مشروعية الأدلة الإلكترونية في الإثبات الجنائي

د. ميسون خلف الحمداني(*)

المقدمة:

مع التطور الكبير والمتسارع الذي تشهده نواحي الحياة المختلفة، واستعمال التقنيات التكنولوجية في جميع مجالات العمل من استخدام للحاسوب والإنترنت، لم تعد الجريمة تُرتكَب بشكلها التقليدي بل تعَدَّته إلى استعمال شبكة المعلومات باستخدام الحاسب الآلي ونظم المعلومات كأداةٍ في ارتكابها، مما استوجب توفير الحماية القانونية وإيجاد نظام عقابي لمرتكب جرائم الحاسوب وشبكة المعلومات التي رافقت نشوء نظم الحاسوب والشبكات وثورة تقنية المعلومات ونموها وتطورها ؛ لما تنطوي عليه من مخاطر عديدة وخسائر كبيرة تلحق بالمؤسسات والأفراد؛ إذ إنها تستهدف الاعتداء على البيانات والمعلومات وتمس الحياة الخاصة للأفراد، فضلًا عن تهديد الأمن الوطني والسيادة الوطنية، وإضعاف الثقة بالتقنيات الحديثة وتهديد إبداع العقل البشري؛ لذا اقتضى الأمر توفير الحماية القانونية لنظم الحاسوب؛ إذ إن المعلوماتية أضحت وسيلةً لارتكاب جرائم عديدة وخطيرة، منها على سبيل المثال استعمال الإنترنت في ارتكاب جرائم الإرهاب والاحتيال والتزوير واختراق المواقع وارتكاب الجرائم الأخلاقية.

ومن الطبيعي أن يثير البحث عن هذه الجرائم مشاكل وصعوبات في استخلاص الأدلة التي تثبت وقوع الجريمة التي تُدين مرتكبها؛ كونها تختلف عن الأدلة

(*) كلية الحقوق - جامعة النهرين، جمهورية العراق.

التقليدية في الجرائم العادية من حيث خصائصها وأنواعها وسبل ارتكابها وحتى صفات مرتكبيها، كما يثير الدليل الإلكتروني صعوبات تتعلق بعدم ظهوره بشكل مرئي وفقدان الآثار التقليدية للجريمة المعلوماتية، بالإضافة إلى صعوبات متعلقةٍ بسلطات الاستدلال والتحقيق من حيث إحجام المجني عليهم عن الإبلاغ، حرصًا على ثقة العملاء، أو لصعوبة اكتشافها من قِبَل الأشخاص العاديين، فضلًا عن نقص الخبرة في سلطات الاستدلال والتحقيق.

كل ذلك يثير تساؤلات عديدة حول مشروعية وجود الدليل الإلكتروني ومشروعية الحصول عليه، وهو ما حاولنا التعرف عليه في بحثنا هذا.

المبحث الأول
الطبيعة القانونية للدليل الإلكتروني

من المسلَّم به أن تقييم أي نظام قانوني لا يمكن أن يصل إلى نتائج صحيحة إلا إذا توفر لدى المقوِّم تصور واضح لذلك النظام؛ إذ إن الحكم على الشيء فرع تصوره، لذا فإننا نتطلع من خلال هذا المبحث إلى دراسة نظام الأدلة الإلكترونية وتناول هذا النوع من الأدلة بالتعريف؛ ليتسنى لنا فهم ماهيته، لنتمكن في النهاية من الحكم علية وبيان دوره في الإثبات الجنائي.

ولذلك فإننا سنتناول في هذا المبحث ماهية الدليل الإلكتروني من خلال المطلبين الآتيين:

المطلب الأول - ماهية الدليل الإلكتروني:

تتركز عملية الإثبات الجنائي في جرائم الإنترنت على الدليل الجنائي الإلكتروني بوصفه الوسيلة الوحيدة أو الرئيسة لإثبات هذه الجرائم وهو محور اهتمامنا؛ لذا

سنتناول في هذا المطلب تعريف الدليل الإلكتروني وتقسيماته وخصائصه، وذلك في فروع ثلاثة، كما يأتي:

الفرع الأول- تعريف الدليل الإلكتروني:

يعرَّف الدليل الإلكتروني بأنه: «الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، 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 القانون وتطبيقه»[1].

والذي يلحظ على هذا التعريف أنه يقصر مفهوم الدليل الرقمي على ذلك الذي يتم استخراجه من الحاسب الآلي، ولا شك أن ذلك فيه تضييقًا لدائرة الأدلة الإلكترونية، فهي كما يمكن أن تستمد من الحاسب الآلي من الممكن أن يُتحصل عليها من أية آلة أخرى، فالهاتف وآلات التصوير وغيرها من الأجهزة والتي تعتمد التقنية الرقمية في تشغيلها يمكن أن تكون مصدرًا للدليل الإلكتروني.

وعرفت الأدلة الإلكترونية كذلك بأنها «الأدلة التي تشمل جميع البيانات الرقمية التي يمكن أن تثبت أن هناك جريمة قد ارتكبت أو توجد علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت، الصورة».

وتعرف كذلك بأنها «معلومات يقبلها المنطق والعقل ويعتمدها العلم، ويتم الحصول عليها بإجراءات قانونية وعلمية، بترجمة البيانات الحسابية المخزنة في

أجهزة الحاسوب وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أية مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء له علاقة بالجريمة أو الجاني أو المجني عليه».

وعرف آخر الدليل الجنائي الإلكتروني بأنه «الدليل الرقمي يمكن أن يكون أي معلومة محددة أو مخزنة في شكل معالج رموز وأرقام، حيث يستخدمها الحاسوب في إنجاز مهمة ما».

وعرفه آخرون بأنه «مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية».

كما عُرِّف الدليل الإلكتروني أيضًا بأنه «المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية»[2].

وقد عرفت المنظمة العالمية لدليل الكمبيوتر الأدلة ذات الصلة على النحو الآتي: الدليل الإلكتروني الأصلي بأنه «الأشياء المادية أو المعلوماتية المتصلة بهذه الأشياء المادية عند الضبط»[3].

أما الدليل الإلكتروني المزدوج فهو: «كل الأشياء المتعلقة بالبيانات عند ضبط الشيء الملموس أصلًا»[4].

ونرى أن التعريف الأرجح للدليل الإلكتروني هو: «الدليل المشتق من (أو بواسطة) النظم البرامجية والمعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصال، من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميًا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال وأصوات لإثبات وقوع الجريمة أو لتقرير البراءة والإدانة فيها»[5].

الفرع الثاني- تقسيمات الدليل الإلكتروني:

لا يظهر الدليل الرقمي المستخلص من جرائم الإنترنت في صورة واحدة بل توجد له العديد من الصور والأشكال، وقد قسمها البعض[6] إلى الأقسام الرئيسة الآتية:

القسم الأول: الأدلة الرقمية الخاصة بأجهزة الكمبيوتر وشبكاتها.

القسم الثاني: الأدلة الرقمية الخاصة بالإنترنت.

القسم الثالث: الأدلة الرقمية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

القسم الرابع: الأدلة الرقمية الخاصة بشبكة المعلومات العالمية.

ووفقًا لما قررته وزارة العدل الأمريكية سنة (2002) فإن الدليل الإلكتروني يمكن تقسيمه إلى 3 مجموعات[7].

1- السجلات المحفوظة في الحاسوب، وهي الوثائق المكتوبة والمحفوظة، مثل البريد الإلكتروني، وملفات برامج معالجة الكلمات، ورسائل غرف المحادثة على الإنترنت.

2- السجلات التي تم إنشاؤها بواسطة الحاسوب، وتعد مخرجات برامج الحاسوب، وبالتالي لم يلمسها الإنسان مثل (LOG FILES) وسجلات الهاتف وفواتير أجهزة السحب الآلي (ATM).

3- السجلات التي تم حفظ جزء منها بالإدخال وجزء آخر تم إنشاؤه بواسطة الحاسوب، ومن الأمثلة عليها: أوراق العمل المالية التي تحتوي على مُدْخَلات تم إدخالها إلى برامج أوراق العمل (EXCEL) ومن ثم تتم معالجتها من خلال البرامج بإجراء العمليات الحسابية عليها.

ويلحظ أن التنوع في الدليل الإلكتروني يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه وإنما تتعدد وسائل التوصل إليه، وفي كل الأحوال يظل الدليل المستمد منه رقميًا حتى إن اتخذ هيئة أخرى، ففي هذه الحالة يكون اعتراف القانون بهذه الهيئة الأخرى مؤسسًا على طابع افتراضي مَبْناه أهمية الدليل الإلكتروني ذاته وضرورته. ولكي يحدث التواصل بين القانون والدليل المذكور - نتيجة لنقص توافر الإمكانيات الإلكترونية في المحاكم - يلزم اتخاذ مسلك الافتراض من حيث اعتباره دليلًا أصليًا[8] كذلك قسم الدليل الجنائي الإلكتروني قسمين: الأول: أُعِدَّ ليكون وسيلة إثبات، والثاني: لم يعد كوسيلة إثبات. ونتناول في ما يلي كلا النوعين على النحو الآتي[9]:

أولًا- أدلة أُعِدَّت لتكون وسيلة إثبات:

أ) السجلات التي تم إنشاؤها بواسطة الحاسوب تلقائيًا، وتعد هذه السجلات من مخرجات الحاسوب التي لم يسهم الأفراد في إنشائها، مثل سجلات الهاتف وفواتير البطاقة البنكية.

ب) السجلات التي تم حفظ جزء منها بالإدخال، وجزء تم إنشاؤه بواسطة الحاسوب. مثل رسائل غرف المحادثة المتبادلة على الإنترنت ورسائل البريد الإلكتروني[10].

ثانيًا- أدلة لم تُعَدَّ لتكون وسيلة إثبات:

وهذا النوع من الدليل الإلكتروني نشأ من دون إرادة الفرد، وله أثر يتركه الجاني دون أن يكون راغبًا في وجوده، ويسمى «البصمة الإلكترونية»، وتتجسد في الآثار التي يتركها مستخدم شبكة الإنترنت بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكذا الاتصالات كافة التي تمت من خلال الحاسوب وشبكة الإنترنت، حيث إن هذا النوع من الأدلة لم يعد أساسًا للحفظ مِن قِبَل مَن

صدَر عنه، غير أن الوسائل الفنية الخاصة التي تجري عبر الإنترنت والمراسلات الصادرة عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك[12].

الفرع الثالث- خصائص الدليل الإلكتروني:

يتميز الدليل الجنائي الإلكتروني عن الدليل التقليدي بالخصائص التالية:

أولًا- الطبيعة التقنية للأدلة الجنائية الإلكترونية: الأدلة الإلكترونية ذات طبيعة تقنية وفنية، وكيفية معنوية غير ملموسة، لا تدرك بالحواس العادية، ويتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبة الآلية (Hard Ware) واستخدام نظم برامجية حاسوبية[13] (Soft Ware)، فالدليل الإلكتروني - كما أسلفنا - عبارة عن مجالات مغناطيسية كهربائية، ومن ثَمَّ فإن ترجمة الدليل الإلكتروني وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعد هو الدليل، بل إن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الاستدلال بها على معلومة معينة.

ثانيًا- الأدلة الرقمية أدلة علمية: لما كانت التقنية ابنة العلم فكذلك يعد جميع ما ينشأ عنها سببًا في تقرير أن الأدلة الجنائية الإلكترونية هي أدلة علمية يرجع إلى أنها تستمد مما يصنعه أهل العلوم التقنية من آراء واستنتاجات علمية، على ضوء ما يتم الوصول إليه من برامج وأجهزة وبرامج تقنية، والدليل الإلكتروني يعد من طائفة ما يعرف بـ«الأدلة المستمدة من الآلة»[14].

ثالثًا- الأدلة الرقمية متطورة بطبيعتها: الأدلة الرقمية ذات طبيعة ديناميكية فائقة السرعة من مكان لآخر عبر شبكات الاتصال، غير معترفة بحدود الزمان والمكان، وتعتمد الأدلة الجنائية على التطور التلقائي لبيئتها التقنية المتطورة

بطبيعتها، ومن خلال الدليل الإلكتروني يمكن رصد المعلومات عن الجاني وتحليلها في الوقت ذاته، فالدليل الإلكتروني يمكنه أن يسجل تحركات الفرد كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه؛ لذا فإن البحث قد يجد غايته بسهولة أيسر من الدليل التقليدي من هذه الناحية[15].

رابعًا- صعوبة طمس الأدلة الإلكترونية أو حذفها: الأدلة الإلكترونية يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، مما يؤدي إلى صعوبة التخلص منها، وهي خصيصة من أهم خصائص الدليل الإلكتروني بالمقارنة مع الدليل التقليدي، فهناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغاؤها، سواء تم ذلك بالأمر (Delete)، أو حتى لو تم عمل إعادة التهيئة أو التشكيل للقرص الصلب (Hard Disk) باستخدام الأمر (Format)، والبرامج التي تم إتلافها أو إخفاؤها سواء كانت صورًا أم رسومًا أم كتابات أم غيرها (فإن الملف الذي تم حذفه يمكن استرداده باستخدام أداة استرداد للملفات المحذوفة Undeleted Tool)[16]، مما يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة طالما وصل علم رجال البحث والتحقيق الجنائي بوقوع الجريمة[17]، بل إن محاولة الجاني محو الدليل الإلكتروني بذاتها تُسجَّل عليه دليلًا، حيث إن قيامه بذلك يتم تسجيله في ذاكرة الآلة، وهو ما يمكن استخراجه واستخدامه كدليل ضده.

ويزيد من صعوبة التخلص من الأدلة الإلكترونية أنه يمكن استخراج نسخ مطابقة للأصل ولها القيمة والحجية الثبوتية ذاتهما، الشيء الذي لا يتوافر في أنواع الأدلة الأخرى (التقليدية)، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد أو التلف أو التغيير عند عمل نسخ طبق الأصل من الدليل، مما جعل المشرع البلجيكي، بمقتضى قانون 28 نوفمبر 2000م، يقوم بتعديل قانون

التحقيق الجنائي (Code Destruction Criminal) بإضافة المادة (39 Bis) التي سمحت بضبط الأدلة الرقمية مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات، بقصد عرضها على الجهات القضائية[18].

ويترتب على هذه الخصيصة مسائل مهمة في القانون، أبرزها على الإطلاق مسائل التخلص من الدليل، وهي الموضوع المعاقب عليه بمقتضى القانون.

المطلب الثاني - جمع الأدلة الإلكترونية:

هناك أمور رئيسة ينبغي الإشارة إليها، تتعلق بالدليل الإلكتروني، وأول هذه الأمور هو تحديد العلوم التي تمكننا من استخلاص الدليل الإلكتروني وجمعه من مسرح الحادث لتحديد البصمة الإلكترونية، وهذه العلوم نطلق عليها علوم الأدلة الإلكترونية (Digital Evidence Science).

وتشمل هذه العلوم: علوم الكمبيوتر، وعلوم الأدلة الجنائية وعلوم التحليل السلوكي للأدلة الإلكترونية، حيث إن علوم الكمبيوتر تقدم المعلومات التكنولوجية الدقيقة، وهي مطلوبة لفهم المظهر أو الهيئة أو الكينونة الفريدة للدليل الإلكتروني، بينما علوم الأدلة الجنائية من شأنها أن تقدم منظورًا علميًا لتحليل أي شكل من أشكال الدليل الإلكتروني، وتسهم علوم التحليل السلوكي للأدلة الإلكترونية في الربط المحدد بين المعارف التكنولوجية وبين الطرق العلمية لاستخلاص الدليل الإلكتروني، لفهم أفضل للسلوك الإجرامي التقني[19].

وبناءً على ما تقدم نتناول موضوع جمع الأدلة الجنائية الإلكترونية من خلال تقسيم هذا المطلب إلى ثلاثة فروع، نتناول في الأول والثاني وسائل جمع الأدلة الإلكترونية وتخصيصها وتوثيقها، أما الفرع الثالث فنخصصه لتحديد نطاق العمل بالدليل الإلكتروني.

الفرع الأول - وسائل جمع الأدلة الإلكترونية:

توجد الأدلة الإلكترونية عادة في مخرجات الطابعة والتقارير والرسوم، وفي أجهزة الكمبيوتر وملحقاته، وفي الأقراص الصلبة والمرنة وأشرطة تخزين المعلومات، وفي أجهزة المودم والبرامج وأجهزة التصوير ومواقع الويب والبريد الإلكتروني، ولذلك تستخدم عدة وسائل وأدوات تسهم في جمع الأدلة الرقمية منها[20]:

أولًا- برنامج إذن التفتيش Computer Scorch Warrant Program: وهو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات المهمة المطلوبة لترقيم الأدلة وتسجيل البيانات منها، ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل.

ثانيًا- قرص بدء تشغيل الكمبيوتر Bootable Diskette: وهو قرص يمكّن المحقق من تشغيل الكمبيوتر، إذا كان نظام التشغيل فيه محميًا بكلمة مرور (Pass Word)، ويجب أن يكون القرص مزودًا ببرنامج مضاعفة المساحة (Double space) فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.

ثالثًا- برنامج معالجة الملفات X tree pro Gold: وهو برنامج يمكّن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضغوطة، أو يستخدم لقراءة البرامج في صورتها الأصلية، كما أنه يمكن من خلاله البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها[21].

رابعًا- برنامج النسخ Lap Link: هو برنامج يمكن تشغيله من خلال أقراص مرنة، ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى

قرص آخر سواء على التوازي (Parallel Port) أو على التوالي (Serial Port) وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم[22].

خامسًا- برامج كشف الدسك AMA Disk View Disk,: ويمكن من خلال هذا البرنامج الحصول محتويات القرص المرن مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان، نسخة عادية خاصة بالأفراد، ونسخة خاصة بالشرطة[23].

سادسًا- برامج اتصالات مثل LAN Tastic: يستطيع هذا البرنامج ربط جهاز حاسب المحقق بجهاز حاسب المتهم لنقل ما به من معلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب[24].

هذه هي أهم الوسائل العامة لجمع الأدلة الإلكترونية والتي يجب أن يقوم الخبراء بها في هذا المجال، نظرًا لعلمية ودقة هذه الأدلة، ومن وجهة نظر جهات التحقيق فإن جمع الأدلة الإلكترونية يمكن أن يشكل صعوبة نسبية، فبالرغم من أن ملفات الولوج (Log File) تبدو مشابهة للملفات العادية، ويمكن جمعها مثل أي ملف آخر، وهي تحتوي على كمية هائلة من المعلومات التي قد تفيد البحث والتحقيق الجنائي.

إلا أن الصعوبة في جمع هذه المعلومات الجنائية، تتمثل في أن هذه الأدلة عادة ما تكون مختلطة بغيرها من معلومات مستخدمي الكمبيوتر الأبرياء، مما يشكل تهديدًا لخصوصية هؤلاء، ويعد ذلك في الوقت ذاته ضبطًا دون تفويض أو تصريح أو أمر قانوني أو قضائي. لذلك تعمد بعض منظمات تشغيل الكمبيوتر أو الشبكات المعلوماتية إلى عدم إفشاء أسرار جميع ملفات الولوج إلا الخاصة بالمتورطين فقط في قضايا مدنية أو جنائية، وبناءً على أمر قضائي طبقًا للنظام القانوني السائد في الدولة.

