

## "الانترنت والجريمة الالكترونية وطرق التغلب عليها"

إعداد

د/ فهد دخين العدوانى

ملخص البحث :

تسارع إيقاع التقدم التكنولوجي والتقني الهائل ، وظهور الفضاء الإلكتروني ووسائل الاتصالات الحديثة كالفكس والإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية استغله مرتكبو الجرائم الإلكترونية في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة ، بل تجاوزت حدود الدول ، وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي ، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية ، ومن حيث ما يرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة ، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية ، مما أوجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة علي المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة ، بما يضمن في الأحوال كافة احترام مبدأ شرعية الجرائم والعقوبات من ناحية ، ومبدأ الشرعية الإجرائية من ناحية أخرى ، وتتكامل فيه في الدور والهدف مع المعاهدات الدولية .

الكلمات الدالة : الجريمة الإلكترونية- الإثبات- الدليل الرقمي- السرقات الالكترونية.

### Abstract:

The acceleration of the rhythm of considerable technological progress and technical, and the emergence of cyberspace and modern communications, the Internet and other images of electronic communication via satellite exploited by the perpetrators of cyber crimes in the implementation of their crimes are no longer limited to the territory of one country, but exceeded the limits of states, an innovative crimes the novel represents a form of intelligence criminal, eluded included in the traditional criminal descriptions in national and foreign criminal laws, and in terms of what is linked to the fragility of procedural prosecution that seem inadequate to absorb these new criminal phenomenon, both in terms of criminal prosecution under national laws or at the level of system international criminal prosecution, thereby requiring the national legislative structure Criminal develop intelligently legislative similar reflect the accuracy due to the legal level and other aspects and dimensions of these new technologies, so as to ensure in all circumstances respect for the principle of legality of offenses and punishments on the one hand, and the principle of

legality of procedure on the other hand, are integrated in it in the role and purpose with the international treaties.

### المقدمة :

تسارع إيقاع التقدم التكنولوجي والتقني الهائل، وظهور الفضاء الإلكتروني ووسائل الاتصالات الحديثة كالفكس والإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية استغله مرتكبو الجرائم الإلكترونية<sup>(١)</sup> في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة ، بل تجاوزت حدود الدول، وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية، ومن حيث ما يرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية، مما أوجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل يعكس فيه الدقة الواجبة علي المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة، بما يضمن في الأحوال كافة احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى، وتتكامل فيه في الدور والهدف مع المعاهدات الدولية.

والتحديات التي تواجه الجريمة الإلكترونية يمكن رصدها من خلال ما نطرحه من حلول لتجاوزها ، وذلك في موضعه مظاهر تحديات الجريمة الإلكترونية في المطلب الثاني من المبحث الأول.

### أهمية موضوع البحث :

يكتسب موضوع البحث أهمية متزايدة بسبب استغلال وسائل الاتصالات الحديثة كالفكس والإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية التي استغلها مرتكبو الجرائم لتسهيل ارتكابهم لجرائمهم .

ولموضوع البحث أهمية من الناحية النظرية والعملية لكونه يمس كثيرا من مصالح المجتمع وعلى وجه الخصوص المصارف من خلال التعامل الإلكتروني والسحب من الأرصدة بواسطة البطاقة الممغنطة أو الدفع الإلكتروني ، وأيضا المساس بالحياة الخاصة للأفراد عن طريق التسجيل وغيرها من المجالات التي تدخل في استعمال الحاسب الآلي .

<sup>١</sup> - من أمثلتها قرصنة واختراق غير مشروع لأنظمة الغير وبرامجهم وتدميرها بواسطة ما يعرف بالفيروسات المعلوماتية وتقليد برامج الغير ونسخها وكذلك جرائم السرقة الإلكترونية والنصب والتزوير وتسهيل الدعاية وانتهاك حمت الحياة الخاصة وعرض المواد الإباحية للأطفال وانتهاك خصوصية الغير ، والمعلومات المشوهة والإعلانات الكاذبة والأفلام المخلة بالأداب العامة ، وعمليات التجسس والإرهاب وعمليات الابتزاز التي تمارسها بعض العصابات ضد الشركات بإقضاء سرها ، والسطو على أموال البنوك وانتهاك حرمة الحياة الخاصة والأسرار الشخصية . .

## إشكاليات البحث :

ترجع إشكاليات البحث إلى ما يتميز به من صفة فنية، ومفردات ومصطلحات جديدة كالبرامج والبيانات التي تشكل محلا للاعتداء أو تستخدم كوسيلة للاعتداء ، معظم مستندات موضوعه ( الجريمة الإلكترونية ) عبارة عن تسجيلات إلكترونية تتم عبر شبكات الاتصال المعلوماتي ، ذات طبيعة خاصة متميزة، وذلك راجع إلى عدة عوامل منها طبيعة المال المعلوماتي وحادثة ظهور الحاسب الآلي وتقنية تشغيله، ولهذا أصبح لا يكفي أن يكون الباحث متخصصا في القانون ، بل يتعين عليه أن يكون ملما بالجوانب الفنية للحاسب الآلي والإنترنت ليتمكن من إيجاد الحلول للتحديات والمشاكل القانونية التي تثيرها شبكة الاتصال والمعلومات وجرائمها الإلكترونية ، كما أن عدم وجود قانون يجرم التقنيات الفنية الجديدة الناشئة عن استخدام الانترنت في ارتكاب الجرائم التقليدية أدى إلى اللجوء إلى التفسير ، الأمر الذي أثار إشكاليات التكيف القانوني للفعل كما يثير مشكلة التمييز بين العمل التحضيري والبدء في تنفيذ الجريمة وغيرها، كما أن التعامل مع دليل هذا النمط من الجرائم فتح مجالا جديدا في الإثبات ، فبعد أن كان مجال الإثبات ينحصر فقط في المستند الورقي أصبح الدليل الرقمي ينازعه في هذه المرتبة، ناهيك عن وجود بعض الصعوبات العملية في تطبيق الأفكار التقليدية والمستقرة بالقانون الجنائي كمبدأ الشرعية وسريان القانون من حيث الزمان والمكان واختصاص القضاء الوطني .

وبناءً علي ما تقدم تكون خطة البحث علي النحو التالي :

المبحث التمهيدي : الحاسب الآلي ، إيجابياته وسلبياته

المطلب الأول : إيجابيات الحاسب الآلي

المطلب الثاني : سلبيات الحاسب الآلي وموقف التشريعات من الجرائم الإلكترونية

المبحث الأول : الأحكام العامة للجريمة الإلكترونية

المطلب الأول : مفهوم الجريمة الإلكترونية وموضوعها وخصائصها وطبيعتها

المطلب الثاني : مظاهر تحديات الجريمة الإلكترونية

المبحث الثاني : الإثبات وأدلته

المطلب الأول : في الإثبات

المطلب الثاني : وسائل جمع الأدلة

**المبحث الأول****الأحكام العامة للجريمة الإلكترونية****تمهيد وتقسيم :**

الأحكام العامة للجريمة الإلكترونية لا تختلف عن الأحكام العامة للجريمة العادية التقليدية إلا فيما ندر في ركنها المادي وخاصة فيما يتعلق بعنصري المكان والزمان، وما يتعلق بمدى انطباق القوانين الوطنية على بعض الأفعال التي ترتكب في الخارج وتحديد القضاء المختص داخل الدولة الواحدة<sup>(٢)</sup>، ناهيك عن أن السلوك الإجرامي في هذه الجريمة عبارة عن تدفق للمعلومات عبر نظم الحاسب الآلي لا يمكن الإمساك ماديا بها، ولذلك ينبغي الوقوف على تحليل سلوكها الإجرامي، خاصة ما يتعلق ببعض الأفكار مثل فكرة المال في جريمة الاعتداء على المال الخاص أو المال العام ، وكذلك فكرة التزوير في مخرجات الحاسب الآلي<sup>(٣)</sup> .

ويبدو أنه لا اتفاق بين الفقهاء حول مصطلح للدلالة على هذه الظاهرة المستحدثة ، باعتبار أن موضوع الجريمة الإلكترونية يختلف بحسب ما إذا كان الاعتداء موجَّهاً إلى أحد مكونات النظام المعلوماتي أو كان وسيلة لتنفيذ جرائم معينة ، فالجريمة الإلكترونية كظاهرة إجرامية ذات طبيعة خاصة ، تقنية وعابرة للحدود تتعلق في الغالب بما يسمى القانون الجنائي المعلوماتي ، لذلك سوف نتناول في هذا المبحث تعريف الجريمة الإلكترونية وموضوعها وخصائصها وطبيعتها في المطلب الأول ، ونردف الأحكام العامة للجريمة الإلكترونية باستعراض مظاهر تحديات هذه الجريمة في المطلب الثاني.

**المطلب الأول- مفهوم الجريمة الإلكترونية وموضوعها وخصائصها وطبيعتها:****مفهوم الجريمة الإلكترونية :**

تعددت الآراء بشأن تعريف الجريمة الإلكترونية ، كل رأي تبنى مفهوماً بالنظر إلى الزاوية التي رآها ، فهناك جانب من الفقه عرفها من زاوية فنية، وأخرى قانونية ، وهناك جانب آخر يرى تعريفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استنادا لمعايير أخرى حسب القائلين بها<sup>(٤)</sup> ، وهذا ما حدا بالأمم المتحدة - مدونتها بشأن الجريمة المعلوماتية - إلى عدم التوصل لتعريف متفق عليه دوليا ، ولكن ورغم صعوبة وضع تعريف لظاهرة هذه الجريمة وحصرها في مجال ضيق ، إلا أن مكتب تقييم التقنية في الولايات المتحدة الأمريكية عرفها من خلال تعريف الحاسب الآلي بأنها " الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور

<sup>٢</sup> - د. مدحت رمضان ، مرجع سابق ، ص ٩ .

<sup>٣</sup> - د. المستشار عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، بدون ناشر ، طبعة مزيدة ومنقحة ، ٢٠٠٩ ، ص ١١٤ .

<sup>٤</sup> - انظر في تفصيل ذلك د.المستشار عبد الفتاح بيومي حجازي ، المرجع السابق ، ص ١ وما بعدها .

رئيسي " ، كما عرفت أيضا بأنها " نشاط جنائي يمثل اعتداءً على برامج وبيانات الحاسب الإلكتروني " ، وعرفت أيضا بأنها " كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية ، ويهدف إلى الاعتداء على أي مصلحة مشروعة ، سواء أكانت مادية أو معنوية " (٥) .

ومن جانبنا نرى بأن الجريمة الإلكترونية هي عبارة عن أفعال غير مشروعة ، يكون الحاسب الآلي محلا لها أو وسيلة لارتكابها .

كما أن بعض الدراسات و النشاطات العلمية قد اتجهت إلي تبني منهج يقوم علي تصنيف النشاطات المتعلقة بالحاسب الآلي إلي فئات و أنواع بمثابة مفترض و ضروري لهذا الموضوع .

وطبقا لهذا المعني فإن الكاتب دون بيكر (Donn Parker) ردَّ أشكال إساءة الحاسب الآلي إلي أنماط أو أشكال يتميز كل منها بالدور الذي يلعبه هذا الحاسب ذاته ، وهكذا فإن الحاسب الآلي لا يعدو أن يقوم بأحد الأدوار التالية : دور الضحية في الجريمة ؛ دور المحيط أو البيئة التي ترتكب فيها الجريمة؛ دور الوسائل التي ترتكب بواسطتها الجريمة؛ ودور التخويف أو الخداع أو غش الضحية .

وبعض آخر رد الأنشطة التي بالحاسب و التي يمكن أن تعتبر أنشطة غير مشروعة إلي الفئات الرئيسية هي : غش الحاسب الآلي؛ إتلاف المعطيات(البيانات) أو البرامج ؛ سرقة المعلومات .

وقد تناول عدد آخر من الكتاب العديد من أنواع الجرائم التي تقع بواسطة الحاسب الآلي لا تسمح مساحة هذا البحث تناولها بالدراسة .

ورغم الفارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الإنترنت ، فبينما تتحقق الأولى بالاعتداء على مجموعة الأدوات المكونة للحاسب وبرامجه والمعلومات المخزنة به ، فإن جرائم الإنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب عبر خطوط الهاتف أو الشبكات الفضائية ، إلا أن الواقع التقني أدى إلى اندماج الميدانين ( الحوسبة والاتصالات ) وظهر مصطلح (Cybercrime) ، ولكن هذا الاندماج لم يثن جانب من الفقه عن تقسيم تلك الجرائم إلى أربعة أنواع تبعا للمفهوم الذي يتبناه كل منهم .

٥ - وفي عام ٢٠٠٠ أقرت وزارة العدل الأمريكية تصنيفا لجرائم الحاسب الآلي ، تضمن : السطو على بيانات الحاسب ، والاتجار بكلمة السر ، وحقوق الطبع ( البرامج - الأفلام - التسجيل الصوتي ) وعمليات القرصنة ، وسرقة الأسرار التجارية باستخدام الحاسب ، وتزوير الماركات التجارية باستخدام الحاسب ، وتزوير العملة باستخدام الحاسب ، و الصور الفاضحة واستغلال الأطفال ، والاحتيال بواسطة شبكة الإنترنت ، والإزعاج عن طريق شبكة الإنترنت ، وتهديدات القنابل بواسطة شبكة الإنترنت ، و الاتجار بالمتفجرات أو الأسلحة النارية أو المخدرات ، وغسيل الأموال عبر شبكة الإنترنت . وصنف مكتب التحقيقات الفيدرالي الجرائم المعلوماتية في أبريل ٢٠٠٠ إلى سبع جرائم هي : اقتحامات شبكة الهواتف العامة أو الخاصة بواسطة الحاسب ، واقتحامات شبكة الحاسب الرئيسية لأي جهة ، واقتحامات السرية المؤرخة على بعض المواقع بالإنترنت أو الجهات ، وانتهاكات سلامة الشبكة المعلوماتية ، والتجسس الصناعي ، وبرامج الحاسب المسروقة ، والبرامج الأخرى عندما يكون الجنسية الحاسب العامل الرئيسي في اقتراف هذه المخالفات (٤) نقلا عن د.المستشار عبد الفتاح بيومي حجازي ، مرجع سابق ، ص٧-٨ ..

١ - جرائم الحاسب الآلي: ويقصد بها الأفعال التي تشكل اعتداء على أجهزة الحاسب الآلي ، سواء على مكوناته المادية ( Hardware ) كوحدات الإدخال و الإخراج ، و وسائل التخزين المرنة و الصلبة أو الشاشة و الطابعة أو على مكوناته المعنوية (Software data bases) كالبيانات و المعلومات المخزنة داخل الحاسب الآلي ، وعلى ذلك فإن جرائم الحاسب تختلف حسب طبيعة الشيء محل الاعتداء ، فالاعتداء أحياناً يقع على أدوات و آلات الحاسب الآلي وأحياناً أخرى يقع على برامج ومعلومات داخل الحاسب الآلي ، وفي كلتا الحالتين فإن الحاسب ومحتوياته هو هدف السلوك الإجرامي .

٢- جرائم الإنترنت: وهي كل فعل غير مشروع يقع على المواقع بقصد تعطيلها أو تشويهها أو تعديلها والدخول غير المشروع لمواضع غير مصرح بالدخول إليها ، واستخدام عناوين غير حقيقية للدخول في شبكة المعلومات واقتحام الشبكات ونقل الفيروسات، و إرسال الرسائل بكافة أنواعها عبر البريد الإلكتروني كالماسة بكرامة الأشخاص أو المستهدفة ترويج مواد أو أفعال غير مشروعة .

٣- جرائم شبكة المعلومات: وهي كل فعل غير مشروع يقع على وثيقة أو نص موجود بالشبكة ومن أمثلته انتهاك الملكية الفكرية للبرامج والإنتاج الفني والأدبي و العلم، وارتكاب هذه الجرائم عبر شبكة المعلومات يتطلب اتصال بالانترنت واستخدام الحاسب الآلي للوصول إلي قواعد البيانات للاطلاع عليها أو تغييرها .

٤- الجرائم المتعلقة باستخدام الحاسب الآلي : وهي الجرائم التي يكون الحاسب الآلي وسيلة لارتكابها كالاختيال والتزوير بواسطة الحاسب، ولقد كانت هذه الجريمة مندمجة في جرائم الحاسب الآلي وتعتبر جزء منها، إذ كان مصطلح جرائم الحاسب يستخدم للدلالة على كل صور جرائم الحاسب الآلي سواء أكان الحاسب هدفاً صريحاً للفعل الإجرامي أو وسيلة له، إلا أنه بعد اتساع جرائم الحاسب وولادة جرائم الانترنت أصبح مصطلح الجرائم المتعلقة بالحاسب الآلي يعتبر من الجرائم التي يكون الحاسب وسيلة لارتكابها ، أي أنها كل فعل غير مشروع يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية<sup>(١)</sup>.

واشتملت الاتفاقية الأوروبية لجرائم الحاسب الآلي والانترنت المسماة باتفاقية بودابست بشأن الإجرام الكوني (Cybercrime) ، الموقعة في ٢٣/١١/٢٠٠١ على خمسة عناوين ، الأربعة الأول تناولت أربعة أنواع من الجرائم هي : الجرائم التي تمس سرية وأمن وسلامة وتوفير بيانات الحاسب ومنظوماته وهي تضم (الدخول غير المشروع - والإعراض غير المشروع - والتدخل في البيانات - والتدخل غير المشروع في المنظومة - وإساءة استخدام الأجهزة)، والجرائم المتصلة بالحاسب الآلي وتضم (جريمة التزوير المتعلقة بالحاسب - وجريمة التديس المتعلقة بالحاسب)،

<sup>١</sup> - د. سالم محمد الأوجلي ، التحقيق في جرائم الكمبيوتر و الانترنت ، منشور على الموقع <http://afaitouri.maktoobblog.com/1624946> ، ص ٥ .

والجرائم المتصلة بالمواد الإباحية للأطفال (الإنتاج أو النشر غير المشروع للمواد الإباحية وصور الأطفال الفاضحة)، والجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المرتبطة بها ( الطبع والنشر) ؛ والعنوان الخامس خصص للمسؤولية وللجزاءات، وهو يشتمل على بنود إضافية بشأن الشروع و الاشتراك ، وأيضا الجزاءات أو التدبير وذلك طبقا للاتفاقيات أو المعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية<sup>(٧)</sup> .

### موضوع الجريمة الإلكترونية :

يختلف موضوع الجريمة الإلكترونية بحسب الزاوية التي ينظر إليها منه ، فمن ناحية قد يكون الحاسب الآلي أو المعلومات المخزنة فيه موضوعا للجريمة، ومن ناحية أخرى قد يكون فيها الحاسب الآلي أداة للجريمة الإلكترونية ووسيلة تنفيذها.

### - الحالة التي يكون فيها الحاسب الآلي أو المعلومات المخزنة فيه موضوعا أو محلا للجريمة :

في هذه الحالة وهي ما يطلق عليها البعض ( أداء سلبية ) ، يكون هناك صورتان للاعتداء ، اعتداء واقع على المكونات المادية للحاسب الآلي ذاته كالأجهزة والمعدات ، والتي تتمثل في جرائم سرقة أو إتلاف شاشة الحاسب أو شبكة اتصالاته الخاصة أو آلة الطباعة<sup>(٨)</sup> ؛ ومن ناحية أخرى قد يكون الاعتداء موجها إلى مكونات الحاسب الآلي غير المادية كالبيانات والبرامج مثل جرائم الاعتداء على البيانات المخزنة في ذاكرة الحاسب الآلي أو البيانات المنقولة عبر شبكات الاتصال المختلفة والتي تتمثل في جرائم السرقة أو الإتلاف أو التقليد أو محو أو تعطيل هذه البيانات<sup>(٩)</sup>، والصورة الثانية تمثل الاعتداء ذاته موجها إلى برامج الحاسب الآلي من خلال تزوير المستخرجات الإلكترونية وإفشاء محتوياتها وهو ما اصطلح على تسميته (سرقة ساعات الحاسب الآلي)<sup>(١٠)</sup>.

