والجرم من ناحية وبين الجاني و المجني عليه من ناحية أخري .
٢- بناء هذه الأدلة علي نظريات ومعلومات حسابية – غالباً- ما تكون مؤكدة أو صحيحة لا يتطرق إليها الشك مما يدعم ويقوي من تقنيتها.
٣- ارتباط هذه الأدلة بالجرائم المعلوماتية وكذا آثارها وخاصة في مرحلة المحاكمة الجنائية.
٤- إمكانية وسهولة تعقب آثارها وكذا الوصول لمصادرها بدقة شديدة.
٥- الثقة و الكفاءة التي اكتسبتها أنظمة الكمبيوتر والشبكات المعلوماتية (الإنترنت) والتي حققتها في المجال المعلوماتي .
٦- دعم هذه الأدلة عبر آراء الخبراء الفنيين و المتخصصين، إذ للخبير دور كبير في الكشف عن الأدلة وفحصها وتقديرها وعرضها أمام القضاء في المواد الجنائية وفقاً لما قرره القانون والقضاء.

أولاً: نتائج هذه الدراسة :

يمكن القول بأن هذه الدراسة البحثية أدت لعدة نتائج يمكن إجمالها فيما يلي :

١- إن الأدلة المعلوماتية (الرقمية الإلكترونية) هي وسائل إثبات في المسائل والمواد الجنائية انبثقت عن التقدم العلمي التقني الضخم في مجال الإتصالات وتكنولوجيا المعلومات كان لها أثر كبير في النظرية العامة للإثبات وخاصة في المجال الجنائي .

٢- إذا كانت الأدلة الجنائية جمعيها تصلح – طبقا للقواعد العامة – للإثبات الجنائي ، فان البحث عن الأدلة الإلكترونية يلزم أن يكون بوسائل مشروعة وليس بأي وسيلة أخري كما يعد هذا الدليل الإلكتروني الوسيلة الرئيسية لإثبات الجرائم المعلوماتية أو حتي التي تقع علي الوسائل الإلكترونية .

٣- إن القاعدة العامة المتفق عليها في الفقه والقضاء الجنائيين وخاصة فيما يتعلق بسلطة القاضي الجنائي في تقييم هذه الأدلة هي قاعدة حرية القاضي في تكوين عقيدته وقناعته، إذ له أن يستقي عقيدته ويستمد وجدانه من هذا الدليل إذا اطمئن وارتاح إليه وكذا حرية تقيمه عند عرضه عليه .

٤- قبول بعض الأنظمة القانونية وخاصة المتقدم في مجال الإثبات الجنائي – بالنصوص الصريحة في تشريعتها – الأدلة المتحصلة من الوسائل المعلوماتية كوسيلة إثبات، كالنظام الأمريكي .

٥- عدم وضع قواعد وأحكام خاصة للإثبات بالدليل الإلكتروني يتفق وطبيعة هذا الدليل في المواد الجنائية، وإنما ظلت خاضعة للمبادئ العامة في الإثبات المنصوص عليها والجاري العمل عليها في فقه الإجراءات الجنائية فضلاًعن وضوح عجز النصوص التقليدية القانونية للإثبات عن مواكبة الإثبات بالدليل المعلوماتي ومكافحة الجرائم المعلوماتية .

٦- إن الأدلة المعلوماتية كطرق إثبات في المواد الجنائية لها دور كبير في حالات تفتيش الأنظمة الإلكترونية وكذا قواعد معطياتها (بياناتها) فضلاً عن الدور

الجوهري للخبرة الفنية في هذا الإطار فيمكن تطبيق المبادئ العامة في تفتيش أنظمة الكمبيوتر والإنترنت علي الجاني إذا تبين وجود قرائن ودلائل تنبيء بحيازته الأشياء أو أدلة تتعلق بالجرم أو أنه يخفي بيانات أو برامج أو تطبيقات استخدمت في وقوع الجرم .

٧- تعد سهولة محو أوتدمير هذا الدليل في مدة قصيرة من أهم الصعوبات التي تُعرض عملية الإثبات الجنائي لبعض العقبات فضلاً عن مشاكل التخزين المعلوماتي للمعطيات وكذا تشفيرها عن بعد مما يجعلها غير مرئية وغير مفهومة في إثبات الجريمة الإلكترونية والبحث عن أدلتها .

٨- طبقا للقواعد العامة ، يقع عبء إثبات الأفعال الإجرامية الخاصة بالجرائم المعلوماتية علي الإدعاء العام (النيابة العامة) وللمدعي مشاركتها في هذه المهمة (إن أراد) كما يجوز نقل هذا العبء في أحيان أخري منها إلي المجني عليه كما أن للنيابة العامة الإختصاص الأصيل بتفتيش الأجهزة وغيرها مما يتصل بالجرم المعلوماتي – ولأعضاء مأموري الضبط القضائي ذلك الإستثناء فضلاً عن ضرورة تهيئة السلطة القضائية والجهات المختصة بكشف الجرائم بشكل جيد لمواجهة تلك السلوكيات الإجرامية .