وهناك صعوبة أخرىٰ في جمع الأدلة الرقمية من جداول الحالة التشغيلية في البروتوكولات والاتصالات، وتتمثل هذه الصعوبة في أن هذه الجداول تكون متاحة لفترات قصيرة، ولا يمكن التغلب علىٰ هذه الصعوبة بالتحفظ الجنائي علىٰ أجهزة القرص الصلب (Hard Ware) لحين الفحص؛ لأن هذه الجداول تُزال تلقائيًا بمجرد غلق التيار الكهربائي أو انقطاعه عن تلك الأجهزة، لذلك من المستحسن أن يتم استخدام أسلوب القص واللصق (Cut and Post) إلىٰ ملف جديد خاص بجمع الأدلة وقبل غلق الأجهزة. ورغم أن أسلوب القص واللصق أسلوب ناجح بجمع الأدلة إلا أن المشاكل القانونية المترتبة علىٰ قانونية هذا الأسلوب قد تثير بعض الشك في مدىٰ سلامة جمع المعلومات وحجيتها أمام أجهزة العدالة الجنائية[25].

الفرع الثاني - تصنيف الدليل الإلكتروني وتوثيقه:

ذكرنا من قبل أن ملفات الولوج وجداول الحالة التشغيلية يمكن أن تحتوي علىٰ عناوين (IP) للكمبيوتر الوسيط أو الرئيس أو الخادم، وتحتوي علىٰ معلومات من الأنشطة كافة التي قام بها المستخدم أو حاول أن يقوم بها عند استخدامه للشبكة المعلوماتية، وتحتوي كذلك علىٰ معلومات بشأن أنواع الاتصالات التي تمت، وكل هذه المعلومات يمكن أن تستخدم في تصنيف الدليل الإلكتروني وتخصيصه وتوثيقه تجاه الجريمة محل البحث والتحقيق، وملفات الولوج وجداول الحالة التشغيلية يمكن أن تصنف كوحدة معلوماتية كاملة، وهي بذلك يمكن أن تقارن مع وحدة معلوماتية أخرىٰ، وذلك لتحديد الجزء المطلوب للدليل الجنائي[26].

بالإضافة إلىٰ تصنيف ملفات الولوج وجداول الحالة التشغيلية كوحدة معلوماتية كاملة، فإن احتواء هذه الوحدة علىٰ المعلومات الصالحة للتعرف عليها

وتصنيفها وتوثيقها يعطي لها أهمية خاصة في البحث والتحقيق الجنائي، وهناك العديد من أشكال الاتصال باستخدام بروتوكول (TCP) مثل (Wed Telnet, Email,) وهذه الأشكال يمكن أن تصنف بعد إتمام عمليات التصنيف، ويمكن إجراء عمليات مقارنة بين الأفعال المشتبه فيها وبين الأفعال الطبيعية الأخرى، ويلحظ إذا كان الولوج من مشتبه به أو توافرت باقة معلومات عن عنوان (IP) لمستخدم ما، فإن هذا الولوج وهذه المعلومات قد لا تكون مطابقة لمستويات معروفة، ولكن الباحثين الجنائيين في معامل الأدلة الرقمية يمكنهم مقارنة المعلومات المتوافرة مع المعلومات الأخرى الرسمية أو المتفق عليها لاكتشاف الفروق التي يمكن أن تدين المشتبه فيه، حيث إن الطابع الشخصي للأدلة الرقمية في أثناء وجودها في ملفات الولوج أو بروتوكولات الاتصالات والتي يمكن لعلوم التحليل السلوكي للأدلة أن تسهم في اكتشافها عن طريق اختبارات للمقارنة بين الجريمة المرتكبة وسلوك المشتبه فيه المسجل في هذه الملفات، ويتم ذلك باختبارات المقارنة[27].

والأدلة الجنائية الرقمية مثل غيرها من الأدلة المادية تحتاج إلى التوثيق والتأمين، وبالقدر الذي يكفل لها المصداقية ويبعد عنها العيوب، وذلك لأسباب عدة منها[28]:

أولًا: التوثيق الذي يحفظ الأدلة الرقمية في شكلها الأصلي الذي يستعمل لعرض وتأكيد مصداقية الدليل وعدم تعرضه لتحريف أو تعديل، فالصورة المسجلة بالفيديو - مثلًا - يمكن الاستعانة بها في تأكيد مدى صحة المناقشة الحية عن طريق مطابقة النص الرقمي مع النص المصور على الشاشة.

ثانيًا: الأشخاص الذين يقومون بجمع الأدلة عليهم الإدلاء بشهاداتهم حول مطابقة الأدلة التي قاموا بجمعها مع تلك المقدمة أمام المحكمة، والتوثيق هو

الأسلوب الوحيد الذي يمكّن المحققين من القيام بهذا الدور أمام القضاء، ويعد فشل المحققين في التمييز بين أصل الدليل وصورته أمام القضاء سببًا في بطلان الدليل.

ثالثًا: من المهم توثيق مكان ضبط الدليل الرقمي في حالة إعادة تكوين الجريمة؛ إذ إن تشابه أجهزة الحاسوب وملحقاتها يجعل من الصعب إعادة ترتيبها دون توثيق سليم ومفصل يحدد الأجزاء والملحقات وأوضاعها الأصلية بدقة.

رابعًا: يشكل التوثيق جزءًا من عمليات حفظ الأدلة الإلكترونية حتى انتهاء إجراءات التحقيق والمحاكمة؛ إذ إن التوثيق يشمل تحديدًا دقيقًا للجهات التي تحتفظ بالأدلة وقنوات تداولها والتي ينبغي حصرها في نطاقٍ محدودٍ قدر الإمكان[29].

عند توثيق الدليل الرقمي يجب التأكد من أين، كيف، متى، وبواسطة مَن تم ضبط الدليل وتأمينه؟

كما أنه من الضروري توثيق الأدلة الإلكترونية بعدة طرق كالتصوير الفوتوغرافي، التصوير بالفيديو، وطباعة نُسخ من الملفات المخزنة في جهاز الحاسوب أو المحفوظة في الأقراص، وعند حفظ الأدلة الإلكترونية على الأقراص والشرائط يجب تدوين البيانات التالية على كل منها[30]:

- التاريخ والوقت.
- توقيع الشخص الذي قام بإعداد النسخة.
- رسم أو نوع نظام التشغيل.
- رسم البرنامج أو الأوامر المستعملة لإعداد النسخ.
- المعلومات المضمنة في الملف المحفوظ.

الفرع الثالث - نطاق العمل بالدليل الإلكتروني:

نظرًا لتعاظم دور تقنية المعلومات - كما أشرنا سابقًا - خاصة بعد دخول الإنترنت شتى مجالات الحياة، فإن الدليل الإلكتروني هو الدليل الأفضل لإثبات الجرائم التي تقع في هذا الوسط؛ لأنه من طبيعة هذه البيئة ذاتها.

ومن هنا بدت أهمية هذا النوع من الأدلة، ولكن أيعني ذلك أن الدليل الإلكتروني ينحصر مجاله كدليل إثبات فقط على الجرائم المعلوماتية؟

ينبغي التنويه إلى أنه لا تلازم بين نطاق العمل بالدليل الإلكتروني وشكله وإثبات الجريمة المعلوماتية، فمن ناحية فإن الدليل الإلكتروني مثل ما يصلح لإثبات الجريمة المعلوماتية ويعد في الوقت ذاته الدليل الأفضل لإثباتها، فإنه من ناحية أخرى يصلح لإثبات الجرائم التقليدية إن جاز التعبير، حيث يميز الفقه في هذا الشأن بين نوعين من الجرائم[31]:

أولًا- الجرائم المرتكبة بواسطة الآلة: هذا النوع من الجرائم يستخدم فيه الحاسب الآلي والإنترنت كوسيلة مساعدة لارتكاب الجريمة، مثل استخدامه في الغش والاحتيال وغسل الأموال وتهريب المخدرات، وهذا النوع من الجرائم لا صلة له بالوسط الافتراضي إلا من حيث الوسيلة. وبعبارة أوضح فإن الجريمة في هذه الحالة هي جريمة تقليدية استعمل في ارتكابها أداة رقمية، فبرغم عدم اتصال هذه الجريمة بالنظام المعلوماتي إلا أن الدليل الإلكتروني يصلح دليلًا لإثباتها.

ثانيًا- جرائم الإنترنت والآلة الرقمية: هذا النوع من الجرائم يستخدم فيه الحاسب الآلي أو الآلة بصفة عامة، بحيث يكون الاعتداء واقعًا إما على الكيان المادي للآلة - وهذه يمكن اعتبارها جريمة تقليدية تلحق النوع الأول - وإما أن يكون الاعتداء واقعًا على الكيان المعنوي للحاسب أو الآلة، أو على قاعدة

البيانات أو المعلومات التي قد تكون على شبكة المعلومات العالمية، مثل انتهاك الملكية الفكرية وجرائم القرصنة وغيرها، وهذا النوع من الجرائم هو ما يمكن تسميته بـ«جرائم المعلوماتية»، والتي يكون الدليل الإلكتروني هو الدليل الأفضل لإثباتها إن وجد.

ومع ذلك فإننا نعتقد أن الجريمة المعلوماتية رغم شدة صلتها بالدليل الإلكتروني إلا أن إثباتها لا يقتصر عليه، فمن الممكن إثباتها بأدلة الإثبات التقليدية كالشهادة والاعتراف وغيرهما[32].

ولذلك يمكننا أن نقول: إنه لا تلازم بين مشكلة الدليل الإلكتروني وإثبات الجريمة المعلوماتية، فلهذه الأخيرة إشكاليات قانونية أخرى لا شأن لها بالدليل الإلكتروني، فإذا كانت غاية الدليل عمومًا هي إثبات الجريمة ونسبتها إلى مرتكبها، فإن هذا الدليل لا يكون قاصرًا في تقديرنا إذا اقتصر على مجرد إثبات وقوع الجريمة بدون تحديد مقترفها؛ إذ مع ذلك تصح تسميته دليلًا، وتبدو أهمية هذا النوع من الأدلة بالنسبة للجريمة المعلوماتية؛ لصعوبة إثبات وقوعها عادةً.

ومما تقدم نخلص إلى أن الدليل الإلكتروني يصلح لإثبات الجريمة التي ترتكب باستعمال الآلة الرقمية، الحاسوب، الهاتف... إلخ، أو الجريمة التي ترتكب ضد الكيان المعنوي للآلة أو ضد شبكة المعلومات العالمية.

بالإضافة إلى ذلك فإن هذا الدليل يصلح لإثبات بعض الجرائم وإن لم تكن من ضمن النوعين المذكورين، وذلك إذا استعملت الآلة الرقمية للتمهيد لارتكاب الجريمة أو لإخفاء معالمها، كالمراسلات التي يبعث بها الجاني لشريكه، وتتضمن معلومات عن جريمة ينويان ارتكابها، أو يطلب منه إخفاء معالم هذه الجريمة، فتلك المراسلة تصلح دليل إثبات لهذه الجريمة حال وقوعها، رغم أنها لم ترتكب ضد الآلة الرقمية أو بواسطتها.

المبحث الثاني

مشكلات الدليل الإلكتروني

من المعلوم أن الجريمة المعلوماتية كغيرها من الجرائم لها أركانها وعناصرها، وتمر بالمراحل ذاتها التي تمر بها الدعوى الجنائية في شأن الجرائم العادية كالسرقة والقتل، وهذه المراحل هي التفكير في الجريمة والتحضير لها، ثم تنفيذ الجريمة، ومحاولة التخلص من آثارها، ولذلك تثور هنا مسألة (استخلاص الدليل) الذي تثبت به الجريمة المعلوماتية.

وكما نعرف أن الاعتراف هو سيد الأدلة، يليه شهادة الشهود، فضلًا عن القرائن والآثار الناجمة عن النشاط الإجرامي بما لها من دور في إثبات الجريمة المعلوماتية وكشف الحقائق فيها، فهي أمور تعين المحقق على استجواب المتهمين وسؤال الشهود.

وإذا صدق ما سبق بالنسبة لجرائم قانون العقوبات التقليدي، فإن قواعد هذا القانون تبدو قاصرة إزاء ملاحقة مرتكب الجريمة المعلوماتية، مما حدا بالبعض إلى القول إن قواعد قانون العقوبات التقليدية تواجه تحديات إزاء مواجهة الجريمة المعلوماتية، وتبدو قاصرة عن مواجهة العديد من الأفعال التي تهدد مصالح اجتماعية واقتصادية ارتبطت بظهور جهاز الحاسب الآلي وشبكة المعلومات الدولية (الإنترنت) وانتشارهما[33].

ولقد كان ظهور الجريمة المعلوماتية عاملًا حاسمًا في قيام كثير من الدول بسَنَ تشريعات جديدة أو تعديل تشريعاتها القائمة لمواجهة الجريمة المعلوماتية، إلا أن المشرع في البلدان العربية لم يتدخل جديًّا - بعد - لمواجهة هذا النوع من الجرائم بنصوص خاصة، فضلًا عن أن القضاء لم يواجَه بمشكلات قانونية تتعلق بحماية المعلومات والبرامج التي تخص الكمبيوتر[34].

وإزاء هذا القصور التشريعي وندرة التطبيق القضائي يبرز للوجود مسألة صعوبة جمع الاستدلالات والأدلة في الجريمة المعلوماتية حتى يمكن تحقيق عناصرها والتصرف فيها -كباقي الجرائم - إذ إن هذه النوعية من الجرائم توجد في بيئة لا تعتمد التعاملات فيها - أصلًا - على الوثائق والمستندات المكتوبة، بل على نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسب والبيانات التي يمكن استخدامها أدلة ضد الفاعل، ويمكن في أقل من ثانية العبث بها أو محوها بالكامل، لذلك فإن المصادفة وسوء الحظ لهما دور كبير في اكتشافها، وذلك أكثر من الدور الذي تلعبه أساليب التدقيق والرقابة[35].

ولذلك وبعد أن أصبح المجتمع المعلوماتي حقيقة واقعة، وبعد اعتماد المجتمعات المعاصرة في تسيير شؤونها على تقنيات الحاسبات والمعلومات،تعين على أجهزة العدالة الجنائية مع تقلص الدور التقليدي للوثائق في الإثبات وازديادٍ مطردٍ في كمّ المعلومات المنتجَة أو المعروضة في أوعية - لا ورقية مستحدثة - أن تتعامل في ممارستها لحق المجتمع في الدفاع عن كيانه ضد الإجرام، مع أشكال مستحدثةٍ من الأدلة غير المادية، وذلك في مجال الإثبات الجنائي وهو ما يفرض على الفكر الشرطي - سلطة جمع الاستدلالات - من جهة أن تسعى دومًا لتطوير أساليب كشف الجريمة المعلوماتية والوسائل المستخدمة في عمليات البحث الجنائي والتحقيق[36]، ومن ناحية أخرى يجب تحديث الأساليب الإجرائية المتبعة لجمع الأدلة في الجرائم المعلوماتية[37].

ومن هنا تبدو الأهمية العلمية للحديث عن كيفية القيام بالاستدلالات واستخلاص الدليل في الجريمة المعلوماتية، وذلك من خلال بحث هذه الموضوعات في المطالب اللاحقة، وذلك أن صعوبة استخلاص الدليل قد يكون سببُها أمورًا تتعلق بالدليل ذاته مثل إخفاء هذا الدليل وعدم إتاحته وعرضه، فضلًا عن أن

الجرائم المعلوماتية في الغالب لا تترك آثارًا، وتستعصي على أساليب ووسائل البحث الجزائي التقليدي، كما أن وسائل المعاينة وطرقها التقليدية لا تفلح غالبًا في إثبات دليل هذه الجريمة التي تنفرد بطبيعةٍ خاصةٍ بها[38]، لذلك كان من الملائم بحث صعوبات استخلاص الدليل لعوامل تتعلق بذاته، في مطلبٍ مستقل.

كذلك فقد تظهر مشاكل استخلاص الدليل لصعوبات تتعلق بحجم البيانات المتعلقة بهذه الجريمة وكمّها، من حيث ضخامتها وسهولة تدميرها؛ إذ يكفي بضغط زر واحد أن يمكن لشخص ما محو كم من المعلومات قد تنطوي على جريمة معلوماتية في جزء من الثانية، لذلك رأيت حصر المشكلات المتعلقة بالبيانات موضوع الجريمة المعلوماتية في مطلبٍ مستقل.

وأخيرًا فإن أجهزة العدالة الجنائية قد تعيق التحقيق في هذه الجريمة متى انعدمت أو نقصت خبرتهم بشأن الجريمة المعلوماتية، الأمر الذي يقتضي تأهيلهم وتدريبهم، فضلًا عن استعانتهم بخبراء متخصصين في الحاسب الآلي، لا سيما أن الجاني مرتكب هذه الجريمة ينفرد بسمات خاصة عن المجرم العادي[39]، لذلك كان من الملائم تخصيص مطلب مستقل للجرم المعلوماتي وكذلك أجهزة الاستدلال والتحقيق الجنائي والادعاء في هذه الجريمة. وهذا ما سنتناوله في ما يأتي:

المطلب الأول - المشكلات المتعلقة بالدليل ذاته:

الاستدلال عن الجرائم يشمل التحريَ عنها، كما يشمل كل ما يمكن جمعه من المعلومات عن هذه الجرائم متى وصل أمرها إلى علم عضو الضبط القضائي، سواء عن طريق مشاهدتها بنفسه أم نتيجة لتلقيه بلاغًا عنها أو شكوى بشأنها[40].

وقد أشارت المادة 40 من قانون أصول المحاكمات الجزائية العراقي إلى واجبات أعضاء الضبط القضائي في الاستدلال والتي تلخص في الآتي:

1- التحري عن الجرائم.

2- قبول الإخبارات والشكاوى التي ترد إليهم.

3- تقديم المساعدة لقضاة التحقيق والمحققين والضباط وتزويدهم بالمعلومات.

4- ضبط مرتكبي الجرائم وتسليمهم للسلطات المختصة.

5- تحرير محضر بالإجراءات التي يتخذونها.

فالدليل الجنائي هو معنى يدرك من مضمون واقعة تؤدي إلى ثبوت الإدانة أو ثبوت البراءة، ويتم ذلك باستخدام الأسلوب العقلي وإعمال المنطق في وزن تلك الواقعة وتقديرها، ليصبح المعنى المستمد منها أكثر دقة في الدلالة على الإدانة أو البراءة[41].

والدليل الجنائي قد يكون دليلًا ماديًا يتكون من أشياء مادية تدرك بالحواس، دون أن يضاف إليها دليل آخر لإثبات الواقعة التي يثور الخلاف في تحديد معناها وإدراكه، ومن أمثلتها الأعيرة النارية، وقد يكون الدليل المادي مستنديًا موضوعه الكتابة.

وإجراءات التحقيق تهدف إلى جمع الأدلة الكثيرة، ومن هذه الأدلة الانتقال والمعاينة وسماع الشهود، وندب الخبراء والتفتيش والاستجواب والمواجهة، مع ملاحظة أن إجراءات جمع الأدلة لم ترد في القانون على سبيل الحصر، ولذا يجوز للمحقق أن يباشر أي إجراء آخر يرى فيه فائدة للإثبات طالما أنه لا يترتب على اتخاذه تقييد لحريات الأفراد أو مساس لحرمة مساكنهم[42].

