ضبط الأدلة فى الجرائم الإلكترونية
بين الإجراءات التقليدية والإجراءات الحديثة

هند نجيب*

تدور هذه الدراسة حول ضبط الأدلة فى الجرائم الالكترونية، والبحث فى مدى ارتباطها بالإجراءات التقليدية المتعارف عليها فى الجرائم العادية، ومدى احتياجها لإجراءات حديثة خاصة بها ستقتصر هنا على دراسة إحدى إجراءات الحصول على الدليل فى الجرائم الإلكترونية وهو "الضبط" وذلك من خلال الوقوف على الإجراءات التقليدية والإجراءات الحديثة التي تمكن من ضبط الأدلة في هذه النوعية من الجرائم وذلك للأهمية القصوى لهذا الإجراء وللصعوبات التي تواجه جهات الضبط القضائي وجهات التحقيق فى إتمام هذا الإجراء في الجرائم محل الدراسة، حيث إن نظام الحاسب الآلى يتكون من مكونات مادية وأخرى معنوية وهى البيانات والمعلومات، والضبط قد لا يقف عند المكونات المادية فى نظام الحاسب الآلى، وإنما يمكن أن يشمل المكونات المعنوية وكذا المراسلات الإلكترونية التى تتم عبر هذه الوسائل.

مقدمة

منذ العقد الأخير من القرن العشرين أصبح للجرائم الإلكترونية تأثيرات غاية فى السوء على الحياة العامة، وتحملت جميع الدول خسائر فادحة تصل إلى مليارات الدولارات وتتضاعف هذه الخسائر بمرور السنوات، رغم الجهود المبذولة لمكافحة هذه النوعية من الجرائم، وخاصة عقب ظهور الأدلة الإلكترونية وما صاحبه من مشكلات عديدة، ومما لا شك فيه أن الدليل فى الجريمة الإلكترونية يختلف تمامًا عن الدليل فى الجريمة التقليدية، وذلك من حيث كم البيانات المخزنة فى جهاز الحاسب وكيفية إثباتها، سواء من حيث وسيلة الإثبات أو القائم بالإثبات، وما إن كانت تتوافر لديه

* مدرس القانون الجنائى، المركز القومى للبحوث الاجتماعية والجنائية .

خبرة كافية فى هذا المجال من عدمه، ولذلك فالصعوبات التى تعترض إثبات وتحصيل الدليل الجنائى فى الجريمة الإلكترونية كثيرة ومتنوعة، منها ما يتعلق بالدليل الجنائى ذاته وهناك المشكلات التى تتعلق بموضوع الجريمة، وأخرى تتعلق بجهات الاستدلال أو الضبط القضائى أو التحقيق الجنائى فى هذه الجرائم، والحقيقة أن أسلوب الحصول على الدليل الإلكترونى فى هذه الجرائم محكوم بضابطين **الأول:** يتعلق بضرورة وجود قاعدة قانونية تقرر الإجراء القانونى الواجب إتباعه فى مثل هذه الجرائم مع مراعاة الطبيعة الخاصة لها، **والثانى** يتمثل فى ضرورة المعرفة الفنية والتأهيل المهنى والتقنى لرجال الضبط والتحقيق الجنائى والمحاكمة عند التعامل فى مثل هذا النوع من الجرائم[1]؛ وسوف تقتصر الدراسة على أحد إجراءات الحصول على الدليل فى الجرائم الإلكترونية وهو "الضبط" وذلك من خلال الوقوف على الإجراءات التقليدية والإجراءات الحديثة التى تمكن من ضبط الأدلة فى هذه النوعية من الجرائم وذلك للأهمية القصوى لهذا الإجراء وللصعوبات التى تواجه جهات الضبط القضائى وجهات التحقيق فى إتمام هذا الإجراء فى الجرائم محل الدراسة، حيث إن نظام الحاسب الآلى يتكون من مكونات مادية وأخرى معنوية وهى البيانات والمعلومات، والضبط قد لا يقف عند المكونات المادية فى نظام الحاسب الآلى وإنما يمكن أن يشمل المكونات المعنوية وكذا المراسلات الإلكترونية والتى تتم عبر هذه الوسائل، وحيث أن ضبط المكونات المادية لا يثير إشكالية قانونية وإنما الإشكالية تبدأ فى الظهور عندما يمتد الضبط إلى البيانات والمعلومات والأدلة الإلكترونية لتحديد مدى إمكانية ذلك. وكذلك إبراز أوجه الاختلاف فى إجراءات الضبط حال ارتكاب الجريمة الإلكترونية من خلال شبكة الإنترنت. والتى استفاضت فيها اتفاقية بودابست من خلال النص على إجراءات التحفظ واعتراض البيانات كما سنوضح فيما

بعد، وتتمثل الصعوبة فى هذه الحالات من الناحية التشريعية لعدم وجود نصوص خاصة بذلك فى العديد من التشريعات وخاصة العربية وعلى رأسها التشريع المصرى.

وتختلف طبيعة الضبط فى نطاق الجرائم الإلكترونية، فالضبط فى الجرائم الإلكترونية ينطوى على حالات مختلفة من حيث ظروفها وأحوالها، فهى تتطلب لإجراء الضبط بها تقنيات خاصة تغاير حالات ضبط الأدلة التقليدية. وسوف نتناول إجراءات الضبط من خلال ما يلى:

أولًا: الإجراءات التقليدية لضبط الجرائم الإلكترونية

تنص المادة (٥٥) من قانون الإجراءات الجنائية رقم ١٥٠ لسنة ١٩٥٠ "لمأمورى الضبط القضائى أن يضبطوا الأوراق والأسلحة وكل ما يحتمل أن يكون قد استعمل فى ارتكاب الجريمة أو نتج عن ارتكابها أو ما وقعت عليه الجريمة وكل ما يفيد فى كشف الحقيقة".

وتعرض هذه الأشياء على المتهم، ويطلب منه إبداء ملاحظاته عليها، ويعمل بذلك محضر يوقع عليه من المتهم، أو يذكر فيه امتناعه عن التوقيع.

يعرف البعض الضبط فى البيئة الإلكترونية بأنه "وضع اليد على الدعائم المادية المخزن فيها البيانات الإلكترونية أو المعلومات التى تتصل بجريمة من الجرائم الإلكترونية وقعت، وتُفيد فى كشف الحقيقة عنها وعن مرتكبها[٢].

ولم يتطرق قانون الإجراءات الجنائية المصرى إلى قواعد الضبط فى الجرائم الإلكترونية، مكتفيًا بالقواعد العامة للضبط فى الجرائم، وقد تناولت الاتفاقية الأوروبية (بودابست) أحكام الضبط فى الجرائم الإلكترونية من خلال المادة (١٩) فاستخدمت المصطلح التقليدى لهذا الإجراء (الضبط)، وأضافت إلى جانب ذلك عبارة الحصول بأية طريقة مماثلة على البيانات المعلوماتية للإشارة إلى أساليب أخرى مستحدثة

للضبط، فمصطلح الضبط يمكن أن يشمل المكونات المادية التى يمكن تخزين البيانات والمعلومات عليها، كما يشمل طرق الوصول أو التحفظ على نسخة من تلك البيانات والمعلومات بالإضافة إلى استخدام أو ضبط بيانات ضرورية من أجل الولوج إلى البيانات وضبطها، فمصطلح الحصول بطريقة مشابهة يشير إلى الأخذ فى الاعتبار الطرق الأخرى لرفع البيانات غير المادية والتى يسهل الوصول إليها، وبالتالى فإن سلطات الضبط يجب أن تتخذ ما يلزم اتخاذه من أجل الحصول على البيانات والمحافظة على سلامتها، فيجب أن تكون تلك البيانات متحفظًا عليها فى الحالة التى تم العثور عليها فيها لحظة الضبط، وعدم تغييرها من خلال ترميزها عن طريق أى وسيلة[٣].

والضبط بطبيعته وبحسب تنظيمه القانونى وغايته لا يرد إلا على الأشياء التى يكون لها صلة بالجريمة، وكذلك إذا كان الشىء المضبوط مملوكًا للمتهم أو لغيره، وقد يكون الضبط للمكونات المادية أو البيانات والمعلومات والأدلة المستخرجة من الحاسب. وبالتالى الضبط فى الجرائم الالكترونية قد يرد على المكونات المادية أو المعنوية أو كليهما.

١- ضبط المكونات المادية فى نظام الحاسب الآلى

بالنسبة للمكونات المادية للحاسب الآلى فلا يثير ضبطها أى مشكلات، فيمكن ضبط وحدات الحاسب الآلى الآتية: وحدة المدخلات بما تشمله من مفردات كلوحة المفاتيح وشاشة اللمس، نظم الإدخال المرئى، نظام الإدخال الصوتى، نظام القلم الضوئى، نظام القراءة الضوئية للحروف، نظام قراءة الحروف المغناطيسية ونظام إدخال الأشكال والرسومات.

ويمكن أيضًا ضبط وحدة الذاكرة الرئيسة سواًء كانت ذاكرة للقراءة فقط أم كانت للقراءة والكتابة معًا، وضبط وحدة الحساب والمنطق بما تشمله من دائرة إلكترونية ومسجلات، وضبط وحدة التحكم، وضبط وحدة المخرجات، بما تشتمل عليه من وسائل كالشاشة، الطابعة، الرسم والمصغرات الفيلمية، وضبط وحدات التخزين الثانوية بما تشتمل عليه من أقراص مغناطيسية بنوعيها المرن والصلب والأشرطة المغناطيسية[٤]. ويلاحظ كذلك أنه يمكن ضبط كل الأدوات والمستندات التى تكون قد استعملت أو تحصلت من الجرائم التى 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 أيضًا ضبط المحررات الإلكترونية المزورة كمخرجات أو بيانات داخل ذاكرة الحاسب الآلى، ويمكن كذلك ضبط عمليات الغش والنصب التى تتم بالنسبة لأنظمة الصرف الآلى للنقود طبقا لما هو مسجل من بيانات حقيقية داخل هذه الأنظمة[٥] وأيضا فإن الضبط قد يشمل الأشياء التى تكون قد تعرضت للتخزين أو للإتلاف على النحو الذى تكشف عنه الكيانات المادية والمنطقية للحاسبات الآلية.

٢- ضبط المكونات المعنوية للحاسب الآلى

على عكس ضبط المكونات المادية للحاسب الآلى؛ فإن الوضع بالنسبة لضبط المكونات المعنوية للحاسب الآلى أكثر تعقيدًا وتركيبًا- كما ذكر التقرير العام لمؤتمر A.I.D[٦].

