



المعهد القضائي للإبلاغ

الاثبات في دعاوى الجزائية باستخدام وسائل التقنية
(التكنولوجيا) الحديثة

اعداد المحامي: د. رمزي الدبك

2020



المعهد القضاة الأوقاف

نموذج ترخيص

انا الباحث /الطالب : الم.م. الدكتور /المرشد /الم.م. الدكتور /المرشد /الم.م. الدكتور /المرشد أمنح

المعهد القضائي أو/من يفوضه المعهد بذلك ترخيصا غير حصري دون مقابل ،بنشر /واستعمال / او ترجمه / او تصوير او اعادة انتاج سواء كانت ورقية أو إلكترونية او غير ذلك وعنوانها :

الدراسات الخدمية بالبنظام مسأله المنهجية (الكيفية) (المسألة)

.....
.....
.....

وذلك لغايات البحث العلمي / او التبادل مع المؤسسات التعليمية والجامعات او اي اغراض اخرى يراها المعهد القضائي مناسبة .

اسم الباحث/الطالب : الم.م. الدكتور /المرشد /الم.م. الدكتور /المرشد

التوقيع : [Signature]

التاريخ : 1435 / 7 / 15

المقدم الدكتور رمزي رشدي الدبك
ادارة البحث الجنائي

المقدمة

أنعم الله على الإنسان بالعقل والعلم، فعن طريقهما بدأ يطور أسلوب معيشتة، فبعد أن كان يعيش عصر الصيد ويعتمد على الرعي والترحال، بدأ يعرف الزراعة وحياة الاستقرار، ثم دخل عصر الثورة الصناعية التي بدأت بإختراع الآلة وظهور الصناعات المختلفة التي ترتبت عليها آثار ضخمة غيرت خريطة البشرية، كان أبرزها تقسيم دول العالم بين دول متقدمة تزداد تقدما، ودول نامية تحاول التقدم واخرى متخلفة ما زالت قابضة في التخلف.

ولم تقف رحلة الإنسان في تطوره عند العيش في ظل الثورة الصناعية، فما إن أوشك القرن الماضي على الإنصرام حتى بدأ الإنسان يعيش إرهاصات ثورة جديدة قلبت مناحي الحياة المختلفة رأسا على عقب، وهي ثورة تكنولوجيا المعلومات خاصة بعد أن حدث الاندماج بين المعلوماتية ، وبين الاتصال عن بعد وظهور ما يسمى بالمعلوماتية عن بعد فهذه المعلوماتية الأخيرة قد ساهمت بتحويل العالم كله إلى وحدة سكنية واحدة. فلا مرية أن تطور وسائل الإتصال المرئية والمعلوماتية، قد ترتب عليه اكتشاف انظمة تكنولوجيا جديدة أدت إلى ظهور استخدامات جديدة لوسائل الاتصال عن بعد.

وتعد "العمليات الإلكترونية" إحدى التجليات الرئيسية لتكنولوجيا المعلومات عن بعد، فهذه الاعمال قد اثرت تأثيرا كبيرا على البنين الإداري وعلى البنين الاقتصادي من خلال استخدام تقنيات العمل بالإنترنت والشبكات لتطوير أنشطة الأعمال الحالية وخلق أنشطة أعمال افتراضية جديدة.

ولقد أفرزت هذه الثورة التكنولوجية الجديدة الحاجة الماسة إلى تطوير نظم المعلومات في جميع قطاعات الحياة بما يساير التطورات التكنولوجية والاجتماعية والاقتصادية التي تتزايد يوما بعد يوم ، وذلك لأجل الإستفادة من الآثار الإيجابية لهذه الثورة، خاصة وان المستقبل سوف يشهد المزيد من التطور في نظم المعلومات بعد إن اتصلت هذه النظم بالأقمار الصناعية وبدأ العالم يدخل عصرا جديدا وهو عصر الإلكترونيات.

وإذا كان الإنسان بما حباه الله من علم هو المبتكر لهذه الثورة التكنولوجية الحالية، وهو الذي بداخله نفس بشرية قد تُجبل على الخير إذا ذكاه، وقد تجنح إلى الشر إذا دساها، فإنه لم يقف عند جني الثمار الإيجابية لهذه الثورة وانعكاساتها المختلفة في مناحي الحياة، وانما قد استغلها بمكره السيء في اكتشاف العديد من الاساليب الإجرامية الجديدة التي سهلت له ارتكاب العديد من الجرائم.

ولقد تمكن الإنسان عن طريق الوسائل الإلكترونية المستحدثة من ارتكاب العديد من الجرائم ضد الأشخاص والأموال، وضد الاسرار الاقتصادية والسياسية والعسكرية للدولة والملكية الفكرية وغيرها.

ومما لا شك فيه أنه كلما أزداد الإعتماد على الحاسبات في المجالات الاقتصادية والإدارية لمخاطر الغش والتجسس والسرقة والإتلاف العمدي، وغير ذلك من الجرائم التي ترتكب سواء اكان ذلك عند إدخال البيانات إلى الحاسب ام عند تبليغ البيانات إلى مستخدمها ام عند تخزين البيانات لحين إستخدامها ، أم عن طريق الدخول غير المشروع لهذه الحاسبات عن طريق إختراق البرامج الخاصة بها. والتلاعب في البيانات المخزنة فيها، حتى أن جرائم القتل العمد قد ترتكب باستخدام شبكات الإتصال عن بعد.

ومما يزيد من خطورة هذا النوع الجديد من الجرائم أنها قد تتعدى حدود المكان ويصعب بالنسبة لها حساب الزمان. كما وأن محلها قد يتعدى القيم المادية ليكون قيما إفتراضية لا تلمسها الايدي ولا تبصرها الأعين كالبرامج الخاصة بالحاسب والبيانات المخزنة. خصوصا وان السمة الرئيسية التي تتميز بها التكنولوجيا الحديثة للمعلومات انها تعتمد على تحويل البيانات أو المعطيات وهي غير ملموسة من شكل إلى اخر وذلك إما عن طريق معالجتها بواسطة الوسائل الإلكترونية، أو بنقلها من مكان أو من شخص إلى آخر

كذلك فإنه لا يغيب عن الذهن أن الوسائل الإلكترونية المستحدثة قد يضيق بها الإنسان ذرعا ليس – فقط – لأنها ستصيبه بأذى وضرر الجرائم الجديدة التي تتمخض عنها، وإنما أيضا لانها سوف تسهل وتوسع من مجالات انتهاك مكنون حياته الخاصة للحصول على أسرار الشخصية وأساره المالية ، بل إن هذه الوسائل قد تنتهك كذلك الأسرار المهنية والإقتصادية للمؤسسات والشركات والبنوك.

فلا يوجد شك في أن التطور الهائل الذي لحق شبكة الإنترنت وإنتشار أجهزة الحاسب الآلي الصغيرة والاجهزة الذكية (كالهواتف والاجهزة اللوحية)، قد تسبب في تهديد الحريات الفردية بخطر الاعتداء عليها، وهو ما يتطلب إيجاد الوسيلة المناسبة للرقابة عليها لتجنب هذا الخطر في الوقت المناسب . كما أن إنسان هذا العصر قد يهلك الحرث والنسل ويفسد بيديه بدائع خلق الله وجميل صنعه، فإنه ليس بمستغرب عليه أن يستفيد من

التكنولوجيا الحديثة في الإتصالات في المزيد من التنصت والتلصص على الحياة الخاصة لبني جنسه باستخدام الوسائل الإلكترونية الدقيقة، والتي عن طريقها قد تكون حياتهم الخاصة وأسرارهم المالية بدون واقٍ أو ستر. ومما يزيد من خطورة هذا الأمر أن النصوص العقابية المطبقة لا تكفي لحماية حرمة الحياة الخاصة من الاعتداء عليها باستخدام الوسائل الإلكترونية المستحدثة، بحسبان أن هذا الاعتداء لا يعاقب عليه قانون العقوبات إلا إذا كان مرتبطا بمكان خاص، أما تخزين المعلومات عن الافراد وتسجيلها في هذه الوسائل فإنه لا يخضع للتأثيم وفقا للقواعد العامة.

ويكفي في ذلك الإشارة إلى أنه عن طريق استخدام الحاسب الآلي فقد أمكن بواسطة عملياته الدقيقة المتقنة الماهرة أن تكون الحياة الخاصة للإنسان مجردة من كل السواتر أو التحصينات.

وهكذا نرى أن ثورة الإتصالات قد أفرزت وسائل إلكترونية عديدة قد تسببت في ظهور أنواع جديدة من الجرائم التي تختلف من حيث محلها ومن حيث أسلوب ارتكابها عن الجرائم التقليدية، وهو ما أدى إلى ظهور العديد من المشكلات التي كان أبرزها: عجز قوانين العقوبات الحالية التي وضعت نصوصها في ظروف تختلف عن الظروف الحالية التي خلقتها ثورة المعلومات عن مواجهة هذه الأنواع الجديدة من الجرائم. كما ان هذه الوسائل الإلكترونية قد انعكس تأثيرها على القوانين الإجرائية خاصة فيما يتعلق بصعوبة إثبات هذا النوع الجديد من الجرائم التي اوجدتها ثورة الإتصالات عن بعد والطبيع الافتراضية للدلة المتحصلة .

وإذا كانت القوانين العقابية المطبقة قد ضاقت نصوصها بما رحبت عن استيعاب الأنواع الجديدة من الجرائم التي جاءت بها ثورة المعلومات من بعد، وان القوانين الإجرائية ليست بأسعد حظا منها لأنها ستكون أمام جرائم ترتكب وقد يفر مرتكبها من العقاب مما يلحق اشد الضرر بالمجتمع وبالافراد، كما ان هذه القوانين الاخيرة ستواجهها مشكلات عديدة تتطلب حولا قانونية قد تكون في منتهى الصعوبة خاصة فيما يتعلق بمسألة الدليل.

وعلى ضوء هذه النتيجة تبرز اهمية بحث إحدى المشكلات التي يثيرها موضوع الجرائم التي فجرتها ثورة التكنولوجيا وتحديد الإتصالات عن بعد ، والتي تتعلق بصعوبة إثبات هذه الجرائم عن طريق الأدلة المتحصلة من الوسائل الإلكترونية في اطار نظرية الإثبات الجنائي.

فلا يوجد شك في أنه يجب تحقيق تناغم تشريعي داخل المجتمع ، بحيث أن القانون الإجرائي يساعد في تطبيق القانون العقابي الموضوعي على الجرائم المستحدثة التي يفرزها التقدم التكنولوجي، فلا يفر الجناة من العقاب، وفي ذات الوقت لا يحدث اعتداء على الحريات الفردية للافراد وتنتهك حرمت حياتهم الخاصة..

ولذلك فإننا سنحاول هنا تحديد الوسائل التي عن طريقها يتحقق هذا التناغم بين التوأمين التشريعي الجنائي الموضوعي والتشريع الإجرائي وذلك فيما يتعلق بالإثبات بالأدلة المتحصلة من الوسائل الإلكترونية، وهو بذلك قد يميظ اللثام عن بعض الصعوبات التي تكتنف موضوع اثبات الجرائم التي اوجدتها ثورة الاتصالات عن بعد والتي ما زالت في جانبها الإجرائي تحتاج إلى المزيد من التحليل والتأصيل.

ولذلك فإن هذا البحث سيعتق المنهج الاستقرائي الاستنباطي القائم على دراسة طرق إثبات الجرائم التي ترتكب بالوسائل الإلكترونية على ضوء طبيعتها المادية وغير المادية، وذلك لاجل الوصول إلى نتيجة كلية يمكن على ضوئها تحديد بعض الأدلة المتحصلة من الوسائل الإلكترونية والتي تصلح لإثباتها في إطار نظرية الإثبات الجنائي.

واتساقا مع ذلك فإنه يمكن دراسة موضوع هذا البحث في مبحثين، نورد الأول للطبيعة الخاصة بإثبات الجرائم، ونبين في الثاني ادلة إثبات هذه الجرائم وتقديرها في اطار نظرية الإثبات الجنائي لهذه الجرائم.

الطبيعية الخاصة للجرائم الإلكترونية

لا يوجد شك في أنه مع مطلع القرن الواحد والعشرين أفرزت تقنيات تكنولوجيا الاتصالات نماذج جديدة للعمليات الإلكترونية التي كان العقل يتخيلها ولكنه لم يتوقع تحقيقها بهذه السرعة الفائقة، ولعل الفضل في ذلك يرجع إلى التطور الهائل الذي لحق نظم الحواسيب الآلية لتشغيل المعلومات بعد إستغلال السرعة الهائلة للإلكترونيات التي أتاحتها إستخدام الدوائر والصمامات الإلكترونية.

ولقد تعددت صور هذه العمليات الإلكترونية كنتيجة لهذه الثورة التكنولوجية بين التي تتصل بعمليات التجارة الإلكترونية، وتلك التي تتعلق بعمليات التحويلات المالية الإلكترونية، وما يطلق عليه بالحكومة الإلكترونية. التي تعني إنتاج وتقديم الخدمة العامة باستخدام الوسائل الإلكترونية.

وأهم ما يميز هذه العمليات الإلكترونية أنها تدور في فلك شبكة الإنترنت او شبكات الانترنت وبذلك فإنها تستفيد من تقنياتها التكنولوجية العالية، وكذلك فإنها تستفيد أيضا من القدرات المهمة التي تقدمها لها شبكات أخرى مثل شبكة الإنترنت وشبكة الاكسترانت ، وتشكل الشبكة العنكبوتية العالمية (W.W.W) الجزء الأهم من الإنترنت، وتتكون شبكة الويب من مجموعة من المستندات المخترنة على مئات الآلاف من أجهزة الكمبيوتر

والتي تسمى صفحات الويب. وإذا كان العالم قد سعد بهذه الثورة التكنولوجية الجديدة بالنظر إلى الآثار الإيجابية العظيمة التي أفضت إليها، فإنه سوف يقاسى أيضا من الكثير من الآثار السلبية والضارة التي قد تترتب عليها. ولقد بدت مظاهر هذه الآثار السلبية في إختراق النظم الأمنية لحماية البيانات المخزنة ضمن أنظمة الوسائل الإلكترونية، وذلك بالإطلاع على هذه البيانات بطرق غير مشروعة، أو بتخريب وإتلاف برمجيات حماية البيانات أو بالنسخ غير المشروع لها، أو بسرقة معلومات الحاسبات، أو بإنتهاك حرمة الحياة الخاصة للأفراد، أو بالاعتداء على الحقوق الادبية والمالية للمؤلفين وغيرها.

ولا شك أن الثورة التكنولوجية الحالية في مجال الاتصالات عن بعد قد خلفت وراءها إرتكاب العديد من الجرائم المستحدثة التي لا مثيل لها في الماضي، كما وأنها قد أتاحت فرص إرتكاب الجرائم التقليدية بطرق غير تقليدية. فهذه الجرائم المستحدثة لا تعترف بالحدود بين الدول والقارات، فيمكن ان يكون الجاني في بلد معين ويرتكب الجريمة في بلد آخر، كذلك فإن استخدام الوسائل الإلكترونية المستحدثة قد يساعد المجرمين، في إرتكاب العديد من الجرائم دون إمكان القبض عليهم، ومثال ذلك أن استخدام البريد الإلكتروني كوسيلة اتصال بين المجرمين، يتعدى معه مراقبتهم على النحو الذي يحدث في الاتصالات السلكية واللاسلكية، كذلك فإن عمليات التحويلات المالية الإلكترونية قد تتم بين الجناة والذين قد يكونوا فرادى أو جماعات بغرض تمويل العمليات الإجرامية أو المخططات الإرهابية دون أن يتم إكتشافها.

ويلاحظ أن الجرائم التي تقع على العمليات الإلكترونية بسبب الثورة التكنولوجية قد تأثرت بالوسائل المستحدثة التي أوجدتها هذه الثورة مما يترتب عليه انفراد هذه الجرائم بصفات خاصة تزيد من خطورتها ومن الآثار الضارة التي تترتب عليها، ويبدو ذلك فيما يلي:

1- أنعكاس الثورة الرقمية التي فجرتها تكنولوجيا الاتصالات عن بعد على شكل ونوعية وأسلوب الجريمة المعاصرة والتي صاحبها مستجدات غيرت من المفهوم التقليدي لعمليات التزيف والتزوير، وذلك بعد استخدام الناسخات الليزرية الرقمية الملونة وغير الملونة، ودخول الحاسبات الآلية وما يرتبط بها من ماسحات وطابعات في إرتكاب جرائم التزيف والتزوير في المستندات والعملات.

2- أن التطور الذي حدث بسبب تكنولوجيا المعلومات قد تأثرت به كذلك وسائل الدفع النقدي التقليدية، مما أدى إلى ظهور المستندات والوثائق اللدائنية وظهرت أيضا الوسائل الإلكترونية لتحل محل النقود وأوامر الصرف "الشيكات" وبدأت بطاقات الإئتمان اللدائنية تحل محل النقد والشيكات. ولقد ترتب على إزدياد التعامل ببطاقات الإئتمان عالميا أن صاحب ذلك أزداد أساليب التلاعب والتحايل في هذه البطاقات عن طريق تزيفها وعن طريق سرقتها والتحايل في استخدامها بطرق كثيرة غير مشروعة. ولا شك في أن الجرائم التي تقع على بطاقات الإئتمان تتميز بطبيعة خاصة مما يتطلب إتباع طرق بحث وتحري مختلفة عن طرق بحث وإثبات الجرائم التقليدية، وذلك بالنظر إلى المفهوم الجديد لهذه الجرائم والتي قد يتعرض محلها لعمليات تزيف وتحايل مستحدثة بفضل التقنيات التكنولوجية المستحدثة، وهو ما قد يترتب عليه ظهور مجرم جديد ومفاهيم جديدة للجريمة ومسرح يتسع لها قد يسع العالم كله وهكذا نرى أن التطور الذي لحق بالمادة التي تصنع منها النقود غير من طبيعة الجرائم التي تقع عليها، فبعد أن كانت جرائم التزيف والتزوير تقع على العملة الورقية والمعدنية أصبحت اليوم بعد ظهور بطاقات الإئتمان تقع على مواد لدائنية أو بلاستيكية، مما يمكن معه القول بأن العالم يتحول من الجرائم التي يستخدم فيها الورق كوسيط وأداة للجريمة إلى الجرائم البلاستيكية. ومن المنتظر أن يشهد المستقبل تطورا مذهلا سوف يلحق بطاقات الإئتمان، لأنه سوف يتم صنع بطاقات ذات سعة معلوماتية عالية مثل البطاقة الرقائنية وبطاقة الشريط البصري، وأن هذا النوع من البطاقات سيترتب على استخدامه تأمين بطاقة الإئتمان.

3- كذلك فإن ظهور الحاسبات الآلية واستخدامها على نطاق واسع سواء على المستوى الفردي او على المستوى الحكومي، وما صاحب ذلك من تطور تقني بأساليب الاستنساخ الملونة عن طريق الناسخات والطابعات الملونة، قد ترتب عليها افول دور المستندات الورقية والاتجاه نحو تصاعد دور المستندات الإلكترونية، كالأشرطة الممغنطة، إسطوانات الفيديو، الدعامات المثقبة والميكروفيلم، وهذه الدعامات الجديدة لا تتكيف مع قواعد الإثبات التقليدية التي تنصب على المستندات الورقية، ومن ثم فإن إثباتها قد يثير العديد من المشكلات حول مدى إعتبارها محررات يمكن ان يقع عليها التزوير أو التزيف. فالمعلومات المبرمجة في جهاز الكمبيوتر أو على اسطوانة أو شريط قد يصعب انطباق وصف المحرر عليها، لأن المحرر الذي يحميه تجريم التزوير هو الذي يصلح ليحتج به، وهذا لا يتحقق إلا بإستعماله في التعامل، وهذا ما لا يتحقق بالنسبة للمعلومات المبرمجة قبل طباعتها في أوراق. (وهذا لا يمنع من القول أن هناك رأيا فقهيًا يذهب إلى اعتبار المعلومات المبرمجة من عداد المحررات ما دامت مدونة

على اسطوانة أو شريط أو مسجلة بجهاز الحاسب الآلي نفسه، إستنادا إلى أنه يمكن الاطلاع عليها بالوسيلة المناسبة لذلك).

ولقد أدرك المشرع الفرنسي هذه المشكلة فأعاد تنظيم مواد التجريم في قانون العقوبات الجديد، بأن أجرى تعديلا على النص الأصلي لجريمة التزوير لكي يشمل المعلومات المبرمجة، وبناء على ذلك فإن المادة 2/441 من قانون العقوبات الفرنسي الجديد تعرف التزوير بأنه (كل تغيير للحقيقة بسوء نية من شأنه الإضرار بالغير، أيا كانت الوسيلة المتبعة في مستند مكتوب أو في أي دعامة من دعائم التعبير عن الفكر التي لها شأن في إثبات حق أو واقعة لها نتائج قانونية).

كما إنه يمكن القول بأن الحاسبات الآلية يمكن أن تتخذ كوسيلة لإرتكاب العديد من الجرائم المستحدثة كتزوير المحررات الرسمية أو تزييف العملة، وقد تستخدم هذه الحاسبات أيضا في تحقيق اغراض الدخول غير المشروع للوصول إلى البيانات والمعلومات المخزنة في حاسب آلي آخر عبر شبكة الاتصال الدولية.

كذلك فإن هناك العديد من الجرائم التي تقع على الحاسب الآلي بكيانه المادي أو جانبه المعنوي، ومثال ذلك جرائم تعديل أو تحوير أو تقليد برامج الحاسب الآلي، وجرائم تدمير المعلومات والبيانات الخاصة بذات الحاسب الآلي . فإذا كان بعض هذه الجرائم قد يكون محله جانبا معنويا (افتراضيا) تقع عليه يتمثل في المعلومات والبيانات والبرامج التي يحتويها الحاسب الآلي فإن ذلك قد يثير العديد من المشكلات حول هذه الكيانات المعنوية من حيث مدى صلاحيتها لقيام الجريمة، لأن ذلك يتطلب وجوب إثبات كونها مالا لكي تكون محلا للتجريم والعقاب. ولذلك نجد أن برامج الحاسبات الآلية قد أثارت مشكلة مدى إعتبارها مالا لكي تخضع الجرائم التي تقع عليها لنصوص جرائم الإعتداء على الأموال، حيث ان هذه البرامج في جوهرها معلومات، وأن هذه المعلومات عبارة عن مجموعة من الافكار تمثل تعبيراً يأخذ شكل رسالة يستطيع الغير إدراكها سواء اكان ذلك عن طريق نقلها أم حفظها أم معالجتها وذلك بعد أن يقوم الحاسب بمعالجتها وتحويلها إلى رموز وشفرات لا يمكن للإنسان العلم بها إلا من خلال الآلة وأثناء تشغيلها . ونقطة البحث في هذه المسألة تتحدد في مدى جواز وقوع أفعال الإعتداء على الأموال على المعلومات.

ولقد ذهب الفقه الحديث إلى اعتبار الشيء مالا ليس بالنظر إلى كيانه المادي وإنما على أساس قيمته أو منفعته الاقتصادية ، ومن ثم فإنه يمكن اعتبار برامج الحاسبات الآلية مالا متى كانت لها قيمة اقتصادية تستحق الحماية القانونية ، ومتى تحققت بالنسبة لها رابطة ملكية تربط بينها وبين مالكها . ويترتب على ذلك إمكان إدخال أفعال الإعتداء عليها ضمن جرائم الإعتداء على الأموال بحسبان ان برامج الحاسبات الآلية تحتوي على افكار ومعلومات يمكن ان يطلق عليها الطاقة الذهنية، وانها كذلك تقبل التملك والحيازة من خلال الدعوات التي تسجل عليها، وانها ايضا تقبل الانتقال بموافقة حائزها . ولذلك فإنه يمكن القول بأن افعال الإعتداء على برامج الحاسبات الآلية يمكن ان تتمخض عنها جرائم سرقة واخفاء اشياء مسروقة، ونصب واساءة ائتمان وتخريب واتلاف.