وجريمة الحاسب الآلي أو الجريمة المعلوماتية يمكن إثباتها بالأدلة المذكورة، وهناك بعض الأدلة المادية التي لها قيمتها الخاصة في إثبات الجريمة المعلوماتية ونسبتها إلى متهم معين، ومن هذه الأدلة:

أولًا- الأوراق: الجريمة الواقعة على المال أو الإنسان في صورتها العادية قد تخلف قدرًا كبيرًا من الأوراق والمستندات الرسمية أو الخاصة، ولكن في الجريمة المعلوماتية فإن الحاسب الآلي وشبكة الإنترنت يحفظان كمًّا هائلًا من المعلومات والأوراق والملفات قد يقوم الجاني بطباعتها لأغراض المراجعة أو لأجل التأكد من تنسيق المستند أو شكله العام[43].

ومن هذه الأوراق:

1- أوراق تحضيرية يتم إعدادها بخط اليد، كمسوَّدة تصوير العملية التي يتم برمجتها.

2- أوراق تالفة تم طباعتها للتأكد من تمام الجريمة، تلقى في سلة المهملات.

3- أوراق أصلية تطبع ويتم الاحتفاظ بها كمرجع أو لأغراض الجريمة.

4- أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفتر الحسابات، ولها علاقة بالجريمة المعلوماتية، خاصةً عند تقليد هذه الأوراق وتزويرها بواسطة الحاسب الآلي[44].

ثانيًا- جهاز الحاسب الآلي وملحقاته؛ إذ إنه للقول بأن الجريمة (معلوماتية)، يتعين وجود جهاز حاسب آلي له علاقة بمكان وقوع الجريمة أو الشخص الحائز للجهاز، وهو يتكون من المكونات المادية الآتية[45]:

أ) وحدات الإدخال: وهي الفأرة، ومشغِّل الأقراص المغنَطة، والماسح الضوئي، ومشغل الأسطوانات.

ب) وحدات المعالجة المركزية: وهي وحدة الذاكرة الرئيسة وتقاس بوحدات البت Bit والبايت Byte والكيلوبايت، ووحدة الحساب والمنطق (Arithmatic Logic Unit Alu)، ووحدات التحكم (Control Unit Cu).

ج) وحدات الإخراج: وهي الوحدة التي من خلالها يمكن للجرم المعلوماتي أو لأي شخص إخراج النتائج وإظهارها بأشكال مختلفة (مرئية - مسموعة - مطبوعة)، ومن أمثلتها الطابعات Printers، والشاشات Monitors، ومشغل الأقراص Disk Drive، والراسمات Plotters، ووحدات تركيب الأصوات Voice Synthesizers.

د) وحدات التخزين Storggedivices: وهي من أهم أجزاء الحاسب الآلي؛ لأنها تحتوي على المعلومات والبرامج التي يستخدمها المستخدم في عمله، ويمكن له من خلالها تخزين الملفات التي يقوم بعملها، وهذا الجزء مهم جدًّا لمرتكب الجريمة المعلوماتية؛ إذ باقتحام الملفات المخزنة يمكنه الحصول على ما يريد من بيانات أو معلومات، أو تخريب هذه المعلومات أو تدميرها، أو تزييفها أو تزويرها[46].

ومن وحدات التخزين هذه الأقراص الصلبة Hard Disk، والأقراص المرنة Floppy Disk، وأقراص الليزر CD Rom التي تمتاز بسَعة تخزين عالية، وتبدو أهميتها في الجريمة المعلوماتية في أنه يوجد مع جهاز الحاسب الآلي الشخصي (P.C) قدر كبير من هذه الأقراص، ويدوَّن على غلافه بيانات توضح محتوياته، وهي لدى البنوك والشركات تعد بالآلاف، ولكن في التحقيق الجنائي لن يعتد - بالطبع - بما دوِّن على غلاف القرص من بيانات، بل سيتم إفراغ هذه الأقراص بمعرفة خبير ليقدم بيانات دقيقة أمام جهات التحقيق أو المحاكمة، ولا يشترط في الجريمة المعلوماتية أن تضبط أقراص الليزر مع جهاز الحاسب الآلي، لكنها

قد تضبط في مكانٍ آخر، ومع ذلك فهي جزء من ماديات الجريمة أو الدليل اللازم لإثباتها، طالما كانت محتوياتها عنصرًا من عناصر الجريمة[47].

هـ) المودم Modem.

و) الكروت أو البطاقات.

ز) البطاقات الممغنطة[48].

كانت هذه إشارة موجزة لجزء من ماديات الجريمة المعلوماتية التي ينبغي البحث عنها وفحصها والإفادة منها في التحقيق، من أجل إثبات دليل الإدانة أو النفي فيها، وبعد هذا التقدم السريع لمفهوم الدليل الجنائي في الجريمة المعلوماتية، نجد أن الصعوبات التي تواجه سلطة الاستدلال أو التحقيق الجنائي في استخلاص الدليل يمكن حصرها في الآتي:

1- عدم ظهور الدليل المادي للجريمة المعلوماتية.

2- استحالة رؤية ذلك الدليل.

3- عدم وجود آثار مادية ملموسة للجريمة المعلوماتية.

4- عجز وسائل الفحص التقليدية عن ضبط آثار الجريمة المعلوماتية.

وسنقتصر في بحثنا على معالجة الفرعين الآتيين:

الفرع الأول - عدم ظهور الدليل المادي:

الجريمة المعلوماتية - كما هو واضح - تتم في بيئة أو إطار لا علاقة له بالأوراق والمستندات، وإنما تتم عن طريق الحاسب الآلي أو شبكة المعلومات الدولية - الإنترنت - ويمكن للجاني عن طريق (نبضات إلكترونية) - لا ترى - العبث ببيانات الحاسب أو برامجه، وذلك في زمن قياسي قبل أن تصل يد العدالة

إليه، لا سيما أن عملية الضبط لا تتم إلا بمعرفة خبير فني أو متخصص، ذلك أن رجل العدالة لا دراية له بالأمور الفنية في الجريمة المعلوماتية حتىٰ يمكنه مجاراة الجاني في سرعته حتىٰ يصل إلىٰ المتهم ويستصدر أمرًا بالقبض عليه، فالدليل في الجريمة التقليدية مرئي علىٰ العكس من الجريمة المعلوماتية التي تتم دون رؤية لدليل الإدانة، وحتىٰ في حالة وجود الدليل فإن للجاني طمسه أو محوه، فغالبية الجرائم المعلوماتية تكتشف مصادفةً وليس بالإبلاغ عنها.

ففي دراسة مسحية تمت من قِبَل لجنة التدقيق في إنجلترا في شأن الاحتيال المعلوماتي وإساءة استعمال الحاسب شملت 6000 من المؤسسات التجارية وشركات القطاع الخاص - تعتمد علىٰ الحاسب الآلي في إنجاز أعمالها - تبين أن ما يقارب من نصف حالات الاحتيال التي تمت ضد هذه المؤسسات والشركات قد اكتشفت مصادفةً وكبَّدتها خسائر قدرت بنحو (2,5) مليون جنيه إسترليني[49].

ولذلك نجد أن المتخصصين وجانبًا من الفقه الجنائي، بسبب خفاء الدليل في الجريمة المعلوماتية، يطلق علىٰ الجناة فيها اسم «القراصنة»، وهم نوعان: هواة Hackers وهؤلاء هم الشباب الفضوليون الذين يعملون للتسلية ولا يشكلون خطورة علىٰ الصناعات أو أنظمة المعلومات[50]، ولكن الخطورة تكمن في فئة المخادعين Crackers، وهؤلاء يحدثون أضرارًا كثيرة ويؤلفون أندية لتبادل المعلومات في ما بينهم، وبحسب خفاء الدليل في جرائمهم تقسم جرائمهم إلىٰ جرائم:

1- المخادعين Fraudeurs: وهم يتمتعون بقدراتٍ فنية عالية بوصفهم أخصائيين في المعلوماتية، ومن أصحاب الكفاءات، ولديهم مقدرةٌ فائقة علىٰ إخفاء دليل الجريمة المعلوماتية، وتنصب جرائمهم علىٰ شبكات تحويل الأموال والتلاعب في حسابات المصارف.

2- الجواسيس Espions: وهؤلاء يسعون إلى جمع المعلومات لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات المتنافسة بينها، ولا شك أن هؤلاء قادرون كذلك على إخفاء جريمتهم نظرًا لكونهم مجرمين متخصصين، ولديهم قدرةٌ فائقةٌ على طمس الأدلة المتعلقة بجرائمهم المعلوماتية[51].

ولعل خفاء الدليل وعدم ظهوره في الجريمة المعلوماتية يجد سنده في أن هذه الجريمة قائمة على معلومة يتم سرقتها أو الاحتيال عن طريقها أو الغش بها أو تزويرها، وبمعنى آخر أن هذه المعلومة هي الوسيلة لاقتران الجريمة والتي تخلف آثارًا ماديةً في ما بعد، مثل التوصل إلى رقم بطاقة ائتمان خاصة بأحد الأشخاص ومعرفة شفرة البطاقة والرقم السري لها (Pass Ward)، ومن ثَمَّ الدخول إلى حسابه عن طريق الصراف الآلي وسرقته وسرقة مال من حسابه المودع في البنك، هذه الجريمة التي اعتمدت على معلومة، يجد الفقه الجنائي صعوبة في التسليم بكونها موضوعًا للسرقة واعتبارها من قبيل المال الذي يمكن سرقته، ذلك أن المعلومات ليست من الأشياء؛ لأنها ليست من المنقولات، كما لا ترد عليها الحيازة ولا تنتقل بالاختلاس[52].

كذلك توجد صعوبة في قياس سرقة المعلومات على سرقة بعض الأشياء الأخرى كسرقة التيار الكهربائي مثلًا[53].

بل أكثر من ذلك أن البعض يرى أن الإتلاف العمدي لهذه المعلومات والبيانات يثير مشكلات عدة بسبب طبيعة هذه البيانات والمعلومات، وهل هي من قبيل المال أو لا[54].

الفرع الثاني - فقدان الآثار التقليدية للجريمة:

تبقى الجريمة المعلوماتية مجهولة ما لم تُبلَّغْ عنها الجهات الخاصة بالاستدلال أو التحقيق الجنائي، والمشكلة التي تواجه أجهزة العدالة الجنائية هي أن هذه الجرائم لا تصل لعلم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية لا تخلف آثارًا ماديةً كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة، وجثة المجني عليه في جريمة القتل ... إلخ.

ويرجع ذلك إلى صعوبة اكتشاف الجريمة المعلوماتية، وذلك أن الجهات التي تتعامل بالحاسب الآلي في معاملاتها اليومية لا تراجع حساباتها يوميًّا وحتى التي تقوم بالمراجعة اليومية أو الأسبوعية أو الشهرية قد لا تكتشف الجريمة وتبدو لها كأنها خسائر عادية إثر ممارسة نشاطها، وفي حال اكتشافها قد لا تقوم بالإبلاغ عنها خوفًا على سمعتها في أوساط العمل[55] والعملاء.

ولذلك يتعين عند البحث عن آثار الجريمة الإلكترونية وأدلتها بمعرفة سلطات الاستدلال والتحقيق، أن توجه تحرياتها إلى دائرة المتعاملين في نطاق المؤسسة أو الجهة التي وقعت بها الجريمة، سواء كانوا موظفين بتلك الجهة أو من المتعاملين معها، وذلك برصد حركة المعاملات التجارية ومراقبة المشبوهين داخل المؤسسات المالية وحولها[56]. ويتعين على رجال الأمن جمع المعلومات السرية عن حركة السوق وتداول الأموال والممتلكات المالية والتغيرات الاجتماعية والسلوكية للموظفين وصغار رجال الأعمال الذين قد يرتبطون بمؤسسات الجريمة المنظمة، ذلك أن جرائم الحاسب الآلي هي من أسلحة مرتكبي هذه الجريمة، وهم يستغلون إمكانياتهم وقدراتهم لاستقطاب صغار الموظفين وذوي القدرات الفنية والذين هم على مقربة من أسرار برامج الحاسب الآلي في المؤسسات المالية والشركات التجارية[57].

ومن الأسباب التي تسهم في تعذر الحصول على آثار تقليدية تَخْلُف الجريمة المعلوماتية، أن الجاني نفسه يملك محو الأدلة التي تُدِينه أو تدميرها في زمنٍ قصير جدًّا، وحتى لو تم ضبطه فقد يُرجع هذه الجريمة إلى خطأ في نظام الحاسب أو الشبكة أو الأجهزة[58].

المطلب الثاني- المشكلات المتعلقة بسلطات الاستدلال والتحقيق:

الجريمة المعلوماتية شأنها شأن الجرائم الأخرى، تمر بمرحلتي الاستدلال والتحقيق الجنائي المتكامل ذاتيهما، وما يترتب على ذلك من إجراءات قانونية وفنية وشكلية، وإجراءات التحقيق الجنائي العام هي الأساس في تحقيق جرائم الحاسب الآلي؛ من سماع للشهود ومعاينة وقبض وتفتيش واستجواب، لكن إجراءات التحقيق الأخرى الفنية والنفسية يتوقف استخدامها على ظروف كل جريمة على حدة، مع مراعاة الخصوصية التي تتسم بها الجريمة المعلوماتية[59].

وهناك صعوبات كثيرة في ما يتعلق بعمل سلطات الاستدلال والتحقيق، نتطرق إلى بعض منها في الفروع الآتية:

الفرع الأول - صعوبات مَصْدَرها الإحجامُ عن الإبلاغ:

تظل الجريمة المعلوماتية مستترة ما لم يتم الإبلاغ عنها، ومن ثم عمل الاستدلالات أو تحريك الدعوى الجزائية حسب القانون السائد. والصعوبة التي تواجه أجهزة الأمن والمحققين هي أن هذه الجرائم لا تصل إلى علم السلطات المعنية بالصورة العادية - كما هو الحال في الجريمة التقليدية - وذلك لصعوبة اكتشافها من قِبَل الأشخاص العاديين أو حتى الشركات والمؤسسات التي وقعت مجنيًا عليها في هذه الجرائم، أو لأن هذه الجهات تحاول دَرْء الأثر السلبي للإبلاغ عما وقع لها، وحرصًا على ثقة العملاء فلا تبلغ عن تلك الجرائم التي ارتكبت ضدها[60].

والجريمة في صورتها التقليدية تصل إلى علم سلطات الضبط عن طريق الشكوى أو الإبلاغ، وكذلك قد يصل علم الجريمة إلى أعضاء الضبط القضائي متى تم ضبط الجريمة متلبَّسًا بوقوعها؛ إذ إن هناك إجراءات وجوبية على مأموري الضبط وسلطات التحقيق اتخاذها في حالات التلبس، ومن المعلوم أن الجريمة تكون مشهودة في بضع حالات هي (حصرًا)[61]:

1- مشاهدة الجريمة حال ارتكابها.

2- مشاهدة الجريمة عقب ارتكابها ببرهة يسيرة.

3- تتبُّع الجاني إثر وقوع الجريمة من قِبَل المجني عليه أو الجمهور مصحوبًا بالصياح.

4- مشاهدة الجاني بعد وقوع الجريمة بوقت قريب حاملًا أشياء أو أوراق، أو به آثار يستدل منها على أنه فاعل الجريمة أو شريك فيها.

أما الجريمة المعلوماتية فيصل العلم بوقوعها إلى سلطات الضبط بإحدى الطرق الآتية[62]:

1- تلقي سلطات الضبط أو أجهزة التحقيق معلومات عن ممارسة أشخاص معروفين أو غير معروفين أنشطة تندرج تحت تعريف الجريمة المعلوماتية، وذلك في مكان معروف وعلى أجهزة محددة ووفق لغات برمجية معلومة.

2- ضبط شخص معين وبحوزته أموال مشبوهة أو بطاقات مزورة أو بطاقات تعريف مشبوهة (حالة تلبس).

3- بلاغ إلى سلطات الضبط أو التحقيق من أحد المجني عليهم يفيد صدور تلاعب أو ممارسات خاطئة بحقه أو حقوق الآخرين، سواء تمثل ذلك في صورة عجز مالي في حسابات مؤسسة مالية، أو ضياع حقوق، أو حصول تغيرات

في الودائع، وذلك دون بيان ما إذا كانت هذه جريمة معلوماتية من عدمها؛ لأن عملية تكييف السلوك الإجرامي هي مسألة أخرى لا دخْل للمبلِّغ بها.

4- توافر معلومات عن نشر فيروسات تخريبية عبر شبكة الإنترنت.

علمًا أن تطبيق القانون في مجال مكافحة الفيروسات المعلوماتية تواجهه صعوبات وموانع كثيرة هي[63]:

أ) عدم معرفة المجني عليه بالمخرِّب الذي صمم الفيروس الذي هاجمه.

ب) عدم رغبة المجني عليه في الإبلاغ عن وجود فيروس بنظامه المعلوماتي؛ حفاظًا على الثقة التي بينه وبين الذين يستخدمون هذا النظام.

ج) عدم دراية المجني عليه بإصابة نظامه بفيروس معلوماتي لفترة غير محددة من الزمن، وبالتالي يصعب تحديد وقت الإصابة.

د) عدم القدرة على قياس الخسائر التي يُحْدِثها هذا الفيروس.

وكذلك فإن من صعوبات الإبلاغ عن هذه الجرائم (على نطاق دولي)، عدم وجود شبكة دولية لتبادل المعلومات الأمنية كما هو الحال في شبكة (يورب بول) التي تعمل حاليًا في إطار الشرطة الدولية، بمعزل عن الشبكة العامة المستخدمة حاليًا، كما هو الحال بالنسبة لشبكة إنترنت (2) التي تمثل اتحاد شركات عالمية تعمل بمعزلٍ عما تواجهه شبكة الإنترنت الحالية من مشاكل وثغرات، وفي هذا الإطار استحدثت الصين شرطة متخصصة لمراقبة استخدام شبكة الإنترنت[64].

كذلك فإن الشرطة الدولية - الإنتربول - بدأت تهتم بمكافحة جرائم الكمبيوتر، وأنشأت لديها فرقة خاصة لهذا الغرض هي على اتصال دائم بفِرَق مكافحة الجريمة المعلوماتية في أوروبا والولايات المتحدة الأمريكية وأستراليا، إضافة إلى تبادل المعلومات حول كيفية اكتشاف هذا النوع من الجرائم -

الإبلاغ - وتعزيز الإجراءات الأمنية في شأن معلومات الحاسب الآلي وبياناته، خاصةً لدول أوروبا الشرقية في السابق[65].

وتثير مسألة الإبلاغ عن الجريمة المعلوماتية مسائل تتعلق بمدى ما هو متاح من نصوص في التشريعات الجزائية التي توجب الإبلاغ وترتب عقوبة على ذلك.

ففي القانون العراقي وفي ما عدا الجرائم التي يعلق القانون تحريك الدعوى فيها على شكوى أو طلب من المجني عليه، يكون التبليغ عن الجريمة حقًّا لكل شخص، لذلك فقد نصت المادة 47 من قانون أصول المحاكمات الجزائية رقم 23 لسنة 1971، على أنه: «لمن وقعت عليه جريمة ولكل مَن علِم بوقوع جريمة تحرك الدعوى فيها بلا شكوى، أو علِم بوقوع موتٍ مشتبه به أن يخبر قاضيَ التحقيق أو المحقق أو الادعاء العام أو أحد مراكز الشرطة». وهذه هي القاعدة العامة في حق كل مواطن أو شخص في الإبلاغ، طالما أن الجريمة ليست مما يلزم لتحريك الدعوى عنها شكوى أو طلب من الجهة التي حددها القانون، وعلى هذا يحق لكل مَن علم بوقوع جريمة إلكترونية أن يبلغ عنها، ما لم ينص القانون على غير ذلك.