فإذا كان الضبط يتم لمكونات الحاسب المادية كمحتوى للبيانات، فهل الشيء الذى يتم ضبطه هو هذا الشيء المادى؟ أم أنه يتضمن كذلك البيانات غير المادية؟ وما السند القانونى القائم عليه الضبط؟

وتعددت الآراء فى هذا الشأن وتشعبت فى اتجاهات مختلفة

الاتجاه المؤيد لضبط المكونات المعنوية ما ذهبت إليه المادة (٧٦-٣/١) من قانون الأمن الداخلى الفرنسى رقم ٢٣٩ لسنة ٢٠٠٣ من أن البيانات التى يتم الحصول عليها من تفتيش نظام الحاسب الآلى يتعين نسخها على دعامات، ثم يتم تحريز هذه الدعامات فى أحراز[٧] مختومة بالشمع الأحمر، وهذا الأمر شيء طبيعى كون فرنسا من الدول الموقعة على اتفاقية بودابست لعام ٢٠٠١، وقد تم النص فى المادة (١٩) من هذه الاتفاقية على أنه "من سلطة كل دولة طرف أن تتخذ الإجراءات التالية: أن تضبط نظام الحاسب أو جزء منه أو المعلومات المخزنة على أى وسيط من وسائط التخزين الخاصة بالحاسب الآلى، وأن تحافظ على سلامة تلك المعلومات المخزنة ومن التطبيقات التشريعية التى تجيز ضبط مكونات المعلوماتية من خلال ما تخوله بعض التقنينات الإجرائية، لسلطة التحقيق من إتخاذ أى إجراءات أو أى شيء لازم لجمع أدلة الجريمة والحفاظ عليها [٨]، المادة (٢٥١) من قانون الإجراءات الجنائية اليونانى[٩]، حيث تعطى سلطات التحقيق مكنة القيام بأى شيء يكون ضروريا لجمع وحماية الدليل.

ويفسر الفقه اليونانى عبارة أى شيء بأنها تشمل ضبط البيانات المخزنة أو المعالجة إلكترونيًا، ولذلك فإن ضبط البيانات المخزنة فى حاملات البيانات المادية أو فى الذاكرة الداخلية لا تسبب أية مشكلة فى اليونان، إذ بمقدور المحقق أن يعطى أمرًا للخبير بجمع البيانات، التى يمكن أن تكون مقبولة كدليل من المحاكمة الجنائية، كما

تجيز المادة (٢٦٠) من قانون الإجراءات الجنائية اليونانى استخدام القوة العسكرية فى الضبط فى حالات البنوك أو المؤسسات الخاصة والعامة ومن بين المستندات الأخرى التى تكون متعلقة بالجريمة، ولهذا فإن المحققين بمقدورهم أن يأخذوا البيانات المخزنة فى حاملات البيانات.

ولكن قد تثور المشكلة فى الحالات التى تكون فيها البيانات مخزنة فى وحدات معالجة مركزية فى حاسب ضمن شبكة معلومات كبيرة، ففى هذه الحالة فإن صياغة شرط يعطى للمحقق إمكانية ضبط هذا النظام الشبكى بأكمله وعزله عن البيئة المعلوماتية المحيطة به، لا يُعد شرعيًا طبقًا لمبدأ التناسب، لما فيه من مساس بحقوق الغير فى النظام محل الضبط.

وفى كندا نجد الوضع التشريعى نفسه فالمادة (٤٨٧) من القانون الجنائى الكندى، تعطى سلطة إصدار إذن لضبط أى شىء، طالما تتوافر أسس معقولة للاعتقاد بأن الجرم ارتكب، أو يشتبه فى ارتكابه، أو أن هناك نية فى أن يستخدم فى ارتكاب الجرم، أو أنه سوف ينتج دليلًا على وقوع الجريمة[١٠]، وحتى الآن فإن هذا النص يُفسر بوضوح تام على أنه يسمح بضبط بيانات الحاسب غير المحسوسة.

فى فرنسا: ذهب جانب من الفقه إلى الاعتراف بأن للبرنامج كيانًا ماديًا ملموسًا، يتمثل فى نبضات إلكترونية مغناطيسية أو ممغنطة[١١].

ولذلك نجد أن قضاء محكمة النقض الفرنسية وقبل تجريم المشرع لسرقة الطاقة بموجب نص المادة ٢/٣١١ من قانون العقوبات الفرنسى، ذهب إلى صلاحية التيار الكهربائى لقيام جريمة السرقة وأيضًا يمكن أن تقوم جريمة السرقة عن طريق الحاسب الآلى.

وأيضًا فقد ذهبت محكمة النقض المصرية إلى أن جريمة السرقة يمكن أن تقع على سرقة التيار الكهربائى[١٢]، ويمكن أيضًا أن تقع على خط التليفون[١٣]. كما وأن فعل الاختلاس يمكن أن يقع على الأشياء المعنوية طالما كانت قابلة للتحديد كالمعلومات التى تحتويها دعامات مادية كالكتابة وشرائط التسجيل المغناطيسية.

وفى هذا المعنى قضت محكمة النقض الفرنسية بأن: سرقة الأقراص المغناطيسية "الديسكات" تتضمن فى الوقت ذاته سرقة محتوياتها المعلوماتية للفترة الزمنية التى تكون محملة بها[١٤]. وبناءً على ذلك فإن ضبط الأدلة المتحصلة من الجرائم الإلكترونية يمكن أن يقع على الكيانات المعنوية فى الوسائل الإلكترونية، ومثال ذلك أنه يمكن ضبط البيانات الإلكترونية أو قاعدة البيانات بمشتملاتها من ملفات وسجلات وحقول وسواء أتخذت شكل برامج نظام أو برامج تطبيقات[١٥].

فإذا كان التفتيش ينتهى بتحديد موضع ومكان البيانات التى يستهدف الوصول إليها، فإن المعالجة التى تجرى عليها لجعلها مرئية للاطلاع عليها وإثباتها، أو بإخراجها من الحاسب فى صورة مستندات مطبوعة لا تعد تفتيشًا عن أدلة الجريمة، ولكنها تمثل وصولًا إلى هذه الأدلة ومن ثم تعد ضبطًا لها[١٦].

وقد نصت الاتفاقية الأوروبية حول الجريمة الافتراضية لعام ٢٠٠١ على جواز ضبط المعلومات المخزنة بالحاسب أو على أى وسيط تخزين، فنصت تلك المادة على أنه "كل دولة طرف لها سلطة أن تتخذ الإجراءات الآتية: أن تضبط نظام الحاسب، أو أى جزء منه، أو المعلومات المخزنة به، أو على أى وسيط من وسائط الحاسب المتعلقة بالحاسب، وأن تحافظ على سلامة هذه المعلومات المخزنة[١٧].

وفى إطار الاتفاقية الأوروبية حول الجريمة المعلوماتية لعام ٢٠٠١م، فإن مصطلح الضبط كما يشمل الدعامة المادية التى يتم تخزين المعلومات والبيانات

عليها أو الوصول أو التحفظ على نسخة منها، يشمل أيضًا استخدام أو ضبط البرامج الفورية اللازمة للولوج إلى هذه البيانات وضبطها، ومن ثم فقد تم استخدام مصطلح الحصول بطريقة مشابهة ذلك بغرض الأخذ فى الاعتبار الطرق غير التقليدية لرفع بيانات غير مادية التى لا يسهل الحصول عليها وأن ذلك لا يتم بطريقة مادية فى نطاق بيئة المعلومات.

وتجدر الإشارة إلى أن ضبط الأدلة المتحصلة من الحاسبات الآلية قد تكتنفه الصعوبة البالغة عندما يكون متعلقًا بنظام آلى بأكمله، إذ أن هذا الأمر يحتاج إلى تعاون دولى لأجل إتمام هذا الضبط دون إعاقة سير النظام المعلوماتى.

على عكس الرأى السابق، هناك من يرى أن الضبط يقصد به ضبط الأدلة المادية التى تُفيد فى كشف الحقيقة فإن هذا المفهوم المادى لا ينطبق على بيانات الحاسب الآلى غير المحسوسة أو الملموسة، وإزاء هذا القصور التشريعى؛ فإن هذا الرأى يقترح ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة "المواد المعالجة عن طريق الحاسب الآلى أو بيانات الحاسب الآلى"، وبذلك تصبح الغاية الجديدة للتفتيش بعد هذا التعديل اللغوى الذى واكب التطور التقنى الحديث، والذى يجب أن تنص عليه التشريعات الإجرائية على النحو التالى: "البحث عن الأدلة المادية أو أى مادة معالجة بواسطة الحاسب"[١٨].

فى فرنسا: يرى بعض الفقهاء أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة، وبالتالى لا تعتبر شيئًا ماديًا، بالمعنى المألوف للكلمة[١٩]، ولذا لا يمكن ضبطه.

هناك رأى ثالث ينظر إلى الواقع العملى الذى يؤكد أن الضبط لا يتصور، إلا إذا أتخذت البيانات صورة مادية.

فى ألمانيا: الأدلة المضبوطة يجب أن تكون أشياء ملموسة (القسم ٩٤ من قانون الإجراءات الجنائية)، وذلك يشمل ليس فقط نظم الحاسب الآلى، بل أيضًا حاملات البيانات وهذه البيانات تنقصها الخاصية المادية، وبالتالى لا تشكل أشياء يمكن ضبطها.

وذهب رأى فقهى فى ألمانيا إلى أن الأشياء المحسوسة هى التى يمكن ضبطها، ويعنى ذلك بمفهوم المخالفة أن البيانات المجردة لا يمكن ضبطها، بينما المطبوعات أو البيانات المصورة أو التى تنقل إلى حافظة الاحتفاظ بالبيانات فإنه يمكن ضبطها[٢٠].

ونرى أنه يجب ألا نقف من تفسير لفظ شىء على المعنى الحرفى للكلمة، إذ يجب تفسير النص تفسيرًا منطقيًا، فما عناه المشرع من إجازة التفتيش هو إتاحة الفرصة للبحث عن وضبط الدليل الذى يساعد فى كشف الحقيقة بشأن جريمة وقعت، وهذه الغاية تكون متوافرة بصرف النظر عن طبيعة الوسط المراد تفتيشه أو الأشياء محل الضبط، ولذا فإن هذا التفسير لا يمكن عده تفسيرًا موسعًا مادامت الغاية هى البحث عن إرادة المشرع، ومن باب أولى فإننا لم نعمل القياس، لأننا انطلقنا من النص ذاته فى فهم مصطلح الشىء وهذا لا يمكن إعتباره قياسًا لوجود النص الذى نعتقد أنه يستوعب المسألة موضوع البحث.

فالشىء إذا كان يمثل قيمة إقتصادية أو ذهنية فإنه يستحق الحماية الجنائية سواء أكان ذا طبيعة مادية أو معنوية، فليس بشرط أن الشىء لكى تتقرر حمايته ضد السرقة، مثلًا 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[٢١].

إلا أن الإشكالية الأهم بشأن الضبط تظهر حينما يتعين ضبط المعطيات المخزنة على أى وسيط من وسائط التخزين دون توافر إمكانية ضبط الدعامة المادية المخزن عليها هذه المعطيات، كذلك ليس بالإمكان ضبط النظام كله أو الشبكات المتصلة به عندما تظهر أهمية ذلك فى إثبات الجريمة، حيث إن إعمال مبدأ التناسب يقتضى قصر الضبط على الأدلة التى تُفيد فى كشف الحقيقة دون أن يؤدى ذلك إلى تعطيل العمل كله فى النظام أو فى الشبكات المتصلة به. لذا يظهر أن النسخ (Copy) الأسلوب الأمثل الذى يمكن استخدامه فى ضبط المعطيات الإلكترونية.

غير أن اللجوء لاستخدام هذه الوسيلة فى الضبط آثار العديد من التساؤلات، سواء من ناحية مشروعيته أو حجية الدليل المستمد منه.