ومن نافلة القول أن النوع الأخير من الاعتداءات تعجز حياله نصوص قانون العقوبات الحالية - التي قننت في ظل تفكير يقتصر إدراكه على المال الملموس والمستندات ذات الطبعة المادية - عن احتوائه واستيعابه نظرا لأن محل

<sup>٧</sup> - انظر تفصيل ذلك : أ.د. هلالى عبد اللاه أحمد ، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها) ، دار النهضة العربية، الطبعة الأولى ، القاهرة ، ٢٠٠٧ ، ص٤٧ وما بعده.

<sup>٨</sup> - وإذا ما تعرضت هذه الأموال للاختلاس أو الاعتداء بالإتلاف ، فإن النصوص الجنائية القائمة ( السرقة والإتلاف ) كقيلة بحمايتها ، لأن الأمر هنا يتعلق بمال مادي منقول وفقا للمفهوم التقليدي في القانون الجنائي .

<sup>٩</sup> - يطلق البعض على محل الاعتداء في هذه الصورة اسم فن الحاسب الآلي ، وذلك إبرازا لماهيته المغايرة في صورتها لصورة المال التقليدي . انظر في ذلك د. عمر الفاروق الحسيني ، تأملات في بعض صور الحماية الجنائية لبرامج الحاسب الآلي ، مجلة المحاماة ، س١٢ عدد نوفمبر/ديسمبر ١٩٨٩ ص ١٣ .

<sup>١٠</sup> - ويمكن أيضا تصور ارتكاب جرائم السرقة كالسحب من الأرصدة في البنوك أو التحويل من حساب إلى آخر أو تغطية اختلاس أو عجز في عهدة موظف أو السرقة من قوائم الأجور والمرتببات ، وكذلك ارتكاب جرائم التجسس والتنصت والتصوير والتسجيل عن بعد ، وربما القتل عن طريق برمجة أجهزة تفجير أو غيرها ، أو أجهزة إطلاق أشعة قاتلة ، ويمكن أن يتم الاستخدام بوسائل مختلفة منها التدخل في المعطيات ( البيانات ) بإدخال معطيات وهمية أو معلمات مزورة ، أو بالتدخل في الكيان المنطقي للحاسب بتعديل البرامج ( تلاعب أو تغيير أو محو ) أو خلق برنامج جديد ( وهمي أو ناقص فنيا ) ؛ فالمجرم هنا يستخدم الحاسب الآلي بمكوناته أو ملحقاته ووصلاته كوسيلة شأنه في ذلك شأن قلم المزور أو سلاح القاتل ، د. زكي أمين حسونة ص٤٧١-٤٧٢ .

هذه الاعتداءات مال غير مادي (معنوي) ذو طابع خاص، أي أنه في صورة أخرى غير صورة المال بمفهومه الجنائي التقليدي .

### - الحالة يكون فيها الحاسب الآلي أداة لارتكاب الجريمة ووسيلة تنفيذها :

ففي هذه الحالة والتي يطلق عليها البعض ( أداة إيجابية ) يستخدم الجاني الحاسب الآلي في ارتكاب جرائم السرقة أو النصب أو خيانة الأمانة أو تزوير المحررات<sup>(١١)</sup>، وذلك عن طريق التلاعب في الحاسب ، وكذلك النظام المعلوماتي بصفة عامة ، وفي هذه الحالة نكون بصدد جرائم تقليدية بحته .

### خصائص الجريمة الإلكترونية :

من خصوصية الجريمة الإلكترونية أن بعض حالات ارتكابها يتعمد مرتكبها التدخل في مجالات النظام المعلوماتي المختلفة منها مجال المعالجة الإلكترونية للبيانات ، ومجال المعالجة الإلكترونية للنصوص والكلمات الإلكترونية، في المجال الأول: يتدخل الجاني من خلال ارتكاب الجريمة الإلكترونية في مجال المعالجة الإلكترونية ( الآلية ) للبيانات، سواء من حيث تجميعها أو تجهيزها حتى يمكن إدخالها إلى جهاز الحاسب الآلي، وذلك بغرض الحصول على المعلومات ، وفي المجال الثاني : يتدخل الجاني في مجال المعالجة الإلكترونية للنصوص والكلمات، وهي طريقة أوتوماتيكية تمكن مستخدم الحاسب الآلي من كتابة الوثائق المطلوبة بدقة متناهية بفضل الأدوات الموجودة تحت يده ، ويفضل إمكانيات الحاسب الآلي تتاح إمكانية التصحيح والتعديل والمحو والتخزين والاسترجاع والطباعة ، وهي بذلك علاقة وثيقة بارتكاب الجريمة<sup>(١٢)</sup>.

وتتميز الجريمة الإلكترونية في مجال المعالجة الآلية للمعلومات بالآتي :

- ١ - مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها ، في حين أن مرتكب الجريمة التقليدية في - الغالب - شخص أمي بسيط ، متوسط التعليم .
- ٢- مرتكب الجريمة الإلكترونية - في الغالب - يكون متكيفا اجتماعيا وقادرا ماديا، باعته من ارتكاب جريمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي<sup>(١٣)</sup> ، في حين أن مرتكب الجريمة التقليدية - غالبا - ما يكون غير متكيف اجتماعيا وباعته من ارتكابه الجريمة هو النفع المادي السريع .

<sup>١١</sup> - يمكن أيضا أن ترتكب جرائم التزوير في عمليات السحب على الجوائز والتجسس والتصنت على الأفراد والاعتداء على حياتهم الخاصة سواء بالتصوير أو بالتسجيل عن بعد ، والقتل عن طريق برمجة السرقة بطريق السحب من الأرصدة أو تغطية اختلاس أو عجز أو السرقة من قوائم الأجر والمرتببات ، وكذلك يمكن أن يستخدم الحاسب الآلي في ارتكاب جرائم السرقة بالسحب من الأرصدة أو تغطية اختلاس أو عجز أو السرقة من قوائم الأجر والمرتببات . د. زكي أمين حسونة .ال مرجع السابق . ص٤٧٢ .

<sup>١٢</sup> - د. محمد على العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، ٢٠٠٤ ، ص٣٧ .

<sup>١٣</sup> - إذا كان الدافع إلى ارتكاب الجريمة تحقيق النفع المادي ، فإن المبالغ التي يمكن تحقيقها تكون طائلة تفوق ما يتحصل عليه مرتكب الجريمة التقليدية بأضعاف مضاعفة .



٣- تقع الجريمة الإلكترونية في مجال المعالجة الآلية للمعلومات وتستهدف المعنويات لا الماديات، وهي بالتالي أقل عنفاً وأكثر صعوبة في الإثبات لأن الجاني مرتكب هذه الجريمة لا يترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه، وهذا يعسر إجراءات اكتشاف الجريمة ومعرفة مرتكبها، بخلاف الجريمة التقليدية التي عادة ما تترك وراءها دليلاً مادياً أو شهادة شهود أو غيرها من أدلة الإثبات، كما أن موضوع التفتيش والضبط قد يتطلب أحياناً امتداده إلى أشخاص آخرين غير المشتبه فيه أو المتهم .

٤- الجريمة الإلكترونية ذات بعد دولي ، أي أنها عابرة للحدود ، فهي قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية<sup>(١٤)</sup>.

### طبيعة القانونية للجريمة الإلكترونية

يتمحور الحديث عن الطبيعة القانونية للجريمة الإلكترونية حول الوضع القانوني للبرامج والمعلومات ، وهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأية طريقة كانت ، لذلك انقسم الفقه اتجاهاً : الأول يرى أنه وفقاً للقواعد العامة أن الأشياء المادية وحدها هي التي تقبل الحيابة والاستحواذ ، وأن الشيء موضوع السرقة يجب أن يكون مادياً أي له كيان مادي ملموس حتى يمكن انتقاله وحيابته عن طريق الاختلاس المكون للركن المادي في جريمة السرقة ، ولما كانت المعلومة لها طبيعة معنوية ولا يمكن اعتبارها من قبيل القيم القابلة للحيابة والاستحواذ، إلا في ضوء حقوق الملكية الفكرية ، لذلك تستبعد المعلومات ومجرد الأفكار من مجال السرقة ، ما لم تكن مسجلة على اسطوانة أو شريط ، فإذا ما تم سرقة إحدى هاتين الدعامتين الخارجية ، فلا تنثور مشكلة قانونية في تكييف الواقعة على أنها سرقة مال معلوماتي ذو طبيعة مادية ، وإنما المشكلة تنثور عندما نكون أمام سرقة مال معلوماتي غير مادي ؛ والاتجاه الثاني يرى المعلومات ما هي إلا مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعامتها المادية ، على سند من القول أن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيابة غير مشروعة، وأنها ترتبط كما يقول الأستاذان Catala و Vivant بمؤلفها عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشيء الذي يملكه، بمعنى أن المعلومات مال قابل للملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي ، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال<sup>(١٥)</sup>.

<sup>١٤</sup> - سوف نتناول سريان القانون من حيث المكان ( الإقليمية ) بالتفصيل لاحقاً .

<sup>١٥</sup> -- د. محمد على العريان ، المرجع السابق ، ص٤٣ وما بعدها .

وعلى الصعيد نفسه ثمة من يقول إنه يجب أن نفرق بأن هناك مالا معلوماتيا ماديا فقط ولا يمكن أن يخرج عن هذه الطبيعة وهي آلات وأدوات الحاسب الآلي مثل وحدة العرض البصري ووحدة الإدخال ، وأن هناك من المال المعلوماتي المادي ما يحتوي على مضمون معنوي هو الذي يعطيه القيمة الحقيقية وهي المال المادي الشريط الممغنط أو الاسطوانة الممغنطة أو الذاكرة أو الأسلاك التي تنتقل منها الإشارات من على بعد، كما هو الحال في جرائم التجسس عن بعد، إذن من المنطق القول إذا حدثت سرقة فإنه لا يسرق المال المسجل عليه المعلومة والبرامج لقيمتها المادية وهي ثمن الشريط أو ثمن الاسطوانة ، وإنما يسرق ما هو مسجل عليهما من معلومات وبرامج ، ويرى أصحاب هذا الرأي أن التحليل المنطقي يفرض الاعتداد بفكرة الكيان المادي للشيء الناتج عنه اختلاس المال المعنوي البرامج والمعلومات، وأنها لا يمكن أن تكون شيئا ملموسا محسوسا، ولكن لهما كيان مادي قابل للانتقال والاستحواذ عليه بتشغيل الجهاز ورؤيتهما على الشاشة مترجما إلى أفكار تنتقل من الجهاز إلى ذهن المتلقي ، وانتقال المعلومات يتم عن طريق انتقال نبضات ورموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل صادرة عنه يمكن سرقة ، وبالتالي لها كيان مادي ، يمكن الاستحواذ عليه ( البرامج والمعلومات ) ، واستطرد أصحاب هذا الاتجاه في القول بأنه طالما أن موضوع الحيازة ( أي المعلومات ) غير مادي ، فإن واقعية الحيازة تكون من نفس الطبيعة أي غير مادية ( ذهنية ) ، وبالتالي يمكن حيازة المعلومات بواسطة الالتقاط الذهني عن طريق البصر<sup>(١٦)</sup>.

وردا على قول الرافضين لملكية الغير للشيء المعلوماتي بأن البرنامج والمعلومة من ذات نوع الخلق الفكري الذي ليس ملكا لأحد، قال أصحاب هذا الرأي أن البرنامج من الناحية القانونية تعتبر ملكا لمن ابتكرها ، وأن التحليل المنطقي لا يمكنه إنكار ملكية شخص ما للبرنامج والمعلومة ، ومن ثم فهي ليست ملكا للشارق ، بل هو يقوم بالاستحواذ على شيء ليس مملوكا له<sup>(١٧)</sup>.

واستشهد أنصار هذا الاتجاه بما توصلت إليه محكمة النقض المصرية فيما يتعلق بسرقة الكهرباء ، فهي أيضا مال غير ملموس ، وحسمها هذا كان مبنيا على اعتبار التيار الكهربائي وإن كان ليس مالا ملموسا ، فهو ذو كيان مادي متمثل في الأسلاك والتوصيلات التي تمر من خلالها ، وبالتالي يمكن اختلاسه وانطباق نص السرقة عليه<sup>(١٨)</sup>، وكانت محكمة النقض المصرية قد حدث حذو محكمة النقض الفرنسية في حكمها بإمكانية سرقة التيار الكهربائي ، وكذلك ما ذهب إليه في شأن سرقة خط الهاتف من أنه وإن لم يكن مالا ماديا ملموسا ، فإنه قابل للحيازة والانتقال .

١٦ - د. هدى حامد قشقوش ، مرجع سابق ، ص ٥١-٥٢

١٧ - وتأكيذا لرأي أصحاب هذا الاتجاه أورد حكما صادرا عن محكمة جنح بفرنسا يقضي بإدانة شخص عن جريمة سرقة المعلومات لكونه قام بتسجيل معلومات خاصة بشركة سيارات بيجو ، وذلك بعد مدة من الاستغناء عن خدماته وفصله من الشركة ، فعاد إلى مقر الشركة لكي يسجل البرامج التي قد ساهم في إعدادها وقت عمله في الشركة ؛ وقد نفى أصحاب هذا الرأي ما يدعي به معارضي سرقة المعلومات والبرامج ، أن الحكم قصد به تجريم التسجيل وليس سرقة المعلومة في حد ذاتها .

١٨ - حكم نقض إبريل ١٩٣١ ، مجموعة القواعد ج ٢ ، رقم ٣٢٤ . كذلك ٨ ديسمبر ١٩٥٢ مجموعة الأحكام س ٢٤ رقم ٨١ ص ٢٥٥ .

وذهب أصحاب هذا الاتجاه في تحليله لإمكانية التشابه بين سرقة المال المعلوماتي المعنوي وسرقة التيار الكهربائي إلى القول بأنه رغم أن القضاء قد اعتبر التيار الكهربائي شيئاً قابلاً للسرقة ، إلا أنه ليس للتيار الكهربائي نفس مادية الأشياء الملموسة ، معولا في هذا الرأي على تحليله بأن كلمة (هي) ليست مرتبطة بكلمة مادي ، ولا يمكن أن تعطي تكييفاً مساوياً لكلمتي شيء ومادي ، وبالتالي فإن البرنامج والمعلومة شيء تدخل ضمن نطاق الأشياء وليس حتماً ضمن الماديات، وهذا ما يؤكد الفقيه (Vitu) ؛ وأضاف هذا الاتجاه أن تعريف كلمة شيء تعني كل حقيقة ملموسة مادياً أو معنوياً ، وأن استخدام المشرع الفرنسي لكلمة شيء لا تقصر الأشياء على الماديات ، بل تمتد لأشياء لتشمل ما قد يكون مجرداً معنوياً ، ودلل على تصور تطبيق نص السرقة على المعلومات بأن أورد حكماً للقضاء الفرنسي في قضية Loqabax دانت بمقتضاه المحكمة متهماً كان يعمل موظفاً قام بتصوير مستندات سرية ضد رغبة من يعمل لديه، على سرقة المعلومات المدونة بالورقة وليس على سرقة الورقة ذاتها .

**ونعتقد أن المشرع الكويتي أحسن حينما تدخل وحسم الجدل الفقهي والتردد في التطبيقات القضائية بأن أرفد فقرة ثانية إلى المادة ٤٤٤ من قانون العقوبات المتعلقة بالسرقة نص فيها " ويعد من الأموال المنقولة في حكم قانون العقوبات الطاقة الكهربائية وجميع أنواع الطاقة ذات القيمة الاقتصادية " ، وقد حان الآن الوقت لتدخله لمواجهة الجرائم الإلكترونية بالنص على تجريم الاعتداء على المال المعلوماتي المعنوي سواء بالنص على كل جريمة على حده كما فعل المشرع الفرنسي في القانون الجديد، أو أن يقرر التجريم بنص واحد ، يشمل بالحماية الجنائية كل صور الاعتداء ، السرقة أو الإلتاف أو غيرهما ، والحل الأخير نراه الأنسب تجنباً لما وقع فيه المشرع الفرنسي من تقصير وعدم شمولية حينما نص على حماية محل جريمة الإلتاف وتجاهل محل جريمة السرقة ، وقد يحسب للمشرع الفرنسي محاولته - التي لم يكتب لها النجاح - تعديل قانون العقوبات الجديد بالنص على تجريم سرقة المال المعلوماتي المعنوي المتمثل في البرامج والمعلومات ، وذلك في نص المادة ١/٣٠٧ الذي استعمل فيه كلمة التقاط (Capter) لتعبر عن الاختلاس، حيث نص على أن " كل من التقط بطريق الاختلاس والتحايل برنامج أو معلومات أو أي عنصر من عناصر نظام المعالجة الآلية للبيانات يعاقب ....."**

ونعتقد أيضاً بأن التسليم بأن المال المعلوماتي المعنوي غير قابل للاستحواذ وليس مالا، وبالتالي غير قابل للسرقة سيؤدي إلى تجريده من الحماية القانونية الجنائية ويفتح المجال واسعاً أمام مجرمي وقرصنة البرامج والمعلومات .

### المطلب الثاني - مظاهر تحديات الجريمة الإلكترونية

ترتب على ظاهرة الجريمة الإلكترونية تحديات عدة : منها ظهور وتنامي الأنشطة الإجرامية الإلكترونية وتوسُّل مرتكبيها بتقنيات جديدة غير مسبوقه في مجال تكنولوجيا المعلومات والاتصالات يسرت لهم ارتكاب هذه الأنشطة داخل حدود الدولة وخارجها، الأمر الذي أدى إلى انشغال المنظمات والمؤتمرات الدولية بهذا النوع من الجرائم ودعوتها الدول

إلى التصدي لها ومكافحتها، من حيث تستعصي بعض الأنشطة على إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية؛ ومن حيث ما يرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة ، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية .

وعلى خلفية ما ذهب إليه البعض من أن القوانين القائمة تكفي في حد ذاتها لمواجهة الجرائم الإلكترونية ، فإننا نعتقد إن كان لهذا الرأي شيئا من الواقعية ، وهي أن بعض النصوص القائمة تواجه بعض الأنشطة المجرمة التي ترتكب بطريق الإنترنت ، فإنه ينبغي ألا ننكر أن هناك نصوصا آخر صادف تطبيقها بعض الصعوبات ، منها ما يتعلق بطبيعة الجريمة الإلكترونية غير المادية، ومنها ما يتعلق بهاجس التعارض مع مبادئ هامة ومستقرة في القانون الجنائي ، كمبدأ شرعية الجرائم والعقوبات والتفسير الضيق<sup>(١٩)</sup> ، دعا مشرعو بعض الدول إلى التدخل بتعديل بعض النصوص القائمة أو وضع نصوص جديدة تتلاءم وتلك الجرائم ، ودعا أيضا القضاء إلى التوسع في تفسير النصوص الجنائية السارية .