لكن هناك حالات يكون فيها الإبلاغ عن الجريمة واجبًا على كل من علم بوقوعها، ويترتب على الإخلال بهذا الواجب جزاء جنائي أو تأديبي، فقد أوجبت المادة (219) من قانون العقوبات العراقي على كل من علم بوقوع جريمة من الجرائم المنصوص عليها في الباب الثاني من هذا القانون[66]، أن «يسارع بالإبلاغ إلى السلطات المختصة، وإلا عوقب بالحبس والغرامة أو بإحدى هاتين العقوبتين».

كما نصت المادة (247) من القانون المذكور على أن «يعاقب بالحبس أو الغرامة كل مَن كان ملزمًا قانونًا بإخبار أحد المكلفين بخدمةٍ عامة، عن أمر ما أو إخباره عن أمور معلومة له، فامتنع قصدًا عن الإخبار بالكيفية المطلوبة، وفي الوقت الواجب قانونًا. وكل مكلف بخدمة عامة منوط به البحث عن الجرائم أو ضبْطها أهمل الإخبار عن جريمة اتصلت بعلمه، وذلك كله ما لم يكن رفْع الدعوى معلقًا على شكوى...».

كذلك فإن المادة (48) من قانون أصول المحاكمات الجزائية[67] قد أوجبت على المكلف بخدمةٍ عامة أن يُبلغ عن الجرائم التي يعلم بها في أثناء تأدية عمله أو بسبب تأديته، شرط أن لا تكون من جرائم الحق الشخصي، وبذلك يكون الإبلاغ واجبًا على الموظف أو المكلف بخدمة عامة وإلا تعرض للمساءلة التأديبية ومن هذه الزاوية يجب على أي موظف من أولئك العاملين في الحكومة أو المكلفين بخدمة عامة - وذلك حسب النص - أن يبلغ عن أية جريمة إلكترونية وصل عِلْمُها إليه، وإلا تعرض للمساءلة.

وجدير بالذكر أن واجب الإبلاغ المقرر بنص المادة (48) أصولية، لا يمتد إلى أولئك العاملين في القطاع الخاص وشركاته ومؤسساته، وهي الكثرة الغالبة من الجهات التي تستخدم أجهزة الحاسب الآلي مثل الشركات والبنوك الاستثمارية والمصانع الكبرى التي ليست مملوكة للحكومة، أو أنها لا تشترك فيها بنصيب، وكل ذلك يحتم ضرورة الإسراع بوضع تشريع خاص ينظم العقاب على الجريمة المعلوماتية أو تنقيح قانون العقوبات والقوانين ذات العلاقة لتستوعب العقاب على مثل هذه الجرائم.

كذلك فإن المشرع في دولة الإمارات العربية المتحدة جعل الإبلاغ عن الجرائم إلزاميًّا كقاعدة عامة، ومَن يخالف ذلك يتعرض للجزاء الجنائي. ولذلك أوجبت المادة (37) من قانون الإجراءات الجزائية الاتحادي رقم 35 لسنة

1992 على كل من علم بوقوع جريمة مما يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب، أن يبلغ النيابة العامة أو أحد مأموري الضبط القضائي عنها، كما نصت المادة (38) من القانون ذاته على أنه «يجب على كل مَن علم من الموظفين العموميين أو المكلفين بخدمة عامة، أثناء تأدية عمله أو بسبب تأديته، بوقوع جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب، أن يبلغ فورًا النيابة العامة أو أقرب مأموري الضبط القضائي»، ورتب المشرع على الإخلال بهذا الواجب عقوبة جنائية؛ إذ نصت المادة (2/272) من قانون العقوبات الاتحادي على أنه «يعاقب بالغرامة كل موظف غير مكلف بالبحث عن الجرائم أو ضبطها أهمل أو أرجأ إبلاغ السلطة المختصة بجريمةٍ علم بها أثناء أو بسبب تأديته وظيفته، ولا عقاب إذا كان رفْع الدعوى معلقًا على شكوى».

ومؤدى ذلك معاقبة الموظف جنائيًا على عدم الإبلاغ أو الإهمال فيه، حتى لو لم يكن مكلفًا بالبحث عن الجريمة أو ضبطها[68].

وفي هذا يختلف القانونان العراقي والإماراتي عن القانون المصري في أن الأَولَين جعلا هذا الفعل بمثابة جريمةٍ جنائية معاقَب عليها بالغرامة، في حين أن الأمر ليس كذلك في القانون المصري؛ إذ إنه يكتفي بالعقاب التأديبي.

كذلك يختلف القانون الإماراتي عن القانونين العراقي والمصري في أنه جعل عدم الإبلاغ جريمة عامةً حتى للمواطن العادي، وبالنسبة لكل الجرائم وليس لجرائم معينة، كما هو الحال في جرائم أمن الدولة، حسب المادة (48) من قانون العقوبات المصري، ولذلك تنص المادة (274) من قانون العقوبات الاتحادي في الإمارات على أنه «يعاقَب بغرامة لا تجاوز ألف درهم كُلُّ مَن علم بوقوع الجريمة وامتنع عن إبلاغ ذلك للسلطات المختصة».

وعلى ذلك فعدم الإبلاغ يعد جريمة بالنسبة للمواطن العادي، ما لم يتوافر في حقه سبب للإعفاء كعلاقة القرابة والمصاهرة.

وميزة هذا النص أنه فضلًا عن إلزام المواطن العادي بالإبلاغ حتى في الجريمة الإلكترونية التي تصل إلى علمه، فإنه يُلزم كذلك موظفي شركات القطاع الخاص التي تستخدم الحاسب الآلي، متى علموا بجريمةٍ لها علاقة بالحاسب وتصنف ضمن الجرائم الإلكترونية، ويترتب على التقاعس عن هذا الإبلاغ جزاء جنائي قبل المتقاعس، ولا شك أن ذلك كله يصبُّ في مصلحة الدعوى الجنائية وإمكانية استجماع الأدلة في شأن الجريمة المعلوماتية[69].

الفرع الثاني - صعوبات مصدرها نقص خبرة سلطات الاستدلال والتحقيق:

من الصعوبات التي تواجه عملية استخلاص الدليل من الجريمة المعلوماتية نقصُ الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك في ما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجريمة المعلوماتية وكيفية التعامل معها، وذلك - على الأقل - في البلدان العربية؛ نظرًا لأن تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخرًا عن أوروبا وكندا والولايات المتحدة، وأن أجهزة العدالة المقاومة للجرائم المرتبطة بهذه التقنية تبدأ في التكوين والتشكيل عقب ظهور هذه الجرائم، وهو أمرٌ يستغرق وقتًا أبطأ من وقت انتشار الجريمة؛ لأن الجريمة المعلوماتية - كما سبق - تتقدم بسرعة هائلةٍ توازي تقدم التقنية ذاتها، وحتى الآن فإن الحركة التشريعية أو الثقافة الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بالمعدل ذاته، وهذا الفارق في التقدم أو التطور ينعكس سلبًا على فنية إجراء الاستدلالات

والتحقيقات في الدعوة الجزائية عن الجريمة المعلوماتية[70]. وذلك أن حداثة هذه الجرائم وتقنياتها العالية تتطلب من القائمين على البحث الجنائي والتحقيق إلمامًا كافيًا بها، فلا يكفي أن تكون لديهم الخلفية القانونية أو أركان العمل الشُرطي فقط، ولكن لابد من الإلمام بخبرةٍ فنيةٍ في مجال الجريمة المعلوماتية[71].

ولذلك فإن قواعد قانون العقوبات والإجراءات أو أصول المحاكمات الجزائية في الدول العربية قد تكون عاجزة أحيانًا عن أن تسعف رجال الأمن سلطات التحقيق في مواجهة الجريمة المعلوماتية، ولا نقصد بذلك قواعد الشرعية، وذلك أن قواعد الشرعية بوصفها قواعد دستورية يجب مراعاتها في كل الأحوال، لكن ما نقصده هو خصوصية هذه الجريمة، وبالتالي فإن إجراءات مواجهتها يجب أن تكون إجراءات خاصة تتفق وطبيعة الجريمة، سواء من حيث سرعة الحركة لتلمس الدليل وضبطه قبل محوه، أو من حيث كيفية الضبط، لا سيما أن الجريمة المعلومات لا تترك آثارًا، وإن تركت فقد يكون من الصعب تتبعها[72]، فعلى سبيل المثال في جريمة (سرقة البنوك) بطريقة الاحتيال المعلوماتي، يصعب الإمساك بالمجرمين بسبب السرعة التي تتم بها عملية الحوالات النقدية[73].

ويزيد من التحدي الذي يواجه أجهزة العدالة الجنائية في جرائم الحاسب الآلي، أن الجناة في هذه الجرائم لهم مفردات ومصطلحات خاصة بهم، لدرجة أنهم يطلقون على أنفسهم اسم (النخبة) Elites، بدعوى أنهم الأكثر معرفة بأسرار الحاسب الآلي ولغاته المتميزة، ويطلق على رجال الشرطة والنيابة والقضاء صفة الضعفاء القاصرين (Demers)[74].

بالإضافة إلى ذلك فإن هناك صعوبات خاصة بمواجهة الجريمة المعلوماتية بطريق الإنترنت، وهذه الجرائم ترجع أساسًا إلى طبيعة التعامل مع المعلومات أو تداولها على هذه الشبكة، الأمر الذي يزيد من إرهاق سلطات الضبط ورجال القضاء، وهذه الصعوبات تتمثل في الآتي[75]:

1- يشهد قطاع التكنولوجيا المعلوماتي طفرات وسرعة فائقة في الإنتاج الكمي والنوعي، وفضلًا عن ذلك فإن الشبكة يمكن لكافة المستويات الاجتماعية والاقتصادية الاشتراك فيها.

2- عدم وجود قوانين دولية أو نصوص دستورية تجرم هذا النوع من الأفعال إلى الآن، على حد اطلاعي؛ وذلك لكونها لا تزال من الجرائم ذات الطابع الحديث في الشكل والمضمون.

3- عدم وجود قضاء متخصص في الجرائم المعلوماتية.

4- عدم وجود شبكة دولية لتبادل المعلومات الأمنية.

5- صعوبة السيطرة على المشتركين، فلا توجد ضوابط دولية أو محلية تحدد فئة المستخدم أو هدفه.

6- وجود بعض المواقع على شبكة الإنترنت تسهل إرسال الرسائل دون تحديد اسم المرسل، وبالتالي صعوبة معرفة المسؤول عن هذه الجريمة.

الفرع الثالث - صعوبة التعاون الدولي في مكافحة الجرائم المعلوماتية:

تقدم شبكة المعلومات الدولية - الإنترنت - مجموعة متنوعة ومعقدة من الاستخدامات في مجال السياحة والإعلام والثقافة والشؤون العسكرية والاقتصادية والأمنية، الأمر الذي يزيد يوميًا من حالات الاعتداء على خصوصية المعلومات وسرّيتها، بقصد السرقة أو التخريب أو التجسس، مما يمثل هاجسًا للمؤسسات صاحبة هذه الشبكات ولبلدان العالم، نظرًا لتبادل المعلومات المشفرة والتي قد يكون لها صلة بالتجسس السياسي أو العسكري أو الصناعي أو أية نشاطات إجرامية[76].

ولذلك نادى البعض بضرورة إنشاء وحدات خاصة بمكافحة الجريمة المعلوماتية بواسطة الحاسب الآلي والإنترنت، أسوةً بجهات البحث الجنائي الوطنية والدولية - الإنتربول - لإثبات الجريمة عند وقوعها وتحديد أدلتها وفاعليتها، وهو ما يعني كذلك إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الاعتداء على المعلومات الخاصة في الإنترنت، وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبيها وسبل مكافحتها[77].

ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة المعلوماتية إلا أن هناك عوائق تحول دون ذلك، وتجعل هذا التعاون صعبًا؛ وذلك لما يلي:

أولًا: عدم وجود نموذج واحد متفق عليه في ما يتعلق بالنشاط الإجرامي: ذلك أن الأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها ما يسمى بـ«إساءة استخدام نظم المعلومات الواجب اتباعها»، وكذلك فإن ما يراه البعض مباحًا نظرًا للطبيعة الخاصة للمعلوماتية عبر الإنترنت، يراه الآخر غير مباح، ومن ثَمَّ يجرم الاعتداء عليه بالنقل أو النسخ، ومردُّ ذلك إلى طبيعة النظام القانوني السائد في كل بلدٍ من البلدان[78].

صحيح أن بعض البلدان الأوروبية كفرنسا والولايات المتحدة وكندا أصدرت تشريعات تتعلق بمكافحة الجريمة المعلوماتية عبر الحاسب الآلي والإنترنت، إلا أن هذه التشريعات لا زالت في مهدها ولا يمكن اعتبارها جامعة مانعة، بدليل أن المؤسسات المحلية لديها تطالب في كل عام بإضافة نماذج من السلوك الإجرامي المعلوماتي لتكون محلًا للتجريم لم تكن متضمَّنة في التشريعات العقابية المعمول بها[79].

ثانيًا: عدم وجود تنسيق في ما يتعلق بالإجراءات الجنائية المتبعة في شأن

الجريمة المعلوماتية بين الدول المختلفة، خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق، لا سيما أن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود، عن طريق الضبط أو التفتيش في نظام معلوماتي معين، وهو أمرٌ في غاية الصعوبة، فضلًا عن الصعوبة الفنية في الحصول على الدليل ذاته[80].

ثالثًا: عدم وجود معاهدة ثنائية أو جماعية بين الدول على نحوٍ يسمح بالتعاون المثمر في مجال هذه الجرائم، وحتى في حال وجودها فإن هذه المعاهدة قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم الحاسب وشبكة الإنترنت وبرامجهما، ومن ثم تطور الجريمة المعلوماتية بالسرعة ذاتها على نحو يؤدي إلى إرباك المشرع وسلطات الأمن في الدول، ومن ثم يظهر الأثر السلبي في التعاون الدولي، وهو ما حاولت الأمم المتحدة الاهتمام به وكذلك بلدان أوروبا[81].

رابعًا: مشكلة الاختصاص في جرائم الحاسب الآلي، وهي من المشكلات التي تعرقل الحصول على الدليل من الجهة المعلوماتية، ذلك أن هذه الجرائم من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي والدولي، بسبب التداخل والترابط بين شبكات المعلومات، فقد تقع جريمة الحاسب الآلي في مكان معين وتنتج آثارها في مقاطعةٍ أخرى داخل الدولة أو خارجها، ومن هنا تنشأ مشكلة البحث عن الأدلة الجنائية على شبكة الإنترنت، وسبق لها أن اخترقت مواقع عديدة في دول مثل الصين وجورجيا وفيتنام والكويت، بل هاجمت وكالة الفضاء الأمريكية ناسا[82] خارج دائرة الاختصاص التي قدم فيها البلاغ أو تم تحريك الدعوى الجزائية فيها.

المطلب الثالث - الصعوبات المتعلقة بضخامة كم البيانات المعلوماتية:

لعل من الصعوبات الكبيرة التي تواجه رجال الضبط وسلطات التحقيق الجنائي في الجريمة المعلوماتية، كمية المعلومات والبيانات الضخمة والتي هي في حاجة إلى فحص ودراسة؛ كي يُستخلص منها دليل هذه الجريمة، ففضلًا عن ضرورة توافر الخبرة الفنية في مجال الحاسب الآلي والمعلوماتية لدى رجال وأعضاء الضبط أو المحقق، يتعين كذلك أن يتوافر لديه القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة على الحاسب الآلي أو على ديسكات أو أسطوانات منفصلة[83].

لذلك يمكن القول: إن ضخامة هذه البيانات والمعلومات تعد عائقًا في تحقيق جرائم المعلوماتية؛ ذلك أن طباعة كل ما هو موجود على الدَّعامات الممغنطة لحاسب متوسط العمر يتطلب مئات الآلاف من الصفحات في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئًا مفيدًا للتحقيق[84].

هذا عكس ضخامة المعلومات أو وفرتها في الجرائم التقليدية، كالقتل أو السرقة؛ ذلك أن وفرة المعلومات في مثل هذه الجرائم هو أمر يساعد العدالة ويساعد رجال الضبط أو المحقق - على السواء - في استخلاص الدليل الجنائي في هذه الجريمة[85].

لذلك وفي ظل المستوى الفني لرجل الأمن والمحقق الجنائي في ما يتعلق بفنون الحاسب الآلي واستخداماته، فإنه يكون من الملائم وجوب نَدْب خبراء فنيين في مثل هذه الجرائم؛ حتى يمكن فرز المعلومات التي يحتاجها التحقيق عن تلك التي لا حاجة لها، وإلا دخل رجل الضبط والمحقق في دائرة مغلقة من المعلومات لن يخرج منها، وهذا يتطلب أن يكون ندب هؤلاء الخبراء وجوبيًّا

ومن ثَمَّ تعديل التشريعات الجنائية القائمة التي تجعل ندب خبيرٍ في الدعوى أمرًا جوازيًا للمحقق؛ إن شاء أمر به وإن شاء رفضه، وذلك لأن طبيعة الجريمة تستلزم التعامل معها بطريقة حِرْفية أو فنية تفوق قدرات رجل الضبط أو المحقق إلا إذا كان مؤهلًا لذلك، فيمكنه الاعتماد على قدراته الشخصية في ضبط هذه الجرائم وتحقيقها، شرط ألا يخرج عمله عن الأصول الفنية المتعارف عليها[86].

المبحث الثالث
القيمة القانونية للدليل الإلكتروني

إن مجرد وجود دليل يثبت الجريمة وينسبها إلى شخصٍ معينٍ، لا يمكن التعويل عليه لإصدار الحكم بالإدانة؛ إذ يلزم أن يكون لهذا الدليل قيمة قانونية، وهذه القيمة للدليل الإلكتروني تتوقف على مسألتين رئيستين: الأولى مشروعية وجود الدليل الإلكتروني، والثانية: مشروعية الحصول على الدليل الإلكتروني. وسنتناول هاتين المسألتين بالشرح تباعًا في المطلبين الآتيين:

المطلب الأول - مشروعية وجود الدليل الإلكتروني:

يقصد بمشروعية وجود الدليل الإلكتروني أن يكون الدليل معترفًا به، بمعنى أن يجيز القانون للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة[87]، ويمكن القول إن النظم القانونية تختلف في موقفها من الأدلة التي تقبل كأساسٍ للحكم بالإدانة، بحسب الاتجاه الذي تتبناه، فهناك اتجاهان رئيسان: **الأول**: نظام الأدلة القانونية، **والثاني**: نظام الإثبات الحر، وسنتناول هذين الاتجاهين في الفرعين الآتيين:

الفرع الأول - نظام الأدلة القانونية:

وفقًا لنظام الأدلة القانونية فإن المشرع هو الذي يحدد حصرًا الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات، كما يحدد القيمة الإقناعية لكل دليل، بحيث يقتصر دور القاضي على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون[88]، فلا سبيل للاستناد إلى أي دليل إذا لم ينص القانون عليه صراحةً ضمن أدلة الإثبات، كما أنه لا دور للقاضي في تقدير القيمة الإقناعية للدليل، ولذا يسمى هذا النظام بـ«نظام الإثبات القانوني أو المقيد»؛ إذ إن القانون قيد القاضي بقائمةٍ من الأدلة التي حددت قيمتها الإثباتية، وهذا النظام ينتمي للنظم الأنجلوسكسونية كالمملكة المتحدة والولايات المتحدة الأمريكية، ولذا فإن النظم التي تتبنى هذا النظام لا يمكن في ظلها الاعتراف للدليل الإلكتروني بأية قيمةٍ إثباتية، ما لم ينص القانون عليه صراحةً ضمن أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه سيهدر قيمته الإثباتية مهما توافرت فيه شروط اليقين، فلا يجوز للقاضي أن يستند إليه لتكوين عقيدته. وتطبيقًا لهذا فقد نص قانون الإثبات في المواد الجنائية البريطانية على قبول الدليل الرقمي وحدد قيمته الإثباتية اتفاقًا[89].