٩- انطلاقاً من مبدأ تحقيق العدالة الجنائية وضمان الحقوق وخاصة حق المجني عليه، إنه يتعين حضور الجاني عملية تفتيش جهازه وكذا أجهزة ومعلومات غيره- إذا كان الأمرمتعلقاً بضبط دليل ضده حتي يتسني للمجني عليه مواجهة الجاني – بشرط آلا يتسبب حضوره في أي ضرر (عن إجراء التحقيق).

١٠- وضع القاضي أمام خيارين لا ثالث لهما إما الحكم ببراءة المتهم لعدم وجود نصوص عقابية أوإجراء في كثيرمن الأحيان – وهذا يكون انعكاس سئ علي المجتمع وإما البحث عن حل قضائي لمواجهة المجرم المعلوماتي ومحاكمته عبر محاولة وتفسير النصوص القانونية التقليدية لإدراج هذه الأفعال تحت سلطانها مؤقتاً.

ثانيا : توصيات الدراسة :

هذا وفي خاتمة هذه الدراسة البحثية المتعمقة نوصي بما يلي من توصيات في دعم حجية الدليل الإلكتروني والتعبير الرقمي أو المعلوماتي كي تسهل عملية الإثبات الجنائي بما يتفق مع آليات السياسة الجنائية الحديثة في ارساء نظم جديدة متطورة في مجال العدالة الجنائية .

١- وضع مفهوم (أو تعريف) واضح ومحدد للدليل المعلوماتي (الرقمي) والإعتراف بحجيته القانونية كدليل إثبات في المعاملات القانونية بوجه عام والمواد الجنائية بوجه خاص أو حتي ادراجه تحت مظلة أحد أدلة الإثبات المتعارف عليها حتي لا تخضع للسلطة التقديرية للمحاكم.

٢- إلزام أو التزام الدول والحكومات بوضع قوانين وسياسات تشريعية (تشريعات) واضحة جلية فيما يتعلق بمكافحة الجرائم المعلوماتية وسرعة تطورها فضلاً عن التعديل السريع والمواكب للتقدم العلمي للقوانين القائمة أو الحالية المنظمة لتلك الجرائم أو لتداول المعلومات وخاصة عبر الشبكة المعلوماتية (الإنترنت) بما لا يخل أو يخالف حرية تدوالها والنص علي مفاهيم وتعاريف مضبوطة ومحددة غير واسعة أو غامضة لافعال هذه الجرائم في قانون العقوبات وكذا قانون الإجراءات الجنائية.

٣- وجوب النص صراحة من جانب المشرع الإجرائي – وخاصة في فقه الإجراءات الجنائية والإثبات الجنائي – علي شروط الحصول علي الدليل المعلوماتي من حيث مشروعيته وكذا غير قابليته للشك وإمكاينة مناقشته عند عرضه علي القضاء وهذا يتطلب تعديل قوانين الإجراءات الجنائية وغيرها من القوانين المتصلة بهذا الأمر بما يتوافق وطبيعة الجريمة المعلوماتية وبما يساعد في اكتشافها وإثبات إرتكابها وملاحقة وتعقب مرتكبيها وكذا لا بد من النص صراحة علي آليات محددة بشأن التعامل مع هذا الدليل ودوره في الإثبات جنباً إلي جنب مع الضبط والشهادة والخبرة و التفتيش والمعاينة .

٤- التأكيد علي مشروعية الحصول علي هذا الدليل بغير أي مخالفة لأحكام الدستور أو القانون وكذا عدم قابيلته للشك (يقينيته) وإمكانية مناقشته عند طرحه، هذا فضلاً عن الحفاظ على أسرارالجاني غير المتعلقة بالجرم من الإطلاع عليها بمعني إلتزام القائم بالتفتيش بواجب الحيطة والحذر أثنائه؛

فليس له الإطلاع إلا علي ما قد يكون له علاقة بالجريمة (أشياء أو أماكن) وكذا عدم استرساله في الإطلاع علي ما يجده بمحض الصدفة وعدم اطلاع غيره علي محتويات محل التفتيش (معلومات الحاسب)

٥- الإعتراف بصفة المحرر الإلكتروني لمخرجات النظام المعلوماتي، ومن ثم اعتباره حجة في الإثبات الجنائي مع الأخذ في الإعتبار بين إجازة (جواز) المساس بحرمة الحياة الخاصة وحالات الضرورة وخاصة فيما يتعلق بطبيعة هذه الجريمة والدليل المراد استخدامه في إثباتها .

٦- إصدار قانون (أو تشريع) يرسي ويؤكد دعائم وضع نظرية متكاملة للدليل المعلوماتي تتناول أوضاعه وصوره وشروط صحته وحجيته وقيمته القانونية في الإثبات الجنائي ووضع إطار عام للقواعد التقنية الفنية التي غالباً ما يلجأ إليها العاملون به ومعالجة مسائل الإثبات المتصل به .