ومن الطبيعى أن تختلف طريقة ضبط الأشياء المادية، كضبط جهاز الحاسب أو ملحقاته كالأقراص وغيرها عن طريقة ضبط المعطيات الإلكترونية؛ لذا يغدو منطقيًا تمكين المحقق فى الجرائم الإلكترونية من النسخ على الدعامة المادية التى يراها مناسبة للمعطيات الإلكترونية التى يسمح له القانون بالتفتيش فيها متى بدت له أهميتها فى كشف الحقيقة.

ويتمثل إختلاف طريقة الضبط فى "الجرائم الإلكترونية" من خلال النسخ عن الضبط التقليدى فى بقاء الشىء المضبوط تحت يد حائز المعطيات الإلكترونية المضبوطة، بينما "الضبط المادى" يخرج الشىء المضبوط من السيطرة المادية لحائزه، وحتى فى اتفاقية بودابست (المادة ١٩)، وفى بعض القوانين كالقانون البلجيكى[٢٢]، التى نصت المادة ٢٩ مكرر/٣ على إمكانية الأمر بمنع الوصول إلى البيانات التى يتم ضبطها، عندما يشكل الولوج إلى هذه البيانات خطرًا مهمًا على المجتمع، كما فى حالة البرامج التى تحتوى فيروسات أو تقدم الطرق لعمل فيروسات أو طرق

القرصنة... الخ، فإن هذه البيانات تستمر فى الوجود، وكل ما فى الأمر أن يمنع المشتبه به من الولوج إليها.

والعديد من التشريعات تعتبر قواعد الضبط التقليدى صالحة للتطبيق فى مجال الجرائم الإلكترونية. ولهذا السبب لم تشرع معظم الدول نظمًا تختص بالضبط فى "الجرائم الإلكترونية"، وإنما اكتفت بتطبيق القواعد التقليدية على ضبط المعطيات الإلكترونية، فالمشرع الألمانى، على سبيل المثال، الذى خصص المواد (٩٢) وما يليها من قانون الإجراءات الجنائية للضبط، لم ينص صراحة على ضبط المعطيات الإلكترونية بواسطة النسخ، وإنما اكتفى بالنص على ضبط أو تسجيل أى معلومات تظهر مفيدة لكشف الحقيقة.

ويظل التساؤل قائمًا بشأن إمكانية استخدام المعطيات التى تم ضبطها من خلال نسخها فى الإثبات، والحق أن للاشتراطات الشكلية التى يحيط بها القانون إجراءات التفتيش والضبط أهمية كبيرة فيما يتعلق بإمكانية استخدام أدلة الإثبات المتحصل عليها من خلال هذه الإجراءات، وقد تثير هذه الشروط الشكلية صعوبات خاصة عندما يراد تطبيقها على التفتيش عن المعلومات الإلكترونية وضبطها، ولاشك أن أسلوب النسخ ينتج عنه دليل إلكترونى، وفى مجال ضبط المعطيات الإلكترونية، وفى ظل غياب اشتراط إجراءات خاصة تضمن صدق المعطيات المضبوطة، يبقى المجال مفتوحًا للتساؤل حول مصداقية أدلة مستمدة فى الحقيقة من نسخ عن الأصل المخزن فى الوسط الإلكترونى.

فى ظل غياب تشريع خاص، تقدم القواعد المتبعة فى مجال التفتيش والضبط التقليدى تصورًا لما يتعين إتباعه من أجل المحافظة على الدليل الإلكترونى.

وبالإمكان إجمال ذلك فى احتياطيين رئيسين يتعين مراعاتهما:

الأول: إمكانية الرجوع للمعطيات الأصلية التى أخذت عنها النسخة كلما دعت الضرورة إلى ذلك. وتظهر ضرورة هذا الاحتياط من خلال إتاحته إمكانية إثبات مطابقة النسخ المضبوط عليها المعطيات الإلكترونية للأصل.

الثانى: يتعلق هذا الاحتياط بمعالجة المعطيات الإلكترونية المضبوطة، ففى الأغلب يتعين على المحقق، أو الخبير البحث عن المعلومات المطلوبة ضمن المعطيات المضبوطة، ويتم ذلك من خلال العديد من الإجراءات التى تحتاج إلى تحليل ومعالجة المعطيات، الأمر الذى يترتب عنه التغيير فى المعطيات، لذا كان لابد من العناية بتدوين وتصنيف هذه الإجراءات بصورة دقيقة، فمن خلال ذلك يمكن التأكد من مصداقية الدليل.

ولتحقيق الضمانات السابقة يتعين على المحقق المكلف بالتحقيق فى الدليل الإلكترونى، أن يحرص على الحصول على نسخة أخرى إضافية من المعطيات وذلك للعمل بها كدليل على إجراءات المعالجة التى وقعت على المعطيات الإلكترونية.

ويتعين بالإضافة لكل ما سبق، ضرورة مراعاة إجراءات التحرز على الأشياء المضبوطة التى حددها القانون لما لتلك الإجراءات من أهمية لا يستهان بها من ناحية التمكين من استخدام المعطيات الإلكترونية المضبوطة فى الإثبات[٢٣].

ثانياً: الإجراءات الحديثة لضبط الأدلة الإلكترونية

تتم هذه الإجراءات من خلال التحفظ على الأدلة الإلكترونية أو اعتراضها ومراقبتها وجميع هذه الإجراءات مستقاة من اتفاقية بودابست ٢٠٠١[٢٤] وهى أولى المعاهدات الدولية الخاصة بالجرائم الإلكترونية[٢٥]وقد تمت هذه الاتفاقية تحت إشراف المجلس

الأوروبى، ووقع عليها ثلاثون دولة بما فى ذلك الدول الأربعة من غير الأعضاء فى المجلس الأوروبى المشاركة فى إعداد هذه الاتفاقية، وهى كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية، حيث صادقت عليها هذه الأخيرة فى (٢٢ ديسمبر ٢٠٠٦) ودخلت بالفعل حيز النفاذ فى الأول من يناير ٢٠٠٧. وهى مفتوحة لانضمام دول أخرى حتى يمكن أن تسهم فى ضبط وتنظيم مجتمع المعلومات والاتصالات بشكل أفضل، وتتكون هذه الاتفاقية من ثمانى وأربعين (٤٨) مادة تم توزيعها على أربعة أبواب، الباب الأول: استخدام المصطلحات، الباب الثانى الإجراءات الواجب اتخاذها على المستوى القومى، ويضم هذا الباب ثلاثة أقسام: الأول: القانون العقابى المادى أو الموضوعى، والثانى: للقانون الإجرائى، والثالث: للاختصاص القضائى، وستقتصر دراستنا على الجانب الإجرائى فقط وبصفة خاصة الإجراءات المستحدثة التى قررتها الاتفاقية من خلال ما يلى:

١- البيانات المخزنة(الساكنة): ونتناولها من خلال إجراءين

أ- التحفظ العاجل على البيانات.

ب- الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك.

أ- التحفظ العاجل على البيانات

المادة (١٦) من اتفاقية بودابست تمكن السلطات الوطنية المختصة من إصدار الأمر أو الحصول عن طريق مماثل على الحفظ السريع للبيانات الإلكترونية المختصة المخزنة فى إطار تحريات أو إجراء جنائى خاص[٢٦]، فقد نصت هذه المادة على "ضرورة أن يسمح كل طرف لسلطاته المختصة أن تأمر أو تفرض بطريقة أو بأخرى مزود الخدمة بالحفظ السريع للبيانات المعلوماتية المعنية" باعتبارها إجراء مؤقتًا بما فى ذلك البيانات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتى، وذلك عندما تكون

هناك أسباب تدعو للاعتقاد بأن هذه البيانات على وجه الخصوص معرضة للفقد أو التغيير، وذلك خلال مدة ٩٠ يوم كحد أقصى، وتستطيع تلك الأطراف تجديد هذا الإجراء خلال فترة الحفظ، ولا يتم إخطار السلطات الرادعة بتلك البيانات بطريقة آلية، ولكى يتم نشر تلك البيانات يجب إتخاذ إجراء إضافى للتصريح بنشرها أو إصدار أمر بالتفتيش عليها، بالنسبة لارسال البيانات للسلطات المختصة، الفقرة (١٥٢-١٦٠)[٢٧].

وبالتالى فإن إجراء حفظ البيانات يعد لبعض الدول، ومنها مصر سلطة قانونية جديدة، فهو أداة تحقيق مستحدثة فى إطار مكافحة الجرائم الإلكترونية، فهو يتلاءم وطبيعة هذه البيئة من حيث قابلية البيانات فيها للمحو والفقد بسرعة، نص المشرع الأمريكى على هذا الإجراء فى القسم (f) (18 U S.C2703) من قانون خصوصية الاتصالات الإلكترونية الأمريكى (ECPA) [٢٨].

وفيما يلى نتعرض لعدة نقاط:

١- المقصود بمزود الخدمة باعتباره الحائز للبيانات ومدى التزامه بالتعاون مع سلطات التحرى والتحقيق.

٢- إلتزام مزود الخدمة بمدة معينة للتخلص من البيانات.

٣- مفهوم الحفظ السريع للبيانات.

١- المقصود بمزود الخدمة

مزود الخدمات هو من يقدم خدمته إلى الجمهور بوجه عام فى مجال الاتصالات الإلكترونية التى لا تقتصر فى أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود[٢٩]. وقد أوضحت المذكرة التفسيرية لاتفاقية بودابست أن مصطلح مزود الخدمة يشمل العديد من فئات الأشخاص الذين يلعبون دورًا خاصًا فى

الاتصالات أو معالجة البيانات على النظم المعلوماتية، ويشير بصفة خاصة إلى البيانات العامة أو الخاصة التى تقدم إلى المستخدمين إمكانية الاتصال فيما بينهم ويطبق أيضًا مصطلح مزود الخدمة على الكيانات التى تخزن البيانات أو تعالجها لحساب المستخدمين، وكذلك قد يطلق على الأشخاص الذين يقدمون خدمة الاستضافة أو التخزين على الذاكرة بطريقة مستترة أو الاتصال بشبكة، ويفرق قانون حماية الحياة الخاصة فى مجالات الاتصالات الإلكترونية فى الولايات المتحدة الأمريكية (ECPA) بين نوعين من مزودى الخدمات: **النوع الأول** مزودو خدمة الاتصالات الإلكترونية، **والنوع الثانى:** هم مزودو خدمة معالجة المعلومات عن بعد.

ويقصد بالنوع الأول: كل من يقدم خدمة إلى مستخدمى الشبكة والتى تتمثل فى تسهيل إرسال واستقبال الاتصالات السلكية والإلكترونية(٣٠).

أما النوع الثانى: فيعرف حسب ما جاء فى القسم (٢) (c) (18 U S.C2703) من قانون خصوصية الاتصالات الإلكترونية الأمريكى بأنه "كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بوسيلة من وسائل الاتصالات الإلكترونية"، **وبناء** عليه إذا أرسل شخص لشخص آخر رسالة عن طريق البريد الإلكترونى فإنها تمر بالضرورة بمزود خدمة الاتصالات الإلكترونية، وقبل أن يتلقاها المرسل إليه، تظل مخزنة لدى مزود الخدمات، فإذا تلقاها المرسل إليه فإن موقف هذا الأخير يتراوح بين أمرين: إما أن يقوم بمسح تلك الرسالة أو أن يقوم بتخزينها، فى هذا الفرض الأخير تعتبر الرسالة مخزنة لدى مزود الخدمة.