ويمكن أن يعاب على نظام الإثبات القانوني أن من شأنه تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلةٍ لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته لنصوص القانون، ولذلك فإن النظام بدأ ينحصر نطاقه في الدول التي تعد الأكثر اعتناقًا له، فنجد بريطانيا مثلًا قد بدأت تخفف من غلوّه، حيث ظهر ما يعرف بـ«قاعدة الإدانة دون أدنى شك»، والتي مفادها أن القاضي يستطيع أن يكون عقيدته من أي دليل وإن لم يكن من ضمن الأدلة المنصوص عليها، متى كان هذا الدليل قاطعًا في دلالته[90].

الفرع الثاني - نظام الإثبات الحر:

يسود هذا النظام في ظل الأنظمة اللاتينية بتمتع القاضي - وفقًا له - بحريةٍ مطلقةٍ في شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلةٍ للاستناد إليها في تكوين قناعته، فله أن يبني هذه القناعة على أي دليل وإن لم يكن منصوصًا عليه، بل إن المشرع في مثل هذا النظام لا يحفل بالنص على أدلة الإثبات، فكل الأدلة تتساوى قيمتها الإثباتية والقاضي هو الذي يختار من بين ما يطرح عليه من الأدلة ما يراه صالحًا للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا اطمئن إليه، فالمشرع لا يتدخل في تحديد القيمة الإقناعية للدليل، فعلى الرغم من توافر شروط الصحة في الدليل، يملك القاضي أن يرده تحت مبرر عدم الإقناع، وعلى ذلك فالقاضي في مثل هذا النظام يتمتع بدورٍ إيجابي في مجال الإثبات، في مقابل انحسار دور المشرع[91].

وعليه فإن مثل هذا النظام لا تثار حوله مشكلة مشروعية الدليل الإلكتروني من حيث الوجود، على اعتبار أن المشرع لا تعهد عنه سياسة النص على قائمة أدلة الإثبات، ولذلك فمسألة قبول الدليل الإلكتروني لا ينال منها سوى مدى اقتناع القاضي بها، إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي، ووفقًا لهذا النظام فإن الأصل في الأدلة هو مشروعية وجودها، فالدليل الإلكتروني سيكون مشروعًا من حيث الوجود استصحابًا للأصل[92].

فالقاعدة في الدعاوى الجنائية هي جواز الإثبات بالطرق والوسائل القانونية كافة، والقيد على هذه القاعدة أنه يجب أن يكون الدليل من الأدلة المقبولة قانونًا، وبالتالي تظهر أهمية اعتراف القانون بالأدلة الإلكترونية، خاصة مع احتمال ظهور أنماط جديدة لجميع الجرائم، وخاصة في قطاع المعلومات المعالجة بواسطة الكمبيوتر، ومن هنا كان البحث القانوني في العديد من الدول يتجه إلى

الإقرار بحجيةٍ قانونيةٍ للملفات والمستخرجات الحاسوبية والرسائل الإلكترونية ذات المحتوى المعلوماتي ليس بصورتها الموضوعة ضمن وعاء مادي ولكن بطبيعتها الإلكترونية المحضة، ذلك أن التطور العلمي قد أثر - بلا شك - على نظام الاقتناع القضائي[93]، وكما نعلم فإن للقاضي الجنائي الحرية في تقدير قيمة الأدلة المطروحة عليه في الدعوى الجنائية[94]، وفي أن يستمد قناعته الذاتية من أي مصدرٍ يطمئن إليه، دون أن يملي عليه المشرع حجةً معينة أو يلزمه باتباع طرق أو وسائل بعينها للكشف عن الحقيقة الواقعية، ولعل أهم ما يبرر هذا المبدأ الذي خوَّله القانون للقاضي الجنائي، هو ظهور الأدلة العلمية، مثل تلك التي تستمد من الطب الشرعي والتحليل وتحقيق الشخصية ومضاهاة الخطوط. ويلحظ أن هذه الأمور لا تقبل أي قيود بشأنها عند تعويل القاضي عليها لتكوين عقيدته؛ لذا نجد أن المشرع في العديد من الدول قد اتجه إلى الاعتراف بحجية المخرجات الكمبيوترية كأدلة للإثبات الجنائي، حيث بادرت كثير من الدول إلى تنظيم التوقيع الإلكتروني والمحرَّرات الإلكترونية، فقد نظم المشرع العراقي قانون التوقيع الإلكتروني رقم 78 لسنة 2012م، وقد نصت المادة (4/ثانيًا) منه على أنه: «يكون للتوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للتوقيع الخطي إذا روعي في إنشائه الشروط المنصوص عليها في المادة (5) من هذا القانون».

ونصت المادة (13/أولًا) من القانون ذاته على المساواة في الحجية في نطاق المعاملات المدنية والتجارية بين المستندات الإلكترونية والكتابة الإلكترونية والعقود الإلكترونية لمثيلتها الورقية.

كما نصت المادة (14) منه على أن «تكون الصورة عن المستند الإلكتروني حائزة على صفة النسخة الأصلية، إذا توافرت فيها الشروط الآتية:

1- أن تكون معلومات وبيانات الصورة المنسوخة متطابقة مع النسخة الأصلية.

2- أن يكون المستند الإلكتروني والتوقيع الإلكتروني موجودين على الوسيلة الإلكترونية.

3- إمكانية حفظ وتخزين معلومات وبيانات الصورة المنسوخة بحيث يمكن الرجوع إليها عند الحاجة.

4- إمكانية حفظ الصورة المنسوخة في الشكل الذي أنشئت أو أرسلت أو تُسلِّمت به النسخة الأصلية للمستند الإلكتروني.

5- احتواء الصورة المنسوخة على المعلومات الدالة على الموقع والمتسلم وتاريخ ووقت الإرسال والتسلم».

وأخيرًا فقد نصت المادة (5) من القانون المذكور على أنه: «يحوز التوقيع الإلكتروني الحجية في الإثبات إذا كان معتمدًا من جهة التصديق وتوافرت فيه الشروط الآتية:

أولًا: أن يرتبط التوقيع الإلكتروني بالموقع وحده دون غيره.

ثانيًا: أن يكون الوسيط الإلكتروني تحت سيطرة الموقع وحْدَه دون غيره.

ثالثًا: أن يكون أي تعديل أو تبديل في التوقيع الإلكتروني قابلًا للكشف.

رابعًا: أن ينشأ وفقًا للإجراءات التي تحددها الوزارة بتعليمات يصدرها الوزير».

وبهذا فقد أقر المشرع العراقي صراحةً بوجود حجية للمستندات الإلكترونية المستمدة من الحاسوب أو الإنترنت، ولكن ضمن شروط وضوابط معينة؛ وذلك بأن يكون التوقيع الإلكتروني مرتبطًا بالموقع وحده، وأن يكون الوسيط

الإلكتروني[95] خاضعًا لسيطرة الموقع وحده دون غيره، أي أن لا يكون متاحًا للجمهور، وأن أي تعديل أو تغيير في التوقيع الإلكتروني يمكن كشفه بسهولة من قبل صاحب التوقيع، وأن يكون التوقيع الإلكتروني ناشئًا وفقًا للإجراءات التي تحددها الوزارة بالتعليمات التي يصدرها الوزير.

والاتجاه ذاته هو ما أقره المشرع المصري، حيث قرر من خلال نص صريح حجية الأدلة الإلكترونية والاعتداد بها بوصفها أدلة في الإثبات الجنائي، فقد نصت المادة (14) من قانون التوقيع رقم (15) لسنة 2004 على أن: «للتوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للتوقيعات في أحكام الإثبات في المواد المدنية والتجارية، إذا روعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون». ونصت المادة (15) من القانون ذاته على المساواة في الحجية في نطاق المعاملات المدنية والتجارية بين الكتابة والمحرَّر الإلكتروني وغيرها من كتابة أو محرَّر تقليدي.

كما نصت المادة (16) من القانون ذاته على أن: «الصورة المنسوخة على الورق من المحرَّر الإلكتروني الرسمي؛ حجةٌ على الكتابة بالقدر الذي تكون فيها مطابقة لأصل هذا المحرَّر - وذلك ما دام المحرَّر الإلكتروني الرسمي والتوقيع الإلكتروني موجودين على الدَّعامة الإلكترونية»[96].

وأخيرًا نصت المادة (18) من قانون التوقيع الإلكتروني المصري على أن: «يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحرَّرات الإلكترونية بالحجية في الإثبات، إذا ما توافرت فيها الشروط الآتية:

أ) ارتباط التوقيع بالموقع وحده دون غيره.

ب) سيطرة الموقع وَحْده على الوسيط الإلكتروني.

ج) إمكانية كشف أي تعديل أو تبديل في بيانات المحرَّر الإلكتروني أو التوقيع الإلكتروني».

وقد أقر المشرع الإلكتروني كذلك بحجية التوقيع الإلكتروني، حيث قرر من خلال نص صريح توافر الحجية للأدلة الإلكترونية والاعتداد بهذا الدليل؛ إذ تعد الولايات المتحدة من أولى الدول التي أصدرت تشريعات تعترف بالتوقيع الإلكتروني وتمنحه حجية كاملة في الإثبات، شأنه في ذلك شأن التوقيع التقليدي.

فقد أصدرت ولاية (يوتا) في 1995/15/1 قانون التوقيع الرقمي، وضمنت بموجبه الحجية في الإثبات على التوقيع الإلكتروني، طالما تم عن طريق شفرة المفتاح العام. وتم توثيقه بشهادة تصديق إلكتروني[97] ثم تلتها عدة ولايات، وأخيرًا صدر التشريع الفيدرالي في 2000/6/30م الذي اعترف بحجية المحرَّر الإلكتروني في الإثبات، دون أن يتطلب الحصول على شهادة تصديق إلكتروني[98].

أما فرنسا فقد اكتفت بتعديل قانون الإثبات والمرافعات، حيث صدر القانون رقم (230) لسنة 2000م في صورة تعديل للنصوص المنظِّمة للإثبات في القانون المدني الفرنسي، حيث اعترفت بحجية المحرَّر الإلكتروني كدليل كتابي كامل[99].

وفي الأردن صدر قانون المعاملات الإلكتروني المؤقت رقم (85) لسنة 2001م؛ إذ نصت المادة (7/أ) على حجية التوقيع الإلكتروني في الإثبات، ومساواته بالتوقيع الخطي من حيث ترتيب آثاره القانونية.

وفي تونس صدر القانون رقم (83) لسنة 2001م المتعلق بالتجارة والمداولات الإلكترونية، وقد أعطى هذا القانون للمحرَّرات الإلكتروني حجية العقد الكتابي والتوقيع الإلكتروني ذاتيهما.

المطلب الثاني - مشروعية الحصول على الدليل الإلكتروني:

يشترط في الدليل الجنائي عمومًا لقبوله كدليل إثبات، أن يتم الحصول عليه بطريقة مشروعة، وذلك يقتضي أن تكون الجهة المختصة لجمع الأدلة قد التزمت بالشروط التي يحددها القانون في هذا الشأن، فمبدأ مشروعية الدليل الإلكتروني يعني ضرورة اتفاق الإجراء مع القواعد القانونية والأنظمة في وجدان المجتمع المتحضر[100]، أي إن قاعدة المشروعية للدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضًا مراعاة إعلانات حقوق الإنسان والمواثيق والاتفاقات الدولية[101]، وقواعد النظام العام وحسن الآداب في المجتمع، بالإضافة إلى المبادئ التي استقرت عليها المحاكم.

إن الشرعية الإجرائية هي الحلقة التي تكفل احترام الحرية الشخصية للمتهم عن طريق اشتراط أن يكون القانون هو المصدر التنظيمي الإجرائي، وأن تفترض براءة المتهم في كل إجراء من الإجراءات التي تتخذ قِبلهُ، وأن يتوافر الضمان القضائي في الإجراءات، فالشرعية الإجرائية هي امتداد طبيعي لشرعية الجرائم والعقوبات، بل هي - في الواقع - أكثر خطورة منها وأعظم شأنًا، فهي بمثابة الإطار الخارجي الذي لا يمكن تطبيق القاعدة الموضوعية تطبيقًا صحيحًا إلا عن طريقه[102].

ويتضح من ذلك أن الشرعية الإجرائية تقوم على ثلاثة عناصر؛ تتمثل في: الأول: الأصل في المتهم البراءة، بحيث لا يجوز تقييد حريته إلا في إطار من الضمانات الدستورية اللازمة لحمايتها وبناءً على نص في قانون الإجراءات أو أصول المحاكمات الجزائية، فكما هو ثابت في قانون العقوبات أنه لا جريمة ولا عقوبة إلا بنص، فإن الثابت في قوانين الإجراءات الجنائية أنه لا إجراء إلا بنص، وهذا هو العنصر الثاني من عناصر الشرعية الجنائية، أما العنصر الثالث فيتمثل في ضرورة إشراف القضاء على جميع الإجراءات بوصفه الحارس الطبيعي للحقوق والحريات[103].

ونحن هنا إذ نبحث مشروعية الدليل الإلكتروني فإننا سنقتصر على ما يثيره جمع هذا الدليل من إشكاليات قانونية، بالنظر إلى طبيعته الخاصة[104]؛ ولذا يمكننا القول إن ما يثيره الدليل الإلكتروني من حيث مشروعية الحصول عليه يتركز بشكل أساسي في إجراءات التفتيش للبحث عن هذا الدليل، وذلك يثير نقطة مهمة هي مدى مشروعية التفتيش عن الدليل الإلكتروني وضبطه في الوسط الافتراضي.

ومردُّ هذه الإشكالية يتعلق بإجراء التفتيش الذي يجب أن يمارس من ذي صفة وهو عضو الضبط القضائي أو جهة التحقيق، حسب الأحوال، فهل لهؤلاء القدرة على تفتيش الوسط الافتراضي (شبكة الإنترنت) وضبط ما سيسفر عنه من أدلة؟ ولذلك فإننا سنتناول الإجابة عن هذه التساؤلات في الفرعين الآتيين:

الفرع الأول - مشروعية التفتيش عن الدليل الجنائي الإلكتروني في الكيانات المعنوية (الوسط الافتراضي) وضبط محتوياتها:

إن الإشكالية التي نطرحها في شأن مشروعية تفتيش الوسط الافتراضي ترجع في الواقع إلى تحديد المقصود بمصطلح «شيء» الذي يفترض أن يكون محلًا للتفتيش والضبط، فإذا كان التفتيش ينصبّ على شيء فإن التساؤل يثار حول مدى انطباق لفظ «شيء» على الكيانات المعنوية «الوسط الافتراضي»؟ ولذلك أهمية عملية، فإذا كانت هذه المكونات لا تكتسب صفة الشيء بالمعنى الذي يعبر عنه النص القانوني، فإنها لا يمكن أن تكون محلًا للتفتيش والمشكلة لا تقتصر فقط على مشروعية التفتيش، وإنما أيضًا تمتد إلى مشروعية ضبط البيانات التي توجد في الوسط الافتراضي[105]؛ إذ إن النص القانوني ينصرف إلى تفتيش الأشياء وضبط ما يوجد بها من أشياء، فما المقصود بلفظ «شيء»؟ وبعبارة أوضح: أيعد الوسط الافتراضي وما به من بيانات شيئًا في تطبيق أحكام التفتيش والضبط؟

وقد اختلف الفقه في مدى جواز تفتيش الوسط الافتراضي وضبط ما به من محتويات، فذهب في ذلك إلى ثلاثة اتجاهات:

الاتجاه الأول: ذهب إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها، سواء كانت (محسوسة أم غير محسوسة).

الاتجاه الثاني: ذهب إلى عدم جواز ضبط البيانات الإلكترونية.

الاتجاه الثالث: يرى ضرورة إهمال الجدال حول مصطلح «الشيء»، والعبرة عنده الواقع، فالضبط لا يمكن وقوعه عمليًا إلا على أشياء مادية، لذلك فإن المشكلة ليست مشكلة مصطلح عبر عنه النص القانوني، وإنما هي تتعلق بإمكانية اتخاذ الإجراء. وترتيبًا على ذلك فإن تفتيش الوسط الافتراضي يكون صحيحًا إذا أسفر عنه وجود بيانات اتخذت في ما بعد شكلًا ماديًا، وهذا الاتجاه قد أخذ به قانون الإجراءات الألماني في القسم (94)، حيث نص على أن «الأدلة المضبوطة يجب أن تكون ملموسة»، ولذلك فإن البيانات إذا تمت طبعتها تعد أشياء ملموسة، وبالتالي يمكن ضبطها[106]، ونحن برأينا نؤيد الاتجاه الأول والذي يعد حلًا يتلاءم مع طبيعة جرائم الإنترنت؛ إذ إن الأدلة الرقمية يمكن التعويل عليها لإثبات وقوع الجريمة، ويمكن الاعتماد على الأدلة الإلكترونية إذا قدمت أيضًا على شكل رقمي أو ورقي. وقد اتجه المشرع العراقي إلى هذا الاتجاه، حيث أجاز أن تقدم الأدلة الإلكترونية على شكل نسخ إلكترونية أو ورقية[107].

الفرع الثاني - مشروعية التفتيش بالنظر إلى مكان وجود الجهاز المراد تفتيشه:

قد ترتكب الجريمة بواسطة منظومة لمجموعة من أجهزة الحاسوب تتوزع في أكثر من دولة، والسؤال الذي يطرح هنا هو: هل يمكن تفتيش تلك

الحواسب للبحث عن أدلة تتعلق بتلك الجريمة، بما في ذلك تلك الأجهزة الموجودة في إقليم دولة أخرى؟

ومن القواعد المتفق عليها أن نطاق تطبيق قانون أصول المحاكمات الجزائية يرتبط بنطاق تطبيق قانون العقوبات، فكلما كان هذا الأخير واجب التطبيق طُبِّق الأول، ومن القواعد المتفق عليها أيضًا أنه لا تلازم بين تطبيق قانون العقوبات وارتكاب الجريمة على إقليم الدولة؛ إذ قد ترتكب خارج إقليمها ومع ذلك فإن قانونها يكون واجب التطبيق، كالاختصاص وفقًا لمبدأ العينية والشخصية والعالمية الجنائية، فضلًا عن ذلك فإن الجريمة قد ترتكب في إقليم دولة ما وتمتد آثارها إلى إقليم دولة أخرى، فإذا كانت هذه دولة مختصة لتولّي التحقيق في هذه الجريمة؛ لأن قانون عقوباتها واجب التطبيق، فإن التساؤل يثار حول مدى إمكانية تفتيش الآلة الموجودة خارج الإقليم بواسطة السلطات التابعة لهذه الدولة[108].