ولقد حرص المشرع الفرنسي على أن يضمن قانون العقوبات الفرنسي الجديد الصادر في سنة 1994 نصا يجرم فيه سرقة الطاقة، فتتنص المادة 2/311 عقوبات على أن: (يعتبر في حكم السرقة اختلاس الطاقة بسوء نية اضراراً بالغير).

كذلك فقد تدخل المشرع في دول اخرى كالولايات المتحدة الأمريكية والدول الأوروبية وأجرى تعديلات على نصوص جرائم السرقة والنصب واساءة الامانه لكي تشمل المعلومات بإعتبارها أموالا منقولة.

ولم تقف مشكلة الجرائم التي تقع على برامج الحاسبات الآلية بالنظر إلى طبيعتها الخاصة عند مشكلة مدى صلاحية الافعال غير المشروعة التي تقع عليها لأن تتمخض عنها جرائم الإعتداء على المال، بل إن هذه المشكلة تمتد لتشمل كذلك مسألة مدى خضوع هذه البرامج لفعل الاختلاس المكون للسلوك المادي لجريمة السرقة، فالاختلاس الذي يقع على برامج الحاسب الآلي أو المعلومات المعالجة لا يترتب عليه خروج هذه البرامج من حيازة او (ذمة) صاحبها الشرعي، كما وان الاستيلاء على البرامج بإعتبارها معلومات لا يتصور وقوعه الا على اساس اعتباره انتقالا لهذه المعلومات من ذهن إلى ذهن أو من ذاكرة إلى ذاكرة، ايضا فإن المعلومات التي يقع عليها هذا الاستيلاء من طبيعة معنوية ومن ثم فإنه قد لا يتصور أن يقع عليها فعل الاختلاس الذي يتميز بطبيعة مادية.

كذلك فإن ذات المشكلة قد تثار بشأن مدى خضوع برامج الحاسب الآلي للنشاط الإجرامي في جرائم الاحتيال واساءة الائتمان ، فهل يمكن القول بوقوع هذه الجرائم على المعلومات التي يتكون منها

البرنامج . ولقد إنتهت أحكام القضاء الفرنسي إلى اعتبار المعلومات المسجلة على دعامة مادية كتلك المسجلة في جهاز الحاسب الآلي، أو على شريط أو اسطوانة من المنقولات التي تصلح لان تكون محلا للسرقة أو النصب أو خيانة الأمانة، وذلك بعد ان تغلبت على المشكلات التي اثارها الطبيعة الخاصة لهذه الجرائم عندما تقع على المعلومات وذلك من حيث اعتبار هذه المعلومات مالا منقولاً، وأن أفعال الاعتداء عليها يمكن ان تندرج في مفهوم الاختلاس. كما أن هذه الاحكام قد اعتبرت ان اخفاء المعلومة يتساوى مع اخفاء المال المنقول ومن ثم فإنها تصلح محلا لجريمة إخفاء الاشياء المسروقة أو المتحصلة من جريمة بشرط ان تكون متواجدة على دعامة مادية ولذا فإن الأموال المعنوية التي ليس لها دعامة مادية تأخذ حكم المنافع التي لا تنطبق عليها جرائم الأموال التقليدية.

كما أن الفقه قد ذهب إلى أن اصطلاح "الشيء" الذي يرد عليه فعل الإختلاس يستوعب الأموال ذات الكيان غير المادي . ومن ثم فإن جريمة السرقة يمكن ان تقع على المعلومات. فلا يوجد شك في أن دخول برامج الحاسب الآلي ضمن الجرائم سألقة الإشارة إليها ليثير مشكلات عديدة فيما يتعلق بإسنادها لنصوص التجريم والعقاب التي تعاقب على هذه الجرائم لأن الأمر هنا يتطلب إثبات دخول الأفعال التي تتحقق بها هذه الجرائم ضمن نصوص التجريم والعقاب التي يمكن ان تنطبق عليها. وكتطبيق لذلك فإنه قد يصعب وقوع جريمة السرقة على البرامج المشفرة بإستعمال أجهزة مقلدة لحل شفرتها إلا إذا كان هناك نص عقابي يتضمن تجريمها والعقاب عليها. وكتطبيق لذلك فإنه قد يصعب وقوع جريمة السرقة على البرامج المشفرة بإستعمال أجهزة مقلدة لحل شفرتها إلا إذا كان هناك نص عقابي يتضمن تجريمها والعقاب عليها صراحة مثلما فعل المشرع الفرنسي عندما تدخل بسن قانون خاص يعاقب على هذا الفعل

ولذلك فإنه إذا كان المستقبل سيظهر المزيد من التقدم في مجال المعلومات وخاصة في استحداث العديد من الوسائل الإلكترونية التي قد تستغل في الاعتداء على هذه المعلومات. فإن ذلك يتطلب أن يساير المشرع الجنائي الثورة التكنولوجية في المعلومات بأن يتصدى للأفعال الإجرامية المستحدثة التي تفرزها هذه الثورة وذلك بتجريمها والعقاب عليها بما يتناسب مع الاضرار المتوقعة من صور العدوان التي قد تحدث بسببها . فالنظرة إلى المعلومات التي تحتويها الوسائل الإلكترونية يجب ان تكون نظرة خاصة تتفق مع طبيعتها الخاصة.

ولعلنا نلاحظ قيام بعض التشريعات في الوقت الحاضر بإفراد نصوص خاصة لتجريم أفعال الإعتداء على المعلومات في أشكالها المختلفة، فالمشرع الفرنسي قد تدارك النقص الذي بدا واضحا في نصوص قانون العقوبات التقليدية بشأن جرائم المعلومات، فجاء قانون العقوبات الفرنسي الجديد الصادر في سنة 1994، بالمادة 323 والتي نصت في فقراتها من الأولى وحتى السابعة على تجريم الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو في جزء منه، مع النص على تشديد العقوبة إذا نتج عن الدخول أو البقاء محو أو تعطيل المعطيات الموجودة داخل النظام أو إفساد وظيفته، وكذلك تجريم الإدخال غير المشروع لمعطيات في نظام المعالجة الآلية للمعطيات أو المحو أو التعديل غير المشروع لها، وذلك بعد ان اعتبر المشرع الفرنسي هذه المعطيات من قبيل الأموال ذات الطبيعة الخاصة.

ولقد توسع المشرع الفرنسي في تجريم أفعال الاعتداء على معطيات الوسائل الإلكترونية، فجرم كافة صور الإختراق غير المشروع لهذه المعطيات سواء وقعت هذه الأفعال على الأجهزة الإلكترونية نفسها أم على الأنظمة التي تعمل بها هذه الأجهزة.

كذلك فإن هذا المشرع قد مد المسؤولية الجزائية عن هذه الإعتداءات إلى الأشخاص المعنوية بأن نصت المادة 6/323 على ذلك، ولكن وفقا للشروط التي تنص عليها المادة 2/121 التي تعد النص العام في تقرير المسؤولية الجنائية للأشخاص المعنوية في قانون العقوبات الفرنسي.

ونجد أن المشرع الاردني قد حذا حذو المشرع الفرنسي بذلك في كل من قانون المعاملات الالكترونية وقانون الجرائم الالكترونية ، فتنص المادة 3 من قانون الجرائم الالكترونية على انه أ- يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات باي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة اشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلاهما العقوبتين. ب- اذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار. ج- يعاقب كل من دخل قصداً إلى موقع

الكثروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكة بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار. وكذلك نصت المادة 4 على انه يعاقب كل من ادخل أو نشر أو استخدم قسداً برنامجاً عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو النقط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول اليه أو تغيير موقع الكثروني أو إلغائه أو إتلافه أو تعديل محتوياته أو اشغاله أو انتحال صفته أو انتحال شخصية مالكة دون تصريح أو بما يجاوز أو يخالف التصريح بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار. وتنص المادة 5 على انه يعاقب كل من قام قسداً بالتقاط أو باعتراض أو بالتنصت أو اعاق أو حور أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار.

اما المادة 24 من قانون المعاملات الالكترونية الاردني فتتنص على ان يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على ثلاث سنوات أو بغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار أو بكلتا هاتين العقوبتين كل من: أنشأ أو نشر أو قدم شهادة توثيق الكثروني بغرض احتيالي أو لأي غرض غير مشروع- ب قدم إلى جهة التوثيق الإلكتروني معلومات غير صحيحة بقصد إصدار شهادة توثيق أو وقف سريانها أو إلغائها.

4- إن الطبيعة الخاصة التي تتميز بها الجرائم التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية المستحدثة لا تقف عند الطبيعة الخاصة بالأفعال التي تتحقق بها هذه الجرائم، وإنما تمتد هذه الطبيعة لتشمل أيضا البعد العالمي (العابر للحدود) لهذا النوع من الجرائم، فإذا كانت شبكة الاتصالات من بعد ذات نطاق عالمي لا يتفقد بحدود دولة معينة فإنه يتصور تبعا لذلك أن تتميز الجرائم التي تقع عليها أو تقع بسببها أو بواسطتها بالطبيعة العالمية، فيستطيع اي شخص في دولة معينة الدخول إلى شبكة الإنترنت العالمية، ويمكنه ارتكاب نشاطه الإجرامي في دولة أخرى أو مجموعة من الدول الأخرى (بشكل عابر للحدود).

ولذلك فإنه يمكن القول أن جرائم الحاسبات الآلية لا تعترف بالحدود بين الدول والقارات، فمن يتمكن من معرفة كلمة السر للوسائل الإلكترونية التي تتصل بالشبكات العالمية، يستطيع إختراق هذه الشبكات والعبث بمعلوماتها بغض النظر عن مكان تواجده. فجرائم الوسائل الإلكترونية المستحدثة تعد تبعا لذلك شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الاقليمية أو القارية . ولا شك في أن الطبيعة العالمية التي تتميز بها الجرائم التي تتصل بنظم المعالجة الآلية للمعلومات قد تثير مشكلات كثيرة تتعلق بتحديد الاختصاص المكاني لهذه الجرائم، وبقواعد سريان القانون الوطني من حيث المكان.

فإذا كان من المتصور أن تستخدم الوسائل الإلكترونية في ارتكاب جرائم الاعتداء على أمن الدولة الداخلي أو الخارجي، فإن ذلك يجعل الاختصاص بهذه الجرائم للقانون الوطني للدولة التي وقعت عليها هذه الاعتداءات وذلك تطبيقا لمبدأ العينية في سريان قانون العقوبات من حيث المكان الذي تطبقه الكثير من الدول لحمايتها من جرائم معينة تتميز بخطورة معينة، فتمد قانونها الوطني لتطبقه عليها حتى ولو ارتكبت هذه الجرائم خارج حدود اقليمها الوطني . ولا مرية أن هذه الطبيعة الخاصة بهذا النوع من الجرائم ستنعكس أيضا على إثباتها جنائيا لأنها سوف تزيد من صعوبة لهذا الإثبات خاصة في تلك الحالات التي ترتكب فيها هذه الجرائم خارج النطاق المكاني للإقليم، إذ يصعب في مثل هذه الحالات جمع الدليل وملاحقتها.

5- لا تقف الطبيعة الخاصة بالجرائم التي تقع على العمليات الإلكترونية عن طريق الوسائل الإلكترونية عند الطبيعة الخاصة للأفعال التي ترتكب بها، أو أنها عالمية المكان، بل تتميز هذه الجرائم كذلك بأن الذين يرتكبونها هم فئة من المجرمين يتميزون بصفات خاصة، فقد يكون هؤلاء من المحترفين الذين يتميزون بالخبرة والمهارة العالية في مجال الحاسب الآلي وتقنية المعلومات ويعملون كمبرمجين أو محللين أو مشغلين، ولذلك فإن طبيعة عملهم وخبرتهم في هذا المجال تسهل لهم ارتكاب هذا النوع من الجرائم . كذلك فإن هؤلاء الجناة يتميزون غالبا بالذكاء، الذي يستعين بالحاسب الآلي في السرقة أو في الاحتيال أو في إتلاف المعلومات ، لا بد أن يتميز بمستوى عالي من الذكاء لكي يستطيع مواجهة العقوبات التي قد تواجهه أثناء ارتكابه مثل هذه الجرائم.

أيضا فإن " المجرم المعلوماتي " لا يتميز بالعنف، فهو لا يلجأ إلى إستخدام العنف في إرتكاب جرائمه ، حيث أن معظم الجرائم التي ترتكب منه قد تقع على الأموال، ويستخدم في إرتكابها الذكاء الحاد الذي يتميز به. ومما يزيد من خطورة هؤلاء المجرمين أنهم قد يرتكبون جرائمهم ويفلتون من العقاب، فخبرتهم وتخصصاتهم الفنية تساعدهم في إخفاء جرائمهم ومن ثم يتعذر الوصول إليهم، فهم يستخدمون الإمكانيات والأساليب المعلوماتية، ليس فقط من أجل إرتكاب افعال الغش والتزوير والتزييف، بل وللتهرب من كشف أمرهم أو على الأقل إعاقة الملاحقة القضائية التي قد تتم قبلهم . ولا شك في أن هذه الطبيعة الخاصة التي تتميز بها تلك الفئة التي ترتكب جرائم الإعتداء على العمليات الإلكترونية تنعكس على إثبات هذه الجرائم مما يزيد من صعوبته، ومن ثم تعذر جمع الدليل الذي يكفي للادانة عنها.

6- أن الجرائم التي تقع على العمليات الإلكترونية بإستخدام الوسائل الإلكترونية تحتاج إلى تأهيل فني وعلمي خاص يجب توافره في جميع الأشخاص الذين تتصل أيديهم بهذه الجرائم بدءاً من مرحلة التحري وجمع الإستدلالات ومرورا بمرحلة التحقيق الإبتدائي وانتهاءً بمرحلة المحاكمة. فإذا كان هذا النوع من الجرائم يتميز بطبيعة فنية معقدة وقد لا يخلف وراءه آثار تكشف عنه، فإنه يحتاج لكشفه والوصول إلى مرتكبيه إلى خيرة معينة فيمن يتصلون بهذه الجرائم كرجال الشرطة، والنيابة العامة، وقضاء الحكم. ولذلك فإنه يجب تدريب افراد الضبط القضائي (الضابطة العدلية) واعضاء التحقيق الإبتدائي، والقضاة الذين تتصل أيديهم بالجرائم التي ترتكب بالوسائل الإلكترونية أو تلك التي تقع على هذه الوسائل، بحيث تتوافر لديهم الإمكانية الفنية التي تمكنهم من القيام بأعمال وظائفهم في مثل هذا النوع من الجرائم.

فلا يوجد ادنى شك في أن التقدم العلمي كما أنه يؤثر على النصوص التشريعية بحيث أنها قد تبدو عاجزة عن مواجهة الظواهر الإجرامية المستجدة التي يتسبب فيها التقدم، فإنه قد يؤثر أيضا على عقلية القضاة بحيث يجب عليهم الفصل في المنازعات التي تعرض عليهم والتي قد تزداد في تعقيدها وطابعها الفني يوما بعد يوم بسبب الثورة العلمية التي يشهدها عالم اليوم ولا شك أن التقدم الهائل الذي نشهده اليوم بسبب ثورة الإتصالات عن بعد، لا يؤدي أكله إلا إذا تواكب معه تطور في الفكر البشري بحيث يستطيع ان يحافظ على آثاره الإيجابية ويتلافى الآثار السلبية التي قد تترتب عليه، وهذا يتطلب تدريب سلطات التحري وجهات التحقيق والقضاة بحيث تتوافر لديهم القدرة الفنية، التي تمكنهم من القيام بأعمال ووظائفهم المختلفة بشأن هذا النوع من الجرائم الذي يرتكب بإستخدام الوسائل الإلكترونية المتقدمة ولعلنا نصل من خلال هذا العرض الذي سلط الضوء على الطبيعة الخاصة التي تتميز بها الجرائم التي تتمخض عن الآثار السلبية لثورة تقنية الاتصالات عن بعد إلى حقيقة مؤداها: إن هذه الطبيعة ستكون لها انعكاساتها الواضحة على الإثبات الجنائي لهذه الجرائم وهو ما سنفصله بالبيان.

أثر الطبيعة الخاصة للجرائم الإلكترونية على إثباتها جزائيا

من الحقائق المسلم بها أن التقدم العلمي له تأثيره البالغ على القانون وعلى الواقع الذي يطبق عليه هذا القانون. ولكي تتحقق الفائدة المرجوة من هذا التقدم، فإن القانون يجب ألا يفصل عن الواقع الذي يفرزه ويطبق عليه ، بل يجب أن يكون متجاوبا معه ومتطورا بتطوره.

ولا شك في ان التطور الحالي الذي انعكس اثره على قانون العقوبات، قد انعكس اثره ايضا على قانون اصول المحاكمات الجزائية، بحيث ان هذا القانون الأخير قد لا يطبق بسبب عجز القانون الأول عن استيعاب الجرائم المستحدثة التي ترتكب بالوسائل الإلكترونية، كما وأن الإثبات الجنائي وهو احد الموضوعات الهامة لهذا القانون قد تأثر بدوره بالتطور الهائل الذي لحق الأدلة الجنائية بسبب تطور طرق إرتكاب الجريمة، الأمر الذي يتعين معه تغيير النظرة إلى طرق الإثبات الجنائي لكي تقترب الحقيقة العلمية في واقعها الحالي من الحقيقة القضائية .

* * * وسنبين فيما يلي مظاهر الصعوبة في إثبات هذا النوع من الجرائم:

1- غياب الدليل المرئي:

الجرائم التي تقع على العمليات الإلكترونية المختلفة، كالتى تقع على عمليات التجارة الإلكترونية، أو على العمليات الإلكترونية للأعمال المصرفية، أو على أعمال الحكومة الإلكترونية، قد يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات، فإذا وقعت جرائم معينة على هذه الجوانب المعنوية، كجرائم السرقة أو الاختلاس أو الاستيلاء أو الغش أو التزوير أو الإتلاف أو اساءة الأمانه فإنه قد يصعب إقامة الدليل بالنسبة لها

بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة. ويوجد شك في ان إثبات الأمور المادية التي تترك آثارا ملحوظة يكون سهلا ميسورا، بعكس إثبات الأمور المعنوية فإنه يكون في منتهى الصعوبة بالنظر إلى أنه لا يترك وراءه أي آثار قد تدل عليه أو تكشف عنه، بحسبان أن أغلب المعلومات والبيانات التي تتداول عبر الحاسبات الآلية والتي من خلالها تتم العمليات الإلكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحاسبات الآلية.

فالجرائم التي ترتكب على العمليات الإلكترونية التي تعتمد في موضوعها على التشفير والكودات السرية والنبضات والأرقام والتخزين الإلكتروني يصعب أن تخلف وراءها آثارا مرئية قد تكشف عنها أو يستدل من خلالها على الجناة. وكمثال لذلك نجد أن التجسس المعلوماتي بنسخ الملفات وسرقة وقت الآلة يصعب على الشركات التي تكون الضحية لمثل هذه الأفعال اكتشاف أمرها وملاحقة الجناة عنها. ولعل هذه الطبيعة غير المرئية للأدلة المتحصلة من الوسائل الإلكترونية تلقى بظلالها على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية حيث تصعب قدرتهم على فحص واختبار البيانات محل الاشتباه خاصة في حالات التلاعب في برامج الحاسبات، ومن ثم فقد يستحيل عليهم الوصول إلى الجناة. فمن المعلوم أن جهات التحري والتحقيق اعتادت على الاعتماد في جمع الدليل على الوسائل التقليدية للإثبات الجنائي التي تعتمد على الإثبات المادي للجريمة ولكن في محيط الإلكترونيات فالأمر مختلف، فالمتحري أو المحقق لا يستطيع اي منهما تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية (الافتراضية)

2- سهولة إخفاء الدليل:

كما سبق القول فإن الجناة الذين يستخدمون الوسائل الإلكترونية في ارتكاب جرائمهم يتميزون بالذكاء والإتقان الفني للعمل الذي يقومون به والذي يتميز بالطبيعة الفنية، ولذلك فإنهم يتمكنون من إخفاء الأفعال غير المشروعة التي يقومون بها اثناء تشغيلهم لهذه الوسائل الإلكترونية ويستخدمون في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي يتم تسجيل البيانات عن طريقها.

كما وأن هناك بعض الأفعال غير المشروعة التي يرتكبها جناة الوسائل الإلكترونية ويكون أمرها حكرا عليهم كالتجسس على ملفات البيانات المخترنة والوقوف على ما بها من أسرار، كما أنهم قد ينسخون هذه الملفات ويتحصلون على نسخ منها بقصد استعمالها تحقيقا لمصالحهم الخاصة، كذلك فإنهم قد يقومون باختراق قواعد البيانات والتغيير في محتوياتها تحقيقا لمآرب خاصة (الاختراق المعروف عامة بالتهكير)، وقد يخربون الأنظمة تخريبا منطقيا بحيث يمكن تمويهه، كما لو كان مصدره خطأ في البرنامج أو في الأجهزة أو في انظمة التشغيل أو التصميم الكلي للنظام المعالج آليا للمعلومات، وقد يدخلون كذلك بيانات غير معتمدة في نظام الحاسب أو يعدلون برامجه أو يحرفون البيانات المخزنة بداخله دون ان يتخلف من وراء ذلك ما يشير إلى حدوث هذا الإدخال أو التعديل

ومما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل الإلكترونية أنه يمكن محو الدليل في زمن قصير، فالجاني يمكنه ان يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، وفي الحالة التي قد تعلم بها فإنه يستهدف بالموح السريع عدم استطاعة هذه السلطات إقامة الدليل ضده. ويلاحظ أن المجني عليهم قد يساهمون بدورهم في عدم إمارة اللثام عن هذه الجرائم، فقد يحجمون عن تقديم الدليل الذي قد يكون بحوزتهم عن هذه الجرائم، وقد يكون مقصدهم من ذلك استقرار حركة التعامل الاقتصادي بالنسبة لهم، أو رغبتهم في إخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليدها من الآخرين.

ولعل هذا الأمر قد تلجأ إليه عادة المؤسسات المالية كالبنوك والمؤسسات المصرفية وشركات الإقراض والسمسرة، حيث يخشى القائمون على إدارتها من شيوع أمر الجرائم التي تقع داخلها على الثقة فيها من العملاء المتعاملين معها، مما قد يؤدي إلى انصرافهم عنها، وهو ما قد يصيبهم بأضرار قد تزيد بكثير عن كشف ستر هذه الجرائم وتقديم مرتكبيها إلى العدالة.

وإذا نظرنا إلى هذا الإحجام عند الإبلاغ عن مثل هذه الجرائم الفنية نجد أنه قد ترتب عليه نتائج تكون في منتهى الخطورة، فهو يزيد من الرقم مما يعوق رسم السياسة الجنائية السليمة لمواجهة الظاهر الإجرامية المستجدة واختيار افضل الوسائل لمكافحتها. ولذلك فقد اقترح البعض خاصة في الولايات المتحدة الأمريكية بأن تفرض النصوص المتعلقة بجرائم الحاسبات التزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عن الجرائم التي تحدث داخل هذه الجهة ويتحقق علمهم بها.

3- إعاقة الوصول إلى الدليل:

جناة الجرائم الإلكترونية من المجرمين المحترفين الذين لا يرتكبون جرائمهم بسبب الاستفزاز أو الاستثارة في الغالب وإنما هم يخططون لما يفعلون ويستخدمون قدراتهم الفنية والعقلية لنجاح هذا التخطيط، ولذلك نجد انهم

وهم يرتكبون الجرائم الإلكترونية يحيطون انفسهم بتدابير أمنية واقية تزيد من صعوبة كشف هويتهم وإزالة حُجب الشر التي اصطنعوها بأيديهم. وكمثال لذلك نجد أنهم قد يستخدمون التشفير وكلمات السر التي تمكنهم من اخفاء الأدلة التي قد تكون قائمة ضدهم، وقد يدسون تعليمات خفية بين الأدلة لتصبح كالرمز فلا يمكن لغيرهم ان يفهم مقصودها، وقد يقوم هؤلاء ايضا بتشفير التعليمات باستخدام طرق وبرامج تشفير البيانات المتطورة مما يجعل الوصول إليها في منتهى الصعوبة.