٧- نشر الوعي المجتمعي بالمخاطر الإقتصادية والسياسية والاجتماعية والثقافية المنبثقة عن الاستخدام غير الآمن للإنترنت وكذا توعية مستخدم الحاسوب وشبكاته المعلوماتية بخطوره الجرائم التي قد ترتكب عبر استخدامه وضروة الحماية منها والابلاغ والإرشاد عن مجرميها فضلاً عن تبني استراتيجية قومية لتنمية الرصد والتوعية والتحقيق بتلك الجرائم المعلوماتية .

٨- العمل وطنياً وإقليمياً و التنسيق مع الدول العربية والإفريقية ودول منطقة الشرق الأوسط ودولياً (الدول الغربية الكبري) لتحقيق استراتيجية وخطة عمل عاجلة لمكافحة الجريمة الإلكترونية والإستفادة من خبرات جميع الدول بعضها البعض. وهذا يعني ضروة التعاون بين الأجهزة المعنية في هذه الدول لتبادل الخبرات في مجال الاتصالات وتكنولوجيا المعلومات وكذا فيما يخص أدلة الإثبات المعلوماتية الحديثة بهدف تحقيق الأهداف والغايات المنشودة لتحقيق عدالة جنائية رشيدة وكذا قضاء عادل .

٩- ضروة إصدار دليل ارشادي تقني وقانوني Practical Legal Guide حول أشكال وصور الجرائم الإلكترونية وشبكات المعلوماتية والأصول العلمية لكشفها والتحقيق فيها وملاحقة مرتكبيها وأساليب التعامل مع الأدلة الرقمية وغيرها من الأدلة المعلوماتية ذات الصلة بهذة الجرائم ومواصلة

تحديث هذه الأدلة بشكل دوري كلما دعت الحاجة لذلك وتعميمه علي العاملين في مجال التحقيق في الميدان وعلي الأجهزة القضائية وعلى المشتغلين في هذا المجال قانونياً وفنياً ومعلوماتياً فضلاً عن الاستفادة من الدليل الصادر عن المنظمة العالمية للشرطة الجنائية (الأنتربول الدولي).

١٠- تدخل القاضي الجنائي في الأحوال التي تغيب فيها النصوص الجنائية – المنظمة لهذه الجرائم وحتي لكيفية إثباتها بالأدلة الإلكترونية بالتفسير طبقاً للقواعد المقررة فقهاً كي لا يتحول من قاضٍ إلى مشرع، فيجمع بين سلطتين وهم القضائية والتشريعية، إذ تم الفصل بينهما حمايةً للحقوق الفردية والحريات العامة .فضلاً عن تنظيم ورش عمل ودورات ومؤتمرات تدريبية وخاصة للقضاة المحليين بصفة دورية ومنتظمة تساعدهم علي تطوير ثقافتهم القانونية ومنها التقنيات الحديثة وكيفية استخدامها في ارتكاب هذه الجرائم مع استحداث دوائر متخصصة بالمحاكم الجنائية في هذه النوعية من الجرائم إذ أن كل ذلك يسهم ويساعد في بناء مبادئ قانونية وقضائية جديدة تحتاجها الأنظمة القانونية الكلاسيكة المستقرة .

وختاماً نخلص أن الجرائم المعلوماتية وما يتصل بها من مسائل إجرائية أهمها إثباتها بالأدلة الإلكترونية وإن كانت تبدو إنها منظمة من قبل بعض التشريعات إلا إنها تثير العديد والكثير من الصعوبات والمشاكل وخاصة بتحديد شخص الجاني وخاصة إذا ما كان مقيماً خارج الدولة – فيصعب تحديد المسئول جنائياً – إذا وقعت الجريمة عبر الإنترنت وكذا مسائل الإثبات لذا يجب علي التشريع ألا يكون قاصراً علي تنظيم ما هو موضوعي إنما عليه أن يصاحب ما هو موضوعي بكل ما هو إجرائي وذلك كي يتحقق نوع من التوازن بين الحق أو المصلحة وطريقة الوصول إليه (إليها).

"تم بحمد الله تعالى وتوفيقه"

قائمة المصادر والمراجع

أولاً: المراجع العربية

١. د/ نائلة عادل قوره، جرائم الحاسبات الاقتصادية: دراسة نظرية وتطبيقية، دار النهضة العربية ،٢٠٠٤.

٢. د/ رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة والمواثيق الدولية، دار النهضة العربية، طبعة أولى ، ٢٠١١.

٣. الدستور المصري الحالي ٢٠١٤(دستور جمهورية مصر العربية)

٤. د/ عبد العظيم مرسي وزير، شرح قانون العقوبات، دار النهضة العربية،١٩٨٣.

٥. د/ أحمد فتحي سرور، القانون الجنائي الدستوري، دار الشروق، طبعة ثانية،٢٠٠٢.

٦. د/ رمسيس بهنام، الإجراءات الجنائية تأصيلاً وتحليلاً، منشأة المعارف ، الإسكندرية،١٩٨٤.

٧. د/ جلال ثروت، نظم الإجراءات الجنائية ، دار الجامعة الجديدة ،الإسكندرية ، ٢٠٠٣.

٨. د/ على محمود حموده، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، اكاديمية شرطة دبي (٢٠٠٣).