ويجب أن نشير هنا إلى أن الوسط الافتراضي للشبكة العنكبوتية لا يرتبط بنطاق إقليم دولة ما، فإن مكان تفتيشه هو المكان الذي يوجد به الحاسوب المراد تفتيشه فإن اختصاص الدولة بالتحقيق في جريمة ما وإن كان يخولها تطبيق قانون إجراءاتها بشأن هذا التحقيق، بصرف النظر عن مكان وقوع الجريمة، ما دامت خاضعة لقانون العقوبات الخاص بها، إلا أن ذلك لا يعني أن تباشر الدولة هذه الإجراءات خارج إقليمها؛ لأن ذلك من مظاهر سيادتها، فلا يسمح لها بممارسته على إقليم دولة أخرى، ولذا فإن من المتعذر قانونًا مباشرة الدولة المختصة بالتحقيق لأي إجراء خارج إقليمها بشأن الجريمة رغم انعقاد اختصاصها بالتحقيق فيها، ولذا تبدو مشكلة الحصول على دليل بشأن بعض الجرائم إذا كان الدليل المراد الحصول عليه يوجد في جهاز موجود في دولة أخرى في إطار الإشكالية المعروضة؛ إذ لن تتمكن سلطات التحقيق من الحصول عليه،

ولذا تبدو اتفاقيات الإنابة القضائية هي السبيل لتحصيل هذا الدليل، بحيث تفوض الدولة الأخرىٰ في جمع هذا الدليل وإرساله لدولة التحقيق، فقد نصت المادة (25/أ) من قانون الحاسوب الهولندي علىٰ الاعتداد بالدليل المتحصل عليه في إقليم دولة أخرىٰ، إذا تم ذلك تنفيذًا لاتفاقيات التعاون الأمني والقضائي، وأحيانًا تكون تلك الدولة مختصة هي الأخرىٰ بالتحقيق في هذه الجرائم؛ ولذا فإن لم ترغب في مباشرة التحقيق بشأنها قد تتطوع بتزويد دولة التحقيق بالبيانات التي تم ضبطها وفقًا لما يعرف بنظام تبادل المعلومات أو المساعدات.

وقد نصت اتفاقية بودابست علىٰ هذا النظام في المادة (25/أ) بقولها: «تقوم الدول الأطراف بالاتفاقية بتقديم المساعدات المتبادلة لبعضها البعض إلىٰ أقصىٰ حد ممكن، وذلك للأغراض الخاصة بعمليات التحقيق أو الإجراءات المتعلقة بالجرائم التي لها علاقة بنظم الحاسوب وبياناته أو بالنسبة لجمع الأدلة الخاصة بالجريمة الخاصة في شكل إلكتروني».

أما في ما يتعلق بتفتيش الوسط الافتراضي (شبكة الإنترنت)، فإن هذا الوسط الافتراضي يأخذ حكم المكان الذي يوجد فيه الجهاز، فإذا وجد في مكان ينطبق عليه وصف المسكن وجب الالتزام في تفتيشه بالأحكام الخاصة بتفتيش المساكن[109]، غير أن السؤال الذي يطرح هنا هو: ما الحكم لو كانت النهاية الطرفية للنظام المعلوماتي المراد تفتيشه تمتد لمسكن آخر غير مسكن المتهم، فهل يمكن تفتيشه في هذه الحالة؟

حسمت بعض القوانين هذه المسألة بإجازة التفتيش في هذه الحالة كالقانون الهولندي في المادة (25/أ) من قانون جرائم الحاسوب، ودون الحاجة للحصول علىٰ إذن مسبق من أية جهة، بشرط ألا تكون النهاية الطرفية لذلك النظام في إقليم دولة أخرىٰ[110]، ولكننا نرىٰ أن هذا الحكم لا يمكن تطبيقه وفق نصوص

القانون العراقي؛ لأن هذا النوع من التفتيش ينطوي في الحقيقة على معنى تفتيش غير المتهم، ولذلك فإنه لا يجوز تطبيقه إلا في الأحوال التي يجوز فيها للقائم بالتفتيش غير المتهم أو منزله.

ويشترط لصحة التفتيش كإجراء من إجراءات التحقيق، أن يهدف إلى جمع أدلة حول جريمة قد وقعت بالفعل؛ ولذا فإنه في ما يتعلق بصحة التفتيش الوسط الافتراضي أو الحاسوب، يشترط أن يكون الفعل المراد الحصول على دليل بشأنه يشكل جريمة، فإذا كان التفتيش يتعلق بجرائم الإنترنت بالمفهوم الضيق، فإنه قد لا يوجد نص في قانون دولة ما، يؤكد على تجريم هذا النمط من السلوك، وهو ما يجعل التفتيش غير مشروع؛ لتخلف أحد شروطه؛ لانتفاء صفة الجريمة عن الفعل وفقًا لمبدأ الشرعية الجنائية، حيث إن الدليل الإلكتروني لا يقتصر مجال العمل به كدليل إثبات على جرائم الحاسوب؛ فهو يصلح لإثبات الجرائم كافة التي ترتكب بواسطة الحاسوب والإنترنت، ولذا فإنه وإن خلا تشريع دولة ما من النص على تجريم أنماط السلوك التي تمس بنظام المعلومات، فإن ذلك لا يمنع من قيام وصف الجريمة للفعل المراد جمع الدليل بشأنه في حالات كثيرة لاستعمال الحاسوب في تزوير شبكة الإنترنت واستعمالها في إرسال رسائل ذم وقدح وتشهير أو تهديد؛ إذ إن وصف الجريمة يثبت لهذه الأفعال وفقًا للتكييف التقليدي المقرر وفق قانون العقوبات، فالحاسوب في هذه الحالة وسيلة لارتكاب الجريمة ولا يغير من وصفها كجريمة تقليدية إن جاز التعبير[111].

المطلب الثالث - سلطة القاضي الجنائي في قبول الدليل الإلكتروني:

القاعدة التي تسود التشريعات الجزائية في الإثبات هي أن المحكمة تحكم في هذه الدعوة بناءً على اقتناعها الذي تكوَّن لديها من الأدلة المقدمة في أي دور

من أدوار التحقيق أو المحاكمة[112]، لا سلطان عليها في ذلك إلا لضمير القضاة، ولا تطالب إلا ببيان سبب اقتناعها بدليل دون آخر، فهي لا تلزم بقرار صادر من المتهم أو شهادة إثبات أسفرت الجريمة إليه أو شهادة دفاع نفت التهمة عنه أو رأي قدمه خبير[113]، إلا إذا اقتنعت به، كما أن الأدلة الجزائية التي تستقي منها المحاكم قناعاتها ليست محددة حصرًا، لكن القانون ذكر بعضها، وهي الغالب الشائع، وتتمثل في (الإقرار والشهادة ومحاضر التحقيق ومحاضر الكشوف الرسمية الأخرى وتقارير الخبراء والفنيين)، ثم جاء القانون بنص عام ليشمل غيرها من الأدلة بقوله: «والقرائن والأدلة الأخرى المقررة قانونًا»[114].

وعلى ذلك فإنه يكون للقاضي كامل الحرية في تقدير الأدلة كافة المطروحة عليه في الدعوى، وله أن يفاضل بين جميع هذه الأدلة، فيأخذ بما يطمئن إليه من أدلة ويعرض عما لا يطمئن إليه من أدلة أخرى.

وبصدور قانون التوقيع الإلكتروني لسنة 2012م نجد أن المشرع قد أقر للدليل الإلكتروني بالحجية المقررة للدليل التقليدي، وبذلك يمكن اعتبار الأدلة الإلكترونية هي أدلة مقبولة، إذا توافرت فيها شروط معينة[115]، وللقاضي الجنائي الحرية في تقدير جمع أدلة الدعوى الجزائية، بغض النظر عن مَصْدرها الذي استمدت منه طالما كان مشروعًا، ويستوي في ذلك الدليل الجنائي التقليدي والدليل الجنائي الإلكتروني، فباب الإثبات مفتوح على مصراعيه أمامه يأخذ بأي دليل يطمئن إليه وجدانه، ويطرح كل دليل يدور الشك حوله؛ وذلك بغية الوصول للحقيقة، كما يجب أن تكون عقيدة القاضي واقتناعه بالأدلة قد استمدت من مخرجات إلكترونية طرحت بالجلسة؛ لأن القاعدة هي أن لا يحكم إلا بناءً على التحقيقات التي تحصل بالطرق والشروط القانونية، وليس بناءً على معلوماته الشخصية، أو على ما قد يكون رآه بنفسه أو حقيقة في غير مجلس القضاء، كما ينبغي أن يؤسس القاضي الجزائي حكمه على دليل ناتج من الحاسب الآلي لَحِقه

سبب يبطله ويُعْدم أثره[116]، عليه وتحقيقًا لليقينية والشفوية المشروعية في الدليل، فإن مجمل شروط قبول المخرجات الإلكترونية تتلخص في المبادئ الثلاثة الآتية[117]:

1- مبدأ يقينية الدليل الجنائي الإلكتروني.

2- مبدأ وجوب مناقشة الدليل الجنائي الإلكتروني.

3- مبدأ مشروعية الدليل الجنائي الإلكتروني.

وسنتناول هذه المبادئ بالشرح من خلال الفروع الآتية:

الفرع الأول - مبدأ يقينية الدليل الإلكتروني:

إن الراجح في الفقه الجنائي المعاصر هو تقسيم اليقين من حيث مصدره إلى يقين قانوني، ويقين معنوي، فاليقين القانوني: يعني تلك الحالة الناجمة عن القيمة التي يضيفها القانون على الأدلة ويفرضها على القاضي بمقتضى ما يصدره من أدلة قانونية محدودة، فهو نوع من اليقين يتلقاه القاضي عن إرادة، وهذا النوع من اليقين هو السائد في القانون الإنجليزي[118].

إلا أن القانون العام في إنجلترا لم يعد يأخذ بنظرية الأدلة القانونية على الإطلاق، بل بدأ يتقبل مبدأ حرية تقدير الأدلة، لذلك فقد أصبح الحديث عن الإدانة بدون أي شك معقول أو الإدانة الخالية من أي شك، هو السائد في القانون الإنجليزي حاليًا، ومن هذا المنطلق فإن القضاء الإنجليزي يملك حرية الحكم بالإدانة بناء على شهادة شخص واحد، طالما أن هذه الشهادة تحقق اليقين إذا كانت القاعدة العامة في إنجلترا هي أن المحكمة الجنائية لا يجب أن تدين المدعي عليه إلا عندما تكون عناصر الجريمة تم إثباتها بعيدًا عن أي شيء معقول[119].

وإذا انتقلنا لمناقشة يقينية المخرجات الإلكترونية نجد أن قانون البوليس أو الإثبات الجزائي ببريطانيا يشترط لتحقق يقينية المخرجات الإلكترونية، أن تكون البيانات دقيقة وناتجة عن حاسب يعمل بصورة سليمة[120]، أما في فرنسا فإنه لا محل لدحض أصل البراءة وافتراض العكس، إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين. والأمر لا يختلف بالنسبة لمخرجات الحاسب الآلي؛ إذ يشترط القانون الفرنسي في المخرجات الإلكترونية أن تكون يقينية حتى يمكن الحكم بالإدانة؛ ذلك أنّ لا محل لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين، ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من مخرجات كمبيوترية، سواء كانت مخرجات لا ورقية أو إلكترونية كالأشرطة المغناطيسية والأقراص المغناطيسية والمصنفات الفلمية وغيرها من الأشكال الإلكترونية غير التقليدية للتكنولوجيا التي تتوافر عن طريق الوصول المباشر أم كانت أخيرًا مجرد عرض لهذه المخرجات المعالجة بواسطة الإلكترونية على الشاشة الخاصة به أو على الطرفيات[121].

وفي سبيل يقينية الدليل الجنائي ذهبت بعض التشريعات، كما في اليونان والنمسا وسويسرا أو النرويج، إلى ضرورة أن يكون الدليل الإلكتروني مقروءًا، سواء كان مطبوعًا على ورق بعد خروجه من الحاسوب أم كان مقروءًا على شاشة الحاسوب ذاته[122]، وعلى الاتجاه ذاته سار المشرع العراقي؛ إذ نص في المادة (ثانيًا/26) من مشروع قانون جرائم المعلوماتية العراقي على أنه: «تقوم الجهة التي تجمع الأدلة بما يأتي: ب- تقديم النسخ الإلكترونية أو الورقية من الأدلة»، وبذلك فإن المشرع أجاز أن يكون الدليل المقدَّم على شكل نسخ إلكترونية أو ورقية.

إن سلطة القاضي الجنائي في تقدير الدليل لا يمكن أن نتوسع في شأنها

بحيث يقال: إن هذه السلطة تمتد لتشمل الأدلة العلمية، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الرقمي، فضلًا عن ذلك فإن هذا الدليل يتمتع من حيث قوته الإثباتية بقيمة إثباتيةٍ قد تصل إلى حد اليقين، فهذا هو شأن الأدلة العلمية عمومًا، فالدليل الإلكتروني من حيث إثباته على الواقع تتوفر فيه شروط اليقين مما لا يمكن معه القبول بممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع التي يعبر عنها ذلك الدليل، ولكن هذا لا يناقض أن الدليل الإلكتروني هو موضع شك من حيث سلامته من العبث من ناحية، وصحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى، حيث يشكك في سلامة الدليل الرقمي من ناحيتين[123]:

الأولى: الدليل الإلكتروني من الممكن خضوعه للعبث به على نحو يخالف الحقيقة، ومن ثم فقد يقدم هذا الدليل معبرًا عن واقعة معينة صُنع أساسًا لأجل التعبير عنها خلافًا للحقيقة، وذلك دون أن يكون في استطاعة الشخص غير المتخصص إدراك ذلك العبث على نحو يمكن معه القول إن ذلك قد أصبح هو الشأن في النظر لسائر الأدلة الإلكترونية التي قد تقدم إلى القضاء، فالتقنية الحديثة تمكن من العبث بالدليل الإلكتروني بسهولة ويسر، بحيث يظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة.

الثانية: أن نسبة الخطأ الفني في الحصول على الدليل الإلكتروني كانت نادرة للغاية، إلا أنها تظل ممكنة، ويرجع الخطأ في الحصول على الدليل الإلكتروني لسببين[124]:

1- الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الإلكتروني؛ ويرجع ذلك للخلل في الشفرة المستخدمة، أو بسبب استخدام مواصفات خاطئة.

2- الخطأ في استخلاص الدليل، ويرجع إلى اتخاذ قرارات لاستخدام الأداة

تقل نسبة صوابها عن 10٪، ويحدث هذا غالبًا بسبب وسائل اختزال البيانات أو بسبب معالجة البيانات بطريقةٍ تختلف عن الطريقة الأصلية التي يتم تقييمها.

ومن خلال ذلك فإننا نرىٰ أن الشك في الدليل الإلكتروني لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه ولكنها تؤثر في حجيته الإثباتية بسبب الطبيعة الفنية لهذا الدليل. وهناك عدة وسائل يتم بها تقييم الدليل الإلكتروني والتأكد من سلامته وصحة الإجراءات المتبعة للحصول عليه، منها فكرة التحليل التناظري الإلكتروني التي يتم من خلالها مقارنة الدليل الإلكتروني المقدَّم للقضاء، وعن طريق ذلك يتم التأكد من مدىٰ حصول عبث في النسخة المستخرجة[125]، وكذلك استخدام عمليات حسابية تسمىٰ بـ«الخوارزميات» للتأكد من سلامة الدليل الإلكتروني من التبديل أو العبث، بالإضافة إلى الاستعانة بالدليل المحايد، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يسهم في التأكد من مدىٰ سلامة الدليل الإلكتروني المقصود من حيث عدم حصول تعديل في النظم المعلوماتية أو تغيير فيها[126].

الفرع الثاني - مبدأ وجوب مناقشة الدليل الإلكتروني:

الأصل الذي يحكم إجراءات المحاكمة هو أن تكون المرافعة شفوية وحضورية، والمقصود بالمرافعة هنا جميع إجراءات التحقيق النهائي الذي تجريه المحكمة[127]، ومفهوم مبدأ وجوب مناقشة الدليل الإلكتروني بصفةٍ عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا علىٰ العناصر الإثباتية التي طُرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوىٰ، ولا يختلف الأمر بالنسبة للأدلة الإلكترونية بوصفها أدلة إثبات؛ إذ ينبغي أن تطرح في الجلسة، وأن يتم مناقشتها في مواجهة الأطراف[128].

وتأسيسًا على ذلك فإن الأدلة الإلكترونية، سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسب، أم كانت بيانات مدرجة في حاملات البيانات، فإنه يجب مناقشتها وتحليلها[129].

إن قاعدة وجوب مناقشة الدليل الجزائي، سواء كان دليلًا تقليديًا أم كان ناتجًا عن الحاسب الآلي، تعد ضمانات مهمة وأكيدة للعدالة، حتى لا يحكم القاضي الجزائي في الجرائم المعلوماتية بمعلوماته الشخصية أو بناءً على رأي الغير[130].

ففكرة عدم جواز أن يقضي القاضي في جرائم الإنترنت بناءً على معلوماته الشخصية، من أهم النتائج المترتبة على قاعدة وجوب مناقشة الدليل الجنائي أو طرحه، سواء كان دليلًا تقليديًا أم إلكترونيًا في الجلسة؛ لأنه لا يسوغ للقاضي أن يحكم بمقتضى معلوماته الشخصية في الدعوى، أو على ما رآه بنفسه أو حققه في مجلس القضاء بدون حضور الخصوم، وذلك أن هذه المعلومات لم تعرض في الجلسة ولم تتم مناقشتها وتقييمها، ومن ثم يكون الاعتماد عليها مناقضًا لقاعدتي الشفوية والمواجهة التي تسود مرحلة المحاكمة[131]، كذلك فإن هناك تناقضًا بين صفتي القاضي والشاهد؛ إذ إن الشهادة تتطلب إدراك الوقائع ثم نقلها إلى حيز الدعوى، وفي هذه العملية تتدخل اعتباراتٌ عدة، منها عنصر التقدير لدى الشاهد وإدراكه وذاكرته، إلى غير ذلك من العوامل والمؤثرات التي لها دخل كبير في تقدير الشهادة، ولهذا يحتاج الأمر من جهة القاضي إلى تقدير لأقواله، وتمحيص لها، وهو جدير بذلك؛ لما له من ملكتي النقد والتفسير، أما إذا كان مصدر هذه الشهادة هو القاضي نفسه، فيتعذر عليه إجراء الرقابة المطلوبة؛ إذ يقع حينئذ في صراع مع نفسه؛ لأن الأمر يقتضي أن تكون المعلومات التي يدلي بها بعيدة عن التحيز والتأثيرات الشخصية[132].

الفرع الثالث - مبدأ مشروعية الدليل الإلكتروني:

تعني مشروعية الدليـل الإلكتروني ارتكازه على إجراءات مشروعة، سواء كانت تلك الإجراءات قد صـدرت من قِبَـل القـاضي بصـورة مباشرة أو غير مباشرة، أم من قِبَل المتهم عند استجوابه واعترافه، أم من قِبَل الغير بعد القيام بالقبض عليه واستجوابه أو تفتيشه أو تفتيش مسكنه، أو ممارسة أي عمل من أعمال الخبرة الفنية.