وليس بخاف كذلك أن هؤلاء الجناة قد يستخدمون الوسائل الإلكترونية المختلفة لإعاقة الوصول إليهم، فقد يستخدمون البريد الإلكتروني في إصدار تكليفاتهم بإرتكاب جرائم القتل والاعتقالات والتخريب دون ان يتمكن أحد من تحديد امكانهم أو تسجيل هذه التكاليفات على النحو الذي كان يحدث في الاتصالات السلكية واللاسلكية، كذلك فإن مرتكبي جرائم الإنترنت يصعب ملاحظتهم لإستحالة تحديد هويتهم سواء عند قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها، لأنهم في الغالب يستخدمون أسماء مستعارة أو يدخلون إلى الشبكة ليس عن طريق ابواب حاسباتهم الآلية وانما عن طريق مقاهي الإنترنت.

أيضا فإنه يلاحظ أن ملاحقة جرائم الإنترنت قد تتعلق ببيانات تكون مخزنة في داخل دولة اجنبية بواسطة شبكة الاتصال عن بعد، ولذلك فإنه قد يصعب ضبط مثل هذه الأدلة لأن هذا الإجراء يتعارض مع مبدأ السيادة الذي تحرص عليه كل دولة. ولعل هذا الامر يكشف لنا عن اهمية التعاون القضائي الدولي في مجال الإنابة القضائية خاصة في مجال الجرائم العابرة للحدود والقارات والتي منها تلك الجرائم التي تقع بسبب ثورة الإتصالات عن بعد.

4- صعوبة فهم الدليل المتحصل من الوسائل الإلكترونية:

لا شك في ان طبيعة الدليل تنعكس عليه، فالدليل الفني قد يكون مضمونه مسائل فنية لا يقوى على فهمها إلا الخبير المتخصص، بعكس الدليل القولي فإن الكثير ممن يتصلون به يسهل عليهم فهم مضمونه وإدراك حقيقته. وإذا كان الدليل الناتج عن الجرائم التي تقع على العمليات الإلكترونية قد يتحصل من عمليات فنية معقدة عن طريق التلاعب في نبضات وذبذبات الكترونية وعمليات أخرى غير مرئية، فإن الوصول إليه وفهم مضمونه قد يكون في غاية الصعوبة.

فالتبيعة غير المادية للبيانات المخزنة بالحاسب الآلي، والطبيعة المعنوية (الافتراضية) لوسائل نقل هذه البيانات تثير مشكلات عديدة في الإثبات الجنائي، ومثال ذلك أن إثبات التدليس والذي قد يقع على نظام المعالجة الآلية للمعلومات يتطلب تمكين مأمور الضبط القضائي أو سلطة التحقيق من جميع المعطيات الضرورية التي تساعد على إجراء التحريات والتحقق من صحتها للتأكد عما إذا كانت هناك جريمة قد وقعت أم لا. ومثل هذا الامر يتطلب إعادة عرض كافة العمليات الآلية التي تمت لأجل الكشف عن هذا التدليس . وقد يستعصى هذا الأمر فهما على مأمور الضبط القضائي لعدم قدرته على فك رموز الكثير من المسائل الفنية الدقيقة التي من خلال ثناياها قد يتولد الدليل المتحصل من الوسائل الإلكترونية.

كذلك فإن الكثير من العمليات الآلية للبيانات التي قد يقوم بها الحاسب الآلي بطريقة آلية دون الحاجة إلى عمليات إدخال كما هو الحال في احتساب الفائدة على الايداعات البنكية والتي تقيد آليا بأرصدة حسابات العملاء على ضوء الشروط المتفق عليها مسبقا والمخزنة في برنامج الحاسب، قد يكون من السهل إختراقها وإرتكاب جرائم تزوير واستيلاء تقع عليها عن طريق إدخال بيانات غير معتمدة في نظام الحاسب أو اجراء تعديلات في برامجه أو القيام بالتلاعب في البيانات المخزنة.

وبالنظر إلى أن طبيعة هذه العمليات يصعب ان تخلف وراءها آثار مادية ملموسة تكشف عنها، فإن ذلك سيزيد من صعوبة عمل المحققين الذين يعملون في حقل الجرائم التي تتمخض عن هذه العمليات الإلكترونية، فقد يستعصى عليهم فهم الأدلة المتحصلة عن هذه الوسائل بسبب تعقيدها وصعوبة الإهتداء إلى مرتكبي الجرائم الواقعة في سياق مثل هذه العمليات.

أيضا فإن فهم الدليل الموصل إلى اثبات الجرائم التي تقع على العمليات الإلكترونية بالوسائل الإلكترونية قد يزداد صعوبة، في تلك الحالات التي يتصل فيها الحاسب الآلي بشبكة الإتصالات العالمية، ففي مثل هذه الحالات فإن فهم مثل هذا الدليل يحتاج إلى خبرة فنية ومقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجوده واختيار افضل السبل لضبطه.

وبالنظر إلى أهمية الخبرة في فك غموض الجرائم التي تقع بالوسائل الإلكترونية، فإن ذلك يكشف لنا عن الأهمية المتزايدة لتدريب الخبراء القضائيين على تقنيات الحاسبات الآلية لتمكينهم من القيام بمهامهم في المسائل الإلكترونية الدقيقة وإعداد تقاريرهم الفنية فيها والتي تكون ذات اهمية بالنسبة لقضاء الحكم الذي غالبا ما يتخذ منها سندا يرتكن إليه في المسائل الفنية البحتة.

ويجب ان لا يغيب عن الذهن إن فهم الأدلة الفنية التي تتحصل من الوسائل الإلكترونية يتطلب أيضا تدريب جهات الضبط القضائي والتحقيق والقضاء على فهم طبيعة المعطيات التي تقع عليها الجرائم الإلكترونية، والعمل على المامهم بمكونات الحاسب الآلية وكيفية عملها ومعرفة اللغة التي تتعامل بها، والتي تعتمد على المختصرات خاصة وان الجرائم التي تقع باستخدام الوسائل الإلكترونية في الغالب ما تعتمد على رموز تكون معروفة عند اهل العلم والخبرة . ولقد جاء في توصيات المجلس الأوروبي الصادر في سنتي 1985 و 1995 بما يفيد ضرورة استحداث دوائر جديدة تضطلع بمواجهة جرائم الحاسب الآلي وتزويدها بالموظفين الأكفاء ذوي الخبرة والدراية العلمية بالإضافة إلى توفير الاجهزة والمعدات التقنية اللازمة لذلك.

5- مشكلات اجراءات الحصول على الدليل الإلكتروني:

لا تقف صعوبة إثبات الجرائم الإلكترونية عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها، وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة، فإذا كان من السهل على جهات التحري أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع والمساعدة فإنه قد يصعب عليها القيام بهذا التحري وبهذه الطرق بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية.

فلا شك أن المجرمين الذين يرتكبون جرائمهم بالوسائل الإلكترونية الحديثة يزيدون من صعوبة اجراءات التفتيش التي يتوقع حدوثها للبحث عن الأدلة التي قد تدبرهم باستخدام كلمات السر التي لا تمكن غيرهم من الوصول إلى البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال، وقد يلجأ هؤلاء المجرمون أيضا إلى دس تعليمات خفية بين هذه البيانات أو استخدام الرمز أو التشفير بالنسبة لها بحيث قد يستحيل على غيرهم الاطلاع عليها ويتعذر على جهات التحري والضبط الوصول إلى كشف افعالهم غير المشروعة.

كذلك فإن هناك معوقات كثيرة قد تعترض الحصول على الأدلة بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية، ومثال ذلك انه قد يتعذر اتخاذ اجراءات التفتيش لضبط هذه الجرائم عندما يكون الحاسب الآلي متصلا بحاسبات اخرى خارج الدولة، ويكون تفتيش هذه الحاسبات ضرورية لإمطة اللثام عما تشتمله من جرائم

ولا شك في ان اختلاف التشريعات فيما بين الدول فيما يتعلق بشروط قبولها للأدلة وتنفيذ بعض الإجراءات مثل التفتيش عبر الحدود ليثير مشكلات عديدة قد تعوق إتخاذ الإجراءات اللازمة لضبط هذا النوع من الجرائم العابرة للحدود . فعلى الرغم من أن ارهاسات الثورة التكنولوجية في مجال الإتصالات عن بعد قد افرزت العديد من الجرائم ذات الطبيعة الخاصة، فما زالت اجراءات البحث عن هذه الجرائم وضبطها تتم في اطار النصوص الاجرائية التقليدية التي وضعت لكي تطبق على الجرائم التقليدية التي تنص عليها القوانين العقابية، الأمر الذي سترتب عليه الكثير من المشكلات بالنسبة لضبط هذه الجرائم المستجدة ذات الكيان المعنوي والتي قد تتعدد اماكن ارتكابها داخل الدولة الواحدة، أو يمتد نطاقها ليشمل الكثير من الدول عبر شبكة الإنترنت، فيتعذر تبعا لذلك اتخاذ اجراءات جمع الدليل بالنسبة لها، أو قد تلحق عدم المشروعية بهذه الإجراءات.

ولذلك نجد أن بعض الفقه في ألمانيا يشكك في إمكانية الدخول إلى أنظمة تقنية المعلومات لدى الحاسبات الأخرى التي توجد بالخارج بغرض ضبط البيانات المخزنة بها لأنه بدون وجود اتفاق بين الدول المعنية ينظم ذلك، فإن اتخاذ مثل هذا الإجراء يعد خرقا لسيادة كل دولة على اقليمها ويخالف الاتفاقيات الثنائية الخاصة بإمكانية التعاون في مجال العدالة القضائية.

واتساقا مع ذلك فنجد أن هناك تشريعات قليلة قد نصت على قواعد خاصة بتفتيش مكونات الحاسبات الآلية، من ذلك المادة 251 من قانون الإجراءات الجنائي اليوناني ، والمادة 478 من القانون الجنائي الكندي . كذلك فإن القانون الإنجليزي الصادر في سنة 1990 والذي طبق اعتبارا من 29 أغسطس سنة 1990 نظم صراحة تفتيش مكونات الحاسب الآلي، فنص هذا القانون على أن الجرائم المدرجة في القسم الثاني والقسم الثالث والتي تشتمل على أفعال الدخول غير المصرح به على نظام الحاسب الآلي لتسهيل ارتكاب أفعال غير مشروعة عن عمد، أو التعديل غير المصرح به في نظام الحاسب عن عمد، والتي يعاقب عليها بعقوبة السجن لمدة لا تزيد على خمس سنوات، تجيز القبض على المتهم دون حاجة لإذن قضائي، كما تجيز تفتيش محل إقامة المتهم بحثا عن أدلة مادية تكون ذات قيمة في إثبات الجريمة محل القبض. ونجد أن القسم الأول من هذا القانون قد نص على تحريم أفعال الدخول غير المصرح به لنظام الحاسب دون ارتباط ذلك بجريمة أخرى وعاقب عليها بعقوبة الحبس لمدة لا تتجاوز ستة شهور. وبالنسبة لهذه الجريمة فإن إجراء التفتيش الذي قد يتخذ لضبطها لا يتم إلا بناء على إذن قضائي يكون مستندا إلى أسباب منطقية تفيد وقوع هذه الجريمة وبعد ثبوت أن هناك أدلة تتعلق بها ويمكن الحصول عليها في الأماكن الصادر بشأنها الإذن بالتفتيش . ويرجع رأي فقهي السبب في صدور الإذن بالتفتيش بالنسبة لهذه الجريمة البسيطة إلى الصعوبات والمشكلات الخاصة بكشفها وجمع الأدلة عنها.

كذلك فإن الكثير من الدول أجازت التنصت والمراقبة الإلكترونية للحاسبات الآلية، ففي فرنسا اجاز قانون 10 يوليو سنة 1991 فرض الرقابة على الإتصالات عن بعد بما في ذلك شبكات تبادل المعلومات . وفي أمريكا

تجوز الرقابة على الاتصالات الإلكترونية والتي تدخل عدادها شبكات الحاسب الآلي بشرط الحصول على إذن بالتفتيش من القاضي المختص ، وأما في كندا فإن القوانين العادية التي تنظم أعمال المراقبة الإلكترونية يمكن أن تطبق على أنواع عديدة من اتصالات الحاسب الآلي.

ولقد أثار الضبط الذي يترتب على أعمال التفتيش والذي يقع على مكونات وشبكات الحاسب الآلي مشكلات كثيرة، ذلك أن هذا الضبط وإن كان يتصور وقوعه بالنسبة لمكونات الحاسب المادية، وبالنسبة لشبكات الحاسب حيث يمكن رصد الاتصالات التي تتم خلالها وتسجيل محتوياتها إلا أن اتخاذها سيكون في منتهى الصعوبة بالنسبة لمكونات الحاسب المعنوية.

ولقد اختلف الرأي بشأن ضبط الأشياء المعنوية (الافتراضية) من مكونات الحاسب الآلي، فذهب رأي إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط "أي شيء" فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسب المحسوسة وغير المحسوسة بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسب الآلي لا بد أن يشمل "المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي". بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب.

وفي مقابل هذين الرأيين يوجد رأي آخر نأى بنفسه عن البحث عما إذا كانت كلمة "شيء" تشمل البيانات المعنوية لمكونات الحاسب الآلي أم لا، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي والذي يتطلب أن يقع الضبط على بيانات الحاسب الآلي إذا اتخذت شكلا ماديا.

ولذلك نجد أن القسم 94 من قانون الإجراءات الجنائية الألماني مثلا ينص على أن "الأدلة المضبوطة يجب أن تكون ملموسة"، وهي على هذا النحو تشمل ليس فقط نظم الحاسب بل أيضا الدعامات التي تحمل عليها البيانات. ويترتب على ذلك أن البيانات منفردة عن الدعامات لا تعد أشياء لكي يمكن ضبطها، ولكن إذا تم طبع هذه البيانات فإن مطبوعاتها تعد من الأشياء الملموسة وبالتالي يمكن ضبطها.

ويسير قانون العقوبات في رومانيا على ذات النهج، فطبقا لهذا القانون فإن ضبط الأشياء بالنسبة للحاسب الآلي يشمل الجوانب المادية، والتي منها البيانات المحملة على الدعامات كالأشرطة المغناطيسية أو الأقراص المدمجة، وأما البيانات ككيان معنوي فإنها لا تصلح للضبط . فإذا كانت البيانات ككيان معنوي يصعب ضبطها، إلا أنها إذا حملت على دعامات أو تم تفرغها في شكل مستندات أو سجلات فإنه يمكن ضبطها لأنها بذلك تكون قد تحولت إلى كيان مادي ملموس.

ويذهب رأي فقهي إلى أنه في تحديد مدلول الشيء بالنسبة لمكونات الحاسب الآلي يجب عدم الخلط بين الحق الذهني للشخص على البرامج والكيانات المنطقية وبين طبيعة هذه البرامج والكائنات، وإنما يتعين الرجوع في ذلك إلى تحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تعرف بأنها كل ما يشغل حيزا ماديا في فراغ معين وأن الحيز يمكن قياسه والتحكم فيه، وكانت الكيانات المنطقية أو البرامج تشغل حيزا ماديا في ذاكرة الحاسب الآلي ويمكن قياسها بمقياس معين، وانها أيضا تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها تعد طبقا لذلك ذات كيان مادي وتتشابه مع التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبيل الأشياء المادية.

ولقد ذهبت محكمة باريس الابتدائية إلى ذلك عندما قضت بأنه لا يوجد اختلاف في الطبيعة بين مستخرجات البرامج وبين البرامج المستغلة.

والرأي لدينا أن المشكلة التي تثيرها الجرائم التي تقع على الكيان المعنوي (الافتراضي) للحاسب الآلي تتعلق بإثبات الجرائم التي تقع عليها، فالضبط الذي قد يقع بسبب التفتيش لا يتصور وقوعه إلا إذا تبين أن هناك جريمة قد ارتكبت، ولذلك فإن الجرائم التي ترتكب على الكيانات المادية يسهل اكتشاف أمرها وضبطها، وأما الجرائم التي تقع على الكيانات المعنوية فإنه يصعب اكتشافها إذا ظلت على صورتها المعنوية في شكل نبضات أو ذبذبات، وأما إذا تحولت هذه الكيانات إلى مستخرجات أو مستندات أو سجلات فإنه يسهل الوصول إلى الجرائم التي ترتكب عليها.

وليس أدل على ذلك من أن سرقة التيار الكهربائي قد اعتبرها القضاء والفقه من قبيل الأشياء عندما وسع في مفهوم السرقة بحيث يمكن ان تقع على الشيء أو منفعة الشيء، وهي على هذا النحو لا يمكن أن تتمخض عنها جريمة سرقة إلا بوقوع الفعل المادي للسرقة المتمثل في اختلاس التيار الكهربائي بتمريره خارج العداد الذي يحصي كمية التيار الكهربائي المستهلكة، فلو لا هذا السلوك المادي لما أمكن اكتشاف هذه الجريمة والعقاب عليها تحت وصف السرقة.

وبتطبيق ذلك على الجرائم التي تقع على الجوانب المعنوية للحاسبات الآلية فإنه لا يمكن العقاب عليها إلا بوقوع السلوك المادي الذي به تقوم الجريمة. فإذا وقعت جريمة سرقة أو تبديد أو تزوير أو غش على هذه الكيانات المعنوية فإنه يصعب العقاب عليها إلا إذا ثبت التلاعب في هذه الكيانات المعنوية بشيء مادي ملموس يمكن الاستناد إليه للقول بتحقيق السلوك المادي الذي لا عقاب على أي جريمة إلا بتوافره، حتى ولو ثبت هذا التلاعب بعرض البيانات على شاشة الحاسب الآلي وتم اكتشاف السلوك غير المشروع من خلال هذا العرض.

فالبرنامج ككيان معنوي إذا تمثل في مصنف مبتكر، فإنه يخضع للحماية الجزائية المقررة لحق المؤلف، أما استعمال هذا البرنامج بواسطة الحاسبات الآلية المقررة لحق المؤلف، أمام استعمال هذا البرنامج بواسطة الحاسبات الآلية كأداة للتلاعب في المجالات التي يستغل فيها البرنامج وذلك بارتكاب جرائم سرقة أو احتيال أو غش أو تزوير فإن هذه الجرائم لا تكون واقعة على حق المؤلف الذي يحمي البرنامج ككيان ذهني مبتكر ومملوك لصاحبه، وإنما تكون واقعة على مجني عليهم آخرين هم الذين وقعت عليهم الأفعال التي يتحقق بها السلوك المادي لهذه الجرائم.

وكمثال على ذلك فإن من يصمم برنامجاً لبطاقة إئتمان ويقدمه لأحد البنوك لاستغلاله، فإذا وقع اعتداء على هذه البطاقة نفسها بتكرار تصميمها تحت مسمى آخر فإن ذلك يشكل إعتداء على حق المؤلف، وأما إذا استغل أحد الأشخاص هذه البطاقة في صرف كمية من النقود تزيد عن المثبت في رقم حسابه، فإنه يكون مرتكباً لجريمة تكون واقعة على البنك.

وليس أدل على ذلك من أن المشرع الفرنسي وبعيدا عن قانون حماية الملكية الفكرية قد عاقب على الأفعال غير المشروعة التي تقع على المعلومات المعالجة آليا وذلك في قانون العقوبات الجديد المعمول به منذ سنة 1994، فقد نصت المادة 323 من هذا القانون في فقراتها من الأولى وحتى الثالثة على تجريم الدخول أو الإبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، وتشدّد العقوبة على هذا الفعل إذا نتج عن الدخول أو البقاء محل أو تعديل المعطيات الموجودة داخل النظام أو إفساد وظيفته، وكذلك تجريم إفساد النظام لأدائه لوظيفته، وأيضا تجريم الإدخال غير المشروع لمعطيات في نظام المعالجة الآلية للمعطيات أو المحو أو التعديل غير المشروع للمعطيات التي يحتويها. ومن أمثلة الجرائم التي تقع على البرامج ويكون فيها اعتداء على حقوق المؤلف أفعال: النسخ غير المشروع، تغيير أصول البرامج وإزالة الأسماء عنها واستخدام أسلوب الهندسة المعكوسة، وكذلك فعل المشرع الأردني في المواد 3 و4 و5 من قانون الجرائم الإلكترونية.

6- تأثير قصور قانون العقوبات الموضوعي في مواجهة الجرائم الإلكترونية على قانون اصول المحاكمات الجزائية:

إذا كان التقنين العقابي للظاهرة الإجرامية في شكل جرائم محددة يقوم على مبدأ الشرعية والرغبة في تجنب التحكم وتوفير الحماية الفاعلة للفرد ضد المجتمع وحماية المجتمع من أنماط السلوك غير المشروع التي يرتكبها الفرد، فإن المشرع كان يجب عليه مواجهة الظاهرة الإجرامية التي نجمت عن ثورة الإتصالات بتقنين الجرائم التي افرزتها هذه الظاهرة وأيضا كان يجب عليه أن يطور النصوص الإجرائية بحيث تتسع للبحث عن هذه الجرائم وضبطها بما يتفق مع طبيعتها.

ولكن من الملاحظ أن المشرع في الكثير من الدول ومنها دول عربية تقاعس عن مواجهة الجرائم المستحدثة التي افرزتها المجالات الجديدة التي اتت بها ثورة المعلومات، وذلك على الرغم من أن الكثير من هذه المجالات لا يمكن أن توفر النصوص العقابية التقليدية الحماية الكافية لها.

ولقد ترتب على ذلك فراغ تشريعي لأن الواقع الحالي بعد ثورة المعلومات أصبح لا يستظل بالحماية القانونية الكافية التي تقيه شر الجرائم المتطورة التي قد لا تتفقد بنطاق المكان، وقد لا يكون محلها الأشياء المادية التقليدية التي تعارف الناس عليها، وقد ترتكب بوسائل مستحدثة ولا تترك وراءها أثارا مادية ملموسة.

وعلى الرغم من أن هذا القصور التشريعي قد أصبح واقعا ملموسا إذ قد كشف عنه كل من الفقه والقضاء، فإن هذا لا يحول دون الإجهاد في تفسير النصوص العقابية التقليدية التي تعاقب على صور الإعتداء المختلفة على المال بحيث يمكن تطبيقها على الجرائم المستحدثة التي أوجدتها ثورة الإتصالات عن بعد.

ولا شك أن التطور قد يوسع من دائرة المحال التي تحميها نصوص التجريم والعقاب بحيث يمكن أن ندخل في إطارها عناصر أخرى طالما أمكن اعتبارها من جنسها وأن المشرع يحميها بذات هذه النصوص. ولعل هذا الأمر يبدو واضحا بالنسبة لهذا النوع من الجرائم التي أثر المشرع أن ينص عليها في شكل أفكار عامة بحيث يمكن أن تندرج في إطارها أفعال أخرى تكون هذه الأفكار معبرة عنها وتحتوي ذات عناصرها القانونية، ومثال ذلك التجريم في جرائم القذف والذم وجرائم الإعتداء على الشرف. ويمكن أن تدخل الجرائم التي عبر المشرع عن محل التجريم فيها بالإعتداء على الأشياء في إطار هذا النوع من الجرائم.

وإذا كانت نصوص قانون العقوبات التقليدية لا تقوى في وضعها الراهن على مواجهة الجرائم التي تقع على المعلومات والبرامج بالنظر إلى طبيعتها المعنوية وذلك وفقا للرأي الذي ذهب إليه بعض الفقه على النحو سالف

الإشارة إليه، فإن هذا القول يعكس بالطبع على نصوص قانون اصول المحاكمات الجزائية إذ قد تعجز هذه النصوص أيضا عن إستيفاء الإجراءات اللازمة للتفتيش عن هذه الجرائم وجمع الأدلة بشأنها وفقا لطرق الإثبات التقليدية المقبولة جزائيا.