٩. د/ حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة، دار النهضة العربية،(٢٠٠٩).

١٠. د/ هلال عبد الله أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة ٢٣ نوفمبر ٢٠٠١، دار النهضة العربية،٢٠٠٢.

١١. د/ آمال عبد الرحيم عثمان، الإثبات الجنائي ووسائل التحقيق العلمية، دار النهضة العربية ١٩٧٥.

١٢. د/ سعيد عبد اللطيف حسن ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت: الجرائم الواقعة في مجال تكنولوجيا المعلومات، طبعة أولى ، دار النهضة العربية،١٩٩٩.
١٣. د/ أحمد عوض بلال، الإجراءات الجنائية المقارنة والنظام الإجرائي في المملكة العربية السعودية، دار النهضة العربية، القاهرة، طبعة خمسة (٢٠١٣).
١٤. حسنين المحمدي البوادي، الوسائل العلمية الحديثة في الإثبات الجنائي، منشأة المعارف،الإسكندرية، طبعة أولى (٢٠٠٨).
١٥. الدكتور/ هشام محمد رستم، الجوانب الإجرائية للجرائم المعلوماتية: دراسة مقارنة، مكتبة الآلآت الحربية، أسيوط ،١٩٩٤.
١٦. د/ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت: دراسة متعمقة في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة،٢٠٠٢.
١٧. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، ٢٠٠١.
١٨. د/ رمزي رياض عوض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها: دراسة تحليلية تأصيلية مقارنة ، دار النهضة العربية،١٩٩٧.
١٩. د/ هشام محمد رستم، جرائم الحاسوب كصوره من صور الجرائم الإقتصادية المستحدثة ، مجلة الدراسات القانونية، العدد ١٧، جامعة أسيوط،١٩٩٥.
٢٠. د/ فتوح الشاذلي ود/ عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون: دراسة مقارنة ، منشورات الحلبي الحقوقية، بيروت،٢٠٠٣.
٢١. د/ أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية،القاهرة، ١٩٩٤.

٢٢. د/عبد الحافظ عبد الهادي عابد، الإثبات الجنائي بالقرائن: دراسة مقارنة، دار النهضة العربية، القاهرة،١٩٩٨.
٢٣. د/ أحمد حسام تمام، الجرائم الناشئة عن استخدام الحاسوب: الحماية للحاسوب- دراسة مقارنة، دار النهضة العربية، القاهرة ٢٠٠٠.
٢٤. د/ محمد الأمين البشري، الأدلة الجنائية الرقمية: مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب- المجلد١٧- العدد٣٣- السنة ١٧ – الرياض، إبريل (٢٠٠٢).
٢٥. ممدوح عبد الحميد عبد المطلب،البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت- دار الكتب القانونية- القاهرة (٢٠٠٦).
٢٦. المرسوم السلطاني العماني رقم ٧٢ لعام ٢٠٠١.
٢٧. د/ عمر سالم، شرح قانون العقوبات المصري، دار النهضة العربية- القاهرة – ٢٠١٠ .
٢٨. د/ هدى حامد قشقوش، شرح قانون العقوبات – دار النهضة العربية- القاهرة- ٢٠١٠.
٢٩. مجموعة أحكام المحكمة الدستورية العليا المصرية في القضية رقم ٤٨ لسنة ١٧ قضاء دستوري جلسة ١٩٩٧/٢/٢٢ و القضية رقم ١١٤ لسنة ٢١ قضاء دستوري جلسة ٢٠٠١/٦/٢ و في القضية رقم ٤٩ لسنة ١٧ قضاء دستوري جلسة ١٩٩٦/٦/١٥و في القضية رقم ٥٩ لسنة ١٨ قضاء دستوري جلسة ١٩٩٧/٧/٥
٣٠. راجع د/ ابراهيم حامد طنطاوى و د/ على محمود حموده، شرح الأحكام العامة لقانون العقوبات –الجزء الأول، النظرية العامة للجريمة- دار النهضة العربية- القاهرة ،٢٠٠٧.
٣١. قانون حماية الملكية الفكرية المصري رقم ٨٢ لسنة ٢٠٠٢.
٣٢. قانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤.

٣٣. قانون الطفل المعدل رقم ٢٦ لسنة ٢٠٠٨.
٣٤. د/مامون محمد سلامه،الإجراءات الجنائية في التشريع المصري- دار الفكر العربي، القاهرة (١٩٨٨).
٣٥. د/أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة السابعة (١٩٩٦).
٣٦. محمد محمد شتات، فكرة الحماية الجنائية لبرامج الحاسب الآلي – دار الجامعة الجديدة- الإسكندرية (٢٠٠١).
٣٧. د/ هلالي عبد اللاه أحمد – حجية المخرجات الكمبيوترية في الإثبات الجنائي طبعة أولى ، دار النهضة العربية، القاهرة،١٩٩٧.
٣٨. د/ جميل عبد الباقي الصغير- أدلة الإثبات الجنائي والتكنولوجيا الحديثة (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية): دراسة مقارنة – دار النهضة العربية ، القاهرة،٢٠٠١.
٣٩. د/ خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي،الإسكندرية، ٢٠٠٩.
٤٠. هلال بن محمد البوسعيدي- الحماية القانونية والفنية لقواعد المعلومات المحوسبة: دراسة قانونية فنية مقارنة – دار النهضة العربية،القاهرة،٢٠٠٩.
٤١. سامي حمدان الواشدة، قاعدة استبعاد الأدلة غير المشروعة في الإجراءات الجزائية، المجلة الأردنية في القانون والعلوم السياسية،جامعة مؤتة، الأردن، المجلد ٣،العدد ٢،٢٠١١،٣.
٤٢. شمسان ناجي الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت:دراسة مقارنة ، دار النهضة العربية،القاهرة،٢٠٠٩.
٤٣. أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، مكتبة الجامعة، الطبعة الأولى،الشارقة،٢٠١٢.