إذن لا مناص من الاعتراف بأن ظاهرة الجرائم الإلكترونية التي باتت تتخذ أنماطا جديدة وضربا من ضروب الذكاء الإجرامي ، تمثل بلا شك تحديا جديا وجديدا في الوقت الحاضر ، تجاوزه يتطلب التعرف على هذه التحديات وإبراز جوانبها ، بما يعني التشخيص الأمثل للظاهرة ومكافحتها على صعيد التجريم والعقاب من ناحية ، وعلى صعيد الملاحقة الإجرائية من ناحية أخرى، وهذا أمر يستلزم: أولا - الانطلاق من الاقتناع بخطورة هذه الظاهرة ، ومحاولة التوفيق بين احترام مبدأ السيادة الوطنية لكل دولة في صورته التقليدية، والنزول ولو بقدر أمام ضرورات ومقتضيات التعاون القضائي الدولي الذي بقدر نجاحه تتحقق فعالية كل الجهود والإمكانات المسخرة للتصدي لظاهرة الجرائم الإلكترونية ومكافحتها، وثانيا - تطوير البنية التشريعية الجنائية بذكاء تشريعي متواصل ودؤوب يسد ثغرات الأنظمة الجنائية على نحو يجعلها قادرة على إخضاع هذه الجرائم لأوصافها ونصوصها، ومواكبة التطورات التي يتوسل بها مرتكبو هذه الجرائم، على أن يتم هذا التطور في إطار القانون وكفالة احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى ، وأن يتكامل هذا التطور في الدور والهدف مع المعاهدات الدولية .

وعلى ذلك ، فإن أولوية ملحة ينبغي إنجازها على الصعيد التشريعي ، وتتمثل هذه الأولويات في :

١٩ - تقوم المعاهدات سواء بطريق مباشر وغير مباشر بدور كاد يمثل في الآونة الأخيرة مصدرا للقوانين الجنائية الوطنية الأمر الذي يتعين معه إثارة اهتمام الدول ببذل مزيد من صور التعاون الدولي المادي والتقني للدول الأكل إمكانيات بالنظر للكلفة الباهظة لمكافحة الجرائم الإلكترونية لاسيما وهي تتوسل بالتقنيات ، ويرتبط ذلك بدور الأمم المتحدة من خلال لجنة منع الجريمة ، ويملك دور المنظمات والآليات الدولية الأخرى المعنية بالجريمة .

## ١- تحديد الطبيعة القانونية للجريمة الالكترونية:

باعتبار أن المال ينقسم إلى نوعين منفصلين وفقا لطبيعته ، فهو إما مال معلوماتي ذو طبيعة معنوية ويتمثل في البرامج والمعلومات أيا كان نوعها، وإما أن يكون المال المعلوماتي ذو طبيعة مادية ويتمثل في أدوات والآلات الحاسب الآلي الملموسة ، إذ قد يترتب على اختلاف هذه الطبيعة القانونية للمال المعلوماتي اختلافا في النتائج المترتبة على تطبيق بعض نصوص القانون الجنائي التقليدي، ولذلك ظهرت هذه الخلافات الفقهية وتبعها في ذلك عدم استقرار الأحكام القضائية، فالاعتداء على برامج ومعلومات الحاسب الآلي يجعلنا أمام مشكلة قانونية ذات طبيعة خاصة يتطلب فيه البحث في تطبيق الجزاء الجنائي الواجب في حالة الاعتداء على المال المعلوماتي المعنوي أي المحتوى الداخلي للشريط الممغنط أو الاسطوانة الممغنطة ، وهي ما سميت في فرنسا بجريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات، وهي جريمة مستحدثة تناولها المشرع الفرنسي بموجب القانون رقم ١٩ لسنة ١٩٨٨ بشأن بعض جرائم المعلوماتية في مادته ٢/٤٦٢ .

ومن خلال تحديد الطبيعة القانونية للمال المعلوماتي المعتدى عليه، يمكن تحديد الطبيعة القانونية للجريمة الالكترونية والوضع القانوني للبرامج والمعلومات، وهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأية طريقة كانت، وقد سبق التعرض لهذا الموضوع في المطلب الأول من هذا المبحث .

## ٢- تكريس التطور الحاصل في نطاق تطبيق القانون الجنائي الوطني من حيث المكان:

غالبا ما يتحدد السريان المكاني للقانون الجنائي الوطني وفقا لأحد مبادئ أربعة : مبدأ الإقليمية ومبدأ الشخصية ، ومبدأ العينية، ومبدأ العالمية، وتتفاوت أهمية هذه المبادئ فيما بينها ، وتدرج في أهميتها بحسب ترتيبها، وتأخذ معظم التشريعات الجنائية بمبدأ الإقليمية كأصل عام ثم تكمله بالمبادئ الأخرى .

وتحديد مكان وقوع الجريمة، إعمالا لمبدأ الإقليمية جاء بشيء من الغموض في بعض من التشريعات كقانون العقوبات الكويتي الذي نص في مادته الخامسة بأن " تسري أحكام هذا القانون أيضا على الأشخاص الآتي ذكرهم : أولا كل من ارتكب خارج البلاد فعلا يجعله فاعلا لجريمة وقعت كلها أو بعضها في الكويت أو شريكا فيه ...." ، في حين أن البعض الآخر من التشريعات جاءت مفصلة في تحديد متى تعتبر الجريمة واقعة على إقليم الدولة .

وكان الفقه والقضاء وخاصة في فرنسا لا يميلان إلى أن يقتصر تحديد مكان وقوع الجريمة على الحالات المعروفة<sup>(٢٠)</sup> ، بل كانا يميلان إلى التوسع في تحديد مكان وقوع الجريمة الذي من مظاهره تدويل فكرة مكان وقوع الجريمة من حيث

٢٠- ١- وقوع الجريمة بكامل ركنها المادي على إقليم الدولة . ٢- تحقق أحد عناصر الركن المادي فحسب على إقليم الدولة . ٣- تحقق جزء من عنصر السلوك على إقليم الدولة . ٤- وقوع جريمة أصلية على إقليم الدولة من جانب شخص في الخارج يعتبر فاعلا لها أو شريكا فيها . ٥- البدء في تنفيذ فعل مكون لجريمة الشروع على إقليم الدولة . وتمثل الحالة الثالثة مظهرا ملحوظا للتوسع في إعمال مبدأ الإقليمية نص عليها المشرع الفرنسي في المادة ١١٣-٢ من قانون العقوبات الفرنسي الجديد .

الواقع ، واعتبار كل دولة مختصة بنظر هذه الجريمة ، ويمكن رصد مظاهر ذلك التوسع في مجال الجرائم الوقتية متعددة الآثار ، فعلى الرغم من تنفيذ الجريمة على إقليم دولة إلا أن آثار الجريمة قد تتعدى حدود دولة التنفيذ، ولم يتكرر القضاء الفرنسي لانعقاد اختصاصه بنظر مثل هذه الجريمة لكون آثارها قد تحققت على الإقليم الفرنسي ، كما في إحدى جرائم النشر التي وقعت بواسطة صحيفة تم طبعها وتوزيعها في دولة أجنبية ، لكن بعضا من نسخها قد وزع في فرنسا<sup>(٢١)</sup> ، كما أجاز القانون والقضاء الفرنسيين بنظر جريمة اعتداء على الملكية الفكرية وقعت في الخارج متى كانت آثارها قد تحققت في فرنسا<sup>(٢٢)</sup> .

وإعمال السريان المكاني للقانون الجنائي وفقا لأحد المبادئ الأربعة سالفة الذكر ، لا يخلو من صعوبات، تفضي تارة إلى إثارة تنازع إيجابي في الاختصاص بين أكثر من تشريع وطني، وتارة أخرى يقوم تنازع سلبي في الاختصاص يخرج معه اختصاص أي من الدول بملاحقة الجاني ، وهذا النوع الأخير من التنازع نادر الوقوع لأن التشريعات الوطنية تعقد اختصاصها وفقا لمعايير الاختصاص المعروفة<sup>(٢٣)</sup> ؛ أما في حالة قيام تنازع إيجابي في الاختصاص بين أكثر من دولة لملاحقة نفس النشاط الإجرامي، أو في حالة يثور فيها التنازع كما في الجرائم عبرالوطنية التي يتوزع فيها السلوك المادي للجريمة في إقليم أكثر من دولة، أو في حالة تجرد بعض عناصر هذا السلوك من خصيصتها المادية ، كما هو الحال في القرصنة في مجال الحوسبة، وصور المساهمة الجنائية التي تتم باستخدام أجهزة الاتصالات الحديثة ؛ مثل هذه الظاهرة تفرض تنازعا في الاختصاص بل غموضا في تحديد معياره ، تتطلب بطبيعة الحال حولا مستحدثة وابتكارا لمفاهيم قانونية جديدة دون إخلال بمبادئ الشرعية الجنائية التي تركز عليها معظم النظم الجنائية الوطنية .

وقد ثار جدل في مسألة تخزين المعلومات أو البيانات المعالجة إلكترونياً خارج إقليم الدولة، ظهر رأياً: الرأي الأول يقول إنه من غير المشروع أن تقوم سلطات دولة ما بالتدخل وتفثيش النظم المعلوماتية الموجودة في إقليم دولة أخرى، بهدف كشف وضبط أدلة لإثبات جريمة كانت قد وقعت على أراضيها وذلك استنادا إلى مبدأ إقليمية القانون<sup>(٢٤)</sup>، وبهذا الرأي قضت إحدى المحاكم الألمانية في جريمة غش ارتكبت في ألمانيا بأن الحصول على البيانات الخاصة بهذه الجريمة والمخزنة بشبكات اتصال موجودة في سويسرا لا يتحقق إلا بطلب المساعدة من الحكومة السويسرية وفي واقعة نشر فيروس (Love bug) عام ٢٠٠٠ الذي تسبب في إتلاف المعلومات في أجهزة الحاسب الآلي ، فعندما اكتشف

٢١ - v.cass. crim. 30 avril 1908 1.p.553.note. كما حكم باختصاص

٢٢ - v.cass. crim. 2 fevrier 1977,d.1977, information rapide,137, paris30 mars 1987 ,J.C.P.,1988,11,n20965,obs.p.Bouzat .

٢٣ - الأمر يوق بالنسبة لجريمة غسل الأموال أو استخدام عائدات الأنشطة الإجرامية غير المشروعة في الدول التي تجرم تشريعاتها هذا النشاط على أساس أنه فعل من أفعال الاشتراك أو كصورة من صور الإخفاء وليس بوصفه جريمة مستقلة ، وفي الحالتين تكون بصدد جريمة تبعية يتبع اختصاص بملاحقتها الجريمة الأصلية ، وبالتالي يخرج عن اختصاص إحدى تلك الدول ملاحقة مرتكب جريمة غسل الأموال ، خاصة إذا كان المتهم لا يتمتع بجنسيته؛ إذن للتغلب على هذا النوع = من التنازع السلبي في الاختصاص يتعين تقرير مبدأ الاختصاص العالمي الذي يعطي لدولة القبض على المتهم الاختصاص بملاحقته إذ كان يحمل جنسيته ، فإن لم يكن كذلك ، وجب تسليمه في حالة المطالبة به من دولة أخرى وفقا لمبدأ الإقليمية أو الشخصية

٢٤ - د. هشام محمد فريد رستم ، الجوانب الإجرامية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، ١٩٩٤ ، ص ٧٠ ، ٧١ - انظر أيضا : د هلالى عبدالاه احمد ، تفثيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص ٧٧ .

الخبراء الأمريكيون بأن هذا الفيروس أرسل من الفلبين فان تفتيش منزل المشتبه فيه تقتضي تعاون السلطات الفلبينية والحصول على إذن من قاضي التحقيق بالفلبين ؛ أما الرأي الثاني ، فإنه يعون على أن القانون الدولي يمكن أن يتشكل من خلال توافق الآراء على الصعيد الدولي باتجاه السماح بتنفيذ هذه الإجراءات حال توافر ظروف معينة يتم تحديدها ، كإشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة بنظمها المعلوماتية ، وعلى هذه الكيفية أصدر المجلس الأوروبي في ١١ سبتمبر ١٩٩٥ توصية من بين عدة توصيات تناولت مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ، جاء فيها بأن تفترض إجراءات التحقيق مد الإجراءات إلى أنظمة حاسب آلي آخر قد تكون موجودة خارج الدولة وتفترض التدخل السريع ، وحتى لا يمثل مثل هذا الأمر اعتداء على سيادة الدولة أو القانون الدولي ، وجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء ، ولذلك كانت الحاجة ملحة لإبرام اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات ؛ كما يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة ، ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط ، ويتعين كذلك السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها ، وهذا كله لا يتأتى إلا بتفعيل اتفاقيات التعاون الدولي وتكريسها ، والتساؤل الذي يثور هو كيف يمكن إعمال مبدأ الإقليمية على الجرائم التي ترتكب بواسطة شبكة المعلومات الدولية الإنترنت ، وكيف يمكن أيضا تحديد إقليم الدولة الذي وقعت عليه مثل هذه الجرائم بتعددتها وتنوعها وتعقيدها ؟ الإجابة هي أن التقدم العلمي الراهن وتطور وسائل الاتصال الحديثة كالإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية ، أتاح فرصا هائلة للخروج على مبدأ الإقليمية ، وتبني مدونة جديدة لفض مثل هذا التنازع أو بالأقل ترتيب معايير ، لأن معيار الإقليمية القانون لم يعد هو المعيار الوحيد ، ولا ربما الأكثر قبولا في بعض الجرائم ، بل ازدادت أهمية معايير أخرى كانت فيما مضى تعد احتياطية كمعيار العينية ومعيار العالمية ؛ وظهرت الأهمية البالغة لمبدأ المحاكمة أو التسليم ولو في صورته المعكوسة : التسليم أو المحاكمة<sup>(٢٥)</sup> .

كما شهد تطور مفهوم الإقليمية ذاته تطورا ملحوظا فيما يتعلق بتحديد مكان وقوع الجريمة ، فلم يعد بلانزم وقوع فعل مادي أو حتى أحد العناصر المكونة لهذا الفعل المادي ، بل بلغ الأمر حد نزع الصفة المادية كلية عن هذا الفعل ، وهكذا اعتبر مجرد مكاملة هاتفية مع شخص في دولة أخرى مبررا لاعتبار الجريمة قد وقعت بالفعل فوق إقليم الدولة ،

٢٥ - يمثل تسليم المجرمين مظهرا من مظاهر التعاون الدولي في مكافحة ظاهرة الإجرام ، فتقوم دولة من الدول بمطالبة دولة أخرى بتسليمها شخصا ينسب إليه ارتكاب جريمة أو صدر حكم بالعقوبة ضده حتى تتمكن الدولة المطالبة - باعتبارها صاحبة الاختصاص - من محاكمته أو من تنفيذ العقوبة الصادرة في حقه . ويستمد النظام القانوني لتسليم المجرمين مصدره أحيانا من أحكام التشريع الوطني ، ولكن الغالب يكون مصدره الاتفاقيات الدولية أو شبه الدولية أو الثنائية ، وقد يستند التسليم إلى قواعد العرف الدولي أو اتفاق المعاملة بالمثل . والتسليم أكثر جدوى لإدارة إستراتيجية مكافحة الجرائم الإلكترونية ، ولا تتأكد فعاليته إلا بتحقق أمرين أولهما : تجاوز اعتبارات السيادة القضائية ولو بقدر ضرورات التعاون الدولي ؛ ثانيهما : قيام التشريعات الوطنية بتفعيل هذا التعاون وتنظيمه وفق ما تقتضيه المعاهدات الدولية ذات الصلة .

وهكذا يجب على أية محاولة لصياغة معيار الاختصاص الإقليمي لملاحقة الجريمة الإلكترونية أن تعكس مثل هذه المعطيات الجديدة .

للتغلب على التنازع الإيجابي للاختصاص يلوح حلان أو نهجان : الأول يتمثل في محاولة إعطاء الأولوية لأي من الدول المتنازعة وفقا لأحد معايير الاختصاص الأكثر جدوى وفعالية لضمان ملاحقة الجريمة ، ويبدو أن مبدأ الإقليمية هو الأكثر قبولا ، فالدولة التي في إقليمها تقع الجريمة كلها أو الجزء الأكبر من النشاط المكون لركنها المادي ، أو النشاط التبعي كله ، أو بصفة عامة الدولة التي في إقليمها توجد متحصلات الجريمة ، تبدو أرجح الدول اختصاصا بملاحقة الجريمة ومحاكمة فاعلها. ولا يجد هذا الحل مبرراً فقط في اعتبارات السيادة الوطنية للصيقة بمبدأ الإقليمية، وإنما أيضا في جدواه العملية، وأنه حيث تقع الجريمة كلها أو جلها ، تصبح أدلة الإثبات متوافرة ويغدو من اليسير إجراء التحقيقات الكفيلة لإظهار الحقيقة .

ويأتي من بعد مبدأ الإقليمية، مبدأ العالمية، حيث يكون هو الملائم لمعظم الجرائم الإلكترونية التي يتوزع النشاط المكون للركن المادي لها في أكثر من دولة ، ثم يلحقه في أولوية الترتيب مبدأ الشخصية في شقه الإيجابي ، بحيث ينعقد الاختصاص بنظر الجريمة للدولة التي يحمل جنسيتها مرتكب هذه الجريمة ، فإن تعددت جنسياته ، فيكون من حق الدول التي يحمل جنسياتها حتى لا يأخذ البعض من اكتساب جنسية جديدة سبيلا للإفلات من الملاحقة ، كما يمكن اللجوء إلى هذا المعيار تفاديا لإفلات المتهم من الملاحقة حين لا يتيسر ملاحقته وفقا لأي من المعايير السابقة. أما الحل أو النهج الثاني في محاولة التغلب على التنازع الإيجابي المتصور في الاختصاص الجنائي بين دولتين أو أكثر، فيتمثل في تدعيم وتأكيد الملاحقة الجنائية في كل حالة يخشى فيها لسبب إجرائي أو لآخر إفلات مرتكب الجريمة من المحاكمة ، ومثال ذلك حين تقع الجريمة في إقليم دولة معينة ويتم إلقاء القبض على المتهم في دولة أخرى يكون متمتعا بجنسيتها ، ففي هذا الفرض يثور التنازع في الاختصاص وفقا لمبدأين متعارضين : مبدأ الإقليمية الذي يمنح الاختصاص لدولة مكان وقوع الجريمة ، ومبدأ عالمية حق العقاب الذي يعطي الاختصاص بملاحقة الجريمة لدولة مكان القبض على المتهم، ويبيح لها في الوقت نفسه التنصل من تسليمه استنادا إلى أن معظم الدول ليست ملزمة - بغير اتفاق - بتسليم رعاياها .

وفي هذه الحالة يتطلب الاعتراف بمبدأ المحاكمة أو التسليم كما يقتضي، وعلى الاعتراف بإمكانية إحالة الدعوى الجنائية عن الجريمة الواقعة من دولة إلى أخرى ، وكذلك التأكيد على ضرورة تبادل كافة أشكال المساعدة القانونية - بموجب اتفاقيات - بين الدول ، وعلى وجه الخصوص فيما يتعلق بالحصول على شهادات الأشخاص ، وتبليغ الأوراق القضائية، وفحص الأشياء، وتبادل الأدلة، واللجوء إلى الإنابة القضائية، ويتم ذلك وفقا لقانون الدولة المطلوب منها مباشرة هذه الإجراءات أي الدولة المستنابة ، وليس طبقا لقانون الدولة التي أنابتها .