ولذلك فإن استخدام إجراءات علمية جديدة في البحث عن الحقيقة يكون ضد نزاهة الإنسان عندما تحتوي هذه الإجراءات على إكراه قد يقع على جسمه أو نفسه، وعند إستعمالها أيضا أستعمالا يكون فيه مكر وخداع كأستخدام وسائل التجسس المتطورة التي أفاء بها العلم على البشرية.

أيضا فإننا لا نستطيع غض الطرف عن تأثير الإجراءات العلمية الجديدة على الحياة الخاصة للأفراد، فالتقدم العلمي التكنولوجي المتمثل في الإنترنت سيكون أثره خطيرا على حرمة الحياة الخاصة، وسوف يزداد هذا الخطر مع الزيادة المتوقعة في استخدام الإنترنت . ولذلك نجد أن الكثير من التشريعات قد جرم الصور المستخدمة للاعتداء على حياة الإنسان الخاصة بإستخدام شبكة الإنترنت، فالمشرع الفرنسي قد جرم التسجيل غير المشروع للمعلومات الخاصة الإسمية، وكذلك فقد عاقب على الإفشاء غير المشروع لها . فلا يوجد شك في أن مبدأ إحترام كرامة الإنسان وشرفه، يعصم جسمه ونفسه من وسائل القسر العلمية، ويقيه مكر وخداع الإجراءات العلمية المستحدثة. ولذلك فإنه يكون محرما أن يكون جسم الإنسان حقلًا للتجارب العلمية، وكان غير جائز الحصول على الأدلة ضد إرادة الإنسان الحرة المختارة وذلك بالوسائل العلمية المستحدثة كالتنويم المغناطيسي وجهاز كشف الكذب.

ولعل ما سبق ذكره يظهر لنا مشكلة إثبات الجرائم الإلكترونية وصعوبة الوصول إلى الأدلة التي تثبتها وتسندها إلى مرتكبيها، ويفتح الباب أمامنا للحديث عن أهم الأدلة التي تطفو على السطح والتي تتحصل عن الوسائل الإلكترونية ويمكنها ان تثبت هذا النوع من الجرائم في إطار نظرية الإثبات الجزائي.

أدلة إثبات في الجرائم الإلكترونية وتقديرها في الدعاوى الجزائية

لقد شاع مع مولد ثورة المعلومات ظهور تعبير الجريمة المعلوماتية او (الاللكترونية)، حيث أن هذا النوع من الجرائم قد ولد مع هذه الثورة فهي بالنسبة له الأم والأب وهو بالنسبة لها الإبن. ولقد تعددت تعريفات هذه الجريمة ، بالنظر إلى أنها قابلة للتطور بتطور الوسائل الإلكترونية التي ترتكب بها ويتطور القيم والمصالح التي تعتدي عليها، وتتطور التشريعات التي تجرم وتعاقب على صورها المختلفة.

فذهبت آراء الفقهاء إلى تعريفها بأنها: الفعل غير المشروع الذي يساهم في إرتكابه الحاسب الآلي، أو هي: الفعل غير المشروع الذي يكون الحاسب الآلي أداة رئيسة في إرتكابه، أو هي كذلك: مختلف صور السلوك الإحرامي التي ترتكب باستخدام المعالجة الآلية للبيانات، أو هي أيضا: عمل أو إمتناع يأتيه الإنسان إضرارا بمكونات الحاسب وشبكات الإتصال الخاصة به، التي يحميها قانون العقوبات ويفرض لها عقابا . ولقد أضافت ثورة الإتصالات عن بعد بعدا جديدا متطورا للجريمة المعلوماتية بسبب التطور الهائل الذي لحق الوسائل الإلكترونية وتعدد استخداماتها في مناحي الحياة المختلفة، فعن طريق استخدام الشبكة الرقمية يمكن عن طريق ذات الطرق الحصول بنجاح على خدمات متعددة يمكن ان تختلف عن تلك التي يقدمها الهاتف كنقل البرامج عن طرق الحاسب الآلي.

ولذلك يمكن أن تعرف الجريمة الإلكترونية بأنها الفعل غير المشروع الذي يمس مصلحة أو حقا يتعلق بالمكونات المادية والمعنوية للوسائل الإلكترونية – أو أن هذه الوسائل تكون أداة في هذا المساس – ويكون المشرع قد قدر حمايتها بنصوص التجريم والعقاب بأن اعتبر الاعتداء عليها جريمة معاقب عليها وبجزاء جنائي. وإذا كانت الجرائم التي تقع على العمليات الإلكترونية ذات طبيعة خاصة فإن هذه الطبيعة تنعكس على ادلة إثباتها جنائيا بعد التطور الذي لحق طرق الإثبات لكي تفلت هذه الجرائم من العقاب عليها.

ولعل هذا الامر سيحتاج إلى مناقشته في إطار مذاهب الإثبات الجنائي التي تقوم بصفة رئيسة على حرية القاضي في الاقتناع، وهذا ما سنفصله بالبيان في هذا المبحث والذي سنقسمه إلى مطلبين نورد الأول لماهية أدلة الإثبات المتحصلة من الوسائل الإلكترونية ونتناول في الثاني تقديرها في إطار نظرية الإثبات الجنائي.

ماهية صور أدلة الإثبات المتحصلة من الوسائل الإلكترونية

من الملاحظ أن هناك تحولا كبيرا قد بدأ يظهر في وسائل الإثبات المقبولة قانونا خاصة في مجال الإثبات المدني، وذلك بفضل التطور الهائل الذي لحق الوسائل الإلكترونية، فبدأنا نسمع عن الوثائق الرقمية الجديدة

والتي ستحل محل الوثائق المطبوعة على الورق نظرا لأنها ستمدنا بطرائق جديدة . وبدأت بعض التشريعات في الاعتراف بالسندات الإلكترونية والتوقيع الإلكتروني لها، فصدر في فرنسا القانون رقم 230 لسنة 2000 في 13 مارس سنة 2000 والذي عدل نص المادة 1316 من القانون المدني لتأخذ في الاعتبار التطور الذي لحق بالسندات ويعتد بالسندات الإلكترونية والتوقيع الإلكتروني لها، فصدر في فرنسا القانون رقم 230 لسنة 2000 في 13 مارس سنة 2000 والذي عدل نص المادة 1316 من القانون المدني لتأخذ في الاعتبار التطور الذي لحق بالسندات ويعتد بالسندات الإلكترونية والتوقيع الإلكتروني لها.

كذلك فقد صدر في الأردن قانون المعاملات الإلكترونية رقم 15 لسنة 2015م ، والذي اعتد بالتوقيع الإلكتروني وعرفه أنه " البيانات التي تتخذ شكل حروف أو أرقام أو رموز أو اشارات أو غيرها وتكون مدرجة بشكل إلكتروني أو أي وسيلة أخرى مماثلة في السجل الإلكتروني، أو تكون مضافة عليه أو مرتبطة به بهدف تحديد هوية صاحب التوقيع وانفراده باستخدامه وتمييزه عن غيره". كما عرف السند الإلكتروني بأنه " السند الذي يتم إنشاؤه والتوقيع عليه وتداوله إلكترونياً".

كذلك فقد ظهرت أساليب جديدة للتوقيع بخلاف التوقيع الإلكتروني تفوق التوقيع التقليدي من حيث دلالتها القاطعة لنسبة السند إلى الشخص الذي صدر عنه، ومثال ذلك بصمات قزحية العين وهي الجزء الموجود خلف القرنية والذي يمنح العين لونها، وبصمة الصوت والشفافة إذ يمكن برمجة الحاسب الإلكتروني بحيث لا يصدر أوامره بفتح نظامه السري إلا بعد مطابقة كل هذه البصمات أو بعضها على البصمات المبرمجة في ذاكرته وبصمة الوجه الذي يعتمد العلامات الفارقة في الوجه ككل.

أيضا فقد خطت الكثير من التشريعات في الدول المتقدمة خطوات كبيرة في مجال الإثبات المدني والتجاري ونصت صراحة على إعطاء السندات الإلكترونية ومنها السندات المرسله عن طريق جهاز نقل الصورة بالهاتف "الفاكس" حجية متميزة في إثبات التعاقد الذي يتم عن طريقها ، أو عن طريق البريد الإلكتروني (الايمل) كما وأن التشريعات المعاصرة قد سايرت الثورة التكنولوجية التي أفرزت الحاسبات الآلية، فلكي تستفيد هذه التشريعات من التقنية الفنية العالية لهذه الحاسبات فقد تبنت خطة بموجبها اعترفت بإعطاء معطيات الحاسب الإلكتروني حجية السندات الورقية، وهي في ذلك تكون قد اعتنقت المفهوم الحديث لعناصر السندات الكتابية، والذي لا يحصر معنى الكتابة وفقا لمفهومها الحديث في السندات الكتابية الورقية فقط وإنما يدخل في معناها أيضا السندات الإلكترونية المرسله عن طريق التلكس والفاكس والإنترنيت والحاسب الإلكتروني . فهذه السندات الأخيرة التي ترسل عبر الإنترنت أو تحفظ على إسطوانات ضوئية أو ممغنطة قد تنشئ تصرفات قانونية تكون في حاجة إلى إثبات.

ولقد ساعد في اتساع هذا المفهوم للكتابة ، والاعتداد به في الإثبات المدني والتجاري تطبيق المفهوم الحديث للتوقيع والذي لم يعد يقتصر على التوقيع بخط اليد وإنما أصبح يشمل التوقيع الإلكتروني بالرموز أو بأي طريقة إلكترونية أخرى.

ولعلنا نلاحظ كذلك أن كثيرا من التشريعات الحالية لم يغفل عن السندات الإلكترونية التي تستخرج من شبكة الإنترنت والتي تصلح أيضا لإثبات مختلف التصرفات القانونية خاصة بعد أن اتسع نطاق استخدام هذه الشبكة في معاملات الأفراد، فأعطاهما إذا توافرت شروط معينة قوة الإثبات التي تتمتع بها المحررات الورقية المكتوبة وفقا للمفهوم التقليدي للكتابة، فالمفهوم الحديث للكتابة يخرجها من دائرة التحديد فلم تعد تنقيد بالمفهوم التقليدي للورق، وهي كشرط لصحة التصرف أصبح لا يقصد بها الكتابة التقليدية وإنما تعني سائر السندات الإلكترونية ومنها السندات المستخرجة من شبكة الإنترنت. ومن تطبيقات ذلك نجد أن القانون المدني الكندي منذ عام 1991 قد ساوى في الإثبات بين الأدلة الإلكترونية والأدلة الورقية المكتوبة . كذلك نجد أن المشرع الإنجليزي قد أصدر قانون الإثبات الجديد في سنة 1995 والذي قد عمل به اعتبارا من 1997/1/31، وقد وسع هذا القانون من نطاق الأخذ بالأدلة المستمدة من الشهادة السماعية، ووسع كذلك من نطاق المستخرجات فأصبحت تشمل تلك المسجلة بالصوت أو بالصورة الفوتوغرافية، وشرائط الفيديو والراديو والأفلام

وتجدر الإشارة كذلك إلى أن قواعد الإثبات الفيدرالية في الولايات المتحدة الأمريكية والتي تقبل مستخرجات وسائل التكنولوجيا الحديثة في الإثبات سواء تعلق الأمر بالحاسب الإلكتروني أو بالرسائل الإلكترونية أو الميكروفيلم أو بشبكة الإنترنت . ومما يضيف على السندات الإلكترونية قوتها في الإثبات الاعتراف بالتوقيعات الإلكترونية التي توقع بها هذه السندات، فهذه التوقيعات التي تتم عبر شبكة الإنترنت قد تكون أفضل بكثير من التوقيعات التقليدية، إذ أنها تتكون من أرقام تؤمن صحتها وقد يصعب تزويرها.

وإذا ولينا وجهتنا شطر الإثبات الجزائي نجد أنه قد تأثر كثيرا بثورة المعلومات خاصة بالطبيعة الخاصة للجرائم التي أفرزتها هذه الثورة، فقد جعلت هذه الطبيعة الإثبات الجزائي بوسائله التقليدية أمرا في غاية الصعوبة.

كذلك فإن الإثبات الجزائي يتأثر أيضا بالتطور الذي لحق بالإثبات المدني، إذ أن الكثير من مظاهر تطور الإثبات المدني والتي ترتب عليها الاعتداد بالسندات الإلكترونية في الإثبات يمكن ان تكون عناصر تكوينية في بعض الجرائم المنصوص عليها في القوانين العقابية. واتساقا مع ذلك فنقسم هذا المطلب إلى فرعين نورد الأول للتعريف بالدليل المتحصل من الوسائل الإلكترونية، ونتناول في الثاني صور هذا الدليل.

الفرع الأول

التعريفات بالدليل المتحصل من الوسائل الإلكترونية في الإثبات الجزائي

• أولا: التعريف بالدليل عموما:

الدليل هو أداة الإثبات عموما، ويقصد بهذا الإثبات القواعد المتعلقة بالبحث عن الأدلة وإقامتها أمام القضاء وتقديرها من جانبه للوصول إلى حكم بشأن الواقعة محل الإثبات. ويقصر الإثبات على إثبات الوقائع لا بيان وجهة نظر المشرع وحقيقة قصده، فالبحث في هذا يتعلق بتطبيق القانون وتفسيره وهو من عمل المحكمة. وينقسم الإثبات إلى نوعين، الإثبات بالأدلة المباشرة والتي هي الإقرار والشهادة والخبرة والمعاينة لمسرح الواقعة، والإثبات بالأدلة غير المباشرة والتي يصل القاضي إلى الحقيقة عن طريق الاستقراء والاستنتاج. وهذا الإثبات في نوعيه يخضع لمبدأ الإثبات الحر والذي يعتمد على حرية القاضي الجزائي في بناء قناعته الوجدانية

وهذا الدليل يمكن تعريفه بوجه عام بأنه: ما تنهض به الحجة لثبوت قضية. وفي القضاء يقصد به ما يستعين به القاضي في مجلسه لإثبات الواقعة ومدى صحتها لاقتناص يقين القاضي بوجه الحق في الدعوى المعروضة عليه. وغاية الدليل الوصول إلى الحقيقة سواء أثبت وقوع الجريمة واسندها إلى المتهم بإرتكابها أم أثبت عدم إمكان إسنادها إليه. فأهمية الدليل في المواد الجنائية أهمية عظيمة لأنه هو الذي يناصر الحقيقة ويبين مرتكب الجريمة، وهو الذي يحول الشك إلى يقين. فالحقيقة في معناها العام تعني معرفة حقيقة الشيء بأن يكون أو لا يكون، وهذا لا يتحقق إلا بالدليل بحسبان أنه المعبر عن هذه الحقيقة.

والقضاء في الشريعة الإسلامية الغراء يحتاج إلى بيينة لإثبات الحق، وهذا ثابت بحديث رسول الله صلى الله عليه وسلم، فعن ابن عباس رضي الله عنهما أن النبي صلى الله عليه وسلم قال "لو يعطي الناس بدعواهم لإدعى ناس دماء رجال وأموالهم، ولكن اليمين على المدعى عليه"، وفي رواية أخرى للبيهقي بإسناد صحيح "البيينة على المدعي واليمين على من أنكر". ولا يغيب عن الذهن أن البحث عن الدليل يجب أن يتم في إطار الشريعة الإجرائية وفي إطار مبدأ أن الأصل في المتهم البراءة، فالحق في الدليل يجب ان يتركز على حماية كرامة وشرف الإنسان.

ولذلك فإن وسائل البحث عن الدليل تسير في ركب مبدئين الأول: الحرية في الوصول إلى الدليل وأما الثاني: الشرعية في الوصول إلى هذا الدليل.

• ثانيا: التعريف بالدليل المتحصل من الوسائل الإلكترونية:

إذا كانت الأدلة التقليدية تقوى بسهولة على إثبات الجرائم عامة، إلا أنها قد لا تقوى على إثبات الجرائم التي ترتكب بالوسائل الإلكترونية فهذه الوسائل سواء أكانت أداة في ارتكاب الجريمة أم كانت محلا لها تساعد على إخفاء الآثار التي تترتب عليها، مما يعوق الحصول على الأدلة التي قد تتحصل منها.

فنحن نعلم بأن سلطات جمع الاستدلالات والتحقيق قد اعتادت على أن يكون الإثبات ماديا تبصره الاعين وتدركه الحواس وتلمسه الأيدي واما في محيط الإنترنت وغيره من وسائل الاتصال المختلفة فإن المتحري أو المحقق لا يستطيع تطبيق إجراءات الإثبات التقليدية على المعلومات والتي تتميز بطبيعة معنوية. كذلك فإن الجرائم التي تقع على الوسائل الإلكترونية قد تحتاج إلى خبرة فنية متخصصة لكي يمكن البحث عن الأدلة التي تثبتها وذلك من خلال البحث في ذاكرة هذه الوسائل كالأقراص الصلبة وغيرها. أيضا فإن الوسائل الإلكترونية ذاتها قد تكون الأداة في ارتكاب الجرائم وهي بذلك تكون دليلا لإثبات هذه الجرائم. وليس يخاف أن هذا الإثبات سيكون محفوفًا بالمخاطر بالنظر إلى وجود خطر أو شبهة التحريف الإداري أو اللا إداري للأدلة التي يتمخض عنها هذا الإثبات. ويلاحظ كذلك أن الطبيعة المعنوية للمحركات الإلكترونية والتي لا يترك التلاعب أو الغش في محتواها أو فيما أعدت لإثباته أثارا ملموسة تشكل صعوبة كبيرة في عملية إثبات جرائم الغش والتزوير التي تقع على هذه المحركات.

ولا شك في أن الطبيعة الخاصة بإثبات الجرائم التي تقع على العمليات الإلكترونية تجعل الأدلة التي تتحصل منها ذات طبيعة خاصة لأن هذه الأدلة قد يغلب عليها الطابع الفني والعلمي مما يزيد من صعوبة الوصول إليها وإثبات توافرها. ولعل هذه الأمور تتطلب إلقاء الضوء على هذه الأدلة لأجل كشف طبيعتها وبيان تأثير هذه الطبيعة على تعريفها وهذا ما سنفصله بالبيان فيما يلي:

1- طبيعة الدليل المتحصل من الوسائل الإلكترونية:

لقد أثر التقدم العلمي على الواقع الذي يطبق عليه القانون، وأثر كذلك على القانون الذي يطبق على هذا الواقع. وهذا يترتب عليه - بالطبع - تطورا في الدليل الذي يربط بينهما لأنه هو أداة تطبيق القاعدة القانونية على واقعة محددة.

ولا شك في أن التطور الحالي الذي انعكس اثره على الأدلة يستند إلى الآثار الجديدة التي ترتبت على ثورة الاتصالات عن بعد والتي تمخضت عنها حقيقة علمية جديدة غيرت الكثير من المفاهيم التقليدية للقيم والمصالح التي يحميها المشرع الجنائي بنصوص التجريم والعقاب، مما ترتب عليه وجوب توفير الحماية لقيم ومصالح معنوية، والإعتراف بالحجية لمستندات غير مادية تتميز بطبيعة إلكترونية، خاصة بعد أن أصبح الكثير من الجرائم المستحدثة في مجال العمليات الإلكترونية يرتكب باستخدام الوسائل الإلكترونية المتقدمة.

فلا مرية أن التطور الحالي لثورة الاتصالات سينعكس اثره على الأدلة المتحصلة من الوسائل الإلكترونية بحيث يجعل الحقيقة التي ستولد منها تقترب إلى الحقيقة العلمية. وهذا يفرض علينا ونحن نقدر قيمة هذه الأدلة في الإثبات الجنائي ان نحاول تقريب هذه الحقيقة العلمية مع الحقيقة القضائية، بحيث أن الأولى تساعد الثانية في إثبات حقيقة وقائع محددة ومدى نسبتها إلى متهم معين.

ولعل مما قد يساعد في تحقيق ذلك أن التطور العلمي الحالي في نظام الوسائل الإلكترونية سواء على مستوى الأجهزة أو البرامج قد أضفى عليها مصداقية في مجال المعالجة الإلكترونية للمعلومات وذلك بفضل استخدام معالجات ميكرونية معقدة ودوائر ذات قدرة عالية من التكامل يمكن أن تضمن أو توفر للحاسبات الآلية هذه المصداقية، كما وأن الجيل الحديث من هذه الوسائل تم تزويده بأنظمة مراقبة متعددة تسمح بإكتشاف وتحليل أي خلل أو تلاعب بالنسبة للتشغيل أو في البرامج. كذلك فقد لحق التطوير تقنيات ذاكرة بعض أنظمة المعلومات عن طريق استخدام بعض أواسط التسجيل مثل إسطوانة الفيديو والكارت ذو الذاكرة، وهذا يضمن تسجيلات على درجة كبيرة من الدقة، فضلا عن أن هذه التقنية لا تقبل المحو أو التعديل ويمكن لها تسجيل كل عملية تتم من خلالها بما قد يؤدي إلى توافر الدليل عند المنازعة في ذلك.

وتجدر الإشارة إلى أن تأثير التطور العلمي لا يقف عند مضمون الدليل وإنما يمتد هذا التأثير كذلك إلى الإجراءات التي يترتب عليها الحصول على هذا الدليل، ولذلك فإنه يجب أن تكون هذه الإجراءات المتطورة ذات طبيعة مشروعة لكي تحافظ على شرعية الأدلة المتولدة منها.

وكتطبيق لذلك نجد أن محكمة النقض الفرنسية قد قبلت شرعية الدليل الذي نتج عن إجراء قامت به شركة تجارية تمثل في وضعها لجهاز فيديو مزود بكاميرا خفية في إحدى فتحات التهوية لكي لا يراها أحد وذلك لإكتشاف الأفعال غير المشروعة التي ترتكب بداخلها من المستخدمين بها. ولم تعتبر محكمة النقض أن هذا الإجراء فيه مساس بالحياة الخاصة وبالتالي فلم تهدر شرعيته

ولقد تطلب قضاء هذه المحكمة فيما يتصل بالمراقبة التليفونية بالوسائل العلمية المستحدثة بأن ذلك يتم وفقا للإجراءات التي نص عليها القانون والتي تحدد الطرق المشروعة للحصول على الدليل بما يضمن ابتعاد هذه الطرق عن المكر والخداع.

وهكذا نرى أن التطور العلمي الذي لحق بالوسائل الإلكترونية قد أثر تأثيرا كبيرا على الأدلة المتحصلة منها وعلى إجراءات الحصول عليها، فهذا التطور قد جعل أكثر هذه الأدلة يتميز بطبيعة غير مرئية بحيث يصعب الوصول إليها لأنها تكون نتاج تلاعب في رموز ونبضات وإلكترونيات، كما أنه قد زاد من صعوبة إجراءات الحصول عليها لأنه قد أمد الجناة بوسائل متطورة تمكنهم من إخفاء أفعالهم غير المشروعة كاستخدام كلمات السر والتشفير واستطلاع التلاعب في البيانات المخزنة، بل وإتلافها في الوقت الذي يرونه مناسباً وفي ثوان معدودة.

وعلى ضوء ذلك يمكن القول بأن الدليل المتحصل من الوسائل الإلكترونية يستمد طبيعته من ذات العمليات الإلكترونية التي نتج منها في حالة الإعتداء عليها بالأفعال غير المشروعة. ولذلك فهو يتخذ أيضا طبيعة إلكترونية بحيث قد يصعب عليه إلا باتباع إجراءات معينة يكون الغالب منها ذو طبيعة فنية. وليس أدل على ذلك من أن التلاعب في المستندات الإلكترونية لا يمكن كشفه بالطرق التقليدية وإنما قد يحتاج ذلك إلى أدلة إلكترونية قد تتحصل من الوسائل الإلكترونية ذاتها أو باستخدام التقنية العلمية المتقدمة التي يتعين اتباعها للوصول إليه.