٤٤. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى ،٢٠٠٧.
٤٥. د/ جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة: دراسة في الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠١٢.
٤٦. د/ محمود محمود مصطفى، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، طبعة ١١ ،١٩٧٦ .
٤٧. د/ حسين بن سعيد الغافري،السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة، دار النهضة العربية،القاهرة،٢٠٠٩.
٤٨. د/ جميل عبد الباقي الصغير،المواجهة الجنائية لقرصنة البرامج التلفيزيونية المدفوعة: دراسة مقارنة، دار النهضة العربية، القاهرة،٢٠٠١.
٤٩. د/ هلالي عبد اللاه أحمد، إلتزام الشاهد بالاعلام في الجرائم المعلوماتية: دراسة مقارنة، النسر الذهبي،القاهرة،٢٠٠٠.
٥٠. قانون الإثبات في المواد المدنية والتجارية المصري.
٥١. د/ على حسن الطوالبة، التفتيش الجنائي على نظام الحاسوب والإنترنت: دراسة مقارنة، طبعة أولى،عالم الكتب الحديث، اربد،٢٠٠٤.
٥٢. المستشار ادوارد غالي الذهبي،الإجراءات الجنائية في التشريع المصري والمقارن، مكتبة غريب، القاهرة،(طبعة منقحة ومزيدة) طبعة خمسة،٢٠١٠.
٥٣. د/ ثروت عبد الحميد، التوقيع الإلكتروني: ماهيته، مخاطره، وكيفيه مواجهته، مدى حجيته في الإثبات، الجلاء الجديدة، المنصورة،٢٠٠١.
٥٤. د/ طارق سرور، ذاتية جرائم الإعلان الإلكتروني: دراسة مقارنة ، دار النهضة العربية، الطبعة الأولى،القاهرة،٢٠٠١.
٥٥. د/ محمد السيد عرفه، التجارة الإلكترونية عبر الإنترنت: مفهومها، القاعدة القانونية التى تحكمها، ومدى حجية المخرجات في الإثبات، دراسة مقدمة إلى

المؤتمر المنعقد بكلية الشريعة والقانون بجامعة الإمارات العربية المتحدة (في موضوع القانون والكمبيوتر والإنترنت) من ١-٣ مايو ٢٠٠٠.

٥٦. د/ غنام محمد غنام،عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر (٢٠٠٠)

٥٧. د/ محمد سامى الشوا، ثورة المعلومات وانعكاستها على قانون العقوبات، دار النهضة العربية، القاهرة- ١٩٩٤.

٥٨. د/ مدحت عبد الحليم رمضان، جرائم الإعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة(٢٠٠٠)

٥٩. د/ مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية،(٢٠٠١).

٦٠. د/هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن – دار النهضة العربية، القاهرة، ١٩٩٢.

٦١. د/هشام فريد رستم، الحماية الجنائية لسرية السوابق القضائية، مكتبة الآلآت الحديثة،أسيوط ،١٩٩٥.

٦٢. د/ محمد السعيد رشدي، حجية وسائل الإتصال الحديثة في الإثبات، دار النهضة العربية-القاهرة-١٩٩٩.

٦٣. د/ حسن عبد الباسط جميعي،إثبات التصرفات القانونية التى يتم إبرامها عن طريق الإنترنت – دار النهضة العربية-القاهرة-٢٠٠٠.

٦٤. د/أشرف توفيق شمس الدين، الصحافة والحماية الجنائية للحق في الخصوصية : دراسة مقارنة (١٩٩٩).

٦٥. على حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، بحث منشور عبر موقع لكلية الحقوق بجامعة العلوم التطبيقية، مملكة البحرين (٢٠٠٩).

٦٦. د/ محمد الأمين،العدالة الجنائية ومنع الجريمة: دراسة مقارنة ، طبعة أولى، اكاديمية نايف العربية للعلوم الأمنية، الرياض ١٩٩٧.