ولا شك أن خلق آليات جديدة نشطة من جانب الأمم المتحدة في إطار من المساعدة المادية والتقنية ، وتبادل الخبرات وإعداد قواعد بيانات، تمكن الجميع من المساهمة بفعالية في مكافحة الجرائم الإلكترونية .  
وبجوار هذه التطورات الوطنية المتمثلة في توالي الاعتراف المتزايد بحقل حماية المعطيات أو البيانات يركز الاعتقاد الراسخ بان تشغيل أو عمل أنظمة الحاسب الآلي قد تجاوز الحدود الوطنية نتيجة لظهور هذا الحاسب وانتشاره في سائر أنحاء العالم وأنه بفضل ما أفرزته تكنولوجيا المواصلات أن أصبح في مقدور مستخدم الحاسب الآلي في دولة ما أن يتوصل إلى أنظمة الحاسب الآلي في أي مكان في العالم، هذه الأبعاد الدولية لعمل الحاسب الآلي حثت الوكالات والمؤسسات ذات الطابع الدولي على التدخل لحماية المعلومات المخزنة وعدم الاعتداء عليها ، وفي مقدمة هذه الوكالات منظمة التنمية والتعاون الاقتصادي وكذلك المجلس الأوروبي والجماعة الأوروبية .

## ٢- اعتبار بعض صور المساهمة في دورها وآثارها من قبيل الجرائم المستقلة :

جعل اكتمال البناء القانوني لبعض الأنشطة الإجرامية يستند إلى قيام جريمة أصلية سابقة عليها، كجريمة الاعتداء على الملكية الفكرية ، وجريمة تسلم أو إخفاء أشياء مسروقة أو محصلة بأي وجه من الوجوه من جنابة أو جنحة ( أي المحصلة من مصدر غير مشروع الذي يشكل الجريمة الأصلية ) ؛ فثمة قوانين وطنية تعاقب على مثل هذه الأنشطة بوصفها من قبيل المساهمة التبعية في الجريمة الأصلية ، بمعنى أن مصير ملاحقة مرتكبيها وعقابهم يكون متوقفا على مصير ملاحقة وعقاب الفاعلين الأصليين للجريمة الأصلية ، وقد تتعذر ملاحقتهم لعدم خضوعهم للاختصاص الإقليمي للدولة التي ارتكبت عليه الجريمة التبعية ، وهو نهج يترتب عليه التقليل من الحماية الجنائية ويضعف من نظام الملاحقة، على عكس لو اعتبرت هذه الأنشطة جرائم مستقلة بذاتها وليست من الجرائم المساهمة التبعية<sup>(٢٦)</sup> ، والذي من شأنه التقليل من فرص الإفلات من الملاحقة والعقاب أمام مرتكبي مثل هذه الجرائم ، إضافة إلى أن يكون لهذه الأنشطة مدة تقادم خاصة بها ، تعطي مدة زمنية أطول للملاحقة، كما لا ينحصر الاختصاص القضائي بنظرها في الدائرة التي وقعت فيها الجريمة الأصلية، بل حسب القاعدة العامة في تحديد الاختصاص<sup>(٢٧)</sup>.

## ٣- تطوير نظام تقادم الجرائم والعقوبات :

يمثل نظام تقادم الجرائم والعقوبات وسيلة لمرتكبي الجرائم والمحكومين للإفلات من الملاحقة أو تنفيذ الأحكام ، وللمحد من اختراق ثغرات هذا النظام ينبغي تجريم بعض الأنشطة كالجرائم التبعية باعتبارها جرائم ذات طبيعة مستقلة كما سبقت الإشارة، على الأقل فيما يتعلق بالقواعد المنظمة لتقادم الجرائم ، وكذلك اعتبار الجريمة الإلكترونية مرتكبة في وقت اقتراف السلوك أو وقت حدوث النتيجة الإجرامية، أي اعتبار تاريخ السلوك وكذلك تاريخ حدوث النتيجة

٢٦ - المادة ١/٤٦٥ مكررة ( أ ) من قانون العقوبات الكويتي .

٢٧ - تنص المادة ١٩٠ من قانون الإجراءات الجنائية الكويتي على أنه " يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة ، أو الذي يقيم فيه المتهم ، أو الذي يقض عليه فيه .

الإجرامية كنقطة بداية لسريان مدة التقادم ، أو باعتبار بعض الجريمة الإلكترونية من قبيل الجرائم المستمرة ، بما يكفل مدة تقادم أطول، وأخيرا رفع تباين التشريعات الوطنية فيما يخص تحديد مدة التقادم وتدقيق فكرة انقطاعه ووقفه. والجدير بالذكر أن المشرع الكويتي قد أصدر القانون رقم ١١ لسنة ١٩٩٧ بشأن الأحكام الخاصة بالدعوى الجنائية وتعديل قانوني العقوبات والإجراءات الجنائية الذي نصت مادته الأولى على أن " لا تسقط الجريمة ولا تنقضي الدعوى الجنائية بمضي المدة " .

#### ٤- الاعتراف في بعض الحالات بحجية للتشريعات والأحكام الجنائية غير الوطنية :

القاعدة التقليدية هي تلازم السيادة التشريعية والقضائية في المجال الجنائي ، بما يعني أن كل دولة لا تعترف سوى بأحكام قانونها الجنائي الوطني، ولا تعتد، ولا تنفذ على إقليمها سوى الأحكام الجنائية الصادرة عن إحدى محاكمها الوطنية، ويجد ذلك سنداً في أن تطبيق القانون الجنائي يعد تعبيراً عن سيادة الدولة بوصفه يحمي المصالح الأساسية للمجتمع والدولة والحقوق الجوهرية لأفراده، إضافة إلى أن قواعد القانون الجنائي تتعلق في جملتها بالنظام العام ، وهو ما يحول دون الخضوع لحكم قانون أجنبي وتطبيقه<sup>(٢٨)</sup>

أما فيما يتعلق بحجية الأحكام الجنائية الأجنبية في شقها الإيجابي<sup>(٢٩)</sup> فإنه يجب أن يُفسح لها مكاناً بين أحكام المعاهدات الدولية ذات الصلة ، وهكذا يمكن أن يؤخذ في الاعتبار بالآثار الجنائية غير المباشرة للأحكام الجنائية الأجنبية لاسيما في الاعتراف بالآثار الجنائية غير المباشرة للأحكام الجنائية الأجنبية لاسيما في مجال العود ، ووقف التنفيذ وتقدير العقوبة في ضوء ما يثبت من الخطورة الإجرامية للجاني .

أما بالنسبة لحجية الأحكام الجنائية في شقها السلبي ، فقد اعترف بها بعض المشرعين<sup>(٣٠)</sup>، إذ يتمتع إقامة الدعوى الجنائية ضد من ارتكب جريمة في الخارج متى ثبت أن المحاكم الجنائية الأجنبية قد برأته أو أدانته نهائياً واستوفى عقوبته، فكأن هؤلاء المشرعين يعترفون بقوة الشيء المحكوم فيه ولو تعلق الأمر بحكم أجنبي تطبيقاً لقاعدة امتناع محاكمة الشخص عن ذات الفعل مرتين .

ونعتقد أنه حان الأوان لتجاوز بعض المفاهيم التقليدية، وخاصة فيما يتعلق بتلازم السيادة التشريعية والقضائية في المجال الجنائي، وذلك بالتوجه نحو الاعتراف في بعض الحالات وعلى نحو ما بحجية لتشريع جنائي عبر وطني، بل وبحجية لحكم جنائي صادر عن محاكم دولة أخرى ، وتتجلى أهمية ذلك على وجه الخصوص في مجال الجرائم التبعية التي تفترض ارتكاب جريمة أصلية على إقليم الدولة ما، ثم وقوع الجريمة التابعة على إقليم دولة أخرى، ومثال

٢٨ - وإذا كان القاضي الوطني يمكنه تطبيق أحكام قانون أجنبي في مجال القانون الدولي الخاص ، فإن ذلك راجع إلى أن قواعد القانون الأخير لا تتعلق بحسب الأصل بفكرة النظام العام ، بل تحمي مصالح خاصة مدنية أو تجارية أو مسائل الأحوال الشخصية

٢٩ - في معنى الاعتراف بما يتضمنه الحكم من عقوبات وآثار جنائية أخرى .

٣٠ - نص عليها المشرع الكويتي صراحة في المادة السابعة من قانون العقوبات .

ذلك جريمة الاعتداء على الملكية الفكرية ، وقد ظهرت أفكار تتادي بوجود الاعتراف فيما بين الدول بحجية للأحكام الجنائية الأجنبية على إقليم الدول الأخرى وحجة ذلك استفحال ظاهرة الجرائم الإلكترونية وضرورة تعاون دولي فيما بينها لمكافحتها حتى لا يفلت مرتكبوها من العقاب لمجرد أنهم أقاموا في دولة غير تلك التي صدر ضدهم فيها حكم جنائي بالإدانة وصار ممكنا الاعتراف بمثل هذه الحجية استنادا إلى معاهدة دولية تبرم بين الدول .

#### ٥- تفعيل التعاون الدولي ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية المتبادلة :

أدركت الدول أهمية التعاون الدولي وأحست بأنه أمر محتم لتجاوز تحديات الجرائم الإلكترونية ، فعمد الكثير منها إلى عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في هذه جرائم الكمبيوتر<sup>(٣١)</sup> ، ففي عام ١٩٨٣ أجرت منظمة التعاون والإينماء الاقتصادي دراسة حول إمكان تطبيق القوانين الجنائية الوطنية و تكييف نصوصها لمواجهة تحديات الجرائم الإلكترونية وسوء استخدامه، وفي عام ١٩٨٥ أصدرت هذه المنظمة تقريراً ع تضمن قائمة بالحد الأدنى لعدد أفعال سوء استخدام الحاسب الآلي التي يجب علي الدول أن تجرمها وتفرض لها عقوبات في قوانينها ومن أمثلة هذه الأفعال: الغش أو التزوير في الحاسب الآلي، تغيير برامج الحاسب الآلي أو المعلومات المخزنة فيه، سرقة الأسرار المدعمة في قواعد الحاسب الآلي ؛ تفعيل التعاون الدولي في مجال مكافحة الجريمة الإلكترونية ، كما عالجت اتفاقية فيينا لسنة ١٩٨٨ الموضوع ذاته ، وحثت الكثير من الدول على عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في هذه الجرائم ، وكذلك لفت اللقاء التمهيدي الإقليمي لآسيا و الباسفيك المنعقد ١٩٨٩ الممهد للمؤتمر الثامن للأمم المتحدة المنعقد في كوريا ١٩٩٠ النظر إلي نتائج التطور و التقدم التكنولوجي فيما يتعلق بالجريمة الإلكترونية واقترح تشجيع اتخاذ إجراء دولي حيال هذه الجريمة ، والمؤتمر الأخير ناشد في قراره المتعلق بالجرائم ذات الصلة بالحاسب الآلي الدول الأطراف إلى ضرورة تكثيف جهودها لمكافحة الجرائم الإلكترونية في عدة وجوه<sup>(٣٢)</sup> ، منها تحديث القوانين الإجرائية وتبادل المساعدة في المسائل الخاصة بالجرائم الإلكترونية وعقد اتفاقيات دولية تنطوي على نصوص تنظم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية ، ووضع المجلس الأوروبي عام ٢٠٠١ اتفاقية بودابست ، تشكل نصوصها منظومة تعاون دولي تتسم بالمرونة الفعالية وتعمل على إحداث تقارب بين التشريعات الجنائية الخاصة بهذه الجرائم وتكفل استخدام الوسائل الفعالة في البحث والتحقيق وملاحقة مرتكبيها<sup>(٣٣)</sup> وما يتعلق بالنصوص الخاصة بالتعاون الدولي ، ولكن الأمر في كافة الأحوال منوط بقابلية التطبيق من جانب الدول من ناحية ، وخلق

٣١ - د.محمد الأمين البشري ، التحقيق في جرائم الحاسب الآلي ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من ١ - ٣ مايو ٢٠٠٠ بكلية الشريعة والقانون بدولة الإمارات ، ص١٠٧.

٣٢ - انظر في ذلك د. محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ( الكمبيوتر ) ، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة ٢٥ - ٢٨ أكتوبر ، ١٩٩٣ ، ص ٣٢٢

٣٣ - وذلك في المواد ٢٠٠٤،٢٠٠٣،٢٠٠٢ من الاتفاقية .

آليات جديدة ونشطة من جانب الأمم المتحدة من ناحية أخرى في إطار من المساعدة المادية والتقنية ، وتبادل الخبرات وإعداد قواعد بيانات تمكن الجميع من المساهمة بفعالية في التصدي للجريمة الإلكترونية .

وعلى الرغم من ضرورة التعاون الدولي وتضافر الجهود من أجل تفعيله، إلا أن هناك العديد من العقبات التي تعترض سبيله من أبرزها: عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الإلكترونية، عدم وجود توافق بين قوانين الإجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم، والنقص الظاهر في مجال الخبرة لدى الشرطة و جهات الادعاء و القضاء .

### المبحث الثاني - الإثبات وأدلته

نقسم هذا المبحث إلى مطلبين، نتناول في المطلب الأول الإثبات وفي المطلب الثاني نتعرض لوسائل أو إجراءات جمع الأدلة ، ونردف عرضاً لصعوبات جمع الأدلة .

#### المطلب الأول- في الإثبات

الإثبات في المواد الجنائية يخضع لقواعد تختلف عن تلك التي تحكم الإثبات في المواد المدنية، وذلك لاعتبارات قد ترجع إلى اختلاف موضوع الإثبات بين تلك المواد ومنها ما يرجع إلى أهمية الدعوى الجنائية، وأن القواعد التي تحكم المسائل الجنائية تدور كلها حول غاية واحدة وهي الكشف عن حقيقة جريمة تمثل اعتداء على الجماعة وتهم المجتمع بأسره .

ومن القواعد التي تحكم الإثبات في المسائل الجنائية ثلاث : أولها حرية القاضي في تكوين عقيدته ، بمعنى أن له أن يوجه تحقيقه في الجلسة بالشكل الذي يراه مناسباً وملائماً للوصول إلى الحقيقة والكشف عنها دون أن يتقيد في ذلك بإتباع وسائل معينة للكشف عن الحقيقة، كما أن له مطلق الحرية في تقدير أدلة الدعوى ، فله أن يأخذ بها وله أن يطرحها ، كل ذلك بناء على تقييمه لها وقناعته بما ينتهي إليه من مجموع ما طرح من أدلة في الجلسة<sup>(٣٤)</sup>(٣٥) ؛ وأن يحكم في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته مما يطرح أمامه على بساط البحث في الجلسة دون إلزام عليه بالتقيد بطريق معين من طرق الإثبات ، إلا إذا أوجب القانون عليه ذلك ، أو حظر عليه سلوك طريق معين في الإثبات يستمد قناعته من أي ورقة سواء كانت رسمية أو عرفية يستخلص منها ما يطمئن إليه ضميره ووجدانه ويطرح ما لا يطمئن إليه ، شأنه في ذلك شأن سائر الأدلة الأخرى التي قد تطرح أمامه ؛ وثاني القواعد التي تحكم

٣٤ - قد يحدث أن يفترض المشرع بعض عناصر الجريمة وذلك لصعوبة الإثبات وبالتالي يضع قيوداً على حرية القاضي في تكوين عقيدته ، وأحياناً أخرى يفيد المشرع القاضي الجنائي بأدلة معينة يلتزم بها في تكوين رأيه ، كتقييد القاضي الجنائي بطرق الإثبات الخاصة بالمواد غير الجنائية ؛ وحجبة بعض المحاضر في إثبات ما ورد بها من وقائع ؛ وكذلك قد يفيد الإثبات في نوع معين من الجرائم بأدلة معينة ، كما في جرائم الحدود .

٣٥ - من الشروط الخاصة لممارسة القاضي حريته في الاقتناع : أن تكون عقيدته واقتناعه قد استمدا من أدلة طرحت بالجلسة ، وأن يكون اقتناعه مبنياً على دليل مستمد من إجراء صحيح ، ومبنياً على أدلة مستساغة عقلاً وعلى اليقين الذي ينفي الأصل وهو البراءة ، وأن لا يؤسس على قرينة واحدة .

لإثبات في المسائل الجنائية الدور الإيجابي للقاضي الجنائي في البحث عن الحقيقة ، فإنه ليس مجرد موازنة للأدلة المثبتة للإدانة أو البراءة ، وإنما عليه التحري عن الحقيقة والكشف عنها، وهو في ذلك يختلف عن القاضي المدني الذي يكون دوره في الدعوى المدنية المنظورة أمامه سلبيا ومقتصرا على الموازنة بين أدلة الخصوم؛ وآخر القواعد التي تحكم الإثبات في المسائل الجنائية قاعدة عبء الإثبات في المواد الجنائية يقع على سلطة الإدعاء من منطلق أن الأصل في الإنسان البراءة، وعلى من يدعي عكس ذلك إثباته .

ولا شك في أن مجموع هذه القواعد لا اختلاف فيها بين الجرائم التقليدية والجرائم الإلكترونية، إلا أن الطابع الخاص الذي تتميز به الجرائم الإلكترونية أن محل أو موضوع بعضها يكون غير مادي ، إضافة إلى أن إثبات هذه الجرائم يحيط به كثير من الصعوبات التي تتمثل في صعوبة اكتشاف هذه الجرائم بحسب أنها جرائم فنية تتطلب تقنية معينة في مجال الحاسبات الآلية والانترنت ، وهي على الرغم من أنها - غالبا - ما تكون جريمة هادئة لا عنف فيها ولا تترك أشياء مادية تدرك بالحواس، لكونها عبارة عن أرقام وبيانات تتغير أو تمحي من السجلات المخزنة في ذاكرة الحاسبات، إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية (FBI) نظرا لتمثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف<sup>(٣٦)</sup> .

وإلى جانب إمكانية ارتكابها عبر الوطنية باستخدام شبكات الاتصال ، فإن المجني عليه الذي عادة ما يكون مؤسسة مالية أو مشروعاً صناعياً ضخماً يحاول - في الغالب - كتم حصول الجريمة والإحجام عن البلاغ عنها أو مساعدة السلطات المختصة في إثباتها والكشف عنها حتى لا يتم تقليدها من قبل الآخرين، وخشية من أن يترتب على شيوع العلم بوقوعها إساءة واهتزاز لسمعته وثقة المساهمين والعملاء .

دليل الإثبات هو " الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه "<sup>(٣٧)</sup> .

والدليل الجنائي ، معنى يدرك من مضمون واقعة تؤدي إلى ثبوت الإدانة أو استقرار البراءة، ويتم باستخدام الأسلوب العقلي وإعمال المنطق في وزن تقدير تلك الواقعة ليصبح المعنى المستمد منها أكثر دقة في الدلالة على الإدانة أو البراءة .

ولم يحدد المشرع الكويتي الأدلة في المواد الجنائية، وإنما تركها لتقدير القاضي، وأورد بعض أدلة الإثبات وهي شهادة الشهود وندب الخبراء دون أن تتجه إرادته إلى حصر الأدلة التي يمكن للقاضي أن يستند إليها في حكمه .

٣٦ - Computer Hackers : Tomorrows Terrorists , Dgnamics , News For And Aboutmembers Of the American Society For Industrial Security, Varyl February , 1990 , p.7 . نقلا عن د. محمد على

الغريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة لنشر ، الإسكندرية ، ٢٠٠٤ ص ٥٣ و ٥٤ .

٣٧ - د. مأمون محمد سلامة ، الإجراءات الجنائية في التشريع الكويتي ، الجزء الثاني ، منشورات المكتبة الوطنية ، الطبعة الثانية ، ٢٠٠٠ ، ص ١٧٦ .

وقد تعارف الفقه والقضاء على الأدلة التي يمكن للقاضي الاستناد إليها دون أن يحول ذلك عن الاستناد إلى أدلة أخرى ، وهذه الأدلة هي الاعتراف والمعينة والمحركات وشهادة الشهود والخبرة والقرائن ، غير أن هذه الأدلة تبدو في الأعم قاصرة إزاء ملاحقة مرتكب الجريمة الإلكترونية الذي يتوسل بنبضات اليكترونية غير مرئية العبث بالدليل أو محوه بالكامل في وقت قصير جدا ، يتعذر معه كشفها إلا بطريق الصدفة .