٢- التزام مزود الخدمة بمدة معينة للتخلص من البيانات

تضع بعض التشريعات المقارنة كالقانون الفرنسى التزاما على مزودى الخدمات بإزالة البيانات التى يتم تخزينها تلقائيًا وتتعلق بالاتصالات الإلكترونية بين مستعملى شبكة

الإنترنت والتى تتعلق بهوية المتصلين[٣١]وساعة الاتصال[٣٢]، بل إن قانون الأمن اليومى الفرنسى والصادر فى (١٥ نوفمبر سنة ٢٠٠١) قد أورد عقوبات فى حالة عدم قيام مزود الخدمات بمسح تلك البيانات، وذلك احترامًا لحرمة الحياة الخاصة المادة (3-39) L: من قانون الأمن اليومى، إلا أن هذا القانون قد أورد نوعين من الاستثناءات على هذا الالتزام:

- يتعلق الأول بمتطلبات المحاسبة المالية بين مزودى الخدمات والمشتركين فى خدماتهم، حيث يقدم مزودو الخدمات لبعض هؤلاء المشتركين بعض الخدمات مدفوعة الأجر.
- أما الاستثناء الثانى فيتعلق باعتبارات التعاون من الجهات القضائية التى تبرر الاحتفاظ بتلك البيانات لمدة لا تزيد على سنة[٣٣]. وهذا الاستثناء يؤكده التوجيه الأوروبى رقم (٥٨ لسنة ٢٠٠٢)، حيث قرر أنه من حق الدول الأعضاء اتخاذ التدابير اللازمة لحماية الأمن العام والدفاع القومى وأمن الدولة والتحقيق فى الجرائم بما يتضمنه ذلك من وضع استثناءات على الحق فى الخصوصية، ومن بين هذه الاستثناءات ضرورة الحفظ السريع على البيانات المعلوماتية المخزنة حفاظًا عليها من التلف والتغيير.

وتجدر الإشارة فى هذا المقام إلى أنه ترد بعض الاستثناءات على التزام مزودى الخدمات بالتعاون مع سلطات التحقيق، حيث يستبعد القانون الفرنسى البيانات التى تحوزها جهات معينة من القاعدة السابقة والتى تفرض واجب التعاون مع رجال العدالة بوجه عام، وذلك مثل ما نصت عليه الفقرة الثانية من المادة (٣١) من القانون رقم (١٧ لسنة ٧٨ الصادر فى ٦ يناير ١٩٧٨)، الخاص بالمعلوماتية والحريات فى فرنسا، فتنص الفقرة الثانية من المادة (٣١) من هذا القانون على عدم جواز مراقبة

المعلومات التى تجمعها الكنائس أو أى تجمعات دينية أو فلسفية أو سياسية أو نقابية والتى تتعلق بأعضائها والمتراسلين معها.

كما تُستثنى أيضا من القاعدة السابقة أنواع معينة من المعلومات نصت عليها المادة (١٨) من قانون الأمن الداخلى الذى عدل قانون الإجراءات الجنائية الفرنسى، حيث أدخل المادة (٦٠-١) الخاصة بالمعلومات التى يغطيها سر المهنة، فتنص على أنه "باستثناء المعلومات التى تعتبر من أسرار المهنة التى أوردها القانون، والموجودة فى الأنظمة المعلوماتية أو أى أجهزة للمعالجة الآلية".

٣- مفهوم الحفظ السريع للبيانات المخزنة[٣٤]

يقصد به "توجيه السلطة المختصة لمزود الخدمة الأمر بالتحفظ على بيانات معلوماتية مخزنة فى حوزته أو تحت سيطرته، فى انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية". وحتى تتضح صورة هذا الإجراء نعطى المثال التالى: "قد يعلم رجال الضبط القضائى بوجود صور داعرة للأطفال فى اليوم الأول فيقومون باتخاذ إجراءات الحصول على إذن تفتيش فى اليوم التالى، وفى اليوم الثالث يحصلون على الإذن ثم يصل علمهم أن المزود قام بشطب السجلات كالمعتاد فى اليوم الثالث المذكور".

ويتضح من المثال السابق أن الحفظ السريع إجراء أولى أو تمهيدى الهدف منه هو محاولة الاحتفاظ بالبيانات قبل فقدانها.

وقد وردت الأسباب التى تدعو إلى الحفظ السريع للبيانات بالمذكرة التفسيرية لاتفاقية بودابست على النحو التالى[٣٥]:

١- قابلية البيانات المعلوماتية للتلاشى، حيث تكون محلًا للمحو أو التغيير، سواء كان ذلك بدافع إجرامى- بهدف طمس معالم الجريمة وأى عنصر إثباتى لشخصية

المجرم- أو بدافع غير إجرامى وذلك فى إطار الحذف الروتينى للبيانات التى لم تعد هناك حاجة إليها.

٢- غالبا ما يتم ارتكاب الجرائم الإلكترونية عن طريق نقل الاتصالات عبر نظم الحاسب، حيث يمكن أن تتضمن هذه الاتصالات محتويات غير مشروعة، مثل مواد إباحية للأطفال أو فيروسات الحاسب، أو الدليل على إرتكاب جرائم أخرى مثل الإتجار بالمخدرات فتحديد مصدر إرسال هذه الاتصالات يمكن أن يساعد فى تحديد هوية مرتكبى الجريمة.

٣- تأمين الدليل الإلكترونى من الضياع، حيث يتم نسخ الاتصالات ذات المحتوى غير المشروع أو دليل على نشاط جنائى من قبل مزودى الخدمات، مثل المراسلة الإلكترونية التى تم إرسالها أو استقبالها، ومن ثم يمكن الكشف عن دليل جنائى للجرائم المرتكبة.

وتجدر الإشارة إلى أن البيانات المعلوماتية المشمولة بالأمر تتضمن بينها بيانات المرور المتعلقة باتصالات سابقة، وذلك من أجل تحديد خط سير الاتصال بمعنى مصدر أو مكان وصول هذه الاتصالات، والتى تعد من الأمور الجوهرية للتعرف على هوية الأشخاص الذين قاموا بالفعل الإجرامى. وقد عرفت المادة الأولى فقرة "د" من اتفاقية بودابست هذا النوع من البيانات (البيانات المتعلقة بالمرور) "بأنها صنف من بيانات الحاسب التى تشكل محلًا لنظام قانونى محدد، حيث يتم توالد هذه البيانات من الحواسب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصالات من مصدرها إلى الجهة المقصودة، وبذلك فهى تشمل طائفة من البيانات تتمثل فى: مصدر الاتصال ووجهته المقصودة، خط السير ووقت أو زمن الاتصال وفقًا لتوقيت جرينتش، حجم الاتصال ومدته ونوع الخدمة المؤداة (مثل نقل الملفات أو بريد

إلكترونى أو مراسلات فورية). وفى الغالب ما يحوز مقدم الخدمة بمفرده بيانات المرور، ما يكفى للتحديد بدقة مصدر أو نهاية الاتصال، بل إن كل واحد منهم يكون حائزًا بعض أجزاء اللغز، ويتعين أن توضع هذه الأجزاء تحت الاختبار بقصد تحديد مصدرها والجهة المرسلة إليها.

ب- الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك

الأصل أن البيانات الشخصية المتعلقة بمستخدمى الشبكة تدخل فى إطار الحق فى الخصوصية التى تحميه الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية (بتاريخ ٤ نوفمبر ١٩٥٠)، فلا يجوز لمزود الخدمات أو غيره أن يقوم بإفشاء ما لديهم من معلومات إلى الغير. إلا أن بعض التشريعات المقارنة تسمح لرجال الضبط القضائى أن يأمروا الأشخاص بتسليم ما تحت أيديهم من موضوعات، والتى يطلب تقديمها كدليل، ومن بينها البيانات المتعلقة بالمشترك التى يحوزها مزودو الخدمات، وهو ما يلزمه القانون الفرنسى رقم (٧١٩ لسنة ٢٠٠٠) المعدل للقانون رقم (١٠٦٧ لسنة ١٩٨٦) الخاص بحرية الاتصالات، حيث تنص المادة (٤٣-٩) منه على "أنه يتعين على مزودى خدمات الدخول والمسكنين المحافظة على بيانات مستعملى خدماتهم وذلك تمهيدا لطلب السلطات لتلك البيانات التى قد تفيد كدليل فى جريمة معينة وقعت بالفعل".

أما بالنسبة للقانون الأمريكى المعروف بقانون خصوصية الاتصالات الإلكترونية (ECPA)، فقد أجاز لرجال الضبط القضائى فى إطار ما يقومون به من جمع الاستدلالات الإطلاع على البيانات الموجودة فى حوزة مزودى الخدمات والتى تخص مستخدمى شبكة الإنترنت، وذلك من خلال توجيه تكليف إلى مزود الخدمات بتقديم تلك المعلومات، والتى تنقسم إلى ثلاث طوائف هى:

١- المعلومات الشخصيـة الخاصــة بالمشترك، مثل اسمه ورقم تليفونه وعنوانه.
٢- المعلومات الشخصية الخاصة بالمتعامل مع المشترك (أى كل من يتصل به أو يدخل معه فى صفقة).
٣- المعلومات المتعلقة بمحتوى البيانات (مضمون المحادثات- مضمون الملفات).

والملاحظ أن التشريعات ذات الأصل اللاتينى مثل (القانون الفرنسى، والقانون الجزائرى والمصرى) تختلف عن القانون الأمريكى، حيث لا تجيز تلك التشريعات أن يصدر رجل الضبط القضائى مثل هذا الأمر، وإنما تجيزه لسلطة التحقيق، حيث تنص المادة (٩٩) إجراءات جنائية مصرى على أنه "لقاضى التحقيق أن يأمر الحائز لشىء يرى ضبطه أو الاطلاع عليه بتقديمه، ويسرى حكم المادة (٢٧٤)[٣٦] على من يخلف ذلك الأمر..."، ولا تختلف سلطة النيابة العامة فى ذلك عن سلطة قاضى التحقيق. كما أن للمحكمة أن تصدر مثل هذا الأمر وفقًا للقانون المصرى، حيث تنص المادة (٢٩١) إجراءات مصرى "للمحكمة أن تأمر ولو من تلقاء نفسها، أثناء نظر الدعوى، بتقديم أى دليل تراه لازمًا لظهور الحقيقة".

وقد نصت اتفاقية بودابست فى المادة (١٨) منها على "أنه يجوز للدول الأطراف فى تلك الاتفاقية تمكين السلطات المختصة من إلزام مقدمى الخدمات تقديم البيانات المتعلقة بالمشترك، سواء كانت فى حيازته المادية أو تحت سيطرته حيث تكون هذه البيانات مخزنة بعيدًا عن الحيازة المادية لمزود الخدمة، ولكن يمكن السيطرة عليها، ومثال ذلك أن تكون البيانات مخزنة فى وحدة تخزين عن بعد ويتم تقديمها عن طريق شركة أخرى. ويشترط فى هذه البيانات أن تكون مخزنة وقد حددت الاتفاقية المقصود بتلك البيانات بقولها إنها تتعلق:

- بنـوع خدمــة الاتصــال التــى اشترك فيها الشخص والوسائل الفنية لتحقيقها.
- العنوان البريدى أو الجغرافى ورقم تليفون المشترك.
- رقم دخول المشترك للحصول على تلك الخدمة والفواتير التى ترسل إليه، وأى معلومات تتعلق بطريقة الدفع (مثل رقم بطاقة الائتمان أو حسابه البنكى)، أو أى معلومـات أخـرى تتعلـق بـأداء الخدمــة أو بالاتفـاق بـين هـذا المشـترك ومـزود الخدمة[٣٧].