٦٧. د/ لؤي عبد الله نوح، مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي (٢٠١٨).
٦٨. د/ لؤي عبد الله نوح، حجية مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي:دراسة مقارنة ،مركز الدراسات العربية للنشر والتوزيع- القاهرة - ٢٠١٨.
٦٩. د/ محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص- الطبعة الثانية، دار النهضة العربية، القاهرة ١٩٩٤.
٧٠. انظر د/ فوزية عبد الستار، قانون العقوبات- القسم الخاص – الطبعة الثانية- دار النهضة العربية، القاهرة،٢٠٠٠.
٧١. د/ عمر الفاروق الحسيني،المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية: دراسة تحليلية نقدية لنصوص التشريع المصري مقارناً بالتشريع الفرنسي- دار النهضة العربية- القاهرة، الطبعة الثانية ١٩٩٥.
٧٢. قانون العقوبات المصري الصادر عام ١٩٣٧ وتعديلاته.
٧٣. أ. محمد رفيق البطوطي و أ. محمد أحمد حسن، قانون العقوبات في ضوء أحكام محكمة النقض، طبعة نادي القضاة- المجلد الأول-٢٠٠٣ .
٧٤. د/ محمد حسام لطفي، الإطار القانوني للمعاملات الإلكترونية:دراسة في قواعد الإثبات في المواد المدنية والتجارية مع إشارة خاصة لبعض قوانين البلدان العربية، القاهرة٢٠٠٢.
٧٥. الدكتور/ محمد حسام الدين لطفي،استخدام وسائل الإتصال الحديثة في التفاوض على العقود وابرامها (يونيو ١٩٩٨).
٧٦. د/أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات: دراسة مقارنة، دار النهضة العربية- القاهرة (طبعة ثانية)،١٩٨٩.
٧٧. د/ محمد فهمي طلبة (وآخرون)،دائرة معارف الحاسب الإلكتروني- مجموعة كتب دلتا- مطابع المكتب المصري الحديث، القاهرة،١٩٩١.

٧٨. قانون أصول المحاكمات الجزائية الأردني.
٧٩. د/ عبد الحافظ عبد الهادي عابد،الإثبات الجنائي بالقرائن: دراسة مقارنة، دار النهضة العربية، القاهرة،١٩٩٨.
٨٠. د/ محمد المرسي الزهرة، مدى حجية التوقيع الإلكتروني في الإثبات في المواد المدنية والتجارية، جامعة الكويت ١٩٨٩.
٨١. عباس العبودي، التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني، دار الثقافة للنشر، عمان، طبعة ١٩٩٧.
٨٢. د/ اسماعيل غانم، أحكام الالتزام والإثبات، الجزء الثاني، مكتبة عبد الله وهبه،١٩٦٧ .
٨٣. د/ محمود نجيب حسني، شرح قانون العقوبات- القسم الخاص، دار النهضة العربية، القاهرة، طبعة أولى (١٩٨٨).
٨٤. أ/ أحمد أمين- شرح قانون العقوبات الاهلى- القسم الخاص- الطبعة الثانية،١٩٢٤.
٨٥. عمر محمد يونس،الإجراءات الجزائية عبر الإنترنت في القانون الأمريكي، دار النهضة العربية- القاهرة- طبعة أولى (٢٠٠٢).
٨٦. محمد أحمد المنشاوي- سلطة القاضي الجنائي في تقدير الدليل الإلكتروني- بحث منشور في مجلة الحقوق،الكويت،جامعة الكويت،العدد ٢،السنة ٣٦.
٨٧. د/ مأمون محمد سلامه،الإجراءات الجنائية في التشريع المصري، الجزء الأول، دار النهضة العربية ،القاهرة،٢٠٠١.
٨٨. د/ عبد الله على محمود، إجراءات جمع الأدلة في مجال الجرائم المعلوماتية، دار الفكر العربي، القاهرة، طبعة أولى،(٢٠١٣).
٨٩. رأفت عبد الفتاح حلاوه، الإثبات الجنائي وقواعده وأدلته، دار النهضة العربية، القاهرة، طبعة أولى،(٢٠١٣).
٩٠. عبد الحميد الشواربي، الإثبات الجنائي في ضوء الفقه والقضاء، منشأة المعارف،الإسكندرية-(١٩٩٨).

٩١. جميل الشرقاوي،الإثبات في المواد المدنية والتجارية والجنائية، دار النهضة العربية، القاهرة، طبعة أولى، (١٩٨٢).
٩٢. د/محمد حسين منصور –المسئولية الإلكترونية ، دار المعارف –الإسكندرية ٢٠١٠
٩٣. د/ أحمد ابو الوفا، التعليق علي نصوص قانون الإثبات، منشأة المعارف، الإسكندرية (2003).
٩٤. ممدوح منير الجهيني، قوانين اليونسترال النموذجي في مجال التجارة الإلكترونية، دار الفكر الجامعية للنشر،الإسكندرية (٢٠٠٦).
٩٥. د/ محمد حسين منصور،الإثبات التقليدي والإلكتروني – دار الفكر الجامعي،الإسكندرية (٢٠٠٦).
٩٦. د/ محمد حسين منصور، مباديء الإثبات وطرقه– دار الفكر الجامعي،الإسكندرية (٢٠٠٦).
٩٧. أميرفرج يوسف، التوقيع الإلكتروني – دار المطبوعات الجامعية –الإسكندرية ٢٠٠٨.
٩٨. د/ أشرف توفيق شمس الدين : الحماية الجنائية للنشر الإلكتروني : دراسة مقارنة دار النهضة العربية، القاهرة، الطبعة الأولي ، ٢٠٠٦.
٩٩. د/ أيمن سعد سليم التوقيع الإلكتروني : دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٤.
١٠٠. د / عبد الرازق السنهوري ، الوسيط في شرح القانون المدني ، الجزء الثاني – الإثبات، آثار الالتزام، دار إحياء التراث العربي (١٩٨٢).