و في هذا المطلب نفتصر دراستنا علي الخبرة و المحركات ، و نحيل بشأن المعينة و التفتيش و ضبط الأشياء و ندب الخبراء إلي ما سيأتي ذكره في المطلب الثاني من هذا المبحث .

### ١- الخبرة :

الخبرة هي إجراء يتعلق بموضوع يتطلب إماماً بعلم أو فن معين لإمكان استخلاص الدليل منه ، لذلك فإن الخبرة تفترض وجود شيء مادي أو واقعة يستظهر منه الخبير رأيه .  
وللمحكمة أثناء تحقيقها النهائي أن تنتدب الخبراء وذلك إذا ما عرضت أثناء المناقشة مسألة تحتاج لرأي فني أو تقني .

ويعتبر تقرير الخبير من الأدلة، أما إجراء ندب الخبير فهو من إجراءات جمع الأدلة ، ولذلك إذا ما بوشر بمعرفة سلطة التحقيق تحركت به الدعوى العمومية باعتباره إجراء من إجراءات التحقيق .

والخبرة كدليل في الإثبات تتصرف إلى رأي الخبير الذي يثبته في تقريره، ولذلك فإن الخبير يأخذ حكم الشاهد ويجوز استدعاؤه لسماع شهادته ومناقشته في التقرير الذي أعده وتقدم به، غير أن الخبير يختلف عن الشهود من حيث الوقائع التي يشهد بها ، فالشاهد يدلي بأقواله عن الواقعة كما حدثت في مادياتها أما الخبير فشهادته فنية أي تتصرف إلى تقييمه الفني للواقعة محل الخبرة ويترتب على ذلك أنه لا يجوز سماع الخبير كشاهد إذا كان إجراء الخبرة قد وقع باطلا<sup>(٣٨)</sup> .

### ٢- المحررات أو الدليل الكتابي :

الكتابة لا تعدو كونها رموزاً تعبر عن الفكر و القول ، و قد ظلت العلاقة بين الكتابة و الدعامة الورقية المدونة عليها علاقة وثيقة لفترة طويلة من الزمن ، حيث كان يسود الاعتقاد بأن الكتابة تساوي الورق ، كل ذلك علي الرغم من أنه لا في اللغة ولا في القانون ما يتطلب أن تكون الكتابة علي الورق فقط ، بل من الجائز أن تكون علي الورق أو الجلد أو القماش أو الحجر أو الخشب أو علي دعامة أخرى مادية كانت أو رقمية .

٣٨ - د. مأمون محمد سلامة ، الإجراءات الجنائية في التشريع الكويتي ، الجزء الأول ، منشورات الجامعة الكويتية كلية الحقوق ، بنغازي ، بدون تاريخ ، ص ٦٠٣- ٦٠٥ .

والدليل الكتابي هو المحرر ، ويمكن تعريفه بأنه " مجموعة من العلامات والرموز تعبر اصطلاحاً عن مجموعة مترابطة من الأفكار والمعاني " (٣٩) (٤٠)، وهو قد يكون الجريمة نفسها كالورقة المزورة ، وقد يكون أداة إثباتها، وقد تجمع الورقة بين الدورين كالورقة التي تحمل عبارات الفذف والسب .

والمحرر كدليل أو وسيلة إثبات يخضع لمبدأ الاقتناع القضائي ، فكل قيمته مستمدة من اقتناع القاضي بصحة ما يتضمنه من البيانات، ويتعين أن يستمد القاضي هذا الاقتناع وفقاً للقواعد العامة في الإثبات الجنائي، فالأصل أنه لا وجود لأوراق ذات حجية مطلقة بحته يمتنع على المحكمة أن تأخذ بما يخالفها ، أو يمتنع على أطراف الدعوى إثبات عكسها ، ذلك أنه لا يجوز إلزام المحكمة أن تقضي بما يخالف اقتناعها الذي كونته من مجموع الأدلة المقدمة في الدعوى .

فالقاعدة العامة في الإثبات الجنائي هو عدم تقيد القاضي في قناعته بأدلة إثبات معينة، كل ذلك ما لم تكن المحكمة تفصل في مسألة غير جنائية وضرورية للفصل في الدعوى الجنائية وكانت هذه المحررات لها حجيتها في القانون الخاص بتلك المسائل، فالمحكمة في هذه الحالة لا تستطيع أن تطرح ما ورد بتلك المحررات، إلا إذا لم تطمئن إلى صحة المحرر ذاته، أما إذا اقتنعت بصحته فليس لها أن تقضي بخلاف ما ورد به طالما أنها هي وسيلة الإثبات في المواد غير الجنائية .

والمحررات رسمية كانت أو عرفية التي تثبت وقوع الجريمة سواء أكانت هذه المحررات موضوع السلوك الإجرامي ذاته كما في جريمة التزوير أو التهديد كتابية ، أم كانت تتضمن دليلاً على ارتكاب الجريمة ، فهذه بطبيعتها تخضع لمطلق تقدير المحكمة التي لها أن تأخذ بها أو تطرحها دون أن تكون ملزمة بتسبب طرحها لها (٤١).

وهناك ما يسمى بالدليل الرقمي، وهو ما يعرف بأنه " الدليل الذي يجد له أساساً في العالم الافتراضي إلى الجريمة " (٤٢) .

وعرف أيضاً بأنه " الدليل المأخوذ من أجهزة الحاسب الآلي في شكل مجالات و نبضات مغناطيسية أو كهربائية ممكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة ، (٤٣) .

٣٩ - د. محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ، الجزء الأول ، دار النهضة العربية ، الطبعة الثانية ، القاهرة ١٩٨٨ ص ٤٨٣ .

٤٠ - التشريعات العربية ليست متفقة في تحديد مسمى الدليل الكتابي ، فهناك من يستخدم مصطلح المحرر كالمشرع المصري و الإماراتي ، و هناك من يستخدم مصطلح السند كالمشرع الأردني و السوري ، و يستخدم المشرع الكويتي مصطلح الورقة ، أما المشرع الكويتي فقد استخدم مصطلح الورقة في القانون المدني و قانون الإجراءات الجنائية ( م ٤٤ ) ، و استخدم في قانون العقوبات كلمة وثيقة كما هو في جرائم التزوير و إتلاف الوثائق الرسمية المواد ٣٤١ و ٣٤٢ و ٣٤٦ و ٣٤٧ و ٣٤٨ ، أما المشرع الفرنسي فقد اعتمد مصطلح ( الحجج المكتوبة ) .

٤١ - د. مأمون محمد سلامة ، الجزء الثاني ، مرجع سابق ، ص ١٩٣ .

٤٢ - د.عصر محمد أبو بكر بن يونس ، الجرائم الناشئة عن استخدام الإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٤ م ص ٩٦٩ .

٤٣ - مدوح عبد المجيد عبد المطلب ، استخدام بروتوكول TCP/IP في بحث و تحقيق الجرائم على الكمبيوتر ، بحث منشور على الإنترنت ، الموقع الإلكتروني Dpolice.Maktooblog .

و الدليل الرقمي هو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل الرموز و النصوص المكتوبة أو الصور أو الأصوات و الأشكال و الرسوم يعبر عن فكر و قول يطلق عليه الكتابة الرقمية بالمعنى الواسع ، التي لا تشمل الكتابة التقليدية علي الورق فحسب، وإنما تشمل أيضا الكتابة التي تتم عن طريق وسائل الاتصال الحديثة ( شبكة المعلومات الدولية وما في حكمها) مهما كانت الدعامة المستخدمة في تثبيتها. ولهذا نجد بعض الاتفاقيات الدولية<sup>(٤٤)</sup> قد تبنت هذا المفهوم الواسع للكتابة، و كذلك بعض التشريعات المقارنة.

ولقد سايرت بعض القوانين العربية هذا التطور الحاصل في الوسائل المستحدثة وحددت للكتابة الرقمية معنى متأثراً إلي حد كبير بقانون الأونسترال النموذجي الذي بين المراد من رسالة البيانات بأنها : " المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة بما في ذلك علي سبيل المثال لا الحصر تبادل البيانات الإلكترونية أو البرق أو التلكس أو النسخ البرقي"، فجاء مدلول الكتابة في قوانين هذه الدول موسعا ليشمل الكتابة بمفهومها الحديث<sup>(٤٥)</sup>

وللدليل الرقمي ثلاث خصائص، الأولى أنه دليلا غير ملموس ، والثانية أنه دليل من قبيل الأدلة الفنية أو العلمية ( الأدلة المستمدة من الآلة)، والخصيصة الثالثة أن فهم مضمون الدليل الرقمي يعتمد على استخدام أجهزة تجميع وتحليل فحواه ليكون دليل إثباتها .

١ - نذكر منها علي سبيل المثال : أ- اتفاقية نيويورك بشأن التقدم في البيوع الدولية للبيانات ١٩٧٢ : تشير هذه الاتفاقية في مادتها التاسعة إلي أن مصطلح الكتابة ينصرف أيضا إلي المراسلات التي توجه في شكل برقية أو تلكس ب- اتفاقية الأمم المتحدة بشأن النقل متعدد الوسائل للبيانات ١٩٨٠ : حيث اعتبرت في الفقرة الثانية من المادة الخامسة منها السندات الرقمية المستخرجة من وسائل الاتصال الحديثة من ضمن السندات الكتابية بشرط أن تكون هذه السندات واضحة العبارة و مفهومة . ج- اتفاقية هامبورج ١٩٨٧ الخاصة بنقل البضائع بحراً : و جاء في الفقرة الثامنة من مادتها الأولى أن مصطلح الكتابة يشمل البرقية و التلكس .

٤٥ - و من هذه القوانين قانون الإثبات السوداني لعام ١٩٧٣ م في مادته ٣٧ وقانون أصول المحاكمات المدنية الليباني الصادر في ١٦ سبتمبر ١٩٨٣ المعدل بالقانون الصادر في ١٢ يوليو ٢٠٠٠ ، وقانون أصول المحاكمات المدنية الأردني رقم ٢٤ لسنة ١٩٨٨ في مادته ( ١ / ٨٠ ) المعدل بالقانون رقم ١٤ لسنة ٢٠٠١ ، وكما جاء في القانون المدني التونسي ٥٧ لسنة ٢٠٠٠ في الفصل ٤٥٣ مكرر ، و دبي في دولة الإمارات العربية قانون رقم ٢ لسنة ٢٠٠٢ في ١٢ فبراير ٢٠٠٢ قانونا خاصا بالتعاملات الإلكترونية ، والقانون رقم ١٥ لسنة ٢٠٠٤ المصري بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة صناعة تكنولوجيا المعلومات في مادته ١ / م ، وأما القانون الكويتي ، فإنه رغم ما يفهم من بعض النصوص الواردة في المواد من ٣٧٧ وحتى ٣٨٦ من القانون المدني بان هناك تلازما بين الكتابة والورق ، إلا أنه من المسلم به أن الورق ليس هو الدعامة الوحيدة للكتابة وليس هناك ما يمنع - قانونا - من أن تكون دعامة في الكتابة من أية دعامة أخرى ، و مما يدل على ذلك نص المادة ٩٧ من القانون رقم ١ لسنة ٢٠٠٥ بشأن المصارف ، التي جاء في فقرتها الثانية والثالثة " يعتد بالمستندات و التوقيعات الإلكترونية ، التي تتم في إطار المعاملات المصرفية و ما يتصل بها من معاملات أخرى ، وتكون لها الحجية في إثبات ما تتضمنه من بيانات ، و في مصر صدر في ٢٢ أبريل ٢٠٠٤ إعداد مشروع التجارة الإلكترونية

و تعتبر مخرجات الحاسوب المتعلقة بالمعاملات المصرفية وفقاً للمصوص عليه في الفقرة السابعة بمطابقة الدفاتر القانونية المنصوص عليها في القانون التجاري و القوانين المكملة له .  
و للمصارف أن تحتفظ للمدة المقررة في القانون بنسخ مصغرة علي أقراص صلبة أو مرنة أو مضغوطة أو علي غير ذلك من الأدوات التقنية الحديثة أو المعلومات بدلاً من أصول الدفاتر و السجلات و الكشافات و الوثائق و المراسلات و البرقيات و الإشعارات و غيرها من الأوراق المتصلة بأعمالها ، و تكون لهذه النسخ المصغرة حجية الأصل في الإثبات .

و من نظرة القول أن هذا النص رغم تعلقه بالمعاملات المصرفية و التجارية إلا أنه يشكل أول خطوة بخطوها المشرع الكويتي في طريق الأخذ بالكتابة الحديثة أو الكتابة الرقمية ، كما أنه يعتبر دليلاً قاطعاً علي انعدام الارتباط القانوني بين الكتابة و الورق ، و لعل الأمل يحدونا في أن يساير المشرع الكويتي هذا التطور الحاصل في تقنيات الاتصال الحديثة فيما يصدره من تشريعات في المستقبل سواء تعلقت بالقوانين المدنية و التجارية و كذلك الجنائية .  
شريطة أن تتوفر فيه شروط الأمان و الثقة من خلال التقنيات المستخدمة .

و علي صعيد التشريعات المنظمة للمعاملات الرقمية ، نلاحظ أن أكثر القوانين تطوراً و وضوحاً في تحديد معنى الكتابة الرقمية هو التقنين المدني الفرنسي وفقاً لأخر تعديلاته حيث يفهم من مادته (١٣١٦) أن الكتابة الرقمية هي : " كل تدوين للحروف أو العلامات أو الأرقام أو أي إشارة ذات دلالة تعبيرية واضحة و مفهومة أي كانت الدعامة التي تستخدم في إنشائها أو الوسيط الذي تنتقل عبره " .

نستشف من النص أن المشرع الفرنسي أطلق مصطلح الكتابة دون تحديد فيما إذا كانت بدوية أو رقمية و دون التفات لنوع الدعامة المستخدمة في تثبيتها ، فالمهم هو ما تحققه الكتابة من التعبير الدال الواضح و المفهوم ، و لا عورة بالتقنية المستخدمة في إنشاء الكتابة أو حفظها أو نقلها.



والأصل أن الدليل الرقمي غير مادي ، يتكون من بيانات و معلومات ذات هيئة رقمية غير ملموسة و إخراجها في شكل مادي ملموس يتطلب الاستعانة بأجهزة الحاسب الآلي وأدواته واستخدام نظم برمجية حاسوبية، ويتميز بالسرعة والسهولة وصعوبة محوه أو تحطيمه وإن حاول الجاني محو الدليل الرقمي، فإن هذه المحاولة بذاتها تسجل عليه كدليل، كما أن الطبيعة الفنية للدليل الرقمي تكمن في إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان قد تعرض للغش والتحريف ، هذا من ناحية الجانب الايجابي، أما من حيث الجانب السلبي ، فإن ذلك يتمثل في الاستخدام غير المشروع أو غير المصرح به للحاسب الآلي والانترنت وما عرف بجرائم الإلكترونيات أو المعلوماتية وما يكتنف ذلك من مشكلات علي المستوى التنظيمي و القانوني و التقني ، الأمر الذي يتطلب وسائل تقنية و قواعد قانونية تحيطه بسياج من الحماية وهو ما أدى إلي صدور العديد من التشريعات كمحاولة لوضع ضوابط وتنظيم قانوني بقصد توفير الحماية اللازمة للمستخدمين والقائمين على تقديم خدمة الإنترنت .

وللدليل الرقمي ثلاثة أنواع : الأول مخرجات<sup>(٤٦)</sup> ذات طبيعة ورقية ، تسجل فيها المعلومات على الورق ، ويستخدم في ذلك الطابعات والراسم في طباعة الرسومات بدرجات وضوح مختلفة على الورق ؛ النوع الثاني مخرجات ذات طبيعة إلكترونية، تستخدم في تخزين المعلومات بدل الوثائق الورقية كالأشرطة المغناطيسية والأوراق المغناطيسية؛ والنوع الثالث مخرجات مرئية معروضة بواسطة شاشة الحاسب الآلي ذاته، ويتمثل هذا النوع في عرض البيانات المعالجة آليا بواسطة الحاسب الآلي على الشاشة الخاصة به<sup>(٤٧)</sup>

إما عن أنواع الدليل الرقمي كدليل إثبات من عدمه يمكن تقسيمه لنوعين رئيسيين : أدلة أعدت لتكون وسيلة إثبات كالسجلات التي تم إنشائها بواسطة الآلة تلقائيا كذلك السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة، وأدلة لم تعد لتكون وسيلة إثبات وهذا النوع من الأدلة الرقمية ينشأ دون إرادة الشخص أي أنه اثر يتركه الجاني دون إن يكون راعبا في وجوده .

وتبدو أهمية التمييز بين هذين النوعين أن النوع الأول من الأدلة الرقمية هو الأكثر أهمية من النوع الثاني لكونه أعد أصلا ليكون وسيلة إثبات لبعض الوقائع ، وعادة ما يعتمد إلى حفظه للاحتجاج به لاحقا ، بينما النوع الثاني من الأدلة الرقمية لم يعد أصلا ليكون أثرا لمن صدر ضده .

<sup>٤٦</sup> - عرفت مخرجات الحاسب الآلي أو كما أسماها البعض الوثيقة المعلوماتية أو المعالجة معلوماتيا بأنها " كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات ، وقد سجلت عليه معلومات معينة سواء أكان معدا للاستخدام بواسطة نظام المعالجة الآلية للمعلومات أم يكون مشتقا من هذا النوع " راجع د. علي عبد القادر القهوجي، تطور الحماية الجنائية لبرامج الحاسب الآلي والمعلوماتية بوجه عام ص ٣٨ وما بعدها

<sup>٤٧</sup> - وقسمت وزارة العدل الأمريكية عام ٢٠٠٢ الدليل الرقمي إلي ثلاث مجموعات هي : السجلات المحفوظة في الحاسب الآلي ؛ و السجلات التي يتم إنشاؤها بواسطة الحاسب الآلي و مخرجات برامجه التي لم يساهم الإنسان في إنشائها كسجلات الهاتف و فواتير أجهزة الحاسب الآلي ؛ و النوع الثالث هو السجلات التي تم حفظ جزء منها بالإدخال و الجزء الآخر تم إنشاؤه بواسطة الحاسب الآلي و من أمثلة ذلك البيانات التي يتم إدخالها إلي الجهاز و تتم معالجتها من خلال برنامج خاص كإجراء العمليات الحسابية علي تلك البيانات .

إما عن إشكال الدليل الرقمي فيمكن إيجازها في ثلاث إشكال رئيسية : الصور الرقمية ، التسجيلات ، النصوص المكتوبة .

والقيمة القانونية للدليل الرقمي في مجال الإثبات الجنائي تتمثل في مشروعية الدليل الرقمي وحجيته بحيث يمكن القول إن النظم القانونية تختلف في موقفها من الأدلة التي تقبل كأساس للحكم بالإدانة، فهناك اتجاهان رئيسيين : الأول نظام الأدلة القانونية بمعنى أن المشرع يحدد الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات ، كما يحدد القيمة الإقناعية لكل دليل، فلا سبيل للاستناد إلى أي دليل لم ينص القانون عليه صراحة ضمن أدلة الإثبات ، كما أنه لا دور للقاضي في تقدير القيمة الإقناعية للدليل، ولذا يسمى هذا النظام بنظام الإثبات القانوني أو المقيد، ويسود هذا النظام في الأنظمة الانجلوسكسونية ؛ أما عن الثاني ( نظام الإثبات الحر ) فهو يسود في ظل الأنظمة اللاتينية ، ووفقا لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في إثبات الوقائع المعروضة عليه، فلا يلزمه القانون الاستناد إليها في تكوين قناعته، أي أن الأصل في هذا النظام مشروعية وجودها، فالدليل الرقمي سيكون مشروعاً من حيث الوجود استصحاباً للأصل .