كذلك فإن تقليد التوقيع الإلكتروني أو تزويره لا يمكن كشفه وفقا للطرق التقليدية المتبعة في ذلك بفحص الخطوط وغيرها، وإنما يلزم لذلك فك رموز وتشفيرات معينة لا يمكن الوصول إليها إلا باستخدام الوسائل الإلكترونية ذاتها.

أيضا فإن هناك أدلة إلكترونية قد ساعد في الحصول عليها استخدام الوسائل الإلكترونية مثال ذلك: استخدام أجهزة الرادار وكاميرات التصوير، وكاميرات الفيديو والسينومتر، والوسائل الحديثة في التصنت، والتسجيلات بمساعدة مسجلات الصوت والتي تستخدم في ضبط الكثير من الجرائم.

وتجدر الإشارة إلى أن الأدلة المتحصلة من الوسائل الإلكترونية قد تنتمي إلى أدلة الإثبات التقليدية وذلك إذا كانت نتاج شهادة أو اعتراف أو خبرة، فقد يمكن إثبات جرائم الإحتيال والسرقة والاختلاس في الجرائم الإلكترونية عن طريق الوثائق الأصلية المحفوظة بالميكروفيش أو بالشرائط الممغنطة أو بحافظات الأكواد أو بمخرجات الحاسب وسجلات التشغيل.

كما لا يغيب عن الذهن أن الطبيعة الخاصة بالأدلة الإلكترونية ستتعاكس - بالطبع - على الطرق التي من خلالها يتم الوصول إليها، بحيث أن الطرق التقليدية المتبعة في البحث عن الأدلة والوصول إليها لم تعد تصلح أو تكفي للوصول إلى الأدلة المتحصلة من الوسائل الإلكترونية، بل يلزم اتباع طرق جديدة تتناسب مع هذه الأدلة ويمكن باتباعها إثبات الجرائم التي تقع على العمليات الإلكترونية، وهذا ما سنفصله بالبيان، فيما يلي:

2- الطرق الحديثة للوصول إلى الدليل الإلكتروني وتأثيرها على قوته في الإثبات الجزائي:

من المعروف أن لكل عصر سماته وخصائصه، وسمات العصر الحالي الدخول في عالم ثورة الإتصالات عن بعد وما ترتب عليه من تغيير في نمط الحياة سواء كان ذلك على مستوى الأفراد أو الحكومات، فلقد أصبح التعامل اليوم يتم عن طريق الإلكترونيات التي لا تعتمد على الأشياء المادية المحسوسة وإنما تعتمد على النبضات والذبذبات والتشفيرات، فحلت النقود الإلكترونية محل النقود الورقية، وحلت الشيكات ووسائل الدفع الأخرى الإلكترونية محل الشيكات ووسائل الدفع الورقية، وحلت بطاقات الوفاء وبطاقات الإئتمان الإلكترونية مكان الدفع اليدوي وحلت البنوك الإلكترونية محل البنوك التقليدية، وأفل نجم الأوراق التقليدية وأرشيها ومستنداتها ويزغ بدلا منها نجم الحاسبات الآلية وما تتمتع به من مدخلات ومخرجات تتمتع بقدرات هائلة، وظهرت كذلك الحكومة الإلكترونية لكي تتعامل عن طريقها أجهزة الحكومة مع بعضها البعض، أو تتعامل الحكومة عن طريقها مع الأفراد.

ولا شك أن الأفعال غير المشروعة التي تترتب على مظاهر هذا التطور على النحو سالف الإشارة إليه لا بد أن تتصف بذات صفاته وتتخذ ذات طبيعته، ولذلك فلم تعد الجرائم التي ترتكب بالوسائل الإلكترونية والتي تقع على الصور المختلفة للعمليات الإلكترونية من نوع الجرائم التقليدية، وإنما قد أطلق الفقه عليها الجرائم المعلوماتية أو الجرائم الإلكترونية. ولا شك في أن كشف ستر هذا النوع من الجرائم الذي يرتكب بالوسائل الإلكترونية يحتاج أيضا إلى طرق إلكترونية تتناسب مع طبيعته بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقرووة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة. فتطوير الإثبات الجنائي بتطوير طرقه امر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم، لكي نمنع ما يمكن أن يقال من أن صعوبة هذا الإثبات قد يؤدي إلى عدم التجريم.

ولذلك فإن طبيعة الدليل تتشكل من طبيعة الجريمة التي يولد منها، فدليل التزوير مثلا يأتي من إثبات تغيير الحقيقة في المحررات التي يقع عليها، ودليل جريمة القتل العمد قد يولد من فحص الأداة التي استخدمت في القتل وطلقات الذخيرة التي إستعملت فيها، ويمكن تطبيق ذلك أيضا على أدلة إثبات الجرائم الإلكترونية، فإثبات جريمة الغش الإلكتروني أو التزوير في المحررات الإلكترونية أو التلاعب في الجانب المعنوي للحاسبات الآلية، يمكن أن يثبت بأدلة إلكترونية تكون ناتجة أيضا عن الوسائل الإلكترونية.

وإذا كان هناك بعض الأدلة التقليدية التي قد تصلح لإثبات الجرائم التي تقع باستخدام الوسائل الإلكترونية، إلا أنها تكون في حاجة إلى تطوير مستمر لكي يمكنها أن تتناسب مع الطبيعة الخاصة بهذه الجرائم. فالخبرة وعلى الرغم من أنها وسيلة إثبات من الوسائل التقليدية إلا أنها تصلح أيضا لإثبات الجرائم التي ترتكب بالوسائل الإلكترونية، ولكنها تتطلب لكي تقوى على ذلك أن يكون الخبير متمتعا بمستوى عال من العلم والمهارة الفنية التي تمكنه من أن يشق طريقه بنجاح في مجال الجرائم التي ترتكب بالوسائل الإلكترونية والتي تقع على العمليات الإلكترونية المختلفة.

كذلك فإن التفتيش يمكن أن تتطور طرقه بحيث لا تقف - فقط - عند ضبط الأدوات المادية المستخدمة في ارتكاب الجريمة أو ضبط جسم الجريمة الذي يحقق نموذجها القانوني، وإنما يمكن لهذه الطرق كذلك أن تتعامل

مع الجرائم التي ترتكب بالوسائل الإلكترونية، أو التي تقع على هذه الوسائل، فيمكن تبعا لذلك تسجيل البيانات المعالجة إلكترونيا بعد تحويلها من النبضات أو الذبذبات أو الإشارات أو الموجات الكهرومغناطيسية إلى أشياء محسوسة تسجل وتخزن على وسائل معينة، وعلى هذه الوسائل يرد التفتيش أو الضبط.

أيضا فإنه ليس بخافٍ علينا أن الطبيعة الفنية للكثير من الأدلة التي تتحصل من الوسائل الإلكترونية قد يجعلها محلا لفحص معلمي يقوم به خبراء، وهؤلاء الخبراء قد يتأثرون في عملهم بأراء شخصية لهم أو نتائج علمية قد تكون غير صحيحة، وهذا قد يترتب عليه تشويشا في الحقيقة التي يجب أن تتمتع بها هذه الأدلة، مما قد يضلل الاقتناع الذاتي للقضاة عندما ينظرون تقارير الخبرة.

فالحقيقة العلمية أو التكنولوجيا الزائفة يمكن أن تزيف الحقيقة التي تثبت من الأدلة الأخرى القائمة في الدعوى التي ينظرها القاضي وذلك إذا ائثرت في اقتناعه ولم يظن إلى زيفها، فتكون النتيجة المترتبة عليك فساد الحكم الذي سينتهي إليه. ومما قد يؤثر في صحة الدليل المتحصل من الوسائل الإلكترونية أيضا الإجراءات التي تتبع لأجل الوصول إليه، فإذا كانت هذه الإجراءات وليدة طرق غير مشروعة فإنه سيرتب عليها عدم شرعيتها ومن ثم بطلان الدليل المتحصل منها. فالإذن بتفتيش الحاسب الآلي لضبط جرائم تكون محلها الدعامات الإلكترونية للمعلومات المحفوظة به لا بد أن يصدر وفق إجراءات معينة، فإن لم تراعى هذه الإجراءات فإن الأدلة المتحصلة منها ستكون تبعا لذلك غير مشروعة.

فالمشرع وإن كان يحمي القيم والمصالح بنصوص التجريم والعقاب، فإنه في الوقت ذاته يحمي حريات الأفراد بالنصوص الإجرائية، ولذلك فإن الإجراءات الأولية التي تتبع لضبط الجرائم قد تكون غير مشروعة إذا أهدرت هذه النصوص الإجرائية لأنها تكون قد خالفت القيم التي يحميها النظام القانوني بهذه النصوص الإجرائية. ولا يغيب عن الذهن أن الجرائم التي تقع على الوسائل الإلكترونية قد ترتكب كذلك بسبب إختراق الجناة للأمن الإلكتروني للأنظمة والمعطيات الإلكترونية وتمكنهم عن طريق ذلك من الوصول إلى كلمات السر المدخلة على هذه الأنظمة وإرتكاب العديد من الجرائم عليها أو إدخال الفيروسات الضارة إليها.

فالجناة الذين يرتكبون هذه الجرائم قد يستطيعون الوصول إلى البصمة الإلكترونية التي تستخدم في تأمين المستندات وفي تأمين التوقعات الإلكترونية، وبذلك يمكنهم التلاعب في هذه المستندات وإرتكاب العديد من الجرائم عليها. أيضا فهؤلاء الجناة قد يتمكنون من الوصول إلى مفتاح الشيفرة لأنظمة الحاسبات الآلية سواء أكان هذا المفتاح سريا متماثلا أم كان خاصا غير متماثل، وبذلك يستطيعون التلاعب في الجانب المعنوي للحاسب الآلي وفي الشبكات الأخرى التي تربطه بالوسائل الإلكترونية الأخرى. ولا شك في أن الوصول إلى الجرائم التي ترتكب عن طريق إختراق الأمن الإلكتروني، يتطلب إتباع طرق علمية معينة بحيث يمكن إكتشاف مثل هذا الإختراق وجمع الأدلة التي تثبت وقوعه. وكتطبيق لذلك نجد أنه قد صدر في فرنسا القانون رقم 91 - 646 بتاريخ 10 يوليو 1991 لأجل حماية سرية الإتصالات التليفونية، فوفقا لهذا القانون لا يمكن الإعتداء على السرية إلا عن طريق السلطة العامة وحماية لمصلحة عامة وبإتباع الإجراءات المثبتة في القانون وفي نطاق الحدود التي تنص عليها.

3- تأثير طبيعة الدليل الإلكتروني العلمية والفنية على تعريفه:

الدليل الإلكتروني أو الرقمي الذي يعد الوسيلة لإثبات الجرائم التي ترتكب بالوسائل الإلكترونية أو التي تقع على هذه الوسائل، هو نتاج عمليات فنية وعلمية يكون الجناة قد سلكوها لأجل إرتكاب هذه الجرائم على النحو سالف الإشارة إليه.

فالجرائم التي ترتكب بالوسائل الإلكترونية في صورها الغالبة قد تقع بسبب الغش أو التزوير أو التحريف في البيانات المعالجة آليا عن طريق الحاسبات الآلية، سواء تمت هذه الأفعال أثناء إدخال هذه البيانات أو أثناء تخزينها أو أثناء إخراجها. ولذلك فإن الوصول إلى هذه الأفعال يحتاج إلى أدلة علمية وفنية يمكنها أن تثبت وقوعها وتسندها إلى المتهمين بإرتكابها.

والدليل الإلكتروني يعد دليلا متطورا لأنه نتاج وسائل إلكترونية متطورة وهو قابل للتطور في المستقبل على ضوء تطور هذه الوسائل، وهو كما سبق القول يمكن إعاقة الوصول إليه بالوسائل الفنية المستحدثة، كما وان طبيعته غير المرئية قد تعيق إثباته للجرائم التي يكون معد لإثباتها.

وأتساقا مع ذلك فإنه يمكن تعريف الدليل الإلكتروني أو الرقمي بأنه: الدليل الناتج عن استخدام الوسائل الإلكترونية في إرتكاب الأفعال غير المشروعة التي تقع على العمليات الإلكترونية، أو الذي ينتج عن الجرائم التي تقع على الوسائل الإلكترونية، أو الذي ينتج عن الجرائم التي تقع على الوسائل الإلكترونية ذاتها، والذي يتميز في الغالب في صورته بالطبيعة الفنية والعلمية تمشيا مع الطبيعة الفنية الخاصة التي تتميز بها الجرائم التي يكون معدا لإثباتها.

ويمكن القول بأن الأدلة الإلكترونية ستزداد أهميتها في الوقت الحالي وذلك بعد أن اعترف الكثير من التشريعات بالمحرمات الإلكترونية ومنحها حجبتها في الإثبات. واعترف أيضا بالتوقيع الإلكتروني في مجال البيانات المعالجة آليا عن طريق الحاسبات الآلية وشبكات الإنترنت، وأجاز كذلك التعامل ببطاقات الصرف الآلية. ومد حمايته الجنائية إلى الجانب المعنوي الذي تتكون منه الحاسبات الآلية معترفا بصلاحيته لأن يكون محلا لإرتكاب العديد من الجرائم عليه كجرائم السرقة والنصب وخيانة الأمانة والغش والإتلاف . وبتعريف الدليل الإلكتروني فإن الباب سينفتح للحديث عن بعض صورته، وهذا ما سنفصله بالبيان في الفرع الثاني من هذا المطلب.

الفرع الثاني

صور الدليل الإلكتروني المتحصل من الوسائل الإلكترونية

لا شك في أن الدليل سيظل خاضعا للتطور بتطور وسائل الحصول عليه، فكلما تطورت هذه الوسائل تطور هو أيضا ، ولذلك نرى أن التطور الذي لحق البحث العلمي قد انعكس أثره على الدليل، فبدأنا نسمع عن دليل البصمة الوراثية وأثره في التعرف على الجناة والذي يتم الحصول عليه عن طريق تحليل الحامض النووي DNA كذلك فإن العلم قد اعتد حديثا ببصمة قزحية العين وهي الجزء الموجود خلف العين ومنه تستمد لونها، واعتد أيضا ببصمة الصوت والشفافة واستخدام هذه البصمات كمفاتيح سر تستخدمه الحاسبات الآلية.

وليس هذا إلا قليلا من كثير ما زال أمره سرا عند علام الغيوب، فصدق قول الله سبحانه وتعالى في قرآنه المجيد (سنريهم آياتنا في الآفاق وفي أنفسهم حتى يتبين لهم أنه الحق أو لم يكف بربك أنه على كل شيء شهيد) ، وقوله سبحانه وتعالى: (ويخلق ما لا تعلمون) . فكلما أفاء الله بخيره على البشرية كشف لهم جزءا من نعمته فإن أحسنوا استخدامها زادهم من عطائه، وإن أسأوا استخدامها قتر عليهم بمزيد عطائه بعد أن جحدوا نعمة واضروا أنفسهم بأنفسهم وهم لا يشعرون.

ومما أفاء الله به على البشرية ثورة الاتصالات عن بعد والتي لو أنها أحسنت أستخدمها فستؤدي لها خدمات عظيمة في تسيير دفة الحياة على مستوى الأفراد ومستوى الحكومات، ولكن الإنسان المستفيد من هذه الثورة بحكم طبيعته البشرية وما يحمله من نفس أمارة بالسوء قد يستخدم هذا التقدم العلمي الجديد في ارتكاب جرائم وبأساليب متطورة مما يلحق الضرر بنفسه، وبغيره وبالمجتمع الذي يعيش فيه.

ولذلك نجد أن ثورة الاتصالات عن بعد قد أفرزت جرائم جديدة ذات طبيعة خاصة، وذلك بسبب الطبيعة الخاصة بالوسائل التي ترتكب بها هذه الجرائم، وبسبب أيضا الطبيعة الخاصة للقيم والمصالح التي تقع عليها هذه الجرائم، والتي تغير مضمونها بفضل التقدم العلمي فبدأنا نسمع عن البيانات المعالجة آليا والمستندات الإلكترونية والتوقيعات الإلكترونية والنقود الإلكترونية وبطاقات الصرف الإلكترونية والإدارة الإلكترونية. وإذا كانت الجرائم التي تقع بالوسائل الإلكترونية أو التي تقع على هذه الوسائل، قد تطورت من حيث طرق ارتكابها ومن حيث الإستفادة من التقنية العلمية في هذا التطور، فإن الدليل المتحصل منها التي قد تصلح لتطويرها بتطورها وذلك لكي يقوى على إثباتها، لأنه إن ظل تقليديا ومتخلفا فلن يقوى على هذا الإثبات، وسيترتب على هذا الأمر بالطبع تخلف قانون الإجراءات الجنائية وعدم تطور نصوصه بتطور النصوص الموضوعية للعقاب مما يلحق أشد الضرر بالمجتمع، والأفراد، وبالعدالة.

وليس المقصود بتطور الدليل اكتشاف أدلة جديدة، وإنما المقصود بذلك تطور طرق الحصول عليه يتفق مع طبيعة الجريمة التي يكون هذا الدليل أداة لإثباتها وإسنادها إلى مرتكبها. ولذلك نجد أن الدليل ذاته قد يكون دليلا قوليا وقد يكون دليلا فنيا، وقد يكون دليلا علميا وقد يكون دليلا كتابيا، وقد يكون دليلا قانونيا، وقد يكون دليلا مستخلصا من وقائع معينة وهو ما يسمى بالقرائن، وقد يكون إلكترونيا إذا كان متحصلا من وسائل إلكترونية.

ولا شك في أن التطور العلمي قد زاد من أهمية إثبات الجرائم التي تقع بالوسائل الإلكترونية بطرق حديثة للإثبات الجنائي بما يتناسب مع طبيعة هذه الجرائم وبما يتفق مع تطور الوسائل الإلكترونية التي ترتكب بها أو التي تقع عليها، خاصة بعد أن زاد هذا التطور من أهمية الإثبات بالقرائن وذلك بعد ان اتسع مجال الإثبات بها وكمثال لذلك: الإثبات ببصمة الأصابع، بالبصمة الوراثية، ببصمة الصوت، بالأثر الذي تخلفه الجريمة، بالانتقال إلى الأماكن وتفتيشها، وهناك قرائن أخرى من طبيعة تخالف ذلك كتلك التي تتعلق بسلوك المجني عليه قبل أو أثناء أو بعد الجريمة.

وإتساقا مع ذلك سنبين فيما يلي أهم طرق الحصول على الدليل الإلكتروني المتحصل من الوسائل الإلكترونية والتي تصلح أكثر من غيرها لإثبات الجرائم التي تقع بهذه الوسائل، ودون أن نتعرض في ذلك لأدلة الإثبات التقليدية:

• أولاً: الأدلة المتحصلة عن الوسائل الإلكترونية بطريق التفتيش:

لأجل ضبط الجرائم وجمع الأدلة بشأنها فإن سلطة التحقيق قد تلجأ إلى التفتيش لضبط الأدلة المادية التي قد تساعد في إثبات وقائعها وإسنادها إلى المتهم المنسوب إليه ارتكابها والتفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية فيقصد به: أنه إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جنائية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بإرتكابها. ويثير موضوع التفتيش الذي يقع على نظم الوسائل الإلكترونية مسائل عديدة للبحث: كمدى صلاحية الكيانات المعنوية في هذه الوسائل كمحل يرد عليه التفتيش، وحكم تفتيش الوسائل التي تتصل مع بعضها البعض وتقع في أماكن عامة أو خاصة، وضوابط هذا التفتيش والضبط.

مدى صلاحية الكيانات المعنوية في الوسائل الإلكترونية كمحل يرد عليه التفتيش:

إذا كان التفتيش كوسيلة إجرائية يستهدف الحصول على دليل مادي يساعد في إثبات الجريمة، فإن البعض قد تشكك في مدى صلاحيته للبحث عن أدلة الجريمة في الكيانات المعنوية للحاسبات الآلية، وهو ما حدا ببعض التشريعات بأن تنص صراحة على أن التفتيش يتم بالنسبة لجميع أنظمة الحاسب الآلي، ومثال ذلك قانون إساءة استخدام الحاسب الآلي في إنجلترا الصادر في سنة 1990 حيث نص على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي.

وهناك تشريعات أخرى قد أجازت تفتيش أي "شيء" أو اتخاذ أي إجراء يكون لازماً لجمع أدلة الجريمة، وعلى ضوء ذلك فإن تفتيش المكونات المعنوية للحاسبات الآلية يدخل في عداد الأشياء التي جاء النص عليها عاماً دون تقييد، ومثال لهذه التشريعات: المادة 251 من قانون الإجراءات الجنائية اليوناني التي تجيز لسلطة التحقيق أن تتخذ أي إجراء أو شيء يكون لازماً لجمع الدليل، ويفسر الفقه اليوناني عبارة "أي شيء" بأنها تشمل جميع بيانات الحاسب الآلية المادية والمعنوية سواء أكانت هذه البيانات مخزنة في حاملتها أم كانت معالجة آلياً في الذاكرة الداخلية.

وعلى هذا النهج نجد أن المادة 487 من القانون الجنائي الكندي تعطي للسلطة المختصة الحق في إصدار الإذن بضبط "أي شيء" ويفسر الفقه عبارة "أي شيء" بأنها تشمل المكونات المادية والمعنوية في الحاسبات الآلية. وكذلك نجد في القانون الأردني نص المادة 13 من قانون الجرائم الإلكترونية "مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضراً بذلك ويقدمه إلى المدعي العام المختص."

ولقد نظر الفقه في الكثير من دول العالم إلى مصطلح "الأشياء" التي ترد عليها جرائم الإعتداء على المال نظرة واقعية، بحيث أن هذا المصطلح لا يجب أن يظل جامداً عند معناه الحرفي وإنما التي قد تصلح أن يكون متضمناً لكل ما يصلح أن يكون من جنسه. ولذلك نجد أن بعض الفقهاء في فرنسا قد ذهب إلى أن برامج الحاسبات الآلية ذات كيان مادي ملموس يتمثل في نبضات وإشارات وذبذبات إلكترونية مغناطيسية أو كهرومغناطيسية. ويترتب على ذلك أنه يمكن تفتيش نظام معلومات الحاسب ووسائط أو أوعية حفظ وتخزين البيانات المعالجة إلكترونياً كالاسطوانات والأقراص والاشطرة الممغنطة ومخرجات الحاسب. ويدخل في هذا التفتيش أيضاً المحتويات المخزنة في الوحدة المركزية للنظام والتي يمكن عزلها ككيان قائم بذاته.

حكم تفتيش الوسائل الإلكترونية المتصلة مع بعضها البعض والتي تقع في أماكن متفرقة أو تقع في أماكن عامة أو خاصة:

من الخصائص التي تتميز بها الحاسبات الآلية أنها قد تتصل مع بعضها البعض داخل الدولة عن طريق الشبكة المحلية، أو قد تتصل بحاسبات أخرى تقع خارج الدولة عن طريق الربط الشبكي بين أجزاء العالم المختلفة . وفي حالة وقوع جريمة في نظم حاسب آلي يقع داخل الدولة يجوز بالنسبة لها إصدار الإذن بالتفتيش، فإن صدور هذا الإذن وفقا للضوابط القانونية ينفذ بالنسبة للحاسب الآلي الصادر بالنسبة له إذن التفتيش فقط، ويترتب على ذلك أنه إذا كان الحاسب المراد تفتيشه يتصل بحاسب آخر لم يصدر بالنسبة له إذن بالتفتيش، فلا يمكن أن يمتد إليه التفتيش حتى ولو كان يحتوي على جريمة، إذ يلزم في هذه الحالة أن يصدر إذن جديد بالتفتيش من السلطة المختصة بذلك قانونا

وقد لاحظ الفقه الألماني أنه في هذه الحالة قد يتمكن هذا الشخص من التخلص من البيانات المستهدف التوصل إليها عن طريق التفتيش والتي قد تكون مخزنة لدى هذا الشخص الآخر، ولذلك فقد ذهب البعض من هذا الفقه إلى أنه يمكن أن يمتد التفتيش إلى سجلات البيانات التي قد تكون في موقع آخر، واستند هذا الرأي إلى نص المادة 103 من قانون الإجراءات الجنائية الألماني.