ثانياً: البيانات غير المخزنة (المتحركة)

تتمثل الإجراءات المتعلقة بالبيانات المتحركة فى مراقبة [٣٨] الاتصالات الإلكترونية الخاصة، ويقصد بهذا الإجراء مراقبة الاتصالات الإلكترونية أثناء الاتصال بين الطرفين، وليس الحصول على اتصالات إلكترونية مخزنة [٣٩]، ذلك أن لكل من النوعين قواعد خاصة بها، حيث إن ضمانات الحصول على الأولى أكثر شدة من ضمانات الحصول على الثانية. وفى هذا الصدد يثور تساؤل حول تحديد طبيعة البريد الإلكترونى غير المفتوح الموجود فى صندوق خطابات مقدم خدمات الإنترنت والتى لم يدخلها المرسل اليه فى نظامه المعلوماتى بعد (أى استردادها)، فهل يجب اعتبارها بيانات معلوماتية مخزنة، وبالتالى تطبق عليها الإجراءات المتعلقة بالبيانات الساكنة أم أنها بيانات فى مرحلة النقل والتحويل، وبالتالى تطبق عليها الإجراءات المتعلقة بالبيانات المتحركة والمتمثلة فى مراقبة الاتصالات الإلكترونية. ومن ثم لا يتم الحصول عليها إلا عن طريق السلطة المختصة؟

التعريف بالبريد الإلكترونى

يعتبر البريد الإلكترونى من أهم التطبيقات الإلكترونية التى توفرها شبكة المعلومات (الإنترنت) وتتمثل هذه الخدمة بتناقل الرسائل بين الأشخاص عبر هذا البريد المربوط

بشبكة الإنترنت وعلى الرغم من المزايا التى تتمتع بها خدمة البريد الإلكترونى التى تتمثل بسرعة الإرسال مقارنة بالبريد العادى، كما أنها تمتاز بقلة التكلفة والاقتصار فقط على دفع تكلفة الاشتراك فى هذه الخدمة للتزود بالإنترنت، وفى واقع الأمر التكنولوجيا تعمل لجعل الحياة أسهل وأفضل، فدور التكنولوجيا هو توفير المزيد من المرونة والكفاءة لخدمة أصحاب النظرة المستقبلية بإتاحة الفرصة لأداء أفضل، ولقد أصبح ممكنًا الآن بالفعل أن يرسل أى إنسان إلى أى إنسان آخر رسالة عبر الإنترنت، لأغراض تجارية، أو تعليمية أو حتى لمجرد التسلية. وأصبح ممكنًا أن يجرى شخص ما محادثات بالصوت والصورة مع أصدقاء ربما تعذر أن يلتقوا معًا، وذلك من خلال نظم تشغيل الكمبيوتر– التى توفر تطبيقات متعددة أخرى غير البريد الإلكترونى. والواقع أن إتاحة المعلومات إلكترونيًا من خلال هذه التطبيقات يصعب "توصيلها" إلى من لا يستخدم الكمبيوتر [٤٠].

البريد الإلكترونى كوسيلة لإرتكاب الجريمة وكمصدر للدليل

وعلى الرغم من الفوائد السابق ذكرها للبريد الإلكترونى، فإن هذه الوسيلة لها وجه آخر قد يوصف بالقبح، يتمثل فى كثرة الجرائم التى ترتكب بواسطتها، والتى تمثل انتهاكًا سافرًا لحرمة الحياة الخاصة للأفراد، إذا تستخدم هذه الوسيلة لارتكاب العديد من الجرائم، منها ما يمس الإنسان فى سمعته أو اعتباره أو شرفه كالسب والقذف والتهديد، أو تقع على أمواله، كالسرقة، ومنها ما تطال حقه فى الحياة، وإذا ما تمعنا بعمق فى الجرائم التى ترتكب عن طريق البريد الإلكترونى، نلاحظ اختلاف الباعث على ارتكاب هذه الجرائم، البعض من هذه الجرائم يكون الباعث على ارتكابها حب المغامرة والتحدى، وأغلب مرتكبى هذه الجرائم هم من المراهقين الذين تتراوح أعمارهم بين ١٣–١٧ سنة، وقد يكون الباعث شخصى بغرض الانتقام[٤١].

ومن التساؤلات التى تتعلق بالبريد الإلكترونى، ما مدى التشابه بين الرسائل الإلكترونية والرسائل التقليدية، ومدى إمكانية خضوع مراسلات البريد الإلكترونى للقواعد التقليدية دون حاجة لوضع قواعد خاصة بها؟

تنص مادة (٩٥) إجراءات جنائية مصرى على أن "المراسلات هى الرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق والمحادثات السلكية واللاسلكية".

نلاحظ فى هذا النص أن المشرع المصرى قد أدخل المحادثات التليفونية "السلكية واللاسلكية" ضمن المفهوم العام للرسائل، ولم يفرق بين المراسلات الإلكترونية والمراسلات العادية، فالمراسلات الإلكترونية ما هى إلا مراسلات ذات صبغة تقليدية من ناحية المضمون، ولا تختلف عن المراسلات العادية إلا من جهة الوسيلة المستعملة لنقلها، ففى الوقت الذى تتم فيه المراسلات التقليدية عن طريق البريد العادى، فإن المراسلات الإلكترونية تكون عن طريق الكمبيوتر والهاتف المحمول الذى نقلها عن طريق الإنترنت، أى أن هناك أرضية مشتركة بين الاتصالات والمحادثات الإلكترونية وبين البريد العادى والمحادثات التليفونية العادية[٤٢].

ونرى **المشرع المصرى** غير موفق فى المساواة بين المراسلات الإلكترونية والمراسلات العادية "التقليدية"، وذلك لاختلاف الطبيعة بينهما، فالأولى تتم عن طريق شبكة الإنترنت والبريد الإلكترونى، فى حين تتم الأخرى عن طريق الخطابات المرسلة بواسطة البريد العادى، هذا من جهة، ومن جهة أخرى قد تجد الجهات المختصة بالبحث والتحقيق صعوبة فى تحديد مسئولية الفاعل بالنسبة للأولى، فى حين من السهل تحديد الفاعل ومسئوليته بالنسبة للثانى.

وفيما يتعلق بالقواعد التى تطبق على المراسلات الإلكترونية نجد **المشرع المصرى** أخضع ضبط المراسلات والبرقيات لأحكام خاصة، ولم يخضعها للأحكام العامة فى ضبط الأشياء كما أشرنا لذلك من قبل، فى حين أن **المشرع الفرنسى** لم يفرد قواعد خاصة لضبط المراسلات، وإنما اعتبرها من قبيل الأشياء أو الوثائق التى يمكن أن تساعد فى إظهار الحقيقة، بمعنى أنها أخضعها للأحكام العامة لضبط الأشياء، وهو ما جرى عليه القضاء الفرنسى فقد قضت محكمة النقض الفرنسية بأن "سلطة قاض التحقيق فى ضبط جميع الوثائق تمتد لتشمل الخطابات"(٤٣).

الاتصالات الإلكترونية

قد أعتبر المشرع الأمريكى الاتصالات الإلكترونية المخزنة من قبيل البيانات الساكنة، وبالتالى تطبق عليها كل الإجراءات التى تتناسب مع هذا النوع من البيانات من تفتيش والأمر بالتحفظ العاجل وتقديم هذه البيانات، بدليل أنه قام بتعديل القسم (٢٧٠٣) من قانون خصوصية الاتصالات الإلكترونية (ECPA)، ليشمل حماية الاتصالات الإلكترونية المخزنة من بريد إلكترونى ورسائل صوتية غير مفتوحة ومخزنة لدى مزود الخدمة. وقد تم تأكيد هذه القاعدة فى العديد من التطبيقات القضائية مثل قضية (United States v. Smith)(٤٤)، حيث قرر القضاء بأنه لا يمكن مراقبة الاتصالات السلكية وهى فى حالة التخزين الإلكترونى.

وقد ميزت اتفاقية بودابست بين نوعين من البيانات المعلوماتية محل المراقبة، **النوع الأول:** البيانات المتعلقة بالمرور، **النوع الثانى:** البيانات المتعلقة بمحتوى الاتصال، وبالنسبة للنوع الأول فإن المادة الأولى (١) من الاتفاقية قد عرفتها بأنها "كل البيانات التى تعالج الاتصالات التى تمر عن طريق نظام معلوماتى، والتى يتم إنتاجها بواسطة هذا النظام المعلوماتى بوصفه عنصرا فى سلسلة الاتصال، مع تعيين

المعلومات التالية: أصل الاتصال، مقصد الاتصال أو الجهة المقصودة بالاتصال، خط السير، ساعة وتاريخ الاتصال، حجم وفترة الاتصال، أو نوع الخدمة.

أما بالنسبة للنوع الثانى: البيانات المتعلقة بمحتوى الاتصال، فإنه لم يأت تعريف لها فى الاتفاقية لكنها تشير إلى المحتوى الإخبارى للاتصال، بمعنى مضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال، فيما عدا البيانات المتعلقة بالمرور.

ويلاحظ أن هناك نوعًا من التقارب بين هذين النوعين من البيانات، من حيث المعنى إلا أنهما مختلفان تمامًا من حيث درجة المساس بالحق فى الخصوصية، حيث يكون ذلك أكثر أهمية بالنسبة لمراقبة محتوى الاتصال أو المراسلة، ومن ثم تفرض ضمانات أكبر عند تجميع محتوى البيانات فى الزمن الفعلى عن حركة البيانات، سواء من حيث الجرائم التى من أجلها يتم توظيف هذا الإجراء، أو من حيث السلطة المختصة بإصدار أمر المراقبة.

وقد أكدت اتفاقية بودابست هذا التمييز حيث أدرجت كل إجراء على حدة تحت عنوان خاص، فخصت تجميع حركة البيانات بعنوان "التجميع فى الزمن الفعلى لبيانات المرور" المادة (٢٠)، أما تجميع محتوى البيانات فجاء تحت عنوان "مراقبة محتوى البيانات" المادة (٢١).

فى حين تضع بعض الدول مفهومًا موحدًا لكل من تجميع حركة البيانات ومراقبة محتوى البيانات ومن ثم تسرى عليهما الضمانات نفسها الخاصة عند اتخاذ أحد الإجراءين، دون الأخذ فى الاعتبار الحساسية التى تحيط بموضوع مراقبة محتوى البيانات. ويرجع السبب فى ذلك إلى عدم وجود تمييز فى القانون الذى لا يوجد فيه

اختلافات حول المصلحة فى الخصوصية أو لتشابه إجراءات التجميع التقنى ومن هذه الدول فرنسا.