ولا تقتصر رقابة القضاء على أعمال الاستدلال الأصلية أو الاستثنائية. أو على تقـدير الدليـل فقط. وإنما تمتد هذه الرقابة أيضًا إلى مشروعية الدليل والأسلوب الذي حصلت به جهـات التحقيق على الدليل، وهل خالف قاعدةً إجرائيةً أم لا؟ فمشروعية الدليل بصفةٍ عامةٍ شرطٌ أساسيٌّ للوصول إلى اليقين القضـائي عنـد الإدانة، ولا يحـول دون ذلك أن تكون أدلة الإدانة واضـحة وصارخة، ما دامت هذه الأدلة مشـبوهة ولا يتسم مصـدرها بالنزاهة واحترام القانون، ومعيار مشروعية الأدلة يكمن في احـترام ضمانات الحرية الشخصية التي نص عليها القانون لاحترام حرية الفرد بوصفه بريئًا إلى أن تثبت إدانته بحكمٍ باتٍّ[133]، وبالتالي فلا يجوز للقاضي الجنائي أن يعتمد على دليل باطلٍ أو مجرد من قيمته القانونية، ويستمد منه قناعته الذاتية، ويدخل في مدلول الدليل الباطل ذلك الدليل الذي لم يستوفِ شرطًا من الشروط التي يتطلبها القانون فيه كي تكون له قوة إقناعية للقاضي، فاقتناع القاضي يجب أن يكون مبنيًا على دليـلٍ مستمدٍّ من إجراء صحيح ومشروع، أما إذا بني هذا الاقتناع على أدلةٍ باطلةٍ أو إجراءاتٍ غير مشروعةٍ، كان مؤديًا إلى بطلان الحكم، تطبيقًا لقاعدة «ما بني على باطل فهو باطل»[134]، ولذا يجب أن تكون تلك الإجراءات مطابقةً للقانون غير متعارضةٍ مع المبادئ الأخلاقية والعلمية[135].

والإجراءات الجنائية تكون قانونية وتتسم بالمشروعية حينما يلتزم القاضي الجنائي بأحكام القانون فلا يبتعد أو يخرج عن الطريق الذي رسمه القانون، أما إذا جهل أو تجاهل قاعدةً قانونيةً، موضوعيةً كانت أم شكلية، أو أوّل تلك القواعد أو فسَّرها تأويلًا أو تفسيرًا غير حقيقي أو غير منطقي، فإن هذا الجهل أو التجاهل من ناحية، أو الخطأ في التأويل أو التفسير من ناحيةٍ أخرىٰ، ينعكس بصدقٍ علىٰ الاقتناع الذي حصله؛ لأنه ثمرة الخطوات التي خطاها أو محصلتها، وهو نتيجة العمليات التي أجراها بطريقةٍ اتسمت بالخطأ أو بالفساد، وفي مجال جرائم الإنترنت نرىٰ أنه من الضروري الاستعانة بالخبرة القضائية للتأكد من سلامة الدليل الإلكتروني من العبث أو الخطأ، بالإضافة إلىٰ مراقبة القاضي صحة إجراءات جمع الدليل الإلكتروني.

*

الخاتمة:

تبرز خاتمة هذا البحث أهم النتائج التي تم التوصل إليها، وتبين أهم المقترحات التي يفضل اعتمادها، فإذا كان موضوع هذا البحث قد تناول أدلة الإثبات المتحصلة من الوسائل الإلكترونية، فإنه يكون بذلك قد تناول مشكلة من المشكلات التي أفرزتها ثورة الاتصالات عن بعد، فهذه الثورة - كما نعلم رغم أنها أسعدت البشرية ويسرت لها سبل الحياة، فقد أتعستها بهذه النوعية الجديدة من الجرائم التي أسهمت هذه الثورة في ارتكابها والتي تتميز بطبيعةٍ فنيةٍ وعلميةٍ معقدة، ويتصف مرتكبوها بطبيعةٍ ذكيةٍ ماكرة؛ إذ إننا في مجال المعلوماتية بدأنا نسمع عن العمليات المصرفية الإلكترونية وعن النقود الإلكترونية وعن المستندات الإلكترونية، وعن الحكومة الإلكترونية، وعن التوقيعات الإلكترونية.

ولا شـك أن ظهـور هذه العمليات الإلكترونيـة الجديدة ووجوب حمايتها جنائيًا، من صـور الاعتـداء المتطـور التي قد تقـع عليها بالوسـائل الإلكترونية المتطورة، كل هذا قد أظهر أن هناك قصورًا كبيرًا في النصوص الجنائية الموضوعية والإجرائيـة، بحيث إن هذه النصـوص قد أصبحت عاجزة عن كفـالة الحمـاية الفعالة للمصالح والقيم التي أفرزتها ثورة الاتصالات عن بعد.

وليس ثمة شك في وجود صعوبة كبيرة في إثبات الجرائم الإلكترونية بالنظر إلى طبيعة الدليل الذي يتحصل منها؛ إذ قد يكون الدليل غير مرئي، وقد يسهل إخفاؤه أو تدميره، وقد يكون متصلًا بدول أخرى، فتكون هناك صعوبة في الحصول عليه، نظرًا لتمسك كل دولة بسيادتها، كما أن هذا الإثبات قد يحتاج إلى معرفة علمية وفنية قد لا تتوافر بالنسبة لرجال الشرطة وللمحققين وللقضاة.

*

النتائج والمقترحات:

أولاً- النتائج:

لقد توصل البحث من خلال هذه الدراسة إلى النتائج الآتية:

1- أظهر البحث أن هناك قصورًا واضحًا في كثير من التشريعات الجنائية الموضـوعية والإجرائية العربيـة في مواجهـة ظاهرة الجرائم التي تقـع بالوسـائل الإلكترونيـة أو عـلى هذه الوسـائل، فما زال الكثير منهـا يخضـع هذه الجرائم للنصوص التقليدية، وهو ما قد يترتب عليه الاعتداء على مبدأ شرعية الجرائم والعقوبات، أو إفلات الكثير من الجناة من العقاب. فعـلى الرغم من انتشار

الوسائل الإلكترونية في هذه الدول، إلا أن الكثير من تشريعاتها لم تمسها يد التعديل؛ لكي تقوىٰ علىٰ حماية المصالح المستجدة التي أفرزتها هذه الوسائل.

2- أظهر البحث كذلك أن هناك صعوبة تكتنف الدليل الجنائي بالنسبة للجرائم الإلكترونية، سواء من حيث طرق الحصول عليه أو من حيث طبيعته. فالحصول عليه قد يحتاج إلىٰ عمليات فنية وعلمية وحسابية معقدة. كما أن طبيعته قد تكون غير مرئية، كالذبذبات والنبضات، وأنه من السهولة استخدام التقنية العلمية في إخفائه أو إتلافه. وقد يتم ذلك عن طريق التشفير وكلمات المرور السرية واستخدام الفيروسات المدمرة أو التالفة.

3- أظهر البحث أن الإثبات الجنائي مهما تطور بالنسبة للجرائم الإلكترونية وعلا شأن الأدلة العلمية والفنية - في هذا الإثبات - فإنه يجب أن نُبقي علىٰ سلطة القاضي التقديرية في تقديره لهذه الأدلة العلمية والفنية؛ لأننا بذلك نضمن تنقية هذه الأدلة من شوائب الحقيقة العلمية، ويظل القاضي هو المسيطر علىٰ هذه الحقيقة؛ لأنه من خلال سلطته التقديرية يستطيع أن يفسر الشك لصالح المتهم، وأن يستبعد الأدلة التي يتم الحصول عليها بطريقة غير مشروعة.

ثانيًا- المقترحات:

وعلىٰ ضوء النتائج السابقة فقد توصل البحث إلىٰ المقترحات الآتية:

1- من الضروري علىٰ التشريعات العربية أن تسرع الخطىٰ لتعديل قوانينها العقابية لكي تواكب ثورة الاتصالات عن بعد، لكي لا يحدث انفصال بين الواقع والقانون بما يضر المجتمع وأفراده، وعلىٰ النحو الذي سارت عليه الكثير من التشريعات الأجنبية وبعض التشريعات العربية بأن نصت صراحةً علىٰ تجريم الأفعال غير المشروعة التي أفرزتها هذه الثورة.

2- الاهتمام بتدريب الخبراء والمحققين والقضاة على التعامل مع الجرائم الإلكترونية ذات الطبيعة الفنية والعلمية المعقدة، بحيث يمكن الوصول إلى الحقيقة وإماطة اللثام عن هذه الجرائم تحقيقًا لصالح المجتمع وأفراده، لصالح المتهمين أنفسهم؛ لكي لا يدان إلا المسيء.

3- الاهتمام بالإثبات بالقرائن وبالأدلة العلمية؛ كي يستطيع القضاة الوصول إلى الحقيقة من خلال هذه الوسائل الحديثة للإثبات الجنائي.

4- السماح للجهات القائمة على التفتيش بضبط برامج الحاسوب والمعلومات الموجودة في الأجهزة وفقًا للشروط ذاتها الخاصة بإجراءات التفتيش العادية، وضرورة إصدار دليل إرشادي تقني وقانوني حول صور جرائم الحاسوب والأصول العلمية لكشفها والتحقيق فيها وأساليب التعامل مع الأدلة الإلكترونية، ومواصلة تحديث هذا الدليل بشكل دوري، وكلما دعت الحاجة لذلك، وتعميمه على العاملين في مجال التحقيق، وعلى أجهزة القضاء الاستفادة من الدليل الصادر عن المنظمة العالمية للشرطة الجنائية (الإنتربول).

*

الهـوامش

(1) ممـدوح عبـد الحميـد عبد المطلب، البحث والتحقيق الجنـائي الرقمي في جرائم الكمبيـوتر والإنترنت، دار الكتب القانونية، مصر، 2006، ص88.

(2) طارق محمد الجمـلي، الدليـل الرقمي في مجـال الإثبات الجنائي، ورقة عمـل مقـدَّمة للمـؤتمر المغاربي الأول للمعلوماتية القانون، المنعقد في الفترة (28-2009/10/29م) تنظمه أكاديمية الدراسات العليا، طرابلس، ص5.

(3) Interrdpatinorgnazation on Computer Evidence.

(4) هدى طلب علي، الإثبات الجنـائي في جرائم الإنترنت والاختصـاص القضـائي بهـا، رسـالة ماجستير، كلية الحقوق، جامعة النهرين،2012م، ص116.

(5) المرجع نفسه، ص116.

(6) ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنـائي الـرقمي في جـرائم الكمبيـوتر والإنترنت، مرجع سابق، ص88.

(7) خـالد ممـدوح إبراهيم، الدليـل الرقمي في الجـرائم الإلكترونيـة، بحث منشـور عـلى الموقـع الإلكتروني الآتي: www.f-low.net/low/threads/19223.

(8) عبد الناصر حمد محمود فرغلي ومحمد عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونيـة والفنيـة، بحث من ضمن أعمـال المؤتمر العـربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض 2007.

(9) خالد عياد الحلبي، إجراءات التحري والتحقيـق في جـرائم الحاسـوب والإنترنـت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2011، ص234.

(10) المرجع نفسه، ص234.

(11) عبد الفتاح بيومي حجازي، الدليل الجنـائي والتزويـر في جـرائم الكمبيـوتر والإنترنـت، دار الكتب القانونية، مصر، 2005م ، ص64.

(12) ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنـائي الـرقمي في جـرائم الكمبيـوتر والإنترنت، المرجع السابق.

(13) عبد الناصر حمد محمود فرغلي ومحمد عبيد سيف المسماري، مرجع سابق، ص14.

(14) طارق محمد الجميلي، مرجع سابق، ص6.

(15) ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (TCP/IP) في بحث وتحقيق الجرائم على الكومبيوتر والمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليـات الإلكترونيـة وأنظمة أكاديمية شرطة دبي، مركز البحوث والدراسات العدد (4) المحور الأمـني والإداري، الإمارات العربية المتحدة، دبي 2003، ص649-650.

(16) عمر محمد بن يونس، الدليل الرقمي، ط1، مصر، 2007، ص47.
(17) عبد الناصر حمد محمود فرغلي ومحمد عبيد المسماري، مرجع سابق، ص15.
(18) طارق محمد الجملي، مرجع سابق، ص6.
(19) ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص90.
(20) حسين طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1420هـ، 2000، ص288 وما بعدها.
(21) المرجع نفسه، ص123.
(22) المرجع نفسه، ص123.
(23) المرجع نفسه، ص124.
(24) ممدوح عبد الحميد، جرائم الكمبيوتر عبر الإنترنت، إصدارات مكتبة الحقوق، الشارقة، الإمارات، 2000، ص35 وما بعدها.
(25) ممدوح عبد الحميد، استخدام التحليل التناظري الرقمي في تحقيق الجرائم عبر الكمبيوتر، دورية الفكر الشرطي، المجلد الحادي عشر، العدد44، الشارقة، 2003، ص72.
(26) Douglas Tones & Brain D. loader, "cyber", Rout edge, New York, USA, 2002, P144. نقلًا عن هدى طلب علي، الإثبات الجنائي في جرائم الإنترنت والاختصاص القضائي لها، مرجع سابق، ص126.
(27) ممدوح عبد الحميد، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص95.
(28) محمد الأمين البشري، الأدلة الجنائية الرقمية: مفهومها ودورها في الإثبات الجنائي، مرجع سابق، ص120.
(29) Saferstien, R. Criminaties: Inroduction to Forensic Scirnce, Upper Saddle, Nj: Prentice, Hill, ، نقلًا عن هدى طالب علي، إجراءات التحقيق وجمع الأدلة في جرائم الإنترنت، مرجع سابق، ص127.
(30) محمد الأمين البشري، الأدلة الجنائية الرقمية مفهومها ودورها في الإثبات الجنائي، مرجع سابق، ص121.
(31) ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر (الأعمال المصرفية الإلكترونية)، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، في الفترة 5-2003/12/10، المجلد الخامس، ص2237.
(32) علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات

الإلكترونية، مؤتمر نظمته أكاديمية شرطة دبي، مركز البحوث والدراسات رقم (1)، في الفترة 26-4/28/ 2003، ص23.

(33) عنام محمد عنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدَّم لمؤتمر القانون والكمبيوتر والانترنت، المنعقد في الفترة من 1-2000/2/3م بكلية الشريعة والقانون بدولة الإمارات العربية المتحدة، ص1.

(34) المرجع السابق، ص2.

(35) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر 2005، ص15.

(36) هشام فريد رستم، الجرائم المعلوماتية - أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم إلى مؤتمر (القانون والكمبيوتر والإنترنت) سابق التعريف به، ص21 وما بعدها.

(37) هلالي عبد الله، بحث بعنوان (المخرجات الكمبيوترية). مؤتمر القانون والكمبيوتر والإنترنت، سابق الإشارة إليه، ص2. وكذلك مؤلفه (تفتيش جهاز الحاسب الآلي)، دار النهضة العربية، القاهرة، 2000م، ص2.

(38) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص12.

(39) محمد الأمين البشري، بحث بعنوان (التحقيق في جرائم الحاسب الآلي)، مقدم إلى مؤتمر القانون والكومبيوتر والإنترنت، مرجع سابق، ص19.

(40) عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، القاهرة، ص278.

(41) Robert, W. Ferguson and Allan, Hstokke. Legal Asects of Evidence, Harcourt Brace Jovnorich, INC, New York, 1948, P.1.

نقلًا عن عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والإنترنت، ص15.

(42) عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، مرجع سابق، ص369.

(43) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص17.

(44) محمد الأمين البشري، المرجع السابق، ص33.

(45) عبد الفتاح بيومي حجازي، المرجع السابق، ص18 وما بعدها.

(46) هي جريمة تسمى (جريمة الدخول إلى نظام المعالجة الآلية للبيانات وتدميره)، وهو مجرَّم صراحة في القانون الفرنسي، ويجري البحث عن تأصيل لإسناد تجريمه في التشريعات العربية.

(47) محمد الأمين البشري، المرجع السابق، ص35.

(48) عبد الفتاح بيومي الحجازي، المرجع السابق، ص22.

(49) Harold Gosep Highland. "The hidden Dangers of Foroud" Abstracts of Revent Articles and Literature, Omputer- Security, vol.10 no.4 JUIN.

مشار إليه في: هشام فريد، المرجع السابق، ص23.

(50) عبد الفتاح بيومي حجازي، المرجع السابق، ص33.

(51) القاضي وليد عالكوم، بحث بعنوان (مفهوم ظاهرة الإجرام المعلوماتي)، مؤتمر القانون الكومبيوتر والإنترنت، سابق التعريف به، ص4 وما بعدها.

(52) غنام محمد غنام (عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر)، بحث مقدم لمؤتمر قانون الكومبيوتر والإنترنت، سابق التعريف به، ص9 وما بعدها.

(53) عمر الفاروق الحسيني، بحث بعنوان (لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجات الآلية للمعلومات)، مؤتمر القانون والكومبيوتر والإنترنت، سابق التعريف به، ص6 وما بعدها.

(54) هدى حامد قشقوش (الائتلاف لبرامج الحاسب الإلكتروني)، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، سابق التعريف به، ص7 وما بعدها.

(55) محمد الأمين البشري، المرجع السابق، ص20.

(56) عبد الفتاح بيومي حجازي، المرجع السابق، ص42.

(57) جودة حسين محمد جهاد، بحث بعنوان (المواجهة التشريعية للجريمة المنظمة بالأساليب التقدية - دراسة مقارنة)، مؤتمر القانون والكومبيوتر والإنترنت، سابق التعريف به، ص4 وما بعدها.

(58) غنام محمد غنام، المرجع السابق، ص4. وعلى سبيل المثال قام أحد الجناة في ألمانيا بإدخال تعديل في نظام الحاسب، حيث وضعه ضمن نطاق تعليمات أمنية لحماية ما فيه من بيانات مخزونة، بحيث يقوم بمحو هذه البيانات كاملة تلقائيًا عن طريق مجال كهربائي، إذا ما تم اختراق نظام المعلومات من قِبَل شخص غير مرخص له.

(59) عبد الفتاح بيومي حجازي، المرجع السابق، ص67.

(60) لذلك وطبقًا للتقديرات فإن ما بين 20 و 25٪ من جرائم الحاسبات لا يتم الإبلاغ عنها مطلقًا؛ خشية الإساءة للسمعة، إلا أن دراسة أخرى في الولايات المتحدة أجريت على 1000 شركة تنتج جهاز (Fortune)، أظهرت نتائجها أن 2٪ فقط من جرائم الحاسب هي التي يتم الإبلاغ عنها للشركة أو مكاتب التحقيقات الفيدرالي، كما سجلت دراسة أخرى في أمن الحاسبات بالولايات المتحدة عام 1988، أن 6٪ من حوادث الأمن الخطيرة هي فقط التي

يتم الإبلاغ عنها إلى السلطات المختصة. مشار إليه في مؤلّف هشام محمد فريد رستم، المرجع السابق، هامش ص42.

(61) المادة 1/ب من قانون أصول المحاكمات الجزائية العراقي.

(62) عبد الفتاح بيومي حجازي، مرجع سابق، ص70-71.

(63) عبادة أحمد عبادة - بحث بعنوان (التدمير المتعمد لأنظمة المعلومات الإلكترونية)، مركز البحوث والدراسات لدئ شرطة دبي - دولة الإمارات العربية المتحدة - العدد (87)، مارس 1999، ص4.

(64) موزة المزروعي (الاختراقات الإلكترونية: خطر كيف نواجهه)، مجلة آفاق اقتصادية، دولة الإمارات العربية المتحدة، العدد (9)، سنة 2000م، ص54.