ويلاحظ كذلك أن بعض الجناة قد يقومون بتخزين بياناتهم في أنظمة حاسبات آلية تقع خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعيدة ومستهدفين عدم إمكان الوصول إليها، وفي هذه الحالة فإن تفتيش هذه الحاسبات التي تقع خارج حدود الدولة لضبط جريمة تتصل بحاسبات آلية داخل الدولة أمر قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها، ولكن يمكن اتخاذ هذا الإجراء عن طريق اتفاقات خاصة تعقد بين الدول المعنية.

وكتطبيق لهذا الإجراء الأخير: فقد حدث في ألمانيا أثناء جمع إجراءات التحقيق عن جريمة غش وقعت في بيانات حاسب آلي، فقد تبين وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا وبين شبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها. وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات، فلم تتمكن من ذلك إلا عن طريق التماس المساعدة الذي تم بالتبادل بين الدولتين.

ولقد أدرك المجلس الأوروبي مشكلة التفتيش التي قد تثار بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية في أكثر من دولة فأصدر التوصية رقم R9513 والتي أكد فيها على وجود قصور على مستوى التعاون الدولي بالنسبة لإجراء التفتيش عبر الحدود .

أما عن تفتيش الحاسبات الآلية التي تقع في أماكن عامة كالحاسبات الشخصية التي يحملها الشخص خارج منزله، فإن تفتيش انظمتها لا يكون جائزا إلا في الأحوال التي يجيز فيها القانون تفتيش شخصه، بإعتبار أن تفتيش الشخص يشمل ذاته وكل ما في حوزته وقت هذا التفتيش وسواء أكان مملوكا له أم لغيره . وفي الحالة التي يكون فيها الحاسب الآلي المراد تفتيش نظمه داخل منزل أحد الأشخاص، فإنه تسري عليه القيود التي ينص عليها القانون بالنسبة لتفتيش مسكن المتهم أو تفتيش منزل غير المتهم.

ضوابط التفتيش الذي يقع على نظم ومكونات الوسائل الإلكترونية:

التفتيش إجراء من إجراءات التحقيق تصدره سلطة تحقيق مختصة بهدف جمع الأدلة عن جريمة تشكل جناية أو جنحة تكون قد وقعت بالفعل. وهو بالنسبة للوسائل الإلكترونية يتخذ ذات هذا التعريف ولكن محله يكون بالنسبة للجرائم التي تقع على الوسائل الإلكترونية بكياناتها المادية والمعنوية أو الجرائم التي تقع بواسطتها. وإذا كان هذا التفتيش لضبط أدلة جريمة تكون قد وقعت وأنه يمس حرية الأشخاص وحرمة مساكنهم ، فلا بد من توافر مجموعة من الضوابط يجب مراعاتها عند إتخاذها، ولذلك سنبين فيما يلي هذه الضوابط:

• أولا: سبب تفتيش الوسائل الإلكترونية:

لا محل للتفتيش بالنسبة للجرائم التي تقع على الوسائل الإلكترونية أو التي تقع بها، إلا إذا كانت هناك جريمة قد وقعت على هذه الوسائل، أو من هذه الوسائل، وأن تكون هذه الجريمة جناية أو جنحة، ومن أمثلة هذه الجرائم، الغش المرتبط بالحاسب الآلي: ويشمل الإدخال، الإتلاف، المحو، أو الطمس لبيانات أو برامج الحاسب الآلي، التزوير المعلوماتي: يتضمن الإدخال، الإتلاف، المحو أو الطمس للبيانات أو برامج الحاسب، الإضرار ببيانات وبرنامج الحاسبات: ويشمل المحو، الإتلاف، التعطيل أو الطمس غير المشروع لبيانات وبرامج المعلوماتية، تخريب الحاسبات: ويحتوي على الإدخال، الإتلاف، المحو، أو الطمس لبيانات وبرامج الحاسب، الدخول غير المصرح به: وهو الدخول غير المشروع لنظام معلوماتي أو مجموعة نظم، وأخيرا: الإعتراض غير المصرح به: وهو اعتراض غير مصرح به ويتم بدون وجه حق عن طريق استخدام وسائل فنية للاتصال.

فلكي يصدر الإذن بتفتيش الوسائل الإلكترونية لجمع الأدلة عن جرائم تعد هذه الوسائل محلا لها، فإن هذا التفتيش لا يكون صحيحا إلا إذا كانت الجريمة التي يراد جمع الأدلة عنها ذات جسامه معينة بأن تكون من قبيل

الجنايات أو الجرح، فيستبعد من نطاقها المخالفات، ولا يشترط أن تكون الجنحة معاقب عليها بالحبس في حدود معينة، وإنما يكفي أن تكون الواقعة محل التفتيش تتمخض عنها جريمة من نوع الجرح.

ويلاحظ أنه لا محل لإصدار الإذن بتفتيش الحاسبات الآلية إلا إذا كان المشرع قد نص على الجرائم التي تشكل إعتداء عليها في شكل نصوص التجريم والعقاب تطبيقاً لمبدأ شرعية الجرائم والعقوبات، وعلى النحو الذي فعلته الكثير من التشريعات المقارنة، وفعله المشرع المصري بالنسبة لبرامج الحاسب الآلي وقواعد البيانات سواء كانت مقروءة من الحاسب الآلي أو من غيره، إذ أنزل عليها حماية جنائية وجعل الإعتداء عليها يعد جريمة من نوع الجرح على النحو الذي نصت عليه المادتين 140 و 181 من القانون رقم 82 لسنة 2002 بشأن حماية حقوق الملكية الفكرية.

وكذلك فقد أنزل المشرع المصري حمايته الجنائية على البرامج وقواعد البيانات المتعلقة بالأحوال المدنية للمواطنين، والبيانات الفردية التي تقتضي إجراء احصاء للسكان وعلى النحو سالف الإشارة إليه. ولا يكفي لإصدار الإذن بتفتيش الوسائل الإلكترونية مجرد الإبلاغ بوقوع جريمة من قبيل الجناية أو الجنحة وإنما التي قد تصلح أن تكون قد تجمعت بالنسبة لها إمارات قوية تفيد وقوعها بما يبرر المساس بحرية الأفراد عند تفتيش اشخاصهم، أو بحرمة منازلهم عند تفتيش هذه المنازل.

والمعيار لإصدار الإذن بالتفتيش أن تكون الدلائل التي تجمعت حول الجريمة تدعو للاعتقاد المعقول بوقوعها سواء أكان من تجمعت حوله هذه الدلائل فاعلاً أصلياً لها أم يقف دوره الإجرامي عند الشريك. وتقدير هذه الدلائل متروك للسلطة التي تصدر الإذن بالتفتيش بشرط أن يكون تقديرها منطقياً ومتفقاً مع الواقع بحيث تكشف هذه الدلائل بجدية عن وقوع الجريمة محل الإذن بالتفتيش وأن هناك جانباً تنسب إليه.

ولقد عبر قانون الإجراءات الجنائية الأمريكي عن الدلائل الكافية باصطلاح السبب المعقول أو المحتمل، ونص على ذلك أيضاً التعديل الرابع للدستور الأمريكي فذكر بأنه لا يجب إصدار أوامر القبض أو التفتيش ما لم تكن بناء على سبب معقول. وفيما يتعلق بالجرائم التي تقع على الوسائل الإلكترونية ويصدر الإذن بالتفتيش لضبط أدلة تفيد في وقوعها فإنه يقصد بالدلائل الكافية بالنسبة لها مجموعة المظاهر والإمارات التي تكفي وفقاً للسياق العقلي والمنطقي أن ترجح ارتكابها ونيتها إلى شخص معين سواء أكان وصفه فاعلاً لها أم شريكاً.

وإذا كان الغرض من إذن التفتيش جمع الأدلة بشأن الجريمة التي تكون قد وقعت على الوسائل الإلكترونية أو عن طريق هذه الوسائل فإنه يلزم أن تكشف الإمارات القوية والقرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم وترجح إرتكابه للجريمة، ومثال ذلك وجود أدوات تكون قد أستعملت في إرتكاب الجريمة أو لضبط أشياء متحصلة منها أو مستندات إلكترونية أو دعامات تفيد في إمطة اللثام عنها.

فالإذن بالتفتيش الذي يقع على الوسائل الإلكترونية قد يصدر لجمع أدلة عن جرائم تكون قد وقعت على البرنامج أو الكيان المنطقي، أو نظام التشغيل، أو النظم الفرعية، أو البرامج والخدمات المساعدة أي كان شكلها أو دعاماتها المادية أو وعائها، أو على المستندات التي تكون متعلقة بهذا البرنامج أو الكيان المنطقي بما في ذلك البيانات المعدة للتسجيل أو المسجلة في ذاكرة الحاسب أو في مخرجاته أي كانت شكلها أو دعامتها أو وعائها، أو على السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات أي كان شكل هذه السجلات أو الدعامة المادية التي تجسدها، أو على السجلات الخاصة بعمليات دخول نظم المعالجة الآلية للبيانات كسجلات كلمات السر ومفاتيح الدخول ومفاتيح فك الشيفرة أي كان شكلها أو دعامتها أو وعائها.

وبالنظر إلى الطبيعة الفنية للجرائم التي قد تقع على الوسائل الإلكترونية فإنه يمكن الإستعانة في ذلك بمأموري الضبط ذوي الخبرة الفنية في هذا المجال بما يساعد في جمع الدليل بشأن هذا النوع من الجرائم. وقد يدق الأمر بالنسبة للتفتيش الوسائل الإلكترونية إذ قد يحتاج الأمر إلى معرفة كلمات السر أو مفاتيح الشيفرة التي تمكن من الدخول إلى نظمها والإطلاع على محتوياتها، وهو ما يثير مدى إمكانية الحصول عليها سواء من المتهم الذي تجمعت دلائل الجريمة ضده أم من غيره إذا كان عالماً بها، وهذا ما سنوضحه بالبيان فيما يلي:

**** مدى إلزام المتهم أو غيره بالبوح بأسرار الدخول على الوسائل الإلكترونية:**

أ- بالنسبة للمتهم الصادر بحقه إذن التفتيش:

يتمتع المتهم عبر مراحل الدعوى الجنائية بالحماية المقررة له بموجب مبدأ وجوب إفتراض براءته إلا أن يثبت العكس بالحكم الجنائي البات. ويترتب على ذلك أنه لا يجوز إجباره على تقديم دليل يدين به نفسه، بل له

الحق في الصمت إلا إذا كان كلامه دفاعا عنه. ويجب الا يفسر صمته بأنه إقرار منه بصحة الإتهام المنسوب إليه. ويترتب على ذلك أنه لا يجوز إجبار المتهم على كشف مفاتيح الدخول إلى نظم الوسائل الإلكترونية أو طباعة ملفات بيانات مخزنة داخل هذه النظم.

ب- بالنسبة لأشخاص آخرين لم يصدر قبلهم الإذن بالتفتيش:

يلاحظ بداية أن هؤلاء الأشخاص الذين يتعاملون مع الوسائل الإلكترونية بحكم طبيعة عملهم لا يعتبرون - بمطلق القول - شهودا وفقا لمدلول الشهادة كدليل إثبات في المواد الجنائية، والتي يقصد بها المعلومات الصادرة من شهود يكونوا قد شاهدوا بأبصارهم الجريمة لحظة وقوعها أو قد تجمعت لديهم أدلة تفيد في إثبات وقوعها. أما الشاهد بالنسبة للجرائم التي تقع في محيط الوسائل الإلكترونية فيقصد به صاحب الخبرة والتخصص في تقنية علوم الحاسب والذي تكون لديه معلومات جوهرية لازمة لإمكان الدخول في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة بداخلها. ويعد من هؤلاء الشهود: مشغلو الحاسبات، خبراء البرمجة، المحللون، مهندسو الصيانة والإتصالات ومديرو النظم.

وتفرض بعض التشريعات المقارنة التزاما قانونيا بالإدلاء أو بالإفصاح عن الشيفرات وكلمات السر أو المرور التي تلزم للدخول إلى نظم الحاسبات الآلية وذلك من خلال التزامه بالإجابة على الأسئلة التي تتعلق بها، ويقع عليه كذلك واجب المعاونة في طبع واستنساخ ما قد تستلزمه مصلحة التحقيق من ملفات بيانات مخزنة في ذاكرة الحاسب.

فالمشرع الإجرائي الفرنسي يلزم الشهود الذين يقع عليهم التزام قانوني بأداء الشهادة بالكشف عن الأكواد وكلمات السر بالنسبة للحاسبات الآلية، ولا يعفيهم من هذا الإلتزام إلا التمسك باحترام السر المهني. وعلى ضوء ذلك يمكن القول بأن الشاهد يلتزم بالنسبة للجرائم التي تقع في محيط الوسائل الإلكترونية بطبع ملفات البيانات المخزنة في ذاكرة الحاسب أو حاملات البيانات الثانوية، وأن يفصح عن كلمات المرور السرية وعن أكواد الشيفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة.

ولا شك في أن وجود الإلتزام القانوني الذي بموجبه يمكن مطالبة المهنيين والحرفيين من الشهود ومستخدمي الوسائل الإلكترونية بالإعلام عن المعلومات والبيانات الجوهرية التي في حوزتهم، ليمثل أهمية عظيمة في إمكانية جمع الأدلة التي ترتكب على هذه الوسائل، وأنه يلعب دورا وقائيا هاما إذ أن تطبيقه يمنع من ضبط النظام الشبكي بأكمله وعدم عزله عن البيئة المعلوماتية المحيطة به.

ولعل الطبيعة الخاصة بالجرائم التي تقع في محيط الوسائل الإلكترونية تتطلب تأهيلا فنيا خاصة بالنسبة لمأموري الضبط القضائي الذين يناط بهم ضبط هذه الجرائم وجمع الأدلة بشأنها وذلك لكي يمكنهم التعامل السليم مع مخرجات هذه الوسائل ومع دعائمها وبرامجها للحفاظ على سلامة الأدلة المتحصلة عنها من كل تلف أو مسح.

** ثانيا: محل تفتيش نظم الوسائل الإلكترونية:

يمكن أن يشمل تفتيش نظم الوسائل الإلكترونية كل مكوناتها المادية والمعنوية على النحو سالف الإشارة إليه. ويمكن أن يشمل التفتيش أيضا شبكات الإتصال الخاصة بها والأشخاص الذين يستخدمون هذه الوسائل، وتتكون المكونات المادية لهذه الوسائل من وحدة المدخلات ووحدة الذاكرة الرئيسية، ووحدة الحساب والمنطق، ووحدة التحكم، ووحدة المخرجات، ووحدات التخزين الثانوية، وأما المكونات المعنوية فهي عبارة عن برامج النظام وبرامج التطبيقات.

ويضاف إلى ذلك أن الوسائل الإلكترونية بمكوناتها المختلفة تستلزم لتشغيلها وجود مجموعة من الأشخاص أصحاب الخبرة والتخصص في مجال تقنية المعلومات وهم مشغلو الحاسب، خبراء البرمجة سواء كانوا مخططي برامج تطبيقات أم مخططي برامج نظم، والمحللين ومهندسي الصيانة والإتصالات، ومديري النظم المعلوماتية.

** ثالثا: شروط صحة الإذن بتفتيش نظم الوسائل الإلكترونية:

لكي يكون الإذن بالتفتيش صحيحا يجب ان يكون من أصدر الإذن مختصا بالتحقيق في الجريمة التي يصدر الإذن بشأنها، وهذا الإختصاص قد يتحدد بمحل الواقعة أو المكان الذي ضبط فيه الجاني أو بمحل إقامته. ويجوز ان تمتد بعض الإجراءات خارج هذا الإختصاص إذا استوجبت ظروف التحقيق ذلك بشرط أن يكون المحقق قد بدأ إجراءات التحقيق بدائرة اختصاصه المكاني.

ويلزم كذلك أن يكون المحقق مختصا بالإجراء الذي يتخذه، فلا يجوز له ندب مأمور الضبط القضائي لتفتيش غير المتهم أو غير منزله لأن هذا التفتيش يخرج عن إختصاصه.

ويجب لصحة إذن التفتيش الصادر في محيط الجرائم التي تقع على الوسائل الإلكترونية أو عن طريقها أن يكون من صدر له الإذن بالتفتيش من مأموري الضبط القضائي المختصين بذلك وظيفيا ومكانيا ونوعيا، ولا يشترط بعد ذلك التزام المحقق بנדب مأمور ضبط معين.

وإذا كانت الجرائم التي تقع بالوسائل الإلكترونية أو عليها ذات طبيعة فنية فإنه ينبغي توافر خبرة معينة في مأمور الضبط القضائي الذي يندب لتفتيش نظم الوسائل الإلكترونية لكي يتمكن من تأدية عمله وفي ذات الوقت يحافظ على سلامة الأدلة المتحصلة من الجريمة المعلوماتية ، ويشترط في الإذن بالتفتيش الصادر بالنسبة للجرائم التي تقع في محيط الوسائل الإلكترونية أن يكون مكتوبا ومحددا التاريخ وموقعا ممن أصدره، وان يكون صريحا في الدلالة على التفويض في مباشرة التفتيش، وان يتضمن من البيانات ما يحدد نوع الجريمة المطلوب جمع الأدلة عنها. ويجب كذلك تحديد محل التفتيش والذي قد يكون شخصا أو منزلا، وتحديد المدة الزمنية التي يراها المحقق كافية لتنفيذ الإذن.

ولا شك في أن تحديد محل التفتيش تحديدا دقيقا بالنسبة للجرائم الإلكترونية قد تكتفه بعض الصعوبة، ذلك أن تحديد كل أو بعض مكونات الوسائل الإلكترونية وإيرادها في إذن التفتيش وتحديدتها تحديدا دقيقا قد يستلزم ثقافة فنية عالية في تقنية الحاسب الآلي، فلا لا تتوافر للمحقق أو لمأمور الضبط القضائي . وإذا كانت الجرائم التي تقع في محيط الوسائل الإلكترونية تتميز بطبيعة فنية متأثرة في ذلك بالطبيعة الفنية للعمليات الإلكترونية، فإن هذا الأمر يزيد من أهمية الخبرة كإجراء مهم للحصول على الإدلة بالنسبة لهذا النوع من الجرائم، وهذا ما سنوضحه بالبيان فيما يلي:

**** ثانيا: الأدلة المتحصلة عن الوسائل الإلكترونية بطريق الخبرة:**

الخبرة هي بحث لمسائل مادية أو فنية يصعب على المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات، كفحص بصمات عثر عليها بمكان الحادث، أو مدى نسبة توقيع معين إلى شخص بعينه، أو تحديد سبب الوفاة في جريمة قتل عمد.

ولأجل الوقوف على الحقيقة في مثل هذه المسائل العلمية والفنية فإن المحقق أجاز له القانون أن يستعين بخبير متخصص في المسألة موضوع الخبرة، ويعد ندب المحقق للخبير إجراء من إجراءات التحقيق يقطع التقادم، وذات الشأن بالنسبة لإيداع تقرير الخبرة، لكن أعمال الخبرة ذاتها لا اثر لها على التقادم لأنها أعمال مادية.

وإذا ولينا وجهنا شطر ثورة الإتصالات عن بعد نجد أنها قد أتت بتقنيات علمية ذات طبيعة فنية متقدمة، وقد أفرزت هذه التقنيات جرائم ذات طبيعة فنية وعلمية معقدة، يحتاج جمع الدليل بالنسبة لها إلى بحث مسائل علمية وفنية، فالأدلة قد تكون غير مرئية ويلزم تحويلها إلى أدلة مقروءة، وقد تكن نتيجة تلاعب في حسابات معينة أو في نظم إلكترونية معينة بحيث يحتاج الكشف عنها إلى متخصصين لإثبات هذا التلاعب.

وقد يحتاج الأمر إلى عمليات فنية دقيقة لإمكان الدخول إلى أنظمة الوسائل الإلكترونية نتيجة إستخدام الشيفرات الكودات السرية. وإذا كان الهدف من الخبرة الوصول إلى الحقيقة في مسائل علمية وفنية ومادية فإنها لا تكون حكرا على سلطة التحقيق وإنما يحق للمحكمة أن تأمر بها.

وبالنظر إلى الطبيعة الخاصة بالجرائم الإلكترونية فإن إمطة اللثام عنها قد يحتاج إلى خبرة فنية قد تظهر الحاجة إليها منذ بدء مرحلة التحري عن هذه الجرائم، ثم تستمر الحاجة إليها في مرحلتي التحقيق والمحاكمة نظرا للطابع الفني الخاص بأساليب ارتكابها والطبيعة المعنوية لمحل الإعتداء.

**** وسنبين فيما يلي مجالات الخبرة بالنسبة للجرائم الإلكترونية:**

• مجالات الخبرة بالنسبة للجرائم الإلكترونية:

تتنوع العمليات الإلكترونية بإستخدام الوسائل الإلكترونية، فنجد أمثله لها في الأعمال المصرفية، وفي الإدارة الإلكترونية، وفي التجارة الإلكترونية، ولذلك فإنه يتصور تنوع الجرائم التي تقع على هذه العمليات وفقا لنوع الوسائل الإلكترونية المستخدمة في ارتكابها.

**** ومن أمثلة هذه الجرائم:**

أ- تزوير المستندات المدخلة في أنظمة الحاسبات الآلية أو الناتجة بعد المعالجة.
ب- التلاعب لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ البيانات او المعلومات.

ج- الدخول قصدا لبرنامج باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول اليه أو تغيير موقع الكتروني أو الغائه أو إتلافه أو تعديل محتوياته أو اشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح البرامج الأساسية أو برامج التطبيقات.

د- العث أثناء نقل وبث البيانات.

ولا شك في أن طبيعة هذه الجرائم تستوجب توافر شروط خاصة في الخبير الذي ينتدب لبحث مسائل فنية وعلمية بالنسبة لها.

• الشروط المتطلبة في الخبرة في مجال الجرائم الإلكترونية:

إذا كانت الوسائل الإلكترونية متعددة وأن شبكات الإتصال بينها متنوعة، كما وأن طبيعتها الفنية تجعلها موزعة على تخصصات فنية وعلمية دقيقة، فإن ذلك يستوجب من جهات التحقيق والمحاكمة أن تراعى ذلك عند اختيارها للخبير، فيجب أن تتيقن أنه تتوافر لديه الإمكانيات والقدرات العلمية والفنية في مجال التخصص الدقيق للحقل الذي يطلب منه بحثه، ولا يكفي في ذلك حصول الخبير على درجة علمية معينة وإنما يجب أن تتوافر لديه أيضا الخبرة العلمية التي تمكنه من اكتساب كفاءة فنية عالية . وبالنظر إلى الطبيعة الفنية والعلمية للخبرة في مجال الجرائم الإلكترونية فإنه يمكن تحديد هذه الخبرة في الموضوعات الآتية:

1. الإلمام بتركيب الحاسب وصناعته وطراره ونظم تشغيله الرئيسية والفرعية، والأجهزة الطرفية الملحقة به، وكلمات المرور أو السر وأكواد التشفير.
2. طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية، وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.
3. قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك أعطاب أو تدمير الأدلة المتحصلة من الوسائل الإلكترونية.
4. التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة.

وتجدر الإشارة إلى أنه وإن كان من المقرر أن المحكمة تملك سلطة تقديرية بالنسبة لتقدير الخبير الذي يرد إليها، إلا أن ذلك لا يمتد إلى المسائل الفنية فلا يجوز لها تنفيذها إلا بأسانيد فنية . تخضع للتقدير المطلق لمحكمة الموضوع، ومن ثم فلا تستطيع المحكمة أن تفندها وترد عليها إلا بأسانيد فنية قد يصعب عليها أن تشق طريقها فيها إلا عن طريق خبرة فنية أخرى.