ثانياً: المراجع الأجنبية

1 David Gray, Danielle K.Citron, &Liz C.Rinehart, Fighting Cyber Crim After United States v.Jones, 103 Journal of Criminal Law & Criminology 3 (2013).
2 Susan W. Brenner, State Cyber Crime Legeslation in the United States of America: A Survey, 7 Richmond J. of Law & Technology 3 (2001).
3 Okin S.Kerr, Cyber crime's Scope: Intepreting "Acess" and "Authorization" in Computer Misuse Statutes, 78 New York Univ.L Rev.1596(2003).
4 Janaletchumi Appuderai and Chita Rama lingam, Computer Crimes: A Case Study of What Malysia Can Learn from Others? 2 Jounal of Digital Forensics Security, and Law 2 (2007).
5 Jonathun Mayer, Cyber Crime Litgation, 164 Pennsylvaina L. Rev. 145(2016).
6 Eric J.Sinrod and William P.Reilly, Cyber-crimes:A Practical Approach to the Application of Federal Computer Crime Laws,16 Santa Clara High Technology Law Journal 2 (2000).
7 Richard C.Hollinger and Lonn Lanza-Kaduce, The Process of Criminalization: The Case of Computer Crime Laws, 26 Criminology 101,116 (1988).
8 United States V.Simons, 29 f.supp.2d 324 (E.D.va.1988).
9 O'Hara E. Chevles,Fundemantels of Criminal Investigations,3rd Ed.(1973).
10 Konn Parker, Fighting Computer Crime:A New Framework for Protecting Information,New York,John Wiely (1998).
11 United States Sentencing Commission, Sentencing Guidlines for United States Courts, Part II, 62 Fed. Reg. 26616(1997).
12 Robert Richardson, Hackers: Devils or Saints?Network, June 1997.
13 Mark L. Krotoski, Effectively Using Electronic Evidence before and After aTrial,59 Bulletin of United States Attorney 6(2011).

14 David L.Gripman, The Doors are Locked but the Thieves and Vandarls are Still Getting in:A Proposal in Tort to Alleviate Corporate America's Cyber-crime Problem,16 J.Marshell J.Computer &Info.L.167,169-70 (1997).
15 John Nikell and John Fisher, Crime, Science, and Methods of Forensic Detection, Lexington, Univi.of Kentuchky (1999).
16 Ronald L. Mendle, Investigating Computer Crimes:A Primer for Security Manger, New York (Charles Thomas 1998).
17 United States V.Sablan, 92f, 3d867(9thcir.1996)
18 United States v. Czubinski,106 F.3d 1069,1078 (1st cir.1997)
19 National Information Infrastructutre Protection Act of 1996: Hearings on S.982,104 th Cong.90 (1996).
20 Brent schneider, High- Technology Crime: Investigating Cases Involving Computers,(San Jose:KSK Publications 1999).
21 Howard W.Cox, Recent Develpomats and Trends in Searching and Seizing Electronic Evidence,59 The United States Attorney Bulletin 6 (2011).
22 John Parade, Droit Penal General, CuJus (2002-2003) No.181.
23 Richard Power and Rik Farrow,Electronic Commerce Crime,Includes Related Article on Exerpt from a Hacker's Email,Internet/Web/Online Service Information,Network,Dec.1997.
24 Richard Raysman & Peter Brown,Virsues, Worms, and Other Destructive Forces, N.Y.L.J., July 13,1999.
25 Model Law on Electronic Commerce Guide to Enactment (1996), arts. (6) & (7) .
26 Haeji Hong, Hacking through the Computer Fraud and Abuse Act,31 U.C.Davis L.Rev (1997).
27 Wendy Davis, ProsecutorsWatching the Web Street Crime is Down but that May Just Mean its Moving Online,158 N.L.J.935 (1999).
28 United States V.Colterman, 637F.3d 1068 (9th cir.2011).
29 United States V.Abbouchi,502 F.3d 850,855 C (9th Cir)
30 United States V.Morris,928 F.2d 504,505 (2nd cir.1991)