وقد تبنت بعض التشريعات نظام الإثبات المقيد أو ما يعرف بنظام الأدلة القانونية مع تمتع القاضي بسلطة واسعة في تقدير الدليل، والبعض الآخر من التشريعات تبني نظام الأدلة القانونية الحرة ، وقد أخذ المشرع الكويتي بنظام الجمع بين النظامين .

إما عن مشروعية الحصول على الدليل فقد تركز بشكل أساسي في إجراءات التفتيش للبحث عن هذا الدليل والتي يمكن حصره في مدى مشروعية التفتيش عن الدليل الرقمي وضبطه في الوسط الافتراضي ، بالرغم من عدم النص صراحة على جواز تفتيش الوسط الافتراضي وضبط محتوياته، إلا أن هناك اجتهادات بالخصوص على اعتبار إن التفتيش عن الدليل الرقمي في الوسط الافتراضي وضبط محتوياته مشروعاً، حيث إن تمتع الأدلة الرقمية بحجية قاطعة في الدلالة على الوقائع التي يتضمنها، ويمكن التغلب على مشكلة الشك في مصداقيتها من خلال إخضاعها لاختبارات تمكن من التأكد من صحتها ، ويرى البعض أنه لا يمكن اعتبار هذه القيمة المدعى بها للدليل الرقمي بمثابة خروج مستحدث عن القواعد العامة للإثبات الجنائي في القانون الكويتي ، حيث إن هناك من الأدلة ما لا يستطيع القاضي الجنائي تقديرها وفقاً لسلطته المقررة، ويرى أصحاب هذا الرأي عدم الخلط بين الشك الذي يشوب الدليل الرقمي بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه وبين القيمة الإقناعية لهذا الدليل ، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية، فالقول فيها هو قول أهل الخبرة، فإن سلم الدليل الرقمي من العبث والخطأ، فإنه لن

يكون للقاضي سوى القبول بهذا الدليل ولا يمكنه التشكيك في قيمته الدليلية لكونه وبحكم طبيعته الفنية يمثل إخباراً صادقاً عن الواقع ما لم يثبت عدم صلة الدليل الجريمة المراد إثباتها<sup>(٤٨)</sup>.

ونتيجة تردد الفقه والقضاء حيال مشروعية الأدلة المتحصلة من الوسائل الإلكترونية كمخرجات الحاسب الآلي بأنواعها المختلفة، خشية أن تكون قد تعرضت للتغيير في فحواها أو لطمس الحقيقة فيها، خاصة أن معظمها يمس مساساً مباشراً بحقوق الأفراد الأساسية وحررياتهم، ولهذا وضعت شروط ينبغي توافرها في كل دليل مقدم أمام القضاء الجنائي كأن يكون الدليل مشروعاً أي أن يكون وليد إجراءات صحيحة، وأن يكون قد طرح في الجلسة، وأن يكون مبنيًا على الجزم واليقين.

وقد نصت بعض التشريعات المقارنة على بعض الشروط والضوابط التي يجب مراعاتها في مخرجات الحاسب الآلي لكي يمكن قبولها كأدلة إثبات من أهمها: أن يتم تحديد هوية الشخص أو الجهة المنسوب إليه المخرجات بصورة قاطعة؛ وأن يتم أيضاً استخلاص المعلومات المخزنة إلكترونياً وحفظها بصورتها الأصلية التي أنشئت عليها وبصورة تضمن عدم تعرضها لأي شكل من أشكال العبث أو التلف<sup>(٤٩)</sup> وهذا الشرط يتطلب اتخاذ بعض الإجراءات التي من أهمها: التحقق من سلامة الحاسب الآلي ودقته في عرض المعلومات المخزنة، وحفظ مخرجات الحاسب الآلي وتخزينها في بيئة مناسبة، وكفاءة ونزاهة القائمين على جمع الأدلة وتخزينها.

وقد اعترفت بعض التشريعات بالدليل الكتابي الرقمي، فجدد قانون الأمم المتحدة النموذجي للتجارة الإلكترونية يعترف بالدليل الكتابي الرقمي موضحاً أنه في حالة ما إذا اشترط القانون أن تكون المعلومات مكتوبة فإنها تستوفي مثل هذه الشروط متى أمكن تخزينها والاطلاع عليها عند الحاجة لذلك، كما اعترف بعض تشريعات الدول بدليل الكتابي الرقمي<sup>(٥٠)</sup>، واشترط الفقه أن تتوفر مجموعة شروط حتى يضطلع الدليل الكتابي الرقمي بدوره في الإثبات، ومن هذه الشروط ضرورة أن يكون الدليل الكتابي مقروءاً و متصفاً بالاستمرار وغير قابل للتعديل.

وإذا كان التطور التقني في الوقت الحاضر أدى إلي تردد جانب من الفقه والقضاء حيال الأخذ بالكتابة الرقمية واستخدامها في المجال الجنائي كدليل شأنها في ذلك شأن المحررات الورقية في الإثبات، علي اعتبار أن هذا النوع من الجرائم له طبيعة خاصة نظراً لما تتميز به من تقنية عالية و خفاء في ارتكابها حيث يستطيع الجاني أن يرتكبها بسرعة دون أن يترك وراءه أي أثر خارجي ملموس لكونه يتميز عادة بالذكاء و الدهاء و الخبرة و المهارة

<sup>٤٨</sup> - أ. طارق محمد الجملي، الدليل الرقمي في الإثبات الجنائي، منشور علي مواقع الإنترنت، بدون ترقيم للصفحات.

<sup>٤٩</sup> - وقد أكدت ذلك المادة الثامنة من قانون الأونسترال النموذجي الخاص بالتجارة الإلكترونية، والمادة ١/١٣١٦ من القانون المدني الفرنسي، والمادة ٣/١٠٠١ من قانون الإثبات الأمريكي، وتضمنت المادة الثامنة من قانون إمارة دبي للمعاملات التجارية الإلكترونية عدة شروط في هذا الخصوص.

<sup>٥٠</sup> - مثل المادة ٢ من قانون المعاملات الإلكترونية لإمارة دبي و المادة ١ فقرة ب من قانون التوقيع الإلكتروني المصري و المادة ٤٥٣ من القانون المدني التونسي رقم ٥٧ لسنة ٢٠٠٠ و كذلك الفصل الرابع من القانون التونسي رقم ٨٣ لسنة ٢٠٠٠ بشأن المعاملات الإلكترونية و أيضاً نص المادة ٩٢ من قانون البنوك الأردني رقم ٢٨ لسنة ٢٠٠٠.

التقنية العالية ، كما أن هذا النوع من الكتابة له نتائج غير مؤكد و أن معظمها يمس مساساً مباشراً بحقوق و حريات الأفراد الأساسية التي أقرها القانون في مراحل الدعوى الجنائية ، لكن هذا التردد وما قد يثار من صعوبات ينبغي أن لا يقف حاجزاً يمنع الاستفادة الأجهزة الضبطية والقضائية من التقنية الإلكترونية التي يقوم الجناة بتوظيفها في ارتكاب جرائمهم ، والتعامل معهم باستخدام التقنية ذاتها في ملاحقتهم ، بمعنى أن تقبل مستخرجات الحاسب الآلي كدليل من ضمن الأدلة الخاصة<sup>(٥١)</sup> إذا ما توافرت فيها شروط وضوابط معينة.

### الدليل العلمي في مسألة الإثبات الجنائي :

ويقصد به النتيجة التي تسفر عنها التجارب العلمية والمعملية لتعزيز دليل سبق تقديمه سواء لإثبات أو لنفي الواقعة التي يثار الشك بشأنها<sup>(٥٢)</sup> وغني عن البيان أن ما يقدمه المعمل الجنائي من خدمات ، وما يقوم به من دور فعال في مجال الإثبات الجنائي في هذا العصر وفي غالبية دول العالم لاسيما في المسائل التي تكتسي طبيعة فنية بحتة تتطلب معرفة ودراية خاصة لا يملكها القاضي بحكم تكوينه القانوني المحض ويجرى التقرير بمعرفة مختص فنيا وهو بهذه المثابة لا يعدو أن يكون رأياً فنيا طلبه يكون بناء على أمر القاضي أو طلب أحد الخصوم في الدعوى. والخبير في سبيل أداء مهمته مقيدا في اللجوء إلى الأساليب والوسائل المشروعة التي يمكن من خلالها الحصول على الدليل العلمي دون إخلال بما يحفظ للإنسان حقوقه الأساسية ويكفل له عدم إهدار كرامته .

وإذا كان للقاضي في الدليل سلطة تقديرية واسعة في اللجوء إلى الخبرة وتقدير قيمتها الإثباتية انطلاقاً من مبدأ حرية الإثبات في المواد الجنائية والذي تولد عنه مبدأ القاضي خبير الخبراء، فإن ذلك مقتصر على ما يمكن للقاضي أن يثبت فيه لوحده، أما المسائل ذات الصبغة الفنية البحتة ، فلا يجوز للقاضي أن يحل نفسه فيها محل الخبير ، بل عليه الرجوع بشأنها إلى الخبراء المتخصصين ، ولا يمكنه طرح رأيهم إلا لأسباب سائغة و مقبولة ، وهناك من يرى أن الدليل العلمي أصبح يقيد حرية القاضي في تقدير الدليل ويجبره على الحكم بمقتضاه ولو لم يكن مقتنعا بصحة الواقعة المطروحة أمامه، أي لم يعد القاضي حراً في وزن الدليل العلمي الذي بات يأخذ دور الصدارة في الإثبات الجنائي خاصة بعد ظهور الأدلة الرقمية وإنشاء المعامل الجنائية الرقمية لفحص الأدلة وتقييم عمليات الإثبات الجنائي، وثمة رأى آخر يرى أن الوسائل العلمية في أغلب حالاتها ليست دليلاً مستقلاً في ذاته ، إنما هي قرائن يتم دراستها واستخلاص دلالاتها ، وهي غير مستقلة عن القرائن ، ومؤدى ذلك أنها لا تصلح في ذاتها كدليل وحيد في الإثبات الجنائي .

<sup>٥١</sup> - نصت المادة ١١٣١٦ من القانون المدني الفرنسي " تقبل الكتابة في شكل إلكتروني كدليل في الإثبات مثلها في ذلك مثل الكتابة على دعامة ورقية ، ما دام أن الشخص المنسوب إليه هذه الكتابة قد تم تحديده على وجه صحيح ، و قد تم إثبات هذه الكتابة و الاحتفاظ بها في ظروف من شأنها أن تضمن سلامتها " ؛ وقد ساوى المشرعان الفرنسي و الكندي بين الدعائم الإلكترونية و الدعائم الورقية من حيث القبول و الحجية في الإثبات بشرط أن تكون تلك الدعائم مفهومة و مقروءة و خالية من العيوب.

<sup>٥٢</sup> - د حجازي ، مرجع سابق ، ص ٥٠ حجازي .

ونعتقد انه إذ كان يتعين على القاضي الاستعانة بأهل الخبرة في المسائل الفنية البحتة، وأن يعتمد على رأيهم فيما يتعلق بهذه المسائل، إلا أنه من غير المقبول أن يتخلى القاضي عن حقه إذا رأى لأي سبب من الأسباب أن لا يأخذ بتقرير الخبير.

والمتتبع لأحكام القضاء الجنائي يلمس توسعا في الاعتماد على الخبرة و رأي الخبراء، فقد قضت المحكمة العليا الكويتية في الطعن الجنائي رقم ١٨ / ٦٦ ق " ليس لمحكمة الاستئناف أن تخوض في صميم المسائل الفنية التي أبدي فيها الخبير رأيه الفني ، لأن استعانة القاضي بأهل الخبرة في المسائل الفنية التي يتعذر عليه إدراكها يتطلب منه أن يضع في الاعتبار رأي الخبراء فيما يتعلق بالمسائل الفنية و ألا يطرح رأيهم إلا لأسباب سائغة مقبولة".

### المطلب الثاني- وسائل جمع الأدلة

#### المعاينة :

وهي إجراء يتم بمقتضاه الانتقال إلى مكان وقوع الجريمة لجمع الأشياء المتعلقة بالجريمة ومعاينة آثار وقوعها . والمعاينة قد تتم من قبل النيابة العامة أو من قاضي التحقيق أو المحكمة ، وقد أوجب القانون على النيابة العامة الانتقال الفوري إلى محل الواقعة بمجرد إخطارها بارتكاب جنائية متلبس بها، لإثبات حالة الأمانة ووصفها وصفا دقيقا وبيان مدى إمكان وقوع الجريمة فيها ، وكذلك بيان حالة الأشياء والأشخاص وكل ما يلزم إثبات حالته. ولا يترتب على مخالفة واجب الانتقال الفوري للمعاينة أي بطلان في الإجراءات فتقدير قيمة الدليل المستمد منها متروك لقاضي الموضوع<sup>(٥٣)</sup>، أما فيما يتعلق بالجنائيات غير المتلبس بها والجنح عموما ، فالانتقال للمعاينة متروك لتقدير النيابة العامة وفقا لظروف التحقيق وما تراه ضروريا لجمع الأدلة .

وللمحكمة القيام بإجراء معاينة المكان الذي وقعت فيه الجريمة، إذا ما رأت بأن معاينة سلطة التحقيق أو سلطة الاستدلال غير كافية لاستخلاص دليل سائغ لإثبات الجريمة .

وفى كل الأحوال فالأدلة الناتجة من معاينة مكان الجريمة تخضع - كسائر الأدلة الأخرى التي تطرح في الجلسة - لتقدير قاضي الموضوع طبقا لمبدأ حرية الإثبات، فإن أطمأن أستند إليها في حكمه ، وإذا لم يطمئن يقوم بطرحها جانبا دون معقب أو رقابة عليه من المحكمة العليا.

#### التفتيش :

التفتيش هو البحث عن أشياء تفيد الكشف عن جريمة وقعت ونسبتها إلى المتهم ، كما عرف بأنه " البحث في مستودع سر شخص عن أشياء تفيد الكشف عن الجريمة ونسبتها إلى المتهم " <sup>(٥٤)</sup>.

<sup>٥٣</sup> - د. مأمون محمد سلام ، الجزء الأول ، مرجع سابق ، ص ٤٠٦ .

<sup>٥٤</sup> - د. مأمون محمد سلامة ، الإجراءات الجنائية في التشريع الكويتي ، الجزء الأول ، منشورات الجامعة الكويتية كلية الحقوق ، الطبعة الأولى ، ١٩٧١ ، ص ٤٨١ .

والتفتيش وفقا للقواعد قانون الإجراءات الجنائية التقليدية ينقسم من حيث محله قسمين : الأول تفتيش ينصب على المنازل، وتفتيش يقع على الأشخاص ، وتفتيش المنازل هو إجراء من إجراءات التحقيق بمقتضاه يقوم المحقق أو من يأذن له من رجال الضبطية القضائية بالبحث في منزل شخص معين على أشياء تتعلق بجناية أو جنحة قامت قرائن قوية على حيازته لها ، والثاني هو إجراء من إجراءات التحقيق أيضا يقصد به ضبط ما يحوزه الشخص من أشياء تفيد كشف الحقيقة .

وتفتيش المنازل بمعرفة سلطة التحقيق يختلف من حيث شروطه عن التفتيش الذي يجريه مأمور الضبط القضائي استثناء في أحوال معينة ، وهي تفتيش منازل المراقبين وتفتيش منزل المتهم في أحوال التلبس، ونظرا للصفة الاستثنائية فقد استلزم فيه المشرع شروطا تختلف عن الشروط المطلوبة لصحة التفتيش الذي تجريه سلطة التحقيق . وفي الأحوال التي يجوز فيها القبض على المتهم لمأمور الضبط القضائي أن يفتشه، ومفاد ذلك أن صحة التفتيش تتوقف على توافر حالة من حالات القبض وليس على القبض الفعلي .

وأجاز المشرع تفتيش شخص غير المتهم وذلك إذا كان قاضي التحقيق هو الذي يباشر التحقيق، والمقصود بذلك حالات تفتيش غير المتهم استقلالا، وإذا كانت النيابة العامة هي التي تباشر التحقيق فلا يجوز لها تفتيش شخص غير المتهم إلا بعد استئذان القاضي الجزئي ، وفي كلا الحالتين لا يجوز التفتيش إلا بشرط قيام إمارات قوية على أن الشخص المراد تفتيشه يخفي أشياء تفيد في كشف الحقيقة.

وبخصوصية هذا البحث ، فإن التفتيش ينصب على جهاز الحاسب الآلي الذي يعمل طبقا لتعليمات محددة سلفا يستقبل البيانات ويخزنها ويقوم بمعالجة واستخراج النتائج المطلوبة، وهو متصل بالشبكة للحصول على المعلومات وتبادلها عبر الشبكات والبريد الإلكتروني ، ولهذا فإن التفتيش في الجرائم الإلكترونية له طبيعة خاصة ومتميزة عن التفتيش التقليدي للأشخاص والمنازل ، إلا أنه يخضع في إجراءاته للضوابط التي حددها قانون الإجراءات الجنائية وما يستلزمه من وقوع الجريمة واتهام شخص أو أشخاص معينين بارتكاب جريمة، وأن تكون هناك دلائل أو قرائن على ما يفيد في كشف الحقيقة في أجهزة الحاسب الآلي والإنترنت خاصة بالمتهم أو غيره من الأشخاص ، وإذا ما توافرت تلك الشروط ، فإنه يجوز لسلطة التحقيق تفتيش جهاز الحاسب الآلي وملحقاته المكونة له المادية والمعنوية ، وذلك من أجل ضبط أدلة الجريمة، وما يحتمل أن يكون قد استعمل في ارتكابها أو نتج عنها أو وقعت عليه ، وكل ما من شأنه أن يكشف عن الجريمة .

وقد ثار جدلٌ فقهيٌّ بين فقهاء القانون الجنائي ، حول مدى إمكانية تفتيش وضبط البيانات المخزنة أو المعالجة إلكترونياً بصورها وأشكالها المختلفة كالأقراص والأشرطة الممغنطة بما في ذلك ذاكرة جهاز الحاسب الآلي وانقسموا في ذلك لاتجاهين :

**الاتجاه الأول :** ذهب أنصاره إلى القول بعدم صلاحية إجراء التفتيش والضبط على برامج وبيانات الحاسب الآلي باعتباره وسيلة للإثبات المادي ، يهدف لضبط أدلة مادية تتعلق بالجريمة وتفيد في كشف الحقيقة ، وهذا يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي ، ويمثل هذا الرأي جانب من الفقه الفرنسي الذي يرى أن النبضات أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المادية المحسوسة التي يمكن تفتيشها وضبطها<sup>(٥٥)</sup>.

**الاتجاه الثاني :** يرى أنصاره أن المعلومات التي لا تعد شيئاً مادياً وإنما ذات طبيعة معنوية ، الأصل مجرد ذبذبات ونبضات إلكترونية أو إشارات أو موجات كهرومغناطيسية ، إلا أنها قابلة لأن تُخزَّن في أوعية ووسائط مادية كالأقراص والأشرطة الممغنطة، وبالتالي فهي ليست شيئاً معنوياً كالحقوق والآراء والأفكار، بل هي أشياء مادية محسوسة لها وجود ملموس في العالم الخارجي ، ومن ثم يصح أن يرد عليها التفتيش والضبط<sup>(٥٦)</sup> .