ولا جدال أن حق الإنسان فى الخصوصية ليس حقًا مطلقًا، بل مقيدًا بالمصلحة العامة وقد تتعارض خصوصية الإنسان مع مصلحة المجتمع فى كشف الحقيقة فى شأن الجريمة ومعاقبة الجناة، مما يستلزم وجود توازن دقيق بين الحق فى الخصوصية، وحق المجتمع فى العقاب، وحتى نحقق هذا التوازن ينبغى إحاطة هذه المراقبة بضمانات تكفل استعماله فى نطاق الهدف الذى شرع من أجله. وسنتناول ذلك فى النقاط التالية: (أولًا) مدى تمتع الاتصالات بصفة عامة والإلكترونية بصفة خاصة بالحماية الجنائية (ثانيًا) الحالات التى تكون فيها المراقبة مشروعة، سواء كان ذلك بدون الحصول على إذن مسبق أو بناء على إذن.

أولًا: حرمة الاتصالات الإلكترونية الخاصة ومدى تمتعها بالحماية الجنائية

مما لا شك فيه أن مراقبة الأحاديث الخاصة تمس بحق الإنسان فى الخصوصية وما يتفرع عنه من سرية الأحاديث الخاصة، وهو حق لصيق الصلة بالإنسان- بل هو على حد قول أحد الفقهاء- الإنسان نفسه [٤٥]. وهذا الحق أصبح مهددًا بدرجة كبيرة، نتيجة للتطور التكنولوجى الذى أدى إلى إفراز أجهزة للمراقبة ذات تقنية عالية، تلتقط أحاديث الإنسان دون أن يشعر، ولم تقتصر هذه الأجهزة على التنصت (interception) على الاتصالات السلكية واللاسلكية فحسب [٤٦]، بل امتدت بقدرتها الفائقة إلى التقاط الاتصالات التى تتم بطريق الإنترنت، مما أفقد الإنسان حريته وخصوصيته [٤٧]، وهدد على نحو خطير كرامته وإنسانيته، الأمر الذى حدا ببعض الفقهاء إلى القول بأن أجهزة المراقبة السمعية تعد نكسة (retombée) للتقدم المذهل

للتقنيات الحديثة، ولقد حرصت أغلب التشريعات على توفير قدر كبير من الحماية الجنائية لسرية الاتصالات الخاصة للأفراد[٤٨].

فقد عاقب المشرع المصرى بالحبس مدة لا تقل عن سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك فى حالة ارتكب أحد الأفعال الآتية فى غير الأحوال المصرح بها قانونًا أو بغير رضا المجنى عليه: استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيًا كان نوعه محادثات جرت فى مكان خاص أو عن طريق التليفون. التقط أو نقل بجهاز من الأجهزة أيًا كان نوعه صورة شخص فى مكان خاص.

ووفقًا للمادة (٣٠٩ مكرر) عقوبات مصرى، نلاحظ أنها تخص المحادثات الخاصة أو التى تتم فى مكان خاص[٤٩]، وأيضا التى تتم عن طريق تليفونى، دون المحادثات التى تتم عن طريق الحاسب الآلى، والتى تتخذ شكل البريد الإلكترونى أو شكل المحادثة الفورية.

ولهذا قامت العديد من التشريعات بإدخال نصوص خاصة تسرى على الاتصالات الإلكترونية، أى تلك التى تتم بطريق الحاسب الآلى، بالإضافة إلى الاتصالات السلكية واللاسلكية، ومنها ما تضمنه القانون الجنائى الفيدرالى الأمريكى (Chapter 119, Part 1, Title 18 Sec. 2511) على عقاب من قام بمراقبة المراسلات الإلكترونية، مساويًا فى ذلك بينها وبين الاتصالات السلكية، حيث نص على عقاب كل من راقب أو حاول مراقبة أو ساعد غيره على أن يراقب أو يحاول مراقبة أى اتصال سلكى أو شفوى أو إلكترونى.

ولذلك نرى ضرورة أن يتدخل المشرع المصرى لسن قوانين خاصة، لتنظيم الوضع القانونى للاتصالات الإلكترونية لمعرفة ما إذا كان الوضع القانونى لهذه

الاتصالات تسرى عليه القواعد الخاصة بالاتصالات السلكية أم لا. خاصة، وأن هذا النوع من الاتصالات وإن كان يتم عن طريق خط تليفونى، فما هو إلا وسيلة للدخول على الشبكة فقط.

ثانياً: المراقبة المشروعة للاتصالات الإلكترونية الخاصة

ذكرنا سلفًا أن الأصل هو حظر مراقبة الاتصالات الإلكترونية الخاصة، إلا بإذن قضائى مسبق، ولكن هناك حالات تكون فيه المراقبة مشروعة دون صدور هذا الإذن.

١- سلطة مزود الخدمات فى مراقبة النظام دون إذن

ويكون ذلك إما فى إطار المراقبة المعتادة لمزود الخدمة لمتابعة عمل الشبكة، أو تكون بناء على شكوى المشترك، وذلك وفق التفصيل التالى:

أ- **المراقبة المعتادة لمزود الخدمة لعمل الشبكة:** نصت بعض التشريعات المقارنة صراحة - كالقانون الأمريكى - فى (المادة (§.C.S.I 251118 U (2) (a) (I) على حق مزودى الخدمات فى مراقبة الاتصالات الإلكترونية الخاصة بالمشتركين فى خدماتهم، وذلك فى إطار العمل اليومى لشبكاتهم، من أجل حماية أنظمتهم من إساءة الاستعمال أو من الإضرار بها (عن طريق استعمال الفيروسات) أو الاستيلاء عليها بالسرقة مثلًا [٥٠].

ومن التطبيقات القضائية على هذا النوع من المراقبة ما قضى به من أنه يجوز لمزودى الخدمات أن يقوموا بتلك المراقبة لمكافحة الغش والسرقة الواقعة على الخدمات التى يقدمونها، من ذلك أن يقوم أحد الأشخاص بتقليد خط لتليفون محمول للحصول على الخدمة دون دفع الاشتراك، الأمر الذى يقتضى أن يتابع مزود تلك الخدمة هذا الخط المقلد لتحديد مكانه ومعرفة الفاعل لذلك [٥١].

ومن الجدير بالذكر أن المشرع الأمريكى، لم يطلق سلطة مزودى الخدمات فى ممارسة تلك الرقابة، بل اشترط عدة شروط ينبغى توافرها لصحة هذه الرقابة وتتمثل فيما يلى:

١- أن يكون مزود الخدمات مجنيًا عليه فى جريمة.

٢- أن يقوم بالمراقبة وبالتبليغ عما يعلمه من جرائم إلى الجهات القضائية، حماية لحقوقه وليس قياما بدور المساعد للمباحث فى التحريات التى يقومون بها.

٣- ألا يطلب رجل الشرطة من مزود الخدمات القيام بتلك المراقبة عونا له، أى أن المبادرة بالتبليغ يجب أن تأتى من جانب مزود الخدمات.

٤- ألا يشارك رجل الشرطة أو يشرف على مزود الخدمات فى قيامه بأعمال المراقبة(٥٢).

ب- المراقبة بناء على شكوى المشترك: اختلفت التشريعات المقارنة حول مدى إمكانية السماح للسلطات بمراقبة الاتصالات الإلكترونية، بناء على الطلب الصادر من صاحب الجهاز محل الاعتداء، بوضع جهازه تحت المراقبة من قبل رجال الضبط القضائى بذلك (ويقاس هذا الاستثناء على مزود الخدمات)، وكان الأمر يدور بين رأيين: أحدهما مؤيد والثانى معارض لهذه المراقبة.

بالنسبة للموقف المعارض يجسده رأى فى كندا، ويعتبر فيه أن مزود الخدمات متماثل فى عمله مع رجال السلطة العامة، وبالتالى فإنه ليس من حقه القيام بتلك الرقابة وتلك التسجيلات بدون إذن، فإذا قام بذلك، فإنه يخالف حكم المادة (٢٤ فقرة ٢) من ميثاق الحقوق والحريات الكندى.

أما بالنسبة للموقف المؤيد لهذا النوع من المراقبة، فيجسده القانون الأمريكى، حيث يسمح (القسم (I) (2) 18 U. S.C. Sec. 2511) لضحايا الهجوم على الحاسب

بتفويض السلطات لمراقبة الاتصالات السلكية والإلكترونية التى يتم بثها إلى أو من الجهاز محل الاعتداء.

ويلزم لتوافر هذا الاستثناء اجتماع أربعة شروط وهى:

الشرط الأول: أن يسمح المالك– أو صاحب الحق– لرجال الضبط بوضع الجهاز الخاص به تحت المراقبة.

الشرط الثانى: أن يتم ذلك فى إطار تحقيق جنائى قائم.

الشرط الثالث: أن تتوافر دلائل كافية على أن تسجيل الاتصالات القادمة من الجهاز الصادر منه الإعتداء يفيد فى كشف الحقيقة.

الشرط الرابع: أن يقتصر رجال الضبط على اعتراض الاتصالات الصادرة من وإلى الأجهزة محل التحقيق.

وفى تحديد مفهوم "المعتدى على النظام"، يستبعد القانون الأمريكى من هذا المفهوم كل من تربطه علاقة تعاقدية مع مزود الخدمة، والذى يتجاوز الحدود التى تسمح بها تلك العلاقة (المادة (٢١) 18 U.C.S. § 2511)، ومثال ذلك مستخدمو شركة معينة لا يعتبرون فى عداد المعتدين على النظام إذا استغلوا أجهزة الشركة فى أغراض أو فى أوقات بالمخالفة لنظام الشركة [٥٣].

٢- مراقبة الاتصالات الإلكترونية بناء على إذن

مما لا شك فيه أن الحماية التى يكفلها المشرع للاتصالات العادية لا يقتصر نطاقها على هذا النوع من الاتصالات فحسب، بل تمتد هذه الحماية إلى الاتصالات الإلكترونية عبر الإنترنت من باب أولى بحسبان أن الغاية من وراء هذه الحماية هى حماية الحياة الخاصة للإنسان بحماية مستودع أسراره الشخصية، وهذه الأسرار تكون أكثر انتهاكا إذا ما استخدمت الوسائل الإلكترونية فى الوصول إليها، ومن ثم فإنها

تكون فى حاجة إلى حماية أكثر من تلك الحماية التى تحتاجها الاتصالات العادية. وإذا اقتضت ضرورة التحقيق مراقبة هذه الاتصالات وتسجيلها، فسنتبع حينها الضمانات نفسها المقررة للمحادثات التليفونية، مع مراعاة خصوصية هذه الاتصالات الحديثة. وتتمثل أهم الضمانات القانونية فيما يلى:

- **السلطة المختصة بإصدار إذن المراقبة:** السلطة القضائية هى المختصة عموما بإصدار هذا الإذن، ويعد ذلك ضمانة لازمة لمشروعية المراقبة على الاتصالات السلكية واللاسلكية فى القانونين المصرى والفرنسى[٥٤]، حيث إنها ضمانة ضد انتهاك أجهزة الدولة لحرمة الحياة الخاصة، وقد نص الدستور المصرى الحالى ٢٠١٤ على هذه الضمانة فى المادة (٥٧) منه[٥٥]، وجاءت المادتان (٩٥)، (٢٠٦) من قانون الإجراءات الجنائية المصرى لتؤكد ان ذلك[٥٦]، ويتضح من نص هاتين المادتين أن المشرع استلزم صدور الإذن بالمراقبة من قاضى التحقيق المختص أو من القاضى الجزئى، وحرمان النيابة العامة من إصدار هذا الإذن، وذلك للحد من سلطة هذه الأخيرة منعا لأى تعسف، ولكن فى حالة ما إذا كانت النيابة العامة تتولى التحقيق بنفسها وتبين لها ضرورة مراقبة المحادثات التليفونية للمتهم، كان عليها طبقًا لنص المادة (٢٠٦ إجراءات جنائية مصرى) أن تحصل على إذن من القاضى الجزئى بمراقبة المحادثات التليفونية[٥٧]، وهو ما أكدت عليه محكمة النقض فى حكم لها، حيث قررت "أن المشرع أباح لسلطة التحقيق وحدها- وهى قاضى التحقيق وسلطة الاتهام فى أحوال التصدى للتحقيق أو إجراء تحقيقات تكميلية وللنيابة العامة فى التحقيق الذى تجريه بعد استئذان القاضى الجزئى". ولا يشترط أن يقوم قاضى التحقيق أو النيابة العامة فى حالة صدور إذن من القاضى الجزئى بتنفيذ أمر المراقبة، بل لهما أن يعهدا بذلك لمأمور الضبط القضائى[٥٨].