وإذا كان البحث قد تعرض على النحو سالف الإشارة إليه لأهم طرق الحصول على الدليل بالنسبة للجرائم التي تقع في محيط الوسائل الإلكترونية والمتمثلة في إجراء التفتيش وطرق الخبرة، فإن الحديث لن يكتمل إلا بالتعرض لإجراء الضبط بحسبان أنه الوسيلة التي من خلالها يتم الوصول إلى الأدلة التي تثبت الحقيقة التي تبحث عنها الدعوى الجنائية، وهذا ما سنفصله بالبيان فيما يلي:

• ثالثا: ضبط الأدلة المتحصلة من الوسائل الإلكترونية:

لكي يحقق التفتيش غايته في جمع الأدلة عن الجريمة التي إرتكبت فلا بد من إيجاد وسيلة بموجبها يتم وضع اليد على شيء يتصل بها ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهذه الوسيلة تتمثل في الضبط والتي عن طريقها يتم الوصول إلى الأدلة التي تهدف إليها إجراءات الإثبات الجنائي.

والضبط بالنسبة للجرائم التي تقع على الوسائل الإلكترونية أو عن طريقها يشتمل على كل ما استعمل في إرتكابها أو أعد لهذا الغرض، كأجهزة نسخ وتسجيل برامج الحاسب الآلي، أجهزة ربط مع الشبكات الإلكترونية بما يسمى Modem ، أجهزة إختراق الاتصالات وتحليل الشيفرات وكلمات السر، كافة البرامج المقلدة

والمنسوخة، جميع أوراق النقد المزورة، المحررات الإلكترونية المزورة، التوقيعات الإلكترونية المزورة والملفات المعنوية التي تعد وسيلة لإرتكاب الجريمة. والضبط هنا يقصد به الضبط القضائي والذي يستهدف الحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة. والضبط قد يقع على مكونات الوسائل الإلكترونية وقد يكون محله أيضا المراسلات الإلكترونية، وسنفضل ذلك بالبيان فيما يلي:

1- ضبط الكيانات المادية والمعنوية في الوسائل الإلكترونية:

لقد سبق الحديث عن مدى خضوع الكيانات المعنوية في الوسائل الإلكترونية لإجراء التفتيش عليها، وقلنا بأن هناك تشريعات قد نصت صراحة على صلاحية هذه الكيانات لتكون محلا للتفتيش، وأن هناك جانبا من الفقه قد ذهب إلى صلاحية هذه المكونات كمحل يقع عليه التفتيش.

ولقد كان الرأي لدينا هو تأييد خضوع الكيانات المعنوية لإجراء التفتيش لأن لفظ "شيء" لا ينحصر عند مدلوله الضيق في الكيان المادي وإنما يشكل كل ما يدخل في جنسه وفقا للتفسير المنطقي الذي يفسر النص على ضوء المصلحة التي يحققها المشرع من ورائه. ويترتب على ذلك أن الشيء طالما يحقق منفعة أو مصلحة إقتصادية فإنه يكون محلا للحماية سواء أكان هذا الشيء من الكيانات المادية أو المعنوية. فالشيء إذا كان يمثل قيمة إقتصادية أو ذهنية فإنه يستحق الحماية الجنائية سواء أكان ذو طبيعة مادية أو معنوية، فليس بشرط أن الشيء لكي تتقرر حمايته ضد السرقة، مثلا أن يكون ذو قيمة مالية، فالسرقة تقع حتى ولو كان محلها أشياء ليست ذات قيمة مالية، كسرقة مستندات من قضية، أو سرقة أسرار صناعية أو تجارية. ولذلك نجد أن قضاء محكمة النقض الفرنسية وقبل تجريم المشرع لسرقة الطاقة بموجب نص المادة 2/311 من قانون العقوبات الفرنسي، ذهب إلى صلاحية التيار الكهربائي لقيام جريمة السرقة، وأيضا يمكن أن تقوم جريمة السرقة عن طريق الكمبيوتر.

وأیضا فقد ذهبت محكمة النقض المصرية إلى أن جريمة السرقة يمكن أن تقع على سرقة التيار الكهربائي، ويمكن أيضا أن تقع على خط التليفون. كما وأن فعل الإختلاس يمكن أن يقع على الأشياء المعنوية طالما كانت قابلة للتحديد كالمعلومات التي تحتويها دعوات مادية كالكتابة وشرائط التسجيل المغناطيسية.

وفي هذا المعنى قضت محكمة النقض الفرنسية بأن: "سرقة الأقراص المغناطيسية" الديسكات" يتضمن في الوقت ذاته سرقة محتوياتها المعلوماتية للفترة الزمنية التي تكون محملة بها. وبناء على ذلك فإن ضبط الأدلة المتحصلة من التفتيش يمكن أن يقع على الكيانات المعنوية في الوسائل الإلكترونية، ومثال ذلك أنه يمكن ضبط البيانات الإلكترونية أو قاعدة البيانات بمشتملاتها من ملفات وسجلات وحقول وسواء اتخذت برامج نظام أو برامج تطبيقات.

فإذا كان التفتيش ينتهي بتحديد موضع ومكان البيانات التي يستهدف الوصول إليها، فإن المعالجة التي تجري عليها لجعلها مرئية للإطلاع عليها وإثباتها، أو بإخراجها من الحاسب في صورة مستندات مطبوعة لا تعد تفتيشا عن أدلة الجريمة، ولكنها تمثل وصولا إلى هذه الأدلة ومن ثم تعد ضبطا لها.

وتجدر الإشارة إلى أن ضبط الأدلة المتحصلة من الوسائل الإلكترونية قد تكتنفه الصعوبة البالغة عندما يكون متعلقا بنظام آلي بأكمله، إذ أن هذا الأمر يحتاج إلى تعاون دولي لأجل إتمام هذا الضبط دون إعاقة سير النظام المعلوماتي.

وأما بالنسبة للمكونات المادية للحاسب الآلي فلا يثير ضبطها أي مشكلات، فيمكن ضبط الوحدات المعلوماتية الآتية: وحدة المدخلات بما تشمله من مفردات كلوحة المفاتيح وشاشة اللمس، نظم الإدخال المرئي، نظام الإدخال الصوتي، نظام الفأرة، نظام القلم الضوئي، نظام القراءة الضوئية للحروف، نظام قراءة الحروف المغناطيسية ونظام إدخال الأشكال والرسومات.

ويمكن أيضا ضبط وحدة الذاكرة الرئيسية سواء أكانت ذاكرة للقراءة فقط أم كانت للقراءة والكتابة معا، وضبط وحدة الحساب والمنطق بما تشمله من دائرة إلكترونية ومسجلات، وضبط وحدة التحكم، وضبط وحدة المخرجات وما تشتمل عليه من وسائل كالشاشة، الطابعة، الرسم والمصغرات الفيلمية، وضبط وحدات التخزين الثانوية بما تشمل عليه من أقراص مغناطيسية بنوعها المرن والصلب والأشرطة المغناطيسية.

ويلحظ كذلك أنه يمكن ضبط كافة الأدوات والمستندات التي تكون قد أستعملت أو تحصلت من الجرائم التي تقع على العمليات الإلكترونية، فيمكن ضبط الأوراق المالية المزورة، وقد تضبط هذه الأوراق بداخل الحاسبات الآلية، أو تضبط أدواتها بداخل نظم الحاسب كالأوراق المعدلة لذلك والأشرطة المغناطيسية وغير ذلك من وسائل التزوير، ويمكن أيضا ضبط المحررات الإلكترونية المزورة كمخرجات أو بيانات داخل ذاكرة الحاسب

الآلي، ويمكن كذلك ضبط عمليات الغش والاحتيال التي تتم بالنسبة لأنظمة الصرف الآلي للنقود طبقا لما هو مسجل من بيانات حقيقية داخل هذه الأنظمة.

وأياضا فإن الضبط قد يشمل الأشياء التي تكون قد تعرضت للتخزين أو للإتلاف على النحو الذي تكشف عنه الكيانات المادية والمنطقية للحاسبات الآلية. والضبط قد لا يقف عند المكونات المادية والمعنوية في الوسائل الإلكترونية وإنما يمكن أن يشمل المراسلات الإلكترونية والتي تتم عبر هذه الوسائل، وهو ما سنوضحه بالبيان فيما يلي:

2- ضبط المراسلات الإلكترونية:

على الرغم من أن ثورة المعلومات قد أسعدت الأفراد بما وفرتهم لهم من سبل الإتصال الحديثة والتي انعكس أثرها على مختلف مناحي حياتهم، إلا انها قد سببت لهم الكثير من الأضرار الشخصية، ليس فقط فيما يتعلق بالجرائم المستحدثة التي قد ترتكب ضدهم، وإنما كذلك بالنسبة لإنتهاك أسرارهم الشخصية عن طريق الوسائل الإلكترونية المتقدمة. ونظرا لصلة المراسلات بالحياة الخاصة للأفراد، نجد أن الدستور المصري قد اتفق مع الدساتير الأخرى وأنزل حماية دستورية على هذه المراسلات.

وعلى هدى هذه الحماية الدستورية نجد أن المشرع الإجرائي قد قيد سلطة التحقيق في ضبط المراسلات بأنواعها المختلفة، فاشتراط لذلك أن يكون إجراء الضبط مفيدا في ظهور الحقيقة. ولقد تدخل المشرع الفرنسي بإصدار القانون رقم 91 - 649 في 10 يولييه 1991 بشأن المراقبة القضائية للاتصالات التليفونية ونص على حرمة المراسلات التي يتم نقلها بطريق الهاتف أو غيره من وسائل الإتصال فلم يجد الرقابة عليها إلا عن طريق السلطة العامة وفي حالات الضرورة التي تبررها المصلحة العامة المبينة في القانون. والمختص بإصدار قرار المراقبة هو قاضي التحقيق (المادة 1/110) وله أن يندب مامور الضبط القضائي للقيام به. ولا يأذن بالمراقبة إلا إذا كانت هناك ضرورة تستوجبها ظروف كشف الحقيقة وكانت هناك استحالة في الوصول إليها بطرق البحث والتنقيب العادية (م1/100). وتطلب هذا القانون كذلك في الجريمة المراد ضبطها بهذه الوسيلة أن تكون جنائية أو جنحة معاقب عليها بالحبس الذي يزيد عن سنتين (م 2/100) وكذلك حدد ميعادا زمنيا للمراقبة مدته أربعة أشهر في حدها الأقصى وتكون قابلة للتجديد. وأنه يتعين أن يتم التسجيل وتفريغ التسجيل تحت سلطة قاضي التحقيق ورقابته م (100).

ولا مرية أن الحماية التي يكفلها المشرع للمراسلات العادية لا يقتصر نطاقها على الصور المختلفة لهذه المراسلات، وإنما منطوق القول يحتم امتداد هذه الحماية إلى المراسلات الإلكترونية من باب أولى بحسبان أن الغاية من وراء هذه الحماية هي حماية الحياة الخاصة للإنسان بحماية مستودع أسرارته الشخصية، وهذه الأسرار الشخصية تكون أكثر انتهاكا إذا ما استخدمت الوسائل الإلكترونية في الوصول إليها، ومن ثم فإنها تكون في حاجة إلى حماية أكثر من تلك الحماية التي تحتاجها المراسلات في صورتها التقليدية.

وبناء على ذلك فإن الحماية التي يقرها الدستور والمشرع العادي للمراسلات العادية تمتد إلى سائر صور المراسلات الإلكترونية المستحدثة كالتراسل باستخدام أجهزة "الفاكسيميل" الناقلة للنصوص والأشكال والرسومات طبقا لأصولها أو باستخدام "البريد الإلكتروني"، أو بغيرهما من الوسائل التي قد يكشف عنها العلم في المستقبل، طالما كانت هذه الأجهزة أو الأنظمة تابعة لهيئة البريد أو متعهد تعهد إليه بذلك، وكان موضوع الضبط أو المراقبة أو الإطلاع تسجيلات إلكترونية محفوظة لمراسلات تمت، أو مراسلات تبث عبرها. وسنبين فيما يلي ضبط المراسلات الإلكترونية بالنسبة للبريد الإلكتروني، والتصنت والمراقبة الإلكترونية لشبكات الحاسب الآلي.

أ- ضبط مراسلات البريد الإلكتروني Electronic Mail

يقصد بالبريد الإلكتروني استخدام شبكات الإنترنت في نقل الرسائل بدل من الوسائل التقليدية. وبالنظر إلى سهولة استخدامه فقد أصبح من أكثر وسائل الإنترنت شيوعا وإستخداما في الوقت الحالي.

ولعل من المسائل الهامة التي تتعلق بالبريد الإلكتروني وجوب المحافظة على سرية، وهو ما حدا بالمبتكرين لبرامجه بابتكار برامج تشفير خاصة به بحيث لا يمكن الإطلاع على أي رسالة إلا لمن يعرف هذه الشيفرة، ويمكن حفظ البريد الإلكتروني في صناديق بريد خاصة أو في ملف، أو نسخ الرسالة والإحتفاظ بها. ولقد ساعد ظهور التوقيع الإلكتروني في تسيير عملية التراسل عبر البريد الإلكتروني، فالبرنامج يقوم بتخزين توقيع المستخدم كرمز أو شيفرة ويضعه تلقائيا على كل رسالة.

وإذا كان مفهوم المستندات قد تغير اليوم فقد حلت المستندات الرقمية محل الكثير من الوثائق المطبوعة على الورق، فإن الرسائل الإلكترونية تعد مستندات، فالمستند أصبح مفهومه الذي يتفق مع ثورة الإتصالات عن بعد

كل أسلوب به تحدد فكرة معينة أو تعبير محدد من خلال كتابة ورقية أو كتابة إلكترونية، فالعالم يعيش اليوم - وبحق - عصر الثورة الرقمية، حيث صارت الكلمة والصوت والأشعة والصورة والمعلومات رقمية، حتى يمكن القول أنه قد صار للأرقام هيمنة كونية.

ولقد تم الاعتراف في الكثير من التشريعات للمستندات الإلكترونية بحجيتها في الإثبات وأنها تصلح لأن تكون محلا يقع عليه التزوير . فإذا كان محتوى المحرر قد أصبح يعبر عنه بلغة رقمية، فإن هذه اللغة هي التي حلت محل الكتابة، ومن ثم يصلح هذا المحرر الرقمي لتقوم به جريمة التزوير.

فالمستند الإلكتروني طالما عبر عن فكرة وكان في الإمكان قراءته وإدراك معناه وفهم مضمونه فإنه يعد محررا". ومن ثم فإنه يحوز الحجية وفقا لطبيعة الشخص المنسوب إليه إصداره ولمن وضع عليه توقيعه الإلكتروني.

وتجدر الإشارة إلى أنه بصدور القانون الفرنسي الجديد سنة 1994 فقد ألغيت المادتين 5/462 و 6/462 والذي جاء بهما القانون رقم 88/19 الصادر في 1988/1/5 بشأن تجريم غش المعلوماتية، وقد كانت المادة الأولى تنص على تجريم تزوير المستندات المعالجة آليا، بينما كانت الثانية تجرم استعمال هذه المحررات، وقد حلت محلها المادة 441 من الكتاب الرابع من قانون العقوبات، بحيث أضيف إليها تزوير المستندات المعالجة آليا واستعمالها وأصبح نص هذه المادة بعد تعديلها بأنه يعد تزويرا "كل تغيير بطريق الغش للحقيقة في مكتوب أو في أي دعامة أخرى تحتوي على تعبير عن الفكر"، وهكذا تطورت جريمة التزوير في المعلوماتية من مجرد جريمة تزوير المستندات المعالجة آليا فقط وإستعمالها إلى جريمة تزوير المستندات المعلوماتية وإستعمالها.

ويترتب على إعتبار الرسائل الإلكترونية التي تتم عن طريق البريد الإلكتروني بمثابة رسائل شخصية أنه يجب حمايتها بذات الحماية التي تتمتع بها المراسلات الورقية ومن ثم فلا يجوز التصنت عليها أو الإطلاع على الأسرار التي تحتويها إلا بذات الطرق التي تنص عليها قوانين الإجراءات الجنائية. فلا يستطيع المحقق إختراق صندوق البريد الإلكتروني أو الدخول على أنظمة الحاسب الآلي المخزنة به الرسائل البريدية الإلكترونية وضبطها إلا عن طريق إتباع الإجراءات المنصوص عليها في القوانين الإجرائية والتي تنظم ذلك على النحو سالف الإشارة إليه.

ب- التنصت والمراقبة الإلكترونية للشبكات الإلكترونية:

يقصد بمراقبة المحادثات التليفونية وتسجيلها أنها تعد إجراء من إجراءات التحقيق، يباشر في جناية أو جنحة وقعت، للبحث عن أدلتها ضد شخص قامت تحريات جديده على أنه ضالع في ارتكاب هذه الجريمة، أو لديه أدلة تتعلق بها، وأن في مراقبة أحاديثه التليفونية ما يفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية، وكانت الجريمة على درجة من الجسامه تستأهل اتخاذ هذا الإجراء "الإستثنائي" بأن كانت جناية أو جنحة يعاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر.

ولقد اختلف الفقه في تكييف إجراء المراقبة للمحادثات السلوكية واللاسلكية، فذهب رأي إلى أنها تعد تفتيشا وبالتالي تخضع لقيوده. وأستند في ذلك إلى أن هذه المراقبة تتفق مع التفتيش في أن الهدف منها البحث في وعاء للسر توصلنا إلى السر ذاته وإزاحة ستار الكتمان عنه بغرض ضبط ما يفيد في الوصول إلى الحقيقة. ولا أهمية هنا لوجود الكيان المادي لواء السر فيصح أن يكون ماديا يمكن ضبطه بوضع اليد عليه استقلالا، ويمكن أن يكون معنويا يتعذر ضبطه إلا إذا اندمج في كيان مادي، فالغاية من مراقبة المحادثات التليفونية هي البحث عن دليل معين وهي ذات الغاية من مراقبة المحادثات التليفونية من التفتيش.

ولقد ذهب رأي آخر إلى التفرقة بين التفتيش والمراقبة، وأعتبر الأول إجراء غايته العثور على الأدلة المادية وضبطها بوضع اليد عليها وحبسها لمصلحة العدالة، وأما الثانية فليس لها كيان مادي ملموس وأنها قد تؤدي إلى سماع سر للمتحدث ولكنه قولي يسمعه المتحدث ولا يلمس له كيانا، والقول بأن هذا الحديث يندمج في كيان مادي هو أسلاك التليفون أو شريط التسجيل لا يصح أن يفهم منه أن الحديث له كيان مادي يمكن ضبطه، فأسلاك التليفون أو التسجيل ليست هي الدليل ذاته وما هي إلا وسيلة أو أداة لسماع الحديث أو إعادته ويبقى الدليل المستمد منها حديثا غير مادي، حيث لا تتأثر طبيعته بوسيلة أو أداة الحصول عليه.

والرأي لدينا هو تأييد هذا الرأي الأخير، فالمشرع الإجرائي قد أفرد أحكاما خاصة لكل من التفتيش والمراقبة على المراسلات السلوكية واللاسلكية نظرا لإختلاف المحل الذي يقع عليه كل منهما، فالأخير يقع على حرمة الحياة الخاصة، بمطلق القول، أما الأول فقد يمس بالمصادفة هذه الحياة الخاصة حتى ولو تم على كيانات معنوية. ولذلك نجد أن المشرع قد أحاط المراقبة بضمانات تزيد عن تلك المقررة للتفتيش. فليس معنى أنه

يتصور وقوع التفتيش على كيان معنوي وأن المراقبة تتم دائما على كيانات معنوية أن نسوى بينهما من حيث تأثيرهما على حرمة الحياة الخاصة، فالذي لا شك فيه أن المراقبة تكون أشد وطأة في مساسها بحرمة الحياة الخاصة بما قد لا يتوافر بالنسبة للتفتيش.

وانطلاقا من أهمية حماية الحياة الخاصة نجد أن الدستور والمشرع العادي قد كفلا حماية خاصة للمراسلات السلكية واللاسلكية على النحو سالف الإشارة إليه فنظم سبل الرقابة عليها وحدد السلطة التي تملك ذلك والإجراءات التي يلزم اتباعها حيال هذه المراقبة.

وإذا كانت شبكات الحاسب الآلي تستخدم خطوط التليفون وتستعين في ذلك بجهاز معدل الموجات "Modem" والذي يستطيع تحويل الإشارات الرقمية المستخدمة بواسطة الحاسب إلى موجات تناظرية تنقل مع الموجات الصوتية خلال خطوط التليفون، وبذلك فإنه يتبين وجود علاقة بين المراسلات التي تتم بالطرق التقليدية وتلك التي تتم بالوسائل الإلكترونية بحيث يمكن القول أن هناك تنصتا ومراقبة إلكترونية تتم على شبكات الحاسب الآلي . ولذلك فقد أجازت بعض التشريعات هذا التنصت الإلكتروني، فالمشرع الفرنسي أجاز بقانون 10 يوليو 1991 سالف الإشارة إليه إعتراض الإتصالات عن بعد بما في ذلك شبكات تبادل المعلومات. وفي هولندا يجوز لقاضي التحقيق أن يأمر بالتنصت على شبكات إتصالات الحاسب إذا كان لغرض ضبط جرائم خطيرة، ويمكن ان تتم المراقبة أيضا على التلكس والفاكس ونقل البيانات

ولقد تفادى التشريع الفرنسي الصادر في 10 يوليو 1991 هذا النقص بأن نص على حرمة المراسلات التي يتم نقلها بطريق الهاتف أو غيره بأي وسيلة من وسائل الإتصال . وبإنتهاء الحديث عن إجراءات الحصول على الأدلة من الوسائل الإلكترونية وتحديد الأدلة التي ستحصل من هذه الطرق كالمخرجات الإلكترونية، والمستندات الإلكترونية والكيانات المادية والمعنوية وأنواع الغش والتزوير والإتلاف والتلاعب الذي قد تكشف عنه هذه الطرق، فإن الباب يفتح عن تقدير هذه الأدلة في إطار نظرية الإثبات الجنائي وهو ما سنفصله بالبيان.

تقدير الأدلة المتحصلة عن الوسائل الإلكترونية في إطار الدعاوى الجزائية

يسيطر على الإثبات الجنائي مبدأ حرية القاضي في الإقتناع، فالقاضي الجزائي يستطيع ان يستمد عقيدته من أي دليل يرتاح إليه وجدانه . وهذه الحرية التي يتمتع بها القاضي الجنائي ليست مقرررة لكي تتسع سلطته من حيث الإدانة أو البراءة، وإنما هي مقرررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجنائية. فاستنباط الحقيقة من هذا الدليل إنما يتم بمعرفة القاضي ومدى قدرته على الوصول إلى الحقيقة وما حباه الله من علم ومدى توافر حاسة القضاء لديه. ولذلك نجد أن القاضي الجنائي يتمتع دائما بدور إيجابي في الدعوى الجنائية

والقاضي وعلى الرغم من أنه يتمتع بالحرية في تكوين عقيدته إلا أنه يلتزم ببيان الأدلة التي إستمد منها اقتناعه، فليست الحرية أن نطلق له العنان لكي يقتنع بما يحلو له، وإنما هو حر - فقط - في استخلاص الحقيقة من أي مصدر مشروع. فهناك طرق للإثبات نص عليها قانون اصول المحاكمات الجزائية وهي التي تعتبر مشروعة وهي التي يجوز له استخلاص الحقيقة منها.

وعلى ضوء هذه الطبيعة الخاصة بالإثبات الجنائي سنتناول تقدير القاضي لأدلة الإثبات الإلكترونية في هذا المطلب والذي سنقسمه إلى فرعين نورد الأول: لمشكلات قبول المتحصلة من الوسائل الإلكترونية، و سنتناول في الثاني: تقدير هذه الأدلة في ضوء نظام الأدلة العلمية.