ونعتقد أن التركيز في التفتيش على المكونات المعنوية باعتبارها محتوى لمعلومات وبيانات وحوار وكلمات سر يمكن تصفحها وتحليلها لاستظهار الدليل المعلوماتي ، ولا ينال من صحة التفتيش وجود الحاسب الآلي المراد تفتيشه في منزل غير المتهم أو اتصاله بشبكة معلومات محلية طالما توافرت شروطه ، غير أنه إذا كان متصلاً بشبكات معلومات دولية، كأن يقوم مرتكب الجريمة المعلوماتية بتخزين المعلومات والبيانات المتعلقة بجرائمهم في أنظمة تقنية خارج إقليم الدولة المتواجدين على إقليمها، فلا يجوز في هذه الحالة لسلطات التحقيق في الدولة التي ارتكبت الجريمة على إقليمها، أو أضرت بأحد رعاياها أو بمصالحها الأساسية أن تباشر التفتيش أو غيره من إجراءات التحقيق خارج حدودها الإقليمية، وفي هذا الشأن قضت إحدى المحاكم الألمانية في جريمة غش ارتكبت في ألمانيا بأن الحصول على البيانات الخاصة بهذه الجريمة والمخزنة بشبكات اتصال موجودة في سويسرا لا يتحقق إلا بطلب المساعدة من الحكومة السويسرية، وفي واقعة نشر فيروس (Love bug) عام ٢٠٠٠ الذي تسبب في إتلاف المعلومات في أجهزة الحاسب الآلي، فعندما اكتشف الخبراء الأمريكيون بان هذا الفيروس أرسل من الفلبين فإن تفتيش منزل المشتبه فيه تقتضي تعاون السلطات الفلبينية والحصول على إذن من قاضي التحقيق بالفلبين.

ويفترض أن لا يكون الأمر بالتفتيش أمراً عاماً، وإنما يكون الهدف منه محددًا تحديداً دقيقاً وأن يتم وصف الأشياء المطلوب ضبطها بصورة تفصيلية، بحيث لا يترك ذلك للسلطة التقديرية لرجل الشرطة الذي سيقوم بتنفيذ الأمر، وأن لا يكون الأمر بالتفتيش كأمر عام بالتفتيش لضبط الأشياء المتعلقة بالحياة الخاصة أو بالتعبير عن الرأي، ومنها أجهزة الحاسب الآلي - التي تحتوي بيانات شخصية أو بيانات لا تتعلق بالجريمة - فهذه الأجهزة يجب أن تكون موصوفة في أمر التفتيش بصورة دقيقة فلا يصدر أمر بالتفتيش مثلاً لمجرد ظنون أو معتقدات توافرت لدى أحد رجال الشرطة

<sup>٥٥</sup> - د. عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص ٣٨٠ .

<sup>٥٦</sup> - د. هشام محمد فريد رستم ، الجوانب الإجرامية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ١٩٩٤، ص ٦٦-٦٧ .

بوجود صور فاضحة على الأسطوانة الصلبة لأحد أجهزة الحاسب الآلي، وهذا ما أقتضى أن يكون عضو جهة التحقيق ملماً ببعض الجوانب الفنية بالحاسب الآلي واستخداماته حتى لا تكون القرارات القضائية وسيلة لاصطناع الأدلة أو التسلط والاستبداد في يد البعض، حيث إنه لا توجد وسيلة للتأكد من أن البيانات الموجودة على الأجهزة هي تلك التي تم ضبطها، إذ يمكن عن طريق الوسائل العلمية والتقنية الحديثة العبث بالبيانات الموجودة على الحاسب الآلي ومحوها .

ففي الولايات المتحدة الأمريكية أصدر القضاء حكماً بتعويض شركة ستيف جاكسون التي تقوم بأعمال النشر ، وكانت تصدر جريدة إلكترونية وتخضع للحماية المقررة بموجب قانون حماية الخصوصية وقانون حماية الاتصالات الإلكترونية ، اللذان لا يجيزان القبض والتفتيش في حق الناشرين ما لم يتوافر سبب آخر يبرح ارتكاب الشخص للجريمة ، وتتخلص الواقعة في أنه خلال شهر مارس عام ١٩٩٠ قام البوليس السري الأمريكي بتفتيش الشركة وضبط أجهزة الحاسب الآلي وملحقاتها ومجموعة من البرامج وطابعات ليزر وكمية من الأسطوانات وملفات خاصة بجريدة إلكترونية ، وكذلك آلة حاسبة شخصية، ووضعت الأختام على المضبوطات فترتب على هذا الإجراء تعرض الشركة لأزمة مالية كبيرة في الوقت الذي لم توجه أية تهمة لصاحب الشركة أو لأي من العاملين معه ، بل في النهاية تبين أن التفتيش لم يكن متعلقاً به أو بعمله، وأن أحد العاملين بالشركة - والذي لم توجه له تهمة - كان الهدف من الإجراء ، وكانت المعلومات المطلوب ضبطها موجودة بمنزله .

**ضبط الأشياء :** يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الجريمة<sup>(٥٧)</sup>، وسائله

متعددة منها التفتيش والمعاينة وتكليف الحائز للشيء بتقديمه للمحقق .

وإذا ما سفر التفتيش الذي يجريه مأمور الضبط عن آثار أو أشياء تفيد في كشف الجريمة أو تكون قد استعملت في ارتكابها، وجب على مأمور الضبط القضائي ضبط هذه الأشياء ، ومن باب أولى لسلطة التحقيق أن تضبط جميع الأشياء المتعلقة بالجريمة، ومن أجل ذلك، أجاز المشرع التفتيش لتمكين سلطة التحقيق من إجراء الضبط الذي يعد في هذه الحالة إجراء من إجراءات التحقيق .

ويمكن أن يكون موضوعاً للضبط من قبل سلطة التحقيق جميع الأشياء التي تفيد في كشف الحقيقة المتعلقة بالجريمة ، ويجب أن تكون هذه الأشياء مادية ، فسلطة التحقيق لها ضبط الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات لدى مكاتب البريد كافة والتلغراف ، كما يجوز لها أيضاً مراقبة المحادثات التليفونية متى كان لذلك فائدة في ظهور الحقيقة ، وإذا كان القائم بالتحقيق أحد أعضاء النيابة العامة، فيلزم للقيام بهذا الإجراء استصدار إذن من القاضي

<sup>٥٧</sup> - وقد نصت عليه المادة ٢/٧٥ من قانون الإجراءات الجنائية الكويتي "...للمحقق أن يفتش أي مكان ويضبط فيه الأوراق والأسلحة والآلات وكل ما يتحمل انه استعمل في ارتكاب الجريمة أو نتج عنها أو وقعت عليه وكل ما يفيد في كشف الجريمة" .



الجزئي، وقياسا على ذلك يجوز لسلطة التحقيق أن تضبط أيضا لدى البنوك والمؤسسات المختلفة الأوراق والأشياء المتعلقة بالجريمة أو التي تفيد في كشف الحقيقة ، وحظر المشرع على سلطة التحقيق أن تضبط لدى المدافع عن المتهم أو الخبير الاستشاري الأوراق والمستندات التي سلمه المتهم لهما لأداء المهمة التي عهدت إليهما بها ، وكذلك المراسلات المتبادلة بينهما في القضية .

#### أولاً- ضبط المكونات المادية للحاسب الآلي :

الأصل في الضبط أنه يرد على الأشياء المادية التي تصلح لوضع اليد عليها، ولهذا لا يثير ضبط المكونات المادية للحاسب الآلي وملحقاته أية إشكالية باعتبارها أشياء مادية ، وبالتالي يجوز ضبط الأسلاك ومفاتيح التشغيل وحدة الإدخال والمودم ووحدة الذاكرة ووحدة التحكم ، وبما في ذلك مخرجات الحاسوب الموجودة في صورة مخرجات ورقية أو وسائط وأوعية التخزين المادية كالأقراص والأشرطة المغناطيسية ، حيث يتم ضبط الأداة أو الوسيط الذي يتم فيه التخزين .

#### ثانياً- ضبط المكونات المعنوية للحاسب الآلي :

يستخلص من صياغة التشريعات الجنائية لمفهوم الضبط أنه يقتصر على الأشياء المادية، وكان ذلك مثار الجدل حول ما إذا كان يجوز ضبط المكونات المعنوية للحاسب الآلي من معلومات وبرامج، وما تحتويه صناديق البريد الإلكترونية من رسائل وصور وبيانات ؟

الجدل لا يزال محتدماً إلى يومنا هذا بين المؤيد والرافض لإمكانية ضبط البيانات المعالجة إلكترونياً منفصلة عن دعائمها المادية، كذلك التي يتم عرضها على شاشة الحاسب الآلي، فذهب اتجاه إلى أنه من غير الممكن ضبط البيانات إلكترونياً لانقفاء الطابع المادي لهذه البيانات، ذلك أن بيانات الحاسب الآلي ليست كمثل الأشياء المحسوسة، وبالتالي لا تصلح لأن يرد عليها الضبط، وأخذت بعض تشريعات الدول بهذا الاتجاه منه كألمانيا ورومانيا واليابان وجانب من الفقه الفرنسي؛ وذهب اتجاه ثان إلى أنه وإن كانت الغاية من التفيتش هو ضبط الأدلة المادية، إلا أن هذا المفهوم يمكن أن يمتد ليشمل البيانات المعالجة إلكترونياً مجردة. ويجد هذا الاتجاه تجسيده التشريعي في قوانين بعض الدول مثل كندا واليونان والولايات المتحدة الأمريكية التي قضت بإعطاء سلطات التحقيق مكنة القيام بأي شيء يكون ضروريا لجمع الأدلة وحمايتها، بما في ذلك المكونات المعنوية للحاسب الآلي، وإن كان لا يتصور ضبطها باعتبارها أشياء غير محسوسة، فإنه من الممكن ضبطها إذا أصبح لها كيان مادي، كضبط القطعة الصلبة كأداة تخزينية للدليل والمعلومات والبيانات المراد ضبطها على ورق أو تسجيلها في أشرطة أو أقراص أو نسخها في ملفات، إذ في هذه الحالة تتحول المكونات المعنوية للحاسب الآلي إلى أشياء مادية ومقروءة وتكتسب كياناً مادياً يمكن بواسطته

ضبطها ونقلها من مكان لآخر، والقول نفسه يطبق بشأن الرسائل الالكترونية، فللمحقق أن يضبط الرسائل المخزنة بالبريد الالكتروني عن طريق طباعة الرسالة التي يريد ضبطها ، أو تسجيلها في ملف أو قرص . وهناك اتجاه ثالث وأخير يرى أنصاره ، بأنه لا فائدة من تطبيق نصوص الإجراءات الحالية المتعلقة بالضبط على البيانات المعالجة إلكترونيا بصورتها المجردة عن دعائها المادية ، بل لابد من تدخل المشرع لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط ، ليشمل البيانات المعالجة بصورتها غير الملموسة<sup>(٥٨)</sup>.

### الأمر بتقديم الأشياء المراد ضبطها أو الاطلاع عليها :

لسلطة التحقيق أن تأمر الحائز لشيء تري ضبطه أو الاطلاع عليه بتقديمه ، والفرض هنا أن الحائز قد يكون موظف مكتب البريد أو التلغراف ، كما قد يكون شخصاً آخر، ويستوي أن يكون فرداً عادياً أو موظفاً حكومياً يحوز شيئاً متعلقاً بالجريمة أو يفيد في كشفها بمناسبة أو بسبب وظيفته، والمفروض أن الشيء موضوع الحيازة لا يكون جريمة في حد ذاته وإلا جاز تفتيشه ، وقد خول القانون لسلطة التحقيق هذا الحق بدلاً من أن تلجأ إلى إجراء تفتيش منزل غير المتهم بعد الحصول على إذن القاضي الجزئي إذا كان التحقيق تباشره النيابة العامة .

كما راعى المشرع أيضاً أنه قد لا يمكن ضبط هذه الأشياء بسبب إخفاء الحائز للأوراق أو الأشياء في مكان ما لم يتم التوصل إلى اكتشافه، فجعل المشرع من الامتناع عن تقديم الأشياء التي في حيازة الشخص الذي يؤمر بتقديمها من قبل سلطة التحقيق جريمة معاقبا عليها في قانون العقوبات، اللهم إذا توافر بالنسبة للحائز حالة من الحالات التي يخوله القانون فيها الامتناع عن أداء الشهادة .

### ندب الخبراء :

أجاز المشرع لجهات التحقيق ندب الخبراء إذا كانت طبيعة الجريمة محل التحقيق تقتضي الاستعانة بذوي الخبرة لحسم مسألة فنية معينة أو للبحث عن أدلة الجريمة وضبطها، وللمحكمة أن تتخذ ما تراه من وسائل - بما في ذلك ندب الخبراء - لبحث وفهم أية واقعة فنية اعترضتها .

والقاعدة أن المحكمة هي الخبير الأعلى، ولذلك فتقارير الخبراء تخضع دائماً لتقديرها، فلها أن تطرحها كلية ولها أن تأخذ برأي خبير دون الآخر، كما أن للمحكمة سلطة الجزم في المسائل التي تتسق ووقائع الدعوى حتى ولو كان تقرير الخبير لم يجزم فيها برأي، وإذا اختلف خبيران في الرأي فليست المحكمة ملزمة بمواجهتهما وإنما تملك ترجيح أحدهما علي الآخر وفقاً لاقتناعها وما تراه مؤيداً بوقائع الدعوى، وهي في ذلك غير ملزمة ببيان أسباب الترجيح كما أنها غير ملزمة بمناقشة التقارير الأخرى طالما لم تر محلاً ولم يطلب الخصوم منها شيئاً من ذلك ، وللمحكمة السلطة

<sup>٥٨</sup> - د. هشام محمد فريد ، مرجع سابق ، ص ٩٦. وانظر في ذلك المادة ١٩ من اتفاقية بودابست .

التقديرية أيضا أن تأخذ ببعض ما ورد بتقرير الخبير وتطرح الجزء الآخر دون إبداء أسباب لذلك اللهم إلا في المسائل الفنية فلا يجوز تنفيذها إلا بأسانيد فنية.

وإذا كان لندب الخبراء أهمية في الجرائم التقليدية، فإن أهميتها أكثر وضرورتها أشد في إجراءات جمع أدلة المكونات المعنوية في كل وحدات التخزين وتحليلها وكشف أي تلاعب في البرامج والمعلومات، غير أن ذلك لا يعني عدم الاكتراث بمسألة تأهيل سلطات الملاحقة وتزويد أفرادها بالمعرفة العلمية والتقنية ليكونوا على دراية فيما يستلزم ندب الخبراء وفهم ما يقدمونه من آراء، ولذلك نجد الكثير من الدول المتقدمة قد اهتمت بتدريب المحققين في الجرائم الإلكترونية، كما دعا المجلس الأوروبي في إحدى توصياته سنة ١٩٩٩ إلى ضرورة تدريب الشرطة وأجهزة العدالة بما يواكب التطور المتلاحق لتقنية المعلومات واستخدامها لتحقيق التوازن بين وسائل ارتكاب الجريمة وبين سبل مواجهتها، وعقدت كذلك المنظمة الدولية للشرطة الدولية العديد من الدورات التدريبية لمحقيقي جرائم الحاسب الآلي .

#### الإجراءات الحديثة لجمع الأدلة في اتفاقية بودابست :

استشعارا بصعوبة الحصول على أدلة الجرائم الإلكترونية وضبطها بالوسائل التقليدية تضمنت اتفاقية بودابست بشأن جرائم الحاسب الآلي والإنترنت مجموعتين من الإجراءات الجديدة إحداهما تتعلق بالإجراءات الممهدة لجمع الأدلة ، والثانية الإجراءات الخاصة بجمع الأدلة .

**الإجراءات الممهدة لجمع الأدلة:** وهي نوع من المراقبة والمتابعة لاستخدام تقنية الاتصالات (الحاسب الآلي والإنترنت) ، ويتولى القيام بهذه الإجراءات مقدمو خدمات الحاسب الآلي والإنترنت بتكليف من السلطة المختصة ، ومباشرة هذه الإجراءات لا يعد تحريكا للدعوى .

وتنقسم الإجراءات الممهدة إلى نوعين : النوع الأول إجراءات التحفظ السريع على مضمون البيانات المخزنة<sup>(٥٩)</sup>، وهذا النوع يتمثل في أمرين : الأمر الأول هو إصدار أوامر إلى مقدمي الخدمات من أفراد وشركات بالحفاظ على البيانات المخزنة بمنظومة الحاسب الآلي والإنترنت لفترة زمنية معينة<sup>(٦٠)</sup>؛ والأمر الثاني هو تمكين السلطة المختصة بالتحقيق لمعرفة مضمون البيانات التي أرسلها أو استقبلها المشترك، سواء عن طريق مقدمي الخدمة أو من خلال ما أسفر عنه التفتيش؛ أما النوع الثاني من الإجراءات الممهدة لجمع الأدلة فهو إجراءات التحفظ السريع على البيانات المتعلقة بخط سير البيانات<sup>(٦١)</sup>، وقصد بها إلزام مقدمي الخدمات أفرادا أو شركات بالحفاظ على البيانات والمعلومات

<sup>٥٩</sup> - المادة ١٦ من اتفاقية بودابست .

<sup>٦٠</sup> - حددت اتفاقية بودابست هذه المدة بما لا يتجاوز ٩٠ يوما .

<sup>٦١</sup> - المادة ١٧ من اتفاقية بودابست .

المخزنة ووقت إرسالها ووقت استقبالها، ومن قام بنقلها، وذلك يساعد على التعرف على مرتكب الجريمة الإلكترونية والمساهمين معه في ارتكابها، وقد استجاب بعض المشرعين لما قرره اتفاقية بودابست في مادتها ١٧/١ و٢٠ .

### إجراءات جمع الأدلة ومن أهمها :

**أولاً - إصدار أمر بتقديم بيانات محددة<sup>(٦٢)</sup> :** ويقصد به أن تصدر السلطة المخولة أمراً إلى مقدم الخدمة أو أي شخص في حيازته أو تحت سيطرته بيانات معينة أن يقوم بتقديمها، سواء أكانت هذه البيانات تتعلق بالمحتوى أم بخط السير .

**ثانياً - تفتيش وضبط البيانات المخزنة<sup>(٦٣)</sup> :** ويقصد به البحث عن طريق التفتيش والضبط عن البيانات المخزنة في النظام المعلوماتي للحاسب الآلي أو في دعامة تخزين المعلومات ، سواء كانت هذه البيانات مخزنة في جهاز واحد أو في منظومة اتصالات .

وقد حصرت المادة ١٩ من اتفاقية بودابست الإجراءات الخاصة بجمع الأدلة في : التفتيش أو الدخول المشابه<sup>(٦٤)</sup>، الضبط أو الحصول ويشمل الضبط أو الحصول إلى البيانات ، وأيضاً التحقق والتحقق على نسخة من البيانات، وكذلك المحافظة على سلامة البيانات، وأخيراً منع الوصول إلى هذه البيانات أو رفعها من النظام المعلوماتي .

ويمكن تقسيم هذه الإجراءات إلى نوعين من الإجراءات :

**أ- إجراءات تحفظية :** تهدف إلى الحفاظ على البيانات المخزنة التي ترى الجهة المختصة أهميتها في التحقيق ببقائها في أمكنتها في النظام المعلوماتي للحاسب الآلي أو في دعامة التخزين ومنع الوصول إليها أو إلغائها أو التصرف فيها .