ونرى أن الطبيعة الخاصة التى يتمتع بها الدليل الإلكترونى من حيث سرعة فقده وزواله، تفرض على المشرع أن يخفف وفقط فى بعض الحالات من حدة شرط ضرورة استئذان النيابة العامة القاضى الجزئى، حتى تتمكن من مباشرة الاعتراض فى الحالة التى تتولى التحقيق بنفسها بصدد جريمة من الجرائم الإلكترونية وتبين لها ضرورة اعتراض وتسجيل اتصالات إلكترونية عبر الإنترنت. وذلك كسبًا للوقت للتحفظ على الدليل وضبطه.

وجدير بالذكر أن قرار رئيس الجمهورية بالقانون رقم ٩٤ لسنة ٢٠١٥ بإصدار قانون مكافحة الإرهاب [٥٩] قد نص فى مادته (٤٦) على أن "للنيابة العامة أو سلطة التحقيق المختصة بحسب الأحوال فى جريمة إرهابية، أن تأذن بأمر مسبب لمدة لا تزيد على ثلاثين يوما بمراقبة وتسجيل المحادثات والرسائل التى ترد على وسائل الاتصال السلكية واللاسلكية وغيرها من وسائل الاتصال الحديثة، وتسجيل وتصوير ما يجرى فى الأماكن الخاصة أو عبر شبكات الاتصال أو المعلومات أو المواقع الإلكترونية، وما يدون فيها وضبط المكاتبات والرسائل العادية أو الإلكترونية والمطبوعات والطرود والبرقيات بجميع أنواعها.

ويجوز تجديد الأمر المشار إليه فى الفقرة الأولى من هذه المادة مدة أو مددا أخرى مماثلة".

– **فائدة المراقبة فى إظهار الحقيقة:** تقرر التشريعات أن "ضابط فائدة المراقبة فى ظهور الحقيقة" يعتبر السند الشرعى المبرر للمراقبة، ذلك بسبب أن هذا الإجراء يتضمن اعتداء جسيما على حرمة الحياة الخاصة وسرية الاتصالات، فيباح استثناء وفى حدود ضيقة وذلك للفائدة المنتظرة منه والتى تتعلق بإظهار الحقيقة بكشف غموض الجريمة وضبط الجناة. ويترك لقاضى التحقيق أو للقاضى الجزئى تقدير مدى فائدة مراقبة المحادثات التليفونية فى كشف الحقيقة ويخضع فى هذا التقدير لرقابة قضاء الموضوع [٦٠].

المراجع والهوامش

١- عبد الفتاح بيومى حجازى، الإثبات الجنائى فى جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٥، ص٣.

٢- نبيلة هبة هرول، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات – دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، ٢٠٠٦، ص٢٦٦.

٣- هلالى عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٧، ص ٢٥٠، ص ٢٥٣.

٤- انظر: علاء عبد الرزاق السالمى، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، ٢٠١٠، المملكة العربية السعودية، ص ١٢١ وما بعده؛ هلالى عبد اللاه أحمد، تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى- دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٦، ص ص ١٩٨-١٩٩.

٥- هناك خدمات مصرفية إلكترونية عديدة قد أدخلتها المصارف وأهمها: خدمات التوكيل الإلكترونى، خدمة الصراف الآلى والتى تستخدم فى السحب والإيداع النقدى وتحويل الأموال بين الحاسبات لنفس الشخص أو لشخص آخر، وإجراء الحوالات التجارية وتسديد أقساط القروض، وتسديد فواتير الهاتف والكهرباء، ودفع فواتير المشتريات، وإيداع الشيكات فى الحساب، وغيرها.

٦- المؤتمر الدولى الخامس عشر للجمعية الدولية لقانون العقوبات، والذى عقد فى ريو دى جانيرو بالبرازيل فى الفترة من ٤-٩ سبتمبر ١٩٩٤.

7 - L'Article 17-1/3du Loi no 2003-239 du 18 mars 2003 pour la sécurité intérieure en Frqnce dispose que:(Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article pouvent ètre copiées sur tout support Les supports de stockage informatique peuvent ètre saisis et placés sous scellés dans les conditions prévues par le présnt code.

٨ – هلالى عبد اللاه أحمد، تفتيش نظم الحاسب الآلى، مرجع سابق، ص ١٩٩.

٩- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤، ص١٠٠.

١٠- هلالى عبد اللاه أحمد، مرجع سابق، ص ٢٠١.

11 - Sagros "Pierre" et Masse "Michel": le "droit pénal et informatique", études du 15 Nov 1990 – Publication d'institut de sciences Criminelle, faculté de droit poitierséd. cujas tom. IV .p.25.

١٢- نقض ١٩٣٧/٤/٥، مجموعة القواعد القانونية، ص ٦٣.

١٣- نقض ١٩٨٠/١١/١٧، مجموعة أحكام النقض، السنة ٢١، ص ١٠٠٦.

١٤ – هلالى عبد اللاه أحمد، تفتيش نظم الحاسب الآلى، مرجع سابق، ص ٢٠٠.

١٥- هلالى عبد اللاه أحمد، المرجع السابق، ص ٢٠٠.

١٦ – هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص ٩٨.

١٧- المادة رقم (١٩) الاتفاقية الأوروبية حول الجريمة الافتراضية لعام ٢٠٠١.

١٨ – هلالى عبد اللاه أحمد، مرجع سابق، ص٨٣.

19- CROZE (H): "L' Apport du Droit Pénal a la théorié générale du droit de l'informatique ".J. c. p. 1988, 1.333. No. 16.

20- Moehrenschlager (manfred): "Computer crimes and other crimes against information technology in Germany. National Report." R. I. D. P. 1993. p. 351.

21- Roger Merle – Andre vitu: Traité de droit criminel. Proc-édure pénal. Cujas, Paris, (5 édition), 2001. p. 1802.

22- Meunier (c): La loi du 28 November 2000 relative a la criminalite informatique Crime. Rev. dr. pen. 2002, p. 674.

٢٣- تنص المادة (٥٦) من قانون الإجراءات الجنائية المصرى على أنه "توضع الأشياء والأوراق التى تضبط فى حرز مغلق وتربط كلما أمكن، ويختم عليها، ويكتب على شريط داخل الختم تاريخ المحضر المحرر بضبط تلك الأشياء، ويشار إلى الموضوع الذى حصل الضبط من أجله".

٢٤- فى ٨ نوفمبر ٢٠٠١ قامت لجنة الوزراء للمجلس الأوروبى باعتماد الاتفاقية وتقريرها التفسيرى خلال دورتها ١٠٩ وكانت الاتفاقية جاهزة على التوقيع فى ٢٣ نوفمبر ٢٠٠١ فى بودابست بمناسبة المؤتمر الدولى عن جرائم الكمبيوتر.

٢٥- للاطلاع على النص الكامل لاتفاقية بودابست، يرجى مراجعة الموقع الخاص بالمجلس الأوروبى:

http://www.convention.coe.int/treaty/EN/treaties/htm1/185.htm.

– وقد جاء فى ديباجة اتفاقية المجلس الأوروبى حول الإجرام السيبيرى بيانُ لمخاطر انتشار شبكة المعلومات على ما يلى:

اقتناعًا من الدول أعضاء مجلس الاتحاد الأوروبى بضرورة منح الأولوية للسعى من أجل تنفيذ سياسة جنائية مشتركة، تهدف إلى حماية المجتمع من أخطار جرائم الإنترنت، وهى التى تشمل أمورًا من بينها تبنى التشريع المناسب ودعم التعاون الدولى.

– وإدراكا لعمق التغيرات التى أحدثها التحول إلى الإلكترونية وارتباط شبكات الكمبيوتر مع بعضها البعض مع استمرار عولمتها.

– وانشغالًا بمخاطر احتمال استخدام شبكات الكمبيوتر والمعلومات الإلكترونية أيضا فى ارتكاب جرائم جنائية.

٢٦– الوثيقة التفسيرية لاتفاقية بودابست، الذى أعدته لجنة الوزراء للمجلس الأوروبى خلال دورتها، ١٠٩، فى ٨ نوفمبر ٢٠٠١.

٢٧ – الوثيقة التفسيرية لنص اتفاقية بودابست، لمرجع سابق.

28- Agent may direct providers to preserve existing record pending the issuance of compulsory legal process. Such requests have no however, prospective effect.

– بمعنى "يمكن لرجال الضبط القضائى توجيه مزودى الخدمات للتحفظ على سجلات موجودة فى انتظار اتخاذ إجراء قانونى إجبارى، ومع ذلك فإن مثل هذه الطلبات ليس لها تأثيرًا مستقبلًا".

٢٩– قد عرفت المادة الأولى (١) فقرة (ج) من المذكرة التفسيرية لاتفاقية بودابست مزود الخدمات بأنه "كل من يقوم بخدمات الاتصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، وقد يكون جهة عامة أو جهة خاصة، وقد يقدم خدماته للجمهور أو المجموعة من المستخدمين الذين يشكلون مجموعة مغلقة (كشركة مثلا).

٣٠– عمر محمد أبو بكر بن يونس، الإجراءات الجنائية عبر الإنترنت فى القانون الأمريكى – المرشد الفيدرالى لتفتيش وضبط الحواسيب وصولًا إلى الدليل الإلكترونى فى التحقيقات الجنائية، دار النهضة العربية، ٢٠٠٨، ص٢٨١.

31 - Art. L. 32-3-1 alinéa 1 du code des postes et télécommunications dispose que: "Les opérateurs de télécommunications, et notamment ceux mentionnés á l'aricle 43-7 de la loi n°86-1067 du 30 septembre 1986 précitée, sont tenus d'effacer ou de rendre anonyme toute donnée relative á une communication dés que celle-ci est achevée, sous réserve des dispositions des II, III et IV".

٣٢- ينبغى التنبيه أن المشرع الفرنسى مد التزام مزودى الخدمات فى الحفاظ على البيانات المتعلقة بشخصية المتراسلين عبر شبكة الإنترنت، وأسماء المواقع التى رجعوا إليها، ليشمل محتوى المراسلة نفسها والتى كان يحظر قانون الأمن اليومى الاحتفاظ بها، ليصبح ذلك جائزًا بمقتضى قانون الأمن الداخلى لسنة ٢٠٠٣، وبالتالى يصبح القانون الفرنسى يتوافق مع قانون خصوصية الاتصالات الإلكترونية الأمريكى (ECPA).