الفرع الأول

مشكلات قبول الأدلة المتحصلة عن الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي

بالنظر إلى الطبيعة الخاصة التي تتميز بها الأدلة المتحصلة من الوسائل الإلكترونية وما قد يصاحب الحصول عليها من خطوات معقدة، فإن قبولها في الإثبات قد يثير العديد من المشكلات، فكما تعلم أن مستودع هذه الأدلة هو الوسائل الإلكترونية، ولذلك فيمكن التلاعب فيها وتغيير الحقيقة التي يجب أن تعبر عنها.

ولذلك فإن المشكلات التي تثيرها هذه الأدلة ليس بسبب أنها قد تصلح لتكون طرق إثبات أم لا؟ وإنما المشكلة التي تتعلق بها تتحدد في: كيف نضمن مصداقية هذه الأدلة وأن تعبر بالفعل عن الحقيقة التي تهدف إليها الدعوى الجنائية.

أولا: مدى قبول تسجيلات ومخرجات الوسائل الإلكترونية كأدلة إثبات جنائية:

تذهب التشريعات المقارنة إلى قبول مصادر المعلومات الخاصة بالحساب الآلي أو المتحصل عليها من أنظمتها مثل مخرجات نظام المعالجة الآلية للبيانات والبيانات المكتوبة على شاشته، والبيانات المسجلة على دعائم ممغنطة أو المخزنة داخل نظام المعالجة كأدلة يقوم عليها الإثبات الجنائي.

وهذه الأدلة المتحصلة من الوسائل الإلكترونية تخضع للسلطة التقديرية للقاضي الجنائي، فإن استراح إليها ضميره ووجدتها كافية ومنطقية فيمكنه ان يستمد اقتناعه ويعول عليها في الحكم الذي ينتهي إليه.

ولقد أثيرت في فرنسا مشكلة الإثبات لمحاضر المخالفات التي تتم عن طريق جهاز السينموتير، وانتهى القضاء هناك إلى عدم اعتبار محاضر المخالفات المحررة بإثبات المخالفة حجة بذاتها في الإثبات، وإنما ذهب كل من الفقه والقضاء، إلى أن أي محضر لا تكون له قوة إثباتية إلا إذا أثبت فيه محرره وقائع تدخل في اختصاصه، وأن يكون قد شاهدها أو سمعها أو تحقق منها بنفسه، وبناء على ذلك فإن المحضر الذي يحرره عقب عملية المراقبة الإلكترونية للسيارات لا يصلح دليلا على ارتكاب الجريمة، حيث أن محرري المحضر لم يتحققوا بأنفسهم من ارتكاب المخالفة.

وإذا كان الضابط الذي يحزر المخالفة للقيادة بسرعة تزيد عن السرعة المقررة والتي يتم ضبطها عن طريق جهاز الرادار طبقا لقانون المرور المصري، لا يكون قد شاهد بنفسه المخالفة وإنما قام بتسجيلها فقط عن طريق الإشارة اللاسلكية التي تكون قد وصلت إليه، ولذلك فإن تقرير مخالفة المرور عن هذه المخالفة لا يمكن أن يحل محل محضر جمع الاستدلالات ولا يصلح لأن يكون دليلا قائما بذاته لإثبات المخالفة.

ولذلك يمكن القول بأن المخرجات المتحصلة من الوسائل الإلكترونية لا تمثل مشكلة في النظام اللاتيني حيث يسود مبدأ حرية القاضي الجنائي في الاقتناع، فالفقه الفرنسي يتناول حجية هذه المخرجات في المواد الجنائية ضمن مسألة قبول الأدلة المتحصلة عن الآلة أو ما يسمى بالأدلة العلمية والتي يجب ألا تقبل كطرق إثبات إلا إذا توافرت الشروط المقررة لذلك.

ويثير قبول الأدلة المتحصلة من الوسائل الإلكترونية مشكلات عديدة في ظل القواعد الأنجلو أمريكية للإثبات الجنائي، والتي تعتنق كمبدأ أساسي الإثبات بالشهادة التي تتعلق بالواقعة محل الإثبات. ولذلك فإن قبول المستندات المطبوعة لمخرجات الوسائل الإلكترونية والتي هي عبارة عن إشارات الكترونية ونبضات ممغنطة، يمثل مشكلة أمام القضاء في هذا النظام، إذ لا يمكن للمحلفين أو القاضي من مناظرة الأدلة المتولدة منها ووضع أيديهم عليها، وهذا يجعلها بمثابة أدلة ثانوية وليست أصلية.

ولقد صدر في إنجلترا قانون للإثبات الجنائي في سنة 1984 وعمل به بدءا من عام 1986 وقد نصت المادة 68 منه على أن: "يقبل الإثبات بالمحركات التي تتعلق بأي غرض من الأغراض إذا توافرت شروط معينة وهي:

- 1- أن يكون المحرر عبارة عن سجل أو جزء من سجل يعده الشخص بموجب واجب يقع على عاتقه ليثبت فيه معلومات مقدمه إليه من شخص آخر.
- 2- يمكن قبول إفتراض توافر علمه الشخصي بالأمر المتعلقة بها المعلومات.
- 3- ألا يكون الشخص التي تستقي منه المعلومات متاح وجوده أو ممكنا تعيينه أو تتبعه أو يكون غير متوقع منه تذكر الأمور المتعلقة بالمعلومات.

ولقد نصت المادة 69 من ذات هذا القانون على أن الناتج من الوسائل الإلكترونية لا يقبل كدليل إذا تبين وجود سبب معقول يدعو إلى الإعتقاد بأن هذا الناتج غير دقيق أو أن بياناته غير سليمة. ويجب كذلك أن يكون الحاسب الناتج منه المخرج الإلكتروني يعمل بكفاءة وبصورة سليمة.

ويلاحظ أن هذه التحفظات الأخيرة لا تطبق إلا إذا كانت مطبوعات الحاسب دليلا حقيقيا أو أصليا وليس مجرد نقل عن الغير. وتجدر الإشارة إلى أن مخرجات الوسائل الإلكترونية تقبل كوسائل إثبات في الولايات المتحدة الأمريكية وذلك بالنسبة للبرامج والبيانات المخزونة فيها، وبالنسبة للنسخ المستخرجة من البيانات التي يحتويها الحاسب.

وهكذا نرى أن الأنظمة القانونية المختلفة قد قبلت الأدلة المتحصلة من الوسائل الإلكترونية كأدلة إثبات، وإن كان النظام الأنجلو أمريكي قد أورد الكثير من الشروط لقبولها كأدلة إثبات نظرا لطبيعة هذا النظام والذي يعتمد في الأصل على النظام الإتهامي القائم على مبدأ التواجهية وإعلانه للإثبات بالشهادة وتحقيق الأدلة أمام القضاء. وعلى الرغم من التسليم بصلاحيته هذه الأدلة لتكون أدلة إثبات فإنها لا تصلح لتكون معبرة عن الحقيقة إلا إذا توافرت لها ذات الشروط التي يجب توافرها في أدلة الإثبات الجنائي بحسبان أنها تنتمي إليها، وسنبين فيما يلي هذه الشروط.

ثانياً: شروط قبول مخرجات الوسائل الإلكترونية كأدلة إثبات في المواد الجنائية:

إذا كانت الأدلة المتحصلة عن الوسائل الإلكترونية قد توجس منها كل من القضاء والفقهاء خيفة من عدم تعبيرها عن الحقيقة نظراً لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتزيف والتحريف والأخطاء المتعددة، فإنه ذلك قد تطلب وجوب توافر مجموعة من الشروط التي قد تضيء عليها المصادقية ومن ثم اقتربها نحو الحقيقة وقبولها كأدلة إثبات في المواد الجنائية. ولذلك فإنه لقبول هذه الأدلة كأساس تشديد عليه الحقيقة في الدعوى الجنائية سواء أكان الحكم الصادر فيها بالإدانة أم بالبراءة فإنه يلزم أن تتوافر فيها الشروط الآتية:

1- يجب أن تكون هذه الأدلة يقينية:

وهذا يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات، فلا محل لدحض مبدأ أن الأصل في الإنسان البراءة بالنسبة لهذه الأدلة إلا بتعيين مثله أو أقوى منه، وهذا يقين. ويترتب على ذلك أن كافة مخرجات الوسائل الإلكترونية من مخرجات ورقية أو إلكترونية أو اقراص مغناطيسية أو مصغرات فيلمية تخضع لتقدير القاضي الجنائي، ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والإحتمال.

والقاضي يمكنه أن يصل إلى يقينية المخرجات المتقدم ذكرها عن طريق: المعرفة الحسية التي تدركها الحواس من خلال معاينته لهذه المخرجات وفحصها، وعن طريق المعرفة العقلية عن طريق ما يقوم به من استقراء واستنتاج ليصل إلى الحقيقة التي يهدف إليها ويحبب أن يصدر حكمه أستناداً إليها.

2- يتعين مناقشة مخرجات الوسائل الإلكترونية تطبيقاً لمبدأ شفوية المرافعة:

فإذا كانت مخرجات الوسائل الإلكترونية تعد أدلة إثبات قائمة في أوراق الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم. ويترتب على ذلك أن هذه المخرجات سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسب. أما كانت بيانات مدرجة في حاملات، أم اتخذت شكل اشربة و اقراص ممغنطة أو ضوئية أو مصغرات فيلمية، تكون محلاً للمناقشة عند الإعتماد عليها كأدلة أمام المحكمة. فإذا كان القاضي الجنائي يحكم بإقتناعه هو وليس بإقتناع غيره، فإنه يجب عليه أن يعيد تحقيق كافة الأدلة القائمة في الأوراق لكي يتمكن من تكوين اقتناع بقربه نحو الحقيقة الواقعية التي يصبو إليها كل قاض عادل ومجتهد. ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم الإلكترونية إستناداً إلى علم شخصي له، أو إستناداً إلى رأي للغير، إلا إذا كان الغير من الخبراء وقد إرتاح ضميره إلى التقرير المحرر منه فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه، بحيث أن الاقتناع الذي يكون قد أصدر حكمه بناء عليه يكون متولداً من عقيدته هو وليس من تقرير الخبير.

ولقد ذهب جمهور الفقهاء الإسلامي إلى أن القاضي لا يجوز له أن يقضي بعلمه الشخصي، لأنه لا يجوز له أن يكون شاهداً في القضية التي يحكم فيها.

3- يجب أن تكون الأدلة المتحصلة من الوسائل الإلكترونية مشروعة:

من المقرر أن الإدانة في أي جريمة التي قد تصلح تبنى على دليل أخلاقي، وهذا يتطلب أن تكون الأدلة مشروعة أي أن الحصول عليها يكون قد تم وفق قواعد الأخلاق والنزاهة واحترام القانون، فمبدأ مشروعية الدليل الجنائي بالنسبة لمخرجات الوسائل الإلكترونية يتطلب ضرورة إتفاق إجراءات الحصول على هذه المخرجات بما يتفق والقواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر.

ويترتب على ذلك أن إجراءات جمع الأدلة المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها، فإنها تكون باطلة ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجنائية.

فمشروعية الدليل تتطلب صدقه في مضمونه، وان يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة وتدل على الأمانة والنزاهة من حيث طرق الحصول عليه.

ويجب التحوط بالنسبة لشرط شرعية الأدلة المتحصلة من الوسائل التكنولوجية في الحصول على الأدلة لأن هذه الأدلة قد تحتوي على حقيقة علمية تخالف الحقيقة القضائية التي تتطلب لقبول هذه الحقيقة العلمية أن يكون الوصول إليها قد تم بطرق مشروعة.

ومن امثلة الطرق غير المشروعة التي قد يتم من خلالها الحصول على أدلة تتعلق بالوسائل الإلكترونية، استخدام التعذيب أو الإكراه المادي أو المعنوي في مواجهة الجاني الذي يرتكب جريمة إلكترونية لكي يفك شيفرة أو يبيوح بكلمة السر . ويعد من قبيل هذه الطرق غير المشروعة أيضا: استخدام التدليس أو الغش أو الخديعة في الحصول على الأدلة المتحصلة من الوسائل الإلكترونية.

وفي إيطاليا نصت المادة 191 من قانون سنة 1989 على "عدم صلاحية الدليل الباطل للاستعمال". وهذا يفيد رفض الدليل غير المشروع سواء أكان هذا الدليل ينتمي إلى الأدلة التقليدية أم انه ينتمي إلى الأدلة المتحصلة من الحاسب الآلي.

الفرع الثاني

تقدير ادلة الإثبات المتحصلة عن الوسائل الإلكترونية في ضوء نظم الأدلة الجنائية

تتنوع نظم الأدلة الجنائية في الإثبات الجنائي، بين التي تأخذ بنظام الأدلة القانونية في الإثبات، وأخرى تعتنق نظام الإثبات الحر القائم على حرية القاضي الجنائي في الاقتناع، وتلك التي تجمع بين النظامين بما يسمى بالنظام المختلط.

ووجه الفرق بين هذه النظم أنه في نظام الأدلة القانونية يتقيد القاضي في الإثبات الجنائي بأدلة يحددها له المشرع مقدما ويقدر له قيمتها في الإثبات، فيتقيد القاضي بأن يستمد اقتناعه من هذه الأدلة دون غيرها. أما في نظام الأدلة الإقناعية فإن القاضي لا يقيد المشرع بأدلة إثبات معينة وإنما يترك له حرية الإثبات وفقا لسلطته التقديرية في تقدير الدليل: ويترتب على ذلك أن للقاضي الجنائي قبول أي دليل يمكن أن يتولد منه إقتناعه، وأنه هو الذي يقدر قدرته في الإثبات على قدر اقتناعه به.

وعلى الرغم من سيادة هذا النظام الأخير للإثبات الجنائي في جل التشريعات المقارنة، إلا أن البعض منها قد يطبق في إثبات بعض الجرائم نظام الأدلة القانونية وذلك عندما ينص المشرع على تقييد سلطة القاضي في الإثبات بأدلة معينة. ومثال ذلك إعطاء حجية للمحاضر المحررة في بعض المخالفات بالنسبة لما ورد فيها وقائع إلى ان يثبت العكس ، وتقييد سلطة القاضي في إثبات بعض الجرائم بأدلة معينة، ومثال ذلك نص المادة 276 من قانون العقوبات المصري إذ نصت على وسائل إثبات محددة لإثبات جريمة الزنا. وهذه الحجية وتلك القيود التي ترد على حرية القاضي في الإقتناع ليس المقصود منها افتراض ارتكاب المتهم للوقائع التي تنص على إعطائها الحجية ولكنها تعفي القاضي من إعادة التحقيق فيها، وبظل القاضي يملك سلطة تقدير هذه الأدلة ليستمد منها اقتناعه، وبظل المتهم معتصما بمبدأ افتراض براءته إلى ان يثبت عكس ذلك بالإدلة الكافية والمنطقية.

ويلاحظ كذلك أن نظم القانون العام في كل من إنجلترا والولايات المتحدة الأمريكية تضع تشريعات للإثبات الجنائي، كقانون الإثبات في المواد الجنائية الذي صدر في إنجلترا عام 1984 وعمل به ابتداء من عام 1986 فهذا القانون قد نظم طرق الإثبات بالنسبة لمخرجات الحاسب الآلي كأدلة إثبات في المواد الجنائية، وفي الولايات المتحدة الأمريكية فقد صدرت قوانين في بعض الولايات لتنظيم الإثبات الجنائي، فقد صدر في ولاية كاليفورنيا في عام 1983 تشريعا للإثبات وقد نص هذا التشريع على أن النسخ المستخرجة من البيانات التي يحتويها الحاسب تكون مقبولة بوصفها افضل الأدلة المتاحة لإثبات هذه البيانات، بل أنه في ولاية "أيووا" صدر قانون للحاسب الآلي في سنة 1984 نص على أن مخرجات الحاسب الآلي تكون مقبولة كأدلة إثبات بالنسبة للبرامج والبيانات المخزونة فيه.

وإذا كان التطور العلمي قد أفرز ثورة الإتصالات عن بعد والتي جاءت للبشرية بتكنولوجيا جديدة نراها في مختلف مناحي الحياة، كالتجارة الإلكترونية، وظهور الحاسبات الآلية، وشبكات الإتصال المختلفة، والإدارة الإلكترونية، والتحويلات المصرفية الإلكترونية، وظهور المستندات الإلكترونية، والنقود الإلكترونية، حتى يمكن القول أننا نعيش اليوم عصر الثورة الرقمية التي حلت بالنسبة لها الذبذبات والنبضات محل الأوراق والكتابة والتوقيعات التقليدية.

ولذلك، فإن السؤال الذي يطرح نفسه بالنظر إلى هذه الآثار التي ترتبت على ثورة الإتصالات عن بعد، هل سنشهد نظاما للإثبات الجنائي قد تفرزه أيضا هذه الثورة بحيث يعتمد الإثبات الجنائي على الأدلة العلمية الإلكترونية وتتقيد بالتالي سلطة القاضي في الإقتناع؟

*** تأثير ثورة الإتصال عن بعد على الإثبات الجنائي في الدعاوى الجزائية:

يمكن القول بأن التطور العلمي قد يؤثر بلا شك على نظام الإقتناع القضائي، فقد يعلى هذا التطور من تقارير الخبراء ، بالنظر إلى كثرة المسائل الفنية البحتة التي سوف تفرزها تطبيقات ثورة الإتصالات عن بعد، فهذا التطور قد يزيد من دور الخبرة في المسائل الجنائية، بالنظر إلى أن الكثير من الجرائم التي ترتكب كنتيجة لهذه الثورة ستقع على مسائل إلكترونية ذات طبيعة فنية معقدة، أو قد تستخدم هذه الوسائل في إرتكابها، وبالنظر إلى تطور مجالات الخبرة فإنه سوف تتسع مجالات اللجوء إليها.

كذلك فقد توفر التقنية العلمية طرقا دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في صنع الدليل، بحيث أن هذا الدليل قد يتمتع بقوة علمية يصعب إثبات عكسها. أيضا فقد يعلو شأن الإثبات بالقرائن كنتيجة لاتساع مجال الإثبات بها نتيجة تطور العلوم، ولقد أصبح هذا الأمر جليا واضحا في الإثبات بالبصمة الوراثية ، وببصمة الصوت، وبصمة قزحية العين وببصمة الشفاه. فالقضاء قد قبل الإثبات بالأدلة المتحصلة عنها عن طريق الرادار، التصوير، السينوموتر، كاميرات الفيديو، مسجلات الصوت، الوسائل الإلكترونية في التصنت.

ولا شك في أن ثورة الإتصالات عن بعد في تأثيرها على طبيعة الجرائم التي ترتكب كنتيجة لاستخدام تقنياتها العلمية ستزيد من تعقيد الدليل الجنائي وطرق الوصول إليه، بحيث أن ذلك قد يؤثر على الطرق التقليدية للحصول عليه فتعجز عن الوصول إلى الدليل الذي يكفي لإثبات هذا النوع الجديد من الجرائم. وهذا الأمر يتطلب أن يلحق التطور طرق الحصول على الدليل الجنائي بالنسبة لهذه الجرائم المستجدة لكي يمكن عن طريقها الوصول إليه.

كذلك فإنه يلاحظ أن الكثير من المسائل غير الجنائية التي تدخل عناصر تكوينه في الجرائم الجنائية ستزداد أهميتها كنتيجة لثورة الإتصالات عن بعد، فهذه المسائل قد تغير مفهومها التقليدي فأصبحنا نسمع اليوم عن الشيكات الإلكترونية، وهذا الأمر سيكون له تأثيره بالنسبة لجريمة الشيك بدون رصيد، ويكون إثباته معتمدا على مسائل فنية لإثبات الشيك كورقة تجارية.

وايضا فقد ظهرت الكيانات غير المادية التي قد تكون محلا لجريمة خيانة الأمانة، وهذا الأمر يتطلب البحث في توافر العقد المدني الذي تسلم الجاني هذا الكيان غير المادي بموجبه، فلكي يتم العقاب على هذه الجريمة في قانون العقوبات المصري "المادة 341" فيجب ان يكون المتهم قد تسلم المال بعقد من العقود المنصوص عليها في هذه المادة.

كذلك فإن الإحتيال الذي تقوم به جريمة النصب، قد تطور كنتيجة لإستخدام التقنية العلمية وأصبح هذا الإحتيال كثير الوقوع في العمليات الإلكترونية، وبالنظر إلى الطبيعة غير المرئية التي يتم بها فقد يصعب إثباته. وليس بخاف كذلك أن المستندات الورقية كمحل تقع عليه جرائم التزوير قد تغير مفهومها بسبب ثورة الإتصالات عن بعد، فقد ظهرت اليوم المستندات الإلكترونية وأصبحت هذه المستندات تصلح في الكثير من التشريعات لتكون محلا يقع عليه التزوير.

ولا شك في أن ظهور هذه المستندات الرقمية سيغير كثيرا من طرق الإثبات الجنائية بالنسبة للجرائم التي تقع عليها، ذلك أن الطرق التقليدية قد لا تقوى على إثباتها، ومن ثم فإن الأمر يحتاج إلى إثبات جنائي جديد يكون في استطاعته إثبات هذا النوع من التزوير، خاصة بعد أن ظهر التوقيع الإلكتروني وأصبح يتمتع بحجية في الإثبات في الكثير من التشريعات.

وهكذا نرى أن الثورة العلمية في الإتصالات لم تؤثر - فقط - في نوعية الجرائم التي ترتبت عليها وفي نوعية الجناة الذين يرتكبون هذه الجرائم وإنما أثرت تأثيرا كبيرا على الإثبات الجنائي وعلى طرق هذا الإثبات، بحيث يمكن القول أن طرق الإثبات التقليدية قد اصبحت عقيمة بالنسبة لإثبات الجرائم الإلكترونية، وأن الطرق العلمية والفنية للحصول على الدليل قد أصبحت هي المناسبة لإثبات هذا النوع من الجرائم.

وإذا كانت الغلبة بالنسبة لإثبات الجرائم الإلكترونية ستكون للإثبات بالقرائن والخبرة، فإن ذلك سيزيد من أهمية الدليل العلمي في الإثبات الجنائي، وفي ذات الوقت يزيد من أهمية دور القاضي في هذا الإثبات بحيث يظل القاضي متمتعا بسلطة تقديرية في تقدير هذه الأدلة بحسبان انها قد لا تكون مؤكدة على سبيل القطع ، أو قد تكون مجرد إمارات أو دلالات، أو قد يحوطها الشك، فهنا تظهر أهمية هذه السلطة التقديرية التي يجب أن يظل القاضي متمتعا بها، لأنه من خلالها يستطيع إظهار مواطن الضعف في هذه القرائن، ويستطيع كذلك تفسير الشك لصالح المتهم.

فلا مرية أن الدليل مهما تقدمت طرقه وعلت قيمته العلمية أو الفنية في الإثبات، فإنه يحتاج إلى قاض يتمتع بسلطة تقديرية، لأن هذه السلطة التقديرية تكون لازمة لتتقيد الدليل من الغلط أو الخطأ أو الغش ، وهي تكون ضرورية أيضا لكي تجعل الحقيقة العلمية حقيقة قضائية.

فالحقيقة تحتاج دائما إلى دليل ، وإذا كانت هذه الحقيقة قابلة للتطور، فإن الدليل الذي تقوم به التي قد تصلح
يتطور لكي يقوى على إثباتها، ويجب ألا يقف هذا التطور عند طرق الحصول على الدليل، بل يلزم أن يتطور
أيضا كل من يتعامل مع هذا الدليل من محققين وخبراء وقضاة، لأنه بهذا التطور الأخير تتطور الحقيقة القضائية
وتستطيع أن تجعل الحقيقة العلمية حقيقة عادلة.

واخر دعوانا ان الحمد لله رب العالمين