**ب- إجراءات ضبط :** وهي إجراءات لاحقة للتفتيش والدخول ، ويقصد بها جمع البيانات سواء بأخذ دعامة تخزين المعلومات ذاتها أو بعمل نسخة من البيانات المخزنة بها أو بالنظام المعلوماتي للحاسب الآلي في ورق أو أقراص .

**ثالثاً - التجميع في الوقت الفعلي لبيانات خط سير البيانات<sup>(٦٥)</sup> :**

<sup>٦٢</sup> - المادة ١٨ من اتفاقية بودابست .

<sup>٦٣</sup> - المادة ١٩ من اتفاقية بودابست .

<sup>٦٤</sup> - الدخول مصطلح خاص بنظم التكنولوجيا و الاتصال يحقق الوصول إلى البيانات المخزنة ويقضيه بطبيعة الحال إجراء التفتيش والحصول على الأدلة .ولهذا ثمة فرق بين الدخول والتفتيش ، فالدخول إجراء للتفتيش ، أما التفتيش فهو وسيلة لجمع الأدلة . ورغم هذه التفرقة فإنهما يعتبران من الإجراءات الماسة بحقوق الأفراد ، لذا يجب أن يستند اتخاذها إلى نص قانوني .

<sup>٦٥</sup> - المادة ٢٠ من اتفاقية بودابست .

ويقصد به تجميع أو تسجيل - عن طريق وسائل معينة موجودة على أرض الدولة - البيانات المتعلقة بخط سير البيانات في الوقت الصحيح؛ وكذلك إلزام مقدم الخدمة في حدود قدرته الفنية بجمع وتسجيل البيانات المتعلقة بخط سير البيانات في الوقت الصحيح .

ويهدف هذا الإجراء الخاص بالتجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات الذي قد تقوم به السلطة المختصة في الدولة أو ينفذه مقدمو الخدمة بناء على أوامر صادرة من السلطة المختصة بهذا الإجراء إلى تسهيل مهمة الجهات القائمة بجمع الأدلة .

ويختلف إجراء التجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات الذي نصت عليه المادة (١٦) من اتفاقية بودابست في أن البيانات في حالة التحفظ موجودة لدى مقدم الخدمة أي مخزنة بالنظام المعلوماتي للحاسب الآلي أو في دعامة التخزين ، بينما في حالة التجميع أو التسجيل فالبيانات ليست مخزنة .  
وتهدف هذه الإجراءات إلى تجميعها أو تسجيلها وقت مباشرة الاتصال .

#### رابعا - اعتراض مضمون البيانات :

والمقصود باعتراض مضمون البيانات هو جمع أو تسجيل مضمون البيانات التي تنقل عبر وسائل الاتصالات في حينها حتى تتمكن السلطات المختصة في الدولة من التعرف على الاستخدامات غير المشروعة لأنظمة الاتصالات بما يكفل منع ارتكاب العديد من الجرائم.

والأصل أن إجراء اعتراض مضمون البيانات تباشره سلطة معينة بالدولة، إلا أن اتفاقية بودابست أجازت إلزام مقدم الخدمة للقيام به على أساس أنه قد تتوفر لديه الإمكانيات الفنية اللازمة لذلك، و يلاحظ بأن هذا الإجراء يختلف عن إجراء التحفظ السريع علي مضمون البيانات الذي نصت عليه المادة ١٦ من الاتفاقية في أن البيانات المطلوب التعرف علي مضمونها مخزنة و يلتزم مقدم الخدمة بالتحفظ عليها ، بينما يعد الاعتراض علي مضمون البيانات نوعا من المراقبة المعاصرة للاتصال، وتجميع و تسجيل مضمون أية اتصالات تتعلق بمسائل غير مشروعة.

#### صعوبات جمع الأدلة :

على الرغم من اتجاه العديد من التشريعات الجنائية إلى وضع قواعد موضوعية لمواجهة الجرائم الإلكترونية وإجراء تعديلات في القواعد الإجرائية بتطوير أساليب كشف وضبط هذه الجرائم بما يحقق متطلبات العدالة الجنائية، وحتى لا تكون القواعد الإجرائية عائقا أمام سلطات التحقيق في كشف وملاحقة مرتكبي الجرائم في مجال تقنية المعلومات والاتصالات، فإن التحقيق في الجرائم الإلكترونية يظل يواجه العديد من التحديات والصعوبات مثل :

**أولاً. صعوبات تتعلق بالحصول على الدليل:**

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

**١. إخفاء الدليل :**

نتيجة ضعف الأنظمة الرقابية يتمكن مرتكبو الجرائم الإلكترونية من التسلل والعبث في النبضات والذبذبات الإلكترونية التي تسجل عن طريقها المعلومات والبيانات بغرض إحداث تغييرات في البيانات والمعلومات والتلاعب في منظومة الحاسب الآلي ومحتوياته، أو دس برامج خاصة ضمن برنامجه فلا يشعر بها القائمون بالتشغيل، ومن ثم إخفاء ما قاموا به أو محو الدليل عليه، بحيث يتعذر إعادة عرض أعمال التسلل والدخول، وهكذا يستطيع الجناة في الجرائم الإلكترونية إخفاء جرائمهم وطمس آثارها في وقت قياسي من القصر وقبل أن تصل إليه سلطة التحقيق ، الأمر الذي يؤدي إلى صعوبات تعيق إجراءات التحقيق الرامية إلى الوصول إلى دليل، ومن أمثلة سهولة محو الدليل المعلوماتي في وقت قصير، انه أثناء إجراء المحاكمة للمسؤولين عن أحد المشروعات بألمانيا طلبت سلطات التحقيق المساعدة القضائية من السلطات السويسرية من أجل ضبط البيانات التي توجد في النظام المعلوماتي لإحدى الشركات السويسرية، وأثناء سير الإجراءات تمكن الجناة من محو البيانات التي كانت من الممكن أن تستخدم كدليل ، ولكن لحسن الحظ بعد ضبط الدعامات والأقراص الصلبة وأسطوانات الليزر، تمكن الخبراء بطرق فنية من استعادة البيانات التي كانت مسجلة عليها.

**٢- غياب الدليل ضد متهم معين:**

تختلف الجريمة الإلكترونية عن الجريمة التقليدية، بأن الجريمة الأولى لا تحتاج لارتكابها أي من أنواع العنف إلا فيما ندر، وإنما هي معالجة بواسطة إدخال بيانات معلومات خاطئة أو محظورة ضمن البرامج ، أو تحريف أو تعديل البيانات والمعلومات المخزنة أصلا في الحاسب الآلي، أو إرسال برامج تخريبية أو التجسس على البيانات والمعلومات المخزنة ونسخها ... الخ ، وإذا ما صادف واكتشفت هذه الأفعال وجمعت الأدلة على وقوعها، فإن هذه الأدلة قد لا تفصح عن صلة شخص معين بالجريمة المرتكبة ، نظرا لأن معظم نظم الحاسب الآلي لا تسمح للمراجعين والفنيين بالتتابع العكسي لمسار مخرجاتها ، علاوة على صعوبة تتبع الآثار الإلكترونية ومراجعة وفحص الكم الهائل من البيانات والمعلومات المدرجة بالأنظمة، وتعتمد الجناة على إخفاء هويتهم، وخير مثال على الصعوبات التي تشكلها ضخامة كم البيانات والمعلومات وتأثيرها السلبي على جمع الأدلة بشأن الجريمة المعلوماتية وملاحقة المجرمين الواقعة التي شاهدها

ألمانيا الاتحادية عام ١٩٧١ ف حيث اكتشفت شركة طلبات بريدية (Order –fimmail) سرقة أشرطة ممغنطة تحتوي على (٣٠٠,٠٠٠) عنوانا لعملائها واستصدرت من المحكمة أمرا يسمى وقف الأعمال ، وذلك باستعادة كل هذه العناوين من شركة منافسة كانت قد حصلت على هذه العناوين من الذين ارتكبوا السرقة ، وتنفيذا لذلك سمحت الشركة المنافسة لمساعد مأمور التنفيذ ، أن يدخل مقر الحاسب الآلي الخاص بها ، وذلك للحصول على تلك العناوين ، ووجد نفسه وسط كم هائل من الأشرطة والأقراص الممغنطة التي لا يدري عنها شيئا ، ولا يمكن فحص محتوياتها أو لديه القدرة على ذلك فغادر مقر الشركة دون أية معلومات ، إلا أن الشركة المنافسة قامت من تلقاء نفسها بعد أيام ، بتسليم بيانات العناوين إلى الشركة المعتدى عليها وإن كان ذلك لا يمنع من نسخ هذه الشرائط قبل تسليمها ، الأمر الذي يفرغ أمر المحكمة من مضمونه<sup>(٦٦)</sup> .

### ٣- إعاقة الوصول إلى الدليل :

يضع الجاني في بعض الحالات عقبات فنية لمنع كشف جريمته وضبط أدلتها باستخدام تقنيات التشفير<sup>(٦٧)</sup> أو كلمة السر، وذلك بقصد حجب المعلومة عن التداول العام ، ومنع الغير بما فيه أجهزة الرقابة من الوصول غير المشروع إلى البيانات والمعلومات المخزنة أو التلاعب فيها ، وقد أثبتت التحقيقات في بعض الجرائم الإلكترونية بألمانيا وجود صعوبات تواجه البعض من هذه التحقيقات نتيجة استخدام مرتكبي هذه الجرائم لتقنيات خاصة كالتشفير والترميز لإعاقة الوصول إلى الأدلة التي تدينهم ، ومن الأمثلة التي لجأ فيها الجاني إلى أسلوب التشفير، كوسيلة لمنع ضبطه والإيقاع به ، واقعة حدثت في الولايات المتحدة عام ١٩٩٦ ، إذ كان المشتبه به مشغلا للوحة إعلانات BBC ، وبعد الوصول إلى جهاز الحاسب الشخصي الذي يستخدمه في إدارة اللوحة الالكترونية ، حاول محققو الشرطة العثور على كلمة المرور الخاصة بالمشتبه به ، فقاموا بأخذ نسخة احتياطية من محتويات القرص الصلب، وقاموا بكتابة برنامج يحاول تشغيل النسخة الاحتياطية ، وبعد فحص ملف المستفيدين استطاع المحققون الوصول بسهولة إلى أسماء المستفيدين وأرقامهم ، ولكن لم يتمكنوا من العثور على كلمة المرور الخاصة بالمشتبه به، خاصة وأنها كانت مشفرة ، ولولا تشفير كلمة المرور لأمكن إضافة مستفيد جديد بكلمة مرور جديدة ، ثم تتبع هذه الكلمة داخل قاعدة بيانات المستفيدين حتى يتم معرفة مكانها ، ولكن التشفير حال دون ذلك .

وللوصول إلى كلمة المرور قام المحققون بإنشاء رقمين جديدين من أرقام المستفيدين ، لهم أسماء مختلفة ، ولكن لهم نفس كلمة المرور، وبهذه الطريقة ويتتبع كلمتي المرور المتشابهتين أمكن العثور على مكان وجود كلمات المرور على القرص الصلب، ووضع المحققون يدهم على كلمة المرور الخاصة بالمتهم في ملف المستفيدين، ثم قاموا بإحلال

٦٦ - د. هشام محمد فريد رستم ، مرجع سابق ، هامش رقم (١)، ص ١٩ .

٦٧ - التشفير يعني ، مناهج لخط البيانات من خلال لوغاريتمات أو خوارزميات بحيث لا يمكن لشخص ثالث قراءتها .

كلمة المرور السابق استخدامها مع المستفيدين الوهميين مكان كلمة المرور الخاصة بالمشغل (وهي مشفرة كما هي) ، وبذلك أمكن الدخول إلى الحاسب باستخدام اسم المشغل مع كلمة المرور الخاصة بالمستفيد الوهمي<sup>(٦٨)</sup> .

### ثانيا . صعوبات تتعلق بالجانب الفني :

من المسائل التي تعوق عمليات البحث والتحقيق في الجرائم الإلكترونية نقص في المعرفة التقنية الحديثة والمتجددة لدى القائمين بالبحث والتحقيق في هذه الجرائم ، مما يجعل منهم غير قادرين على أداء واجبهم على الوجه المطلوب، إذ إن نقص الخبرة والكفاءة، سواء في أجهزة الشرطة أو الادعاء يعد من الأسباب الرئيسية في الإخفاق في كشف الجرائم الإلكترونية وجمع أدلتها، ويظهر ذلك بشكل واضح في الدول التي لا تزال تتعامل مع هذه الجرائم بإجراءات البحث والتحقيق التقليدية وتفترق سلطاتها الضبطية والقضائية للأجهزة التقنية المتطورة في متابعة الجرائم الإلكترونية وضبط أدلتها، وبديهيًا أنه في حالة عدم توافر التأهيل والخبرة وشُحّ الإمكانيات التقنية على وجه الخصوص ، فلا يمكن أن نتصور أي وجه للتعامل مع هذه الجرائم ، وبالتالي ستكون النتائج سلبية لا محالة، ما لم تضع الدول برنامج تدريب وتأهيل لرجال الشرطة على أساليب الوقاية من جرائم الحاسب الآلي ووضع التدابير المانعة لوقوعها، والقيام بالتحري عما ارتكب منها وكشفها، وأيضًا كيفية التعامل مع الأدلة وضبطها، والاستعانة بذوي التخصصات الدقيقة المتعمقة في أنظمة الحاسب الآلي والإنترنت وشبكات الاتصال الأخرى.

وهناك صعوبات آخر تتعلق بالاختصاص (سريان القانون من حيث الزمان والمكان) ،نحيل إليها في المطلب

الثاني من المبحث الأول تفاديا للتكرار .

### الخاتمة والتوصيات :

اختيارنا للجريمة الإلكترونية والتغلب على تحدياتها كموضوع لهذه الورقة البحثية كان لأهميته و للتعرف على أبعاده وتنظيم قواعده بعد أن شغل هذا الموضوع بال مواطن ومؤسسات المجتمع والمهتمين بالدراسات القانونية ووقفت حياله أغلب التشريعات العربية عاجزة عن تجاوز تحدياته بسن تشريع خاص ومتطور لمواجهة هذا النوع من الجرائم والتصدي له أو كحد أدنى تعديل نصوص قائمة بما يتلاءم معه ويواكبه في تطوره وتجديده في إطار مبدأ شرعية الجرائم والعقوبات، بحيث لا تقل مراميه وأهدافه عن ما تضمنته توصيات هذه الورقة البحثية التي نلخصها في الآتي:

١- سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية ، على أن يكون شاملا للقواعد الموضوعية والإجرائية

، وعلى وجه الخصوص النص صراحة على تجريم الدخول غير المصرح به إلى الحاسب الآلي وشبكات الاتصال

<sup>٦٨</sup> - م.حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، ٢٠٠٠ ف، ص ٢٣٣\_٢٣٤ .



( الإنترنت ) والبريد الإلكتروني ، وكذلك اعتبار البرامج والمعلومات من الأموال المنقولة ذات القيمة ، أي تحديد الطبيعة القانونية للأنشطة الإجرامية التي تمارس على الحاسب الآلي والإنترنت، وأيضا الاعتراف بحجية للأدلة الرقمية وإعطائها حكم المحررات التي يقبل بها القانون كدليل إثبات .

٢- تكريس التطور الحاصل في نطاق تطبيق القانون الجنائي من حيث الزمان والمكان ، وتطوير نظام تقادم الجريمة الإلكترونية .

٣- اعتبار بعض صور المساهمة في دورها وآثارها من قبيل الجرائم المستقلة .

٤- الاعتراف في بعض الحالات بحجية للتشريعات والأحكام الجنائية غير الوطنية .

٥- منح سلطات الضبط والتحقيق الحق في إجراء تفتيش وضبط أي تقنية خاصة بالجريمة الإلكترونية تفيد في إثباتها، على أن تمتد هذه الإجراءات إلى أية نظم حاسب آلي آخر له صلة بمحل الجريمة .

٦- تفعيل التعاون الدولي ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية المتبادلة .

٧- نشر الوعي بين المواطنين وخاصة الشباب بمخاطر التعامل مع المواقع السيئة والمشبوهة على الشبكات .

٨- تفعيل دور المجتمع المدني والمؤسسات للقيام بدوره التوعوي والوقائي من الوقوع في براثن الرذيلة والممارسات الخاطئة .

٩- إعداد أنظمة ضببية وقضائية مؤهلة في التعامل مع الجرائم الإلكترونية.

**المراجع :**

- م.حسن طاهر داوود : **جرائم نظم المعلومات** ، أكاديمية نايف العربية للعلوم الأمنية ، الطبعة الأولى ، الرياض ، ٢٠٠٠ .
- د. جميل عبد الباقي الصغير : **الانترنت والقانون الجنائي** ، دار النهضة العربية ، القاهرة ، ٢٠٠١ .
- د. زكي أمين حسونة : **جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي** ، بحث مقدم إلي المؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، ٢٥-٢٨ أكتوبر ، ١٩٩٣ .
- د. سالم محمد الأوجلي : **التحقيق في جرائم الكمبيوتر والانترنت** ، منشور علي مواقع الانترنت ، <http://afaitouri.maktoobblog.com/1624946> .
- أ. طارق محمد الجملي ، **الدليل الرقمي في الإثبات الجنائي** ، منشور علي مواقع الإنترنت ، بدون ترقيم للصفحات .
- د. المستشار عبد الفتاح بيومي :
- **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت** ، بدون ناشر ، طبعه مزيدة ومنقحه ، ٢٠٠٩
  - **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت** ، مصر ، المحلة الكبرى ، دار الكتب القانونية ، ٢٠٠٧ .
- د. عمر سالم : **المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن** ، دار النهضة العربية ، الطبعة الأولى ، القاهرة ، ٢٠٠٠ .
- د. مأمون محمد سلامة : **الإجراءات الجنائية في التشريع الكويتي** ، الجزء الأول والثاني ، منشورات الجامعة الكويتية ، كلية الحقوق ، الطبعة الأولى ، ١٩٧١ .
- د. محمد الأمين البشري : **التحقيق في جرائم الحاسب الآلي** ، بحث مقدم إلي مؤتمر القانون والكمبيوتر و الانترنت المنعقد الفترة من ١-٣ مايو ، بكلية الشريعة والقانون بدولة الإمارات ٢٠٠٠ .
- د. محمد العريان : **الجرائم المعلوماتية** ، دار الجامعة الجديدة للنشر ، الإسكندرية ، ٢٠٠٤ .
- د. محمد محي الدين عوض : **مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ( الكمبيوتر )** بحث مقدم إلي المؤتمر السادس للجمعية المصرية للقانون الجنائي ، المنعقد من ٢٥-٢٨ أكتوبر ، سنة ١٩٩٣ .
- د. مدحت رمضان : **جرائم الاعتداء علي الأشخاص والانترنت** ، دار النهضة العربية ، القاهرة ، ٢٠٠٠ .
- د. هدى حامد قشقوش :
- **جرائم الحاسب الاللكتروني في التشريع المقارن** ، دار النهضة العربية ، القاهرة ، ١٩٦٢ .

- الإلتلاف العمدي لبرنامج وبيانات الحاسب الآلي ، بحث مقدم لمؤتمر ( القانون والكمبيوتر والانترنت ) المنعقد في الفترة من ١-٣ مايو ٢٠٠٠ بكلية الشريعة والقانون بدولة الإمارات .
- د. هشام محمد فريد رستم : الجوانب الإجرامية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، ١٩٩٤ .
- د. هلالى عبد اللاه احمد :
- اتفاقية بودابست لمكافحة الجرائم المعلوماتية ( معلقاً عليها ) ، دار النهضة العربية ، الطبعة الأولى ، القاهرة ، ٢٠٠٧ .
- تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، الطبعة الأولى ، ١٩٩٧ .