33 - Art. L. 23-3-1 alinéa 2 du code des postes et télécommunications dispose que: "Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant á effacer ou á rendre anonymes certaines catégories de données techniques".

٣٤- هناك فرق بين التحفظ على البيانات والاحتفاظ أو أرشفة البيانات ويقصد بالأول حفظ بيانات سبق وجودها فى شكل مخزن، وحمايتها من كل شىء يمكن أن يؤدى إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة. أما الثانى فيقصد به تجميع البيانات والاحتفاظ بها فى المستقبل بدون ضمان سلامتها وسريتها، فهو عملية تخزين فقط لا غير.

٣٥- انظر: المذكرة التفسيرية لاتفاقية بودابست، ٢٠٠٢.

٣٦- مادة (٢٧٤) إجراءات جنائية مصرى "لا يجوز استجواب المتهم إلا إذا قبل ذلك، وإذا ظهر أثناء المرافعة والمناقشة بعض وقائع، يرى لزوم تقديم إيضاحات عنها من المتهم لظهور الحقيقة، يلفته القاضى إليها، ويرخص له بتقديم تلك الإيضاحات، .....".

٣٧- انظر: المذكرة التفسيرية لاتفاقية بودابست، مرجع سابق.

٣٨- أغفل المشرع المصرى فى قانون الإجراءات الجنائية تعريف (المراقبة)، واكتفى بوضع تنظيم لهذه العملية فى المادتين (٩٥)، (٢٠٦) من القانون المذكور. فى حين عرفه المشرع الأمريكى فى الباب الثالث من القانون الفيدرالى الأمريكى "المراقبة" والتى يرمز إليها بكلمة "interception"، أنه "الاكتساب السمعى أو أى اكتساب لمحتويات أى اتصال سلكى أو إلكترونى أو شفوى باستخدام أى جهاز إلكترونى، أو ميكانيكى أو أى جهاز آخر". وقد قضى بأن المقصود بكلمة الاكتساب "Acquisition" أن يتم الالتقاط أثناء الاتصال نفسه ومن ثم تسجيله. لمزيد من التفصيل انظر: شيماء عبد الغنى عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، ٢٠٠٧، ص٣٠٥ وما بعدها.

٣٩- عرف قانون الاتصالات الإلكترونية الأمريكى لسنة ١٩٨٦ الاتصالات الإلكترونية بأنها: "كل انتقال بشكل كلى أو جزئى للإشارات أو الصور أو الأصوات أو المعطيات أو المعلومات أيًا كان نوعها، عن طريق الكابل أو الراديو أو النظام الكهرومغناطيسى أو التصوير الكهربائى أو الصور المرئية. فى حين عرف قانون البريد والاتصالات الإلكترونية الفرنسى Code des postes et des communication Décret n°80-567, eléctroniques (Journal الاتصالات الإلكترونية بأنها: "كل انتقال أو إرسال أو استقبال (Officiel du 23 juillet 1980 لإشارات أو علامات أو كتابة أو صور أو أصوات عن طريق النظام الكهرومغناطيسى.

٤٠- اخترع العالم الأمريكى (راى توملينستون) البريد الإلكترونى، إذ صمم على شبكة الإنترنت برنامجًا لكتابة الرسائل سمى (send massage) وذلك بهدف تمكين العاملين بالشبكة من تبادل الرسائل فيما بينهم، ومن ثم ابتكر برنامجا سمى (cygnet) يسمح بنقل الملفات من جهاز حاسب إلى آخر، ومن ثم قام بدمج البرنامجين فى برنامج واحد ونتج عنه البريد الإلكترونى، وقد واجه توملينستون مشكلة مفادها أن الرسالة لا تحمل عنوان مرسلها ففكر بابتكار رمز لا يستخدمه الأشخاص فى أسمائهم، يوضع بين أسم المرسل والموقع الذى ترسل منه الرسالة واختار الرمز (@) وأصبح أول عنوان بريد إلكترونى فى التاريخ عام١٩٧١، تحت عنوان (Tomlinson @ bbn- Tenexa).

- انظر: سامى جلال فقى حسين، الأدلة المتحصلة من الحاسب وحجيتها فى الإثبات الجنائى- دراسة مقارنة، دار الكتب القانونية، ٢٠١١، ص ٢٥٣، وانظر أيضًا: شمسان ناجى صالح الخيلى، الجرائم المستحدثة بطرق غير مشروعة لشبكة الإنترنت – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٧، ص ٢٣٩.

٤١- لمزيد من التفاصيل انظر: عطا عبد العاطى محمد السنباطى، موقف الشريعة الإسلامية من جرائم الحاسب الآلى والإنترنت، ط ١، دار النهضة العربية، القاهرة، ٢٠٠٢، ص٣٧.

٤٢- إيهاب عبد المطلب، الموسوعة الجنائية الحديثة فى شرح قانون الإجراءات الجنائية، المركز القومى للإصدارات القانونية، القاهرة، الجزء ١، ٢٠٠٩، ص ٢٥٠.

43 - crim.4 sept. 1991: Bull.crim.no 132.

44 - United States v. Smith, 155 F. 3d 1051, 1058-59 (9thCir. 1998).

٤٥- ياسر الأمير فاروق محمد، مراقبة الأحاديث الخاصة فى الإجراءات الجنائية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠٠٨، ص١١.

٤٦- انظر: آدم عبد البديع آدم، الحق فى حرمة الحياة الخاصة ومدى الحماية التى يكفلها له القانون الجنائى، رسالة دكتوراة، جامعة القاهرة، ٢٠٠٠، ص٦٧٧؛ عفيفى كامل عفيفى، جرائم

الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ودور الشرطة والقانون، دراسة مقارنة، منشأة المعارف، الإسكندرية، بدون تاريخ، ص ٢٦٤ وما بعدها.

٤٧- أحمد حسام طه تمام، الحماية الجنائية لتكنولوجيا الاتصالات، دراسة مقارنة، دار النهضة العربية، ٢٠٠٢، ص ٣٥.

48– Renault – Brahinskg (Corinne), l'essentiel de la procédure pénale, 5e éd., gualino étiteur, E J A, coll. "les carres" paris, 2004, p. 330.

٤٩- لمزيد من التفاصيل حول المعايير التى تعتد بها التشريعات الجنائية لتحديد مفهوم الحديث الخاص محل المراقبة سواء بالمعيار الموضوعى (مدى تعلق محتوى الحديث بالسرية) أو بمعيار شكلى (معيار طبيعة المكان). انظر: آدم عبد البديع آدم، الحق فى حرمة الحياة الخاصـــة ومدى الحماية التى يكفلها له القانون الجنائى، مرجع سابق، ص ٦٧٧ وما بعدها، طارق سرور، حق المجنى عليه فى تسجيل المحادثات التليفونية الماسة بشخصه، دار النهضة العربية، الطبعة الثانية، ٢٠٠٤، ص ١٨، وما بعدها.

٥٠- عائشة بن قارة، حجية الدليل الإلكترونى فى مجال الإثبات الجنائى – دراسة مقارنة فى القانون الجزائرى والقانون المقارن، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، ٢٠١٠.

٥١- بخصوص هذه النقطة ذهبت المحكمة الابتدائية بباريس فى حكم مختلف صادر بتاريخ ٢٠١٣/١/٣٠ بأن مزودى الخدمات ملزمون بحكم القانون بتمكين الجهات القضائية بالبيانات والمعطيات التى تدخل فى إطار حوزتهم، وذلك لأغراض بحث مدنية أو جنائية، وأن الجهات المذكورة لا تتحمل أية مسئولية قانونية مادام القانون الفرنسى والقوانين الأوروبية تجيز لها ذلك.

٥٢- عمر محمد أبو بكر بن يونس، مرجع سابق، ص٣٨٦ وما بعدها.

٥٣- عائشة بن قارة، حجية الدليل الإلكترونى فى الإثبات فـى المجـال الجنائى، مرجع سابـق، ص ١٧٣.

54- Article (100) de (C.P.P) Francais dispose que: "En matiére criminelle et en matiére corr-ectionnelle, si la peine encourue est égale ou supérieure á deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspon-dances émises par la voie des télécommunications".

٥٥- مادة (٥٧) الدستور المصرى ٢٠١٤ "للحياة الخاصة حرمة، وهى مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التى يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين

فى استخدام وسائل الاتصال العامة بجميع أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك".

٥٦- مادة (٩٥) إجراءات جنائية مصرى "لقاضى التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت فى مكان خاص متى كان لذلك فائدة فى ظهور الحقيقة فى جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر...".

- مادة (٢٠٦) إجراءات جنائية مصرى "لا يجوز للنيابة العامة تفتيش غير المتهم أو منزل غير منزله إلا إذا اتضح من إمارات قوية أنه حائز لأشياء تتعلق بالجريمة. ويجوز لها أن تضبط لدى مكاتب البريد وجميع الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق وجميع البرقيات، وأن تراقب المحادثات السلكية واللاسلكية، وأن تقوم بتسجيلات لمحادثات جرت فى مكان خاص متى كان لذلك فائدة فى ظهور الحقيقة فى جناية أو فى جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. ويشترط لاتخاذ أى إجراء من الإجراءات السابقة الحصول مقدما على أمر مسبب بذلك من القاضى الجزئى بعد اطلاعه على الأوراق. وفى جميع الأحوال يجب أن يكون الأمر بالضبط أو الاطلاع أو المراقبة لمدة لا تزيد على ثلاثين .....".

٥٧- إلا أن هناك حالات خاصة يعقد فيها الاختصاص للنيابة العامة بصفة استثنائية فى مباشرة إجراء المراقبة دون حاجة للحصول على إذن من القاضى الجزئى، وذلك إذا تعلق الأمر بجناية تختـص بنظرها محكمة أمن الدولة العليا وهى الجرائم المضرة بأمن الدولة من جهة الداخل وذلك بموجب نص المادة (٢/٧) من القانون رقم ١٠٥ لسنة ١٩٨٠ والخاص بإنشاء محاكم أمن الدولة إلا أنه تم إلغاء هذا القانون بالقانون رقم (٩٥ لسنة ٢٠٠٣). انظر: هبة أحمد على حسانين، الحماية الجنائية لحرمة الحياة الخاصة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٧، ص٣٩٦.

٥٨- نقض ١٤ فبراير ١٩٦٧، مجموعة أحكام النقض، س ١٨، رقم ٤٢، ص ٢١٩. وأيضا نقض ٢٥ أكتوبر ١٩٧٢، رقم ٢٤، ص ٢١١.

٥٩- الجريدة الرسمية، السنة ٥٨، العدد ٣٣ مكرر، ١٥ أغسطس ٢٠١٥، ص ٢٣.

٦٠- محمود نجيب حسنى، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، ١٩٩٨، ص ٦٦٨.

EVIDENCE SEIZURE IN ELECTRONIC CRIMES: TRADITIONAL AND MODERN PROCEDURES

Hend Nageb

The study focuses on traditional and modern procedures of evidence seizure in electronic crimes. It sheds light on the extreme importance and difficulties faced by law enforcement and investigation authorities, relative to said procedures and crimes., Whereas computer system has material and non-matrial contents, such as data and information, the seizure is not restricted to material contants only; but also involves the non-matrial contents and e-mails as well.