(65) تحقيق بعنوان (إنهم يهاجمون البنوك عبر الفضاء الإلكتروني)، مجلة الإمارات اليوم، العدد (131) سنة 1996، ص19.

(66) وتشمل الجرائم الماسة بأمن الدولة الداخلي.

(67) تنص المادة 48: «كل مكلف بخدمة عامة علم في أثناء تأدية عمله أو بسبب تأديته بوقوع جريمة، أو اشتبه في وقوع جريمة تحرك الدعوئ فيها بلا شكوئ ويخبرون فورًا أحدًا ممن ذكروا في المادة (47)».

(68) جودة حسين جهاد، قانون الإجراءات الجنائية والاتحادي في دولة الإمارات العربية المتحدة، ص40 وما بعدها؛ وكذلك هشام محمد فريد، المرجع السابق، ص43-44.

(69) عبد الفتاح بيومي حجازي - الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص80.

(70) المرجع السابق، ص81.

(71) عبد الفتاح بيومي حجازي، مرجع سابق، ص81.

(72) ممدوح عبد الحميد عبد المطلب (جرائم استخدام شبكة المعلومات الدولية - الجريمة عبر الإنترنت)، بحث مقدم لمؤتمر القانون والكومبيوتر الذي عقد بكلية الشريعة والقانون - جامعة الإمارات، عام 2000م.

(73) محمد الأمين البشري، المرجع السابق، ص19.

(74) عبد الفتاح حجازي، مرجع سابق، ص84.

(75) المرجع نفسه، ص86-87.

(76) ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص41.

(77) هشام محمد فريد رستم، المرجع السابق، ص47.

(78) عبد الفتاح بيومي حجازي، المرجع السابق، ص103.

(79) المرجع السابق، ص104.

(80) المرجع نفسه، ص104.

(81) من جهود الأمم المتحدة في ذلك أن مؤتمرها الثامن من منع الجريمة والمجرمين - والذي عقد في هافانا 1990 - قد حث على قراره المتعلق بالجرائم وذات العلاقة بالحاسب الآلي والدول الأعضاء التي تكثف جهودها لمكافحة إساءة استخدام الحاسب بفعالية، وذلك بتحريم هذه الأفعال جنائيًا.

(82) جريدة الاتحاد الإماراتية، العدد (9345) يوم 2001/2/4.

(83) على سبيل المثال نجد أن قرصًا ضوئيًا واحدًا لا يتعدى وزنه 150 جرامًا وقطره 12سم يمكن أن يحتوي المادة الكاملة المدونة بألف كتاب في حجم القرآن - مثلًا - وهذا لا يمنع من تضاعف هذه السعة حسب التقدم العلمي، نبيل علي، العرب وعصر المعلومات، الكويت، 1994، ص91.

(84) هشام محمد فريد رستم، المرجع السابق، ص36.

(85) عبد الفتاح بيومي حجازي، المرجع السابق، ص109.

(86) هشام محمد فريد رستم، المرجع السابق، ص36-37.

(87) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2000، ص235.

(88) هلالي عبد الله أحمد، المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2006، ص49.

(89) علي محمود حمودة، مرجع سابق، ص30.

(90) هلالي عبد الله أحمد، مرجع سابق، ص91.

(91) علي الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي (دراسة مقارنة)، جامعة العلوم التطبيقية، البحرين، 2009م، ص16، بحث منشور على الموقع الإلكتروني الآتي: www.policeem.gov.bh/reports.

(92) هدى طلب علي، مرجع سابق، ص132.

(93) جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة - دار الثقافة العربية، القاهرة، 20023، ص22.

(94) هدى طلب علي، مرجع سابق، ص12-14.

(95) عرَّفت الفقرة الثامنة من المادة الأولى من قانون التوقيع الإلكتروني الوسيط الإلكتروني بأنه «برنامج الحاسوب أو أية وسيلة إلكترونية أخرى تستخدم من أجل تنفيذ إجراء أو الاستجابة لإجراء، بقصد إنشاء أو إرسال أو تسلم المعلومات».

(96) عرَّفت المادة (14) من القرار رقم (109) لسنة 2005 (اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري) الدعامة الإلكترونية، حيث نصت على أنها «وسيط مادي وتداول

الكتابة، ومنها الأقراص المدمجة والأقراص الضوئية والأقراص المغنطة أو الذاكرة الإلكترونية أو أي وسيط مماثل».

(97) عرَّفت المادة (12/1) من قانون التوقيع الإلكتروني العراقي لسنة 2011م التصديق الإلكتروني بأنه: «الوثيقة التي تصدرها جهة التصديق وفق أحكام هذا القانون والتي تستخدم لإثبات نسبة التوقيع الإلكتروني إلى الموقع».

(98) إبراهيم السوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، جامعة الكويت.

(99) أدرج هذا التعديل في نص المادة (1316) من القانون المدني الفرنسي في ست فقرات وأضفى على الكتابة الإلكترونية الحجية في الإثبات، شأنها في ذلك شأن الكتابة الخطية والمحرَّرات الورقية والتوقيع التقليدي، حيث نصت الفقرة (1) من المادة المذكورة من قانون التوقيع الإلكتروني الفرنسي، على أنه «يعتد بالضرورة المتخذة شكلًا إلكترونيًا كدليل، شأنها في ذلك شان الكتابة على دعامة ورقية، شريطة أن يكون في الإمكان بالضرورة تحديد هوية الشخص المدني الذي صدرت منه، وأن تعد وتحفظ في ظرف من طبيعته ضمان سلامتها». ونصت الفقرة (3) من المادة نفسها على أنه «يكون للكتابة على دعامة إلكترونية نفس القوة في الإثبات التي للكتابة على الورق». ينظر أحمد أبو عيسى عبد الحميد، مدى حجية المحرَّرات الإلكترونية في الإثبات في القانون المدني الليبي مقارنة ببعض التشريعات الأجنبية والمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد يومي (28-29) أكتوبر 2009م، أكاديمية الدراسات العليا، طرابلس.

(100) نصت المادة (10) على أنه: «إذا اشترط القانون وجود توقيع على مستند أو نص على ترتيب نتائج معينة في غياب ذلك، فإن التوقيع الإلكتروني الذي يعول عليه في إطار المعنى الوارد في المادة (21) من هذا القانون يستوفي ذلك الشرط. ويجوز لأي شخص أن يستخدم أي شكل من أشكال التوثيق الإلكتروني، إلا إذا نص القانون بغير ذلك. نقلًا عن أحمد أبو عيسى عبد الحميد، مدى حجية المحرَّرات الإلكترونية في الإثبات في القانون المدني الليبي مقارنة ببعض التشريعات الأجنبية، المؤتمر العلمي المغربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص27.

(101) هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص118.

(102) أوصى المؤتمر الدولي لقانون العقوبات والذي عقد في ريو جانيرو في البرازيل في الفترة 4-9 سبتمبر 1994م في مجال إصلاح الإجراءات الجنائية وحماية حقوق الإنسان بمجموعة من التوصيات يهمنا منها التوصية رقم (189) التي تنص على أن «كل الأدلة التي يتم الحصول عليها عن طريق انتهاك حق أساسي للمتهم، والأدلة الناتجة عنها تكون باطلة ولا يمكن التمسك بها أو مراعاتها في أية مرحلة من مراحل الإجراءات». كما أشار هذا المؤتمر في

المجال الإجرائي بالنسبة لجرائم الحاسب الإلكتروني والجرائم الأكثر تقليدية في بيئة تكنولوجيا المعلومات، إلى أن الاستهلاكات غير المشروعة لحقوق الإنسان التي يرتكبها رجال السلطة العامة تبطل الدليل المتحصل عليه، بالإضافة إلى تقرير المسؤولية الجنائية لرجل السلطة العامة الذي انتهك القانون. ينظر: هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص16.

(103) عصام عفيفي حسين عبد البصير، مبدأ الشرعية الجنائية (دراسة مقارنة في القانون الوضعي والفقه الجنائي الإسلامي)، دار النهضة العربية القاهرة، 2003، ص16.

(104) ممدوح عبد الحميد عبد المطلب وآخرون، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، مرجع سابق، ص2244.

(105) خالد عياد الحلبي، مرجع سابق، ص24.

(106) هلالي عبد الله أحمد، تفتيش نظم الحاسب وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 1997، ص202.

(107) ينظر: المادة (26/ثانيًا-ب) والمادة (26/ثالثًا).

(108) هدى طلب علي، مرجع سابق، ص140.

(109) طارق محمد الجملي، مرجع سابق، ص27.

(110) خالد عياد الحلبي، مرجع سابق، ص244.

(111) هدى طلب علي، مرجع سابق، ص142.

(112) تنظر المواد (427) من قانون الإجراءات الفرنسي رقم (94-653) لسنة 1994 والمادة (302) من قانون الإجراءات الجنائية المصري رقم (150) لسنة 1950م والمادة (275) من قانون الإجراءات الجنائية الليبية لسنة 1953م.

(113) براء منذر عبد اللطيف، شرح قانون أصول المحاكمات الجزائية، ط1، دار الحامد للنشر والتوزيع، عمان 2009، ص216.

(114) المادة (213/أ) من قانون أصول المحاماة الجزائية رقم 23 لسنة 1971م.

(115) المادة (5) من قانون التوقيع الإلكتروني العراقي لسنة 2012م.

(116) راشد بن محمد البلوشي، ورقة عمل حول الدليل في الجريمة المعلوماتية مقدَّمة إلى المؤتمر الدولي حول (حماية أمن المعلومات والخصوصية في قانون الإنترنت) برعاية الجمعية الدولية لمكافحة الإجرام السيبيري، بفرنسا، القاهرة، 2008م.

(117) هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية من المواد الجنائية، مرجع سابق، ص15.

(118) نائلة محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقي، بيروت، 2005، ص82.

(119) راشد بن محمد البلوشي، مرجع سابق، ص17.

(120) محمد فهمي طلبة، فيروسات الحاسب وأمن البيانات، مطابع الكتاب المصري الحديث، القاهرة، 1992، ص19.

(121) راشد بن محمد البلوشي، مرجع سابق، ص18.

(122) هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية من المواد الجنائية، مرجع سابق، ص91.

(123) طارق محمد الجملي، مرجع سابق، ص32.

(124) ممدوح عبد المطلب وآخرون، نموذج مقترح لقواعد الدليل الرقمي للإثبات في جرائم الكمبيوتر، مرجع سابق، ص2253.

(125) ممدوح عبد المطلب وآخرون، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، مرجع سابق، ص2241.

(126) المرجع نفسه، ص2247

(127) راشد بن حمد البلوشي، مرجع سابق، ص19.

(128) المادة (212) من قانون أصول المحاكمات الجزائية رقم 23 لسنة 1971 «لا يجوز للمحكمة أن تسند في الدعوى في حكمها إلى دليل لم يطرح للمناقشة ولم يشر إليه في الجلسة ولا إلى ورقة قدمها، أحد الخصوم دون أن يمكن باقي الخصوم من الاطلاع عليها، وليس للقاضي أن يحكم في الدعوى بناءً على علمه الشخصي».

(129) راشد بن حمد البلوشي، مرجع سابق، ص20.

(130) المرجع نفسه، ص21.

(131) مأمون محمد سلامة، قانون الإجراءات الجنائية معلقًا عليه بالفقه والقضاء، دار الفكر العربي، القاهرة، 1981، ص108.

(132) هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص112.

(133) أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1985، ص292 وما بعدها.

(134) محمد نجيب حسين، شرح قانون الإجراءات الجنائية، مرجع سابق، ص795.

(135) مأمون محمد سلامة، مرجع سابق، ص670.

*

المصادر والمراجع

أولاً - الكتب:

1- إبراهيم دسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، مطبوعات جامعة الكويت، 2003م.

2- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1985م.

3- براء منذر كمال عبد اللطيف، شرح قانون أصول المحاكمات الجزائية، ط1، دار الحامد للنشر والتوزيع، عمان، 2006م.

4- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002م.

5- حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000م.

6- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2011م.

7- عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2007م.

8- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2005م.

9- عصام عفيفي حسينة عبد البصير، مبدأ الشرعية الجنائية - دراسة مقارنة في القانون الوضعي والفقه الجنائي الإسلامي، دار النهضة العربية، القاهرة، 2003م.

10- عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، القاهرة.

11- عمر محمد بن يونس، الدليل الرقمي، الطبعة الأولى، مصر، 2007م.

12- مأمون محمد سلامة، قانون الإجراءات الجنائية معلقًا عليه بالفقه والقضاء، دار الفكر العربي، القاهرة، 1981م.

13- محمد فهمي طلبة، فيروسات الحاسب وأمن البيانات، مطابع الكتاب المصري الحديث، القاهرة، 1992م.

14- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006م.

15- ممدوح عبد الحميد المطلب، جرائم الكمبيوتر عبر الإنترنت، إصدارات مكتبة الحقوق، الشارقة، الإمارات، 2000م.

16-نائلة محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، 2005م.
17-نبيل علي، العرب وعصر المعلومات، الكويت، 1994م.
18-هلالي عبد الله أحمد، تفتيش نظم الحاسب وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 1997م.
19-هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2006م.

ثانيًا- الرسائل الجامعية:

- هدى طلب علي، الإثبات الجنائي في جرائم الإنترنت والاختصاص القضائي بها، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2012م.

ثالثًا- البحوث:

1- أحمد أبو عيسى عبد الحميد، مدى حجية المحرَّرات الإلكترونية في الإثبات في القانون المدني الليبي مقارنةً ببعض التشريعات الأجنبية، المؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد يومي (28-29) أكتوبر 2009م، أكاديمية الدراسات العليا، طرابلس، ليبيا.
2- جودة حسين محمد جهاد، المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية - دراسة مقارنة، بحث مقدَّم لمؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من 1-2000/5/3م بكلية الشريعة والقانون بدولة الإمارات العربية المتحدة.
3- راشد بن حمد البلوشي، ورقة عمل حول الدليل في الجريمة المعلوماتية، مقدَّمة إلى المؤتمر الدولي حول (حماية المعلومات والخصوصية في قانون الإنترنت) برعاية الجمعية الدولية لمكافحة الإجرام بفرنسا، 2008م.
4- طارق محمد الجملي الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدَّمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد يومي (28-29) أكتوبر 2009م، أكاديمية الدراسات العليا، طرابلس.
5- عبادة أحمد عبادة، بحث بعنوان (التدمير المتعمد لأنظمة المعلومات الإلكترونية)، مركز البحوث والدراسات لدى شرطة دبي، دولة الإمارات العربية المتحدة، العدد 87، مارس، 1999م.
6- عبد الناصر حمد محمود فرغلي، د.محمد عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانوني والفنية، بحث ضمن أعمال المؤتمر العربية الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007م.
7- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي،

المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مؤتمر نظمته أكاديمية شرطة دبي، مركز البحوث والدراسات رقم(1)، يومي (27-2003/4/28).
8- عمر الفاروق الحسيني، بحث بعنوان (لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات)، مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من 1-2000/5/3م كلية الشريعة والقانون بدولة الإمارات العربية المتحدة.
9- غنام محمد غنام، بحث بعنوان (عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر)، مقدَّم لمؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من 1-2000/5/3م، كلية الشريعة والقانون بدولة الإمارات العربية المتحدة.
10- محمد الأمين البشري، الأدلة الجنائية الرقمية (مفهومها ودورها في الإثبات)، المجلة العربية للدراسات الأمنية والتدريب، الرياض، المجلد17، العدد 33، 2004 م
11- محمد الأمين البشري، (التحقيق في جرائم الحاسب الآلي)، بحث مقدَّم لمؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من 1-2000/5/3، كلية الشريعة والقانون بدولة الإمارات العربية المتحدة.
12- ممدوح عبد الحميد عبد المطلب، (استخدام أدوات التحليل التناظري الرقمي في تحقيق الجرائم عبر الكمبيوتر)، دورية الفكر الشرطي، المجلد 11، العدد (44)، الشارقة 2003م.
13- ممدوح عبد الحميد عبد المطلب، (استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر)، بحث مقدَّم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية،نظمته أكاديمية شرطة دبي،مركز البحوث والدراسات، العدد (4)، الإمارات العربية المتحدة، دبي، 2003م.
14- ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات الدولية -الجريمة عبر الإنترنت، بحث مقدَّم لمؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من 1-2000/5/3م، كلية الشريعة والقانون بدولة الإمارات العربية المتحدة.
15- ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، (نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر)، منشور ضمن أعمال مؤتمر (الأعمال المصرفية الإلكترونية)، المجلد الخامس، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية وغرفة تجارة وصناعة دبي في الفترة (5-2003/12/10).
16- موزة المزروعي، الاختراقات الإلكترونية: خطر كيف نواجهه، مجلة آفاق اقتصادية، العدد (9)، دولة الإمارات العربية المتحدة، 2000م.
17- هدى حامد قشقوش، الإتلاف العمدي لبرامج الحاسب الإلكتروني، بحث مقدَّم لمؤتمر القانون والكمبيوتر والإنترنت، المنعقد في الفترة من 1-2000/5/3م، كلية الشريعة والقانون بدولة الإمارات العربية المتحدة.

18- هشام فريد رستم، الجرائم المعلوماتية - أصول التحقيق الفني واقتراح بشأن إنشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدّم لمؤتمر القانون والكمبيوتر والإنترنت، المنعقد في الفترة من 1-2000/5/3م، كلية الشريعة والقانون بدولة الإمارات العربية المتحدة.
19- هلالي عبد الله، بحث بعنوان (حجية المخرجات الكمبيوترية)، مقدّم لمؤتمر القانون والكمبيوتر والإنترنت، المنعقد في الفترة من 1-2000/5/3م، كلية الشريعة والقانون بدولة الإمارات العربية المتحدة.
20- القاضي وليد عالكوم، بحث بعنوان مفهوم وظاهرة الإجرام المعلوماتي، بحث مقدّم لمؤتمر القانون والكمبيوتر والإنترنت، المنعقد في الفترة من 1-2000/5/3م، كلية الشريعة والقانون بدولة الإمارات العربية المتحدة.

رابعًا- المواقع الإلكترونية:

1- خالد ممدوح إبراهيم، الدليل في الجرائم الإلكترونية، بحث منشور على الموقع الإلكتروني الآتي:
www.f-law.net/law/threads/19223.
2- علي الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي (دراسة مقارنة)، جامعة العلوم التطبيقية، البحرين، 2009م، بحث منشور على الموقع الآتي:
www.poblicem.gov.bh/reports

خامسًا- القوانين والتشريعات:

1- قانون الإجراءات الجزائية الاتحادي الإماراتي رقم 35 لسنة 1992.
2- قانون الإجراءات الجنائية الليبي لسنة 1953.
3- قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950.
4- قانون أصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971.
5- قانون التوقيع الإلكتروني العراقي رقم 78 لسنة 2012.
6- قانون التوقيع الإلكتروني المصري رقم15 لسنة 2004.
7- قانون العقوبات الاتحادي الإماراتي رقم 3 لسنة 1987.
8- قانون العقوبات العراقي رقم 111 لسنة 1969.
9- قانون العقوبات المصري رقم 58 لسنة 1937.
10- قانون المعاملات الإلكترونية الأردني المؤقت رقم 85 لسنة 2001.

● ○ ●

معهد البحوث والدراسات العربية