31 Robyn E. Bumner, Government Want to Bore Web Pee- phole, St. Petersburg Times, March 12,2000.
32 Carlos Albert O Rohrmann, Legal Aspects of Electronic Criminal Evidence in Brazil, 20 International Rev.of Law, Computers,& Technology Journal 182 (2007).
33 Francis Lim, Is Electronic Evidence Admissible in Criminal Case? Inquirer.Net, March13, 2018.
34 D.Glenn Baker,Trespassers Will be Prosecuted:Computer Crime in the 1990's,12 Computer Law Journal 1 (1993) .
35 Orin S.Kerr,Ex Ante Regulation of Computer Search and Seizure, 96 Va.L.Rev.1241(2010).
36 Criminal Evidence Act of 1992.
37 United States v.Braks,842 F.2d 509,512 (1st cir.1988)
38 Guide to Electronic Commerce Regulations,2002,op.cit
39 United States V.Ickes,393 f.3d 501-06 (4thcir.2000).
40 Thomas A.o'Malley, Using Historical Cell Sit Analysis Evidence in Crimnal Trials, 59 the United States's Attoney 3 Bulliten 6 (2011).
41 State of Connecticut v. Swinton, 847 A.2d 921 (S.Ct.couu.2004).
42 Williams v.Long, 2008 WL 4848362 (D. md., April 7,2008) .
43 Bank v.Eurich, 831N.E 2d 909 (S.J.c mass., August 3,2005).
44 Police and Criminal Evidence Act 1984,op-cit-p.25&281.
45 Naughan Bevan and Ken Lidstone, A Guide to the Police and Criminal Evidence Act 1984. (Bulterworth,London,1985).
46 ABA Standing Committee on Ethics and Professional Responsibility Formal Opinion 06-442, Review and Use of Metadata (August 5, 2006).
47 Vinhnee v.American Express Travel Related Service Company,Inc,336 B.R.437(9th cir.BAP 2005) .
48 People v.Rivera,537 N.E 2d 924 (App.ct. Illinois, April 4,4.1989).
49 McDaniel v.United States, 343 F.2d 789 (5th cir), cert.denied,382 U.S. 826 (1965);people v.McHugh,124 mis.2d 559,560,476 N.Y.S.2d 721,722 (1984).

50 Karl J.Flusche, Computer Crime and Analysis of Computer Evidence it Ain't Just Hackers And Phreakers Anymore! 7 Journal of Information Systems Security 1 (1998).
51 SinisiVincenzo, Digital Signature legeslation in Europe, op.cit.
52 Chris Reed,What is a Signature? 3 Journal of Information,Law,and Technology (J I LT) (2000).
53 Sharon Hatch Hodge, Satellite Data and Environmental Law:Technology: Ripe for Litigation Application,14 Pace Envitl.L.Rev.691-718 (1997).
54 John L. Roberts, Admissibility of Digital Image Data and Animations: Courtroom Concerne, Advanced Imaging 102 (August 1995).
55 United States Department of Justice, Computer Crime and Intellectual Property Section.
56 (CCIPS), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2001).
57 United States v. Evans,892 F.supp.2d 949 N.D.III.(2012), United States v.Wurie,728 F.3d 1,1st cir.(2013).
58 United v.Wlliams, 592 F3.d 511,515-17, 7th cir.(2010).
59 US.Code,Title 18,Crimes and Criminal Procedures, Part,I Crimes,Chapter119,Wire &Electronic Communication Interception and Interception of Oral Communications, March,2015.
60 Valsamis Mitsilegas, EU Criminal Law,Oxford & Port Land, Hart, 2009
61 Council of Europe, The European Convention on Mutual Assistance in Criminal Matters, Strasboung, April 20, 1959.
62 Council Framework Decsion 2003/577/JMA of July 26,2003 on the Execution in the European Union of Orders Freezing Property or Evidence .
63 Kenneth J .Markowitz , Legal Challenges and Market Rewards to the Use and Acceptance of Remote Sensing and Digital Information As Evidience,12 Duke Environmental L. & Policy Forum (2002).

64 JonatheanE.Stern, The Electronic Signatures in Global and National Commerce Act ,16 Berkely Technology Law Journal (2001).
65 C-Bradford Biddle , Misplaced Priorities :The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure ,33 San Diego L.Rev.1146 (1996).
66 Benjamin Beard ,Removing Barriers to E-Commerce :The Unifom
67 Electronic Transactions Act ,Sf06 Al I-ABA B7 -139(2000)
68 David W.Carstens, Contracts Have a New Look Thanks to E-Signature Act,Texas Law , July 31, 2000.
69 Richad Raysmans and Peter Brown, The Impact of the New Federal E- sign New York Law , 224 N.Y.L.J 3 (August 8,2000).
70 Benjamin Wright, Eggs In Baskets : Distrbuting the Risks of Electronic Signatures , 452 PL /I, pat 63.69-70(1996) .
71 15U.S.C.A.S7002(a)(1)8(west sup. 2001)
72 15U.S.C.A.S7003(b)(1)(a)(3).7005(a)- (b)(west sup 2001)
73 Maria Angela Biasiottii , A Proposed Electronic Evidence Exchange Across the European Union, 14 Digital Evidence and Electronic Signatuene L. Rev. (2017).
74 Uniform Commercial Code Sections 1-207 and Article 2 and 2 A, Ss 7003(a)(3).
75 JaneK Winn Open Systems , Free Markets and Regulations of Internet Commerce, 72 Tul .L .Rev. 1177,1232 (1998).