إجراءات ضبط المكونات المعنوية للحاسوب والإنترنت

الدكتور علي حسن الطوالبه

مستشار قانوني بمجلس الشورى

مملكة البحرين

تمهيد وتقسيم:

يُعلّم الباحثون والعاملون في القانون الجنائي إمكانية ضبط الكيانات التقليدية والمتمثلة بالمنقولات والعقارات، والكيانات المادية للحاسوب، والمتمثلة بأجهزته وملحقاته الرئيسة والفرعية، وكذلك الحال بالنسبة لشبكات الحاسوب والإنترنت، إذ يمكن رصد الاتصالات التي تتم خلال عمل الحاسوب أو الإنترنت، وتسجيل محتوياتها، هذا بالإضافة إلى إمكانية ضبط الحاسوب بشكل كامل لتأكيد الاحتفاظ بالدليل إذا كان مُشغل الجهاز غير متعاون بما فيه الكفاية.

أما بالنسبة لمكونات الحاسوب المعنوية والإنترنت فالمسألة تحتاج إلى البحث بشكل دقيق، فعند تفتيش مكونات الحاسوب المادية، هل يضبط الشيء المادي أم تضبط البيانات غير المادية؟ وما هو السند القانوني في ذلك؟

ونجيب عن هذه التساؤلات، عبر ثلاثة مطالب :

المطلب الأول: ضبط البيانات المعالجة بواسطة الحاسوب والإنترنت.

المطلب الثاني: ضبط المراسلات والبريد الإلكتروني عبر شبكة الحاسوب والإنترنت.

المطلب الثالث: أحكام ضبط نظم الحاسوب والإنترنت والمراسلات والبريد الإلكتروني.

المطلب الأول

ضبط البيانات المعالجة بواسطة الحاسوب والإنترنت

اختلفت التشريعات الإجرائية والاتجاهات الفقهية في مسألة ضبط الأشياء المعنوية أو الكيانات المنطقية والتي لا يمكن بطبيعتها أن تكون محلاً لوضع اليد[1]، وانقسمت هذه التشريعات والاتجاهات إلى ثلاث اتجاهات رئيسة:-

الاتجاه الأول: يرى أصحابه أنه لا يمكن تصور إجراء الضبط على الكيانات المنطقية لانتفاء الكيان المادي عنها، ويرى فقهاء هذا الاتجاه أن بيانات الحاسوب ليست مثل الأشياء المادية المحسوسة وبالتالي لا يقع الضبط عليها[2].

ومن التشريعات التي أخذت بهذا الاتجاه قانون الإجراءات الجنائية الألماني، فقد قصرت المادة (94) منه، محل الضبط على الأشياء المادية المحسوسة أو الملموسة، ويفسر الفقه الألماني نص هذه المادة بأن البيانات المعالجة إلكترونيًا لا يمكن ضبطها مجردة، ذلك لأنها تفتقر إلى الكيان المادي، لكن عند تحويلها أو إضافتها إلى كيان مادي يمكن ضبطها مثل طباعة هذه البيانات على الأوراق، ويمكن ضبط البيانات أيضًا بتصوير الشاشة أو نقلها على حافظة البيانات، ومن ثم يمكن التعامل معها، ضمن ما تنص عليه المادة (161) إجراءات ألمانية، والتي تجيز الحصول على البيانات المعروضة على شاشة الحاسوب عن طريق التصوير الفوتوغرافي أو بنقلها على دعامة مادية أو وعاء آخر للبيانات [3].

وفي رومانيا، فإن الضبط ينصب على الدعامة المادية المدون عليها بيانات الحاسوب، كالأشرطة المغناطيسية أو الأقراص، وليس على الكيان غير المادي[4].

واتبعت اليابان نفس النهج، فالسجلات الإلكترومغناطيسية تكون– في منظور الفقه لديها – غير مرئية في حد ذاتها، ولذلك لا يمكن ضبطها، وبالتالي ينبغي تحويل هذه السجلات غير المادية إلى صورة مادية محسوسة يمكن قراءتها بعد طباعتها[5].

1- د. محمد زكي أبو عامر – الإجراءات الجنائية – ط2 – منشأة المعارف الإسكندرية – 1990م – ص 629.

2- انظر: د.هشام محمد فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – 1994م– ص 93-94.

3- انظر: د.هلالي عبداللاه أحمد – تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – دراسة مقارنة – ط1 – دار النهضة العربية – القاهرة – 1997م– ص 85.

4- المصدر السابق – ص 85.

يرى أصحاب هذا الاتجاه أن يُصار إلى التدخل التشريعي لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط لتشمل بجانب الأشياء المادية، البيانات الإلكترونية بكافة أنواعها وأنماطها المحوسبة[6]، ويقترح أتباع هذا الاتجاه إضافة عبارة المواد المعالجة عن طريق الحاسوب أو بيانات الحاسوب إلى النص القانوني الذي ينص على التفتيش والضبط ليشمل هذا التطور التكنولوجي الحاصل في بيئة المعلومات.

الاتجاه الثاني:يذهب إلى أنه لا يوجد ما يمنع من أن يرد الضبط على البيانات الإلكترونية، مستندين إلى أن الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة، وبالتالي يمتد هذا المفهوم ليشمل البيانات الإلكترونية بمختلف أشكالها، ويميز أصحاب هذا الاتجاه بين المعلومات وبين البيانات المعالجة آليًا فينفي الطابع المادي عن أولها، ويؤكد للثانية الطابع المادي على أساس أنها (نبضات أو ذبذبات إلكترونية.. وإشارات أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزن على وسائط معينة ويمكن قياسها)، وبالتالي ينفون الطابع المعنوي لهذه البيانات مؤكدين أنها شيء يمكن لمسه في المحيط الخارجي وأنها كيان مادي لا يمكن إنكاره مستندين في ذلك إلى حكم محكمة جنح بروكسل الذي أكد على كون هذه البيانات أشياء مادية محسوسة[7]، وانتهوا إلى إمكانية خضوع هذه البيانات لقواعد التفتيش التقليدية وبالتالي إمكانية ضبطها. ومن التشريعات التي سارت على هذا النهج، قانون الإجراءات الجنائية اليوناني في المادة (251)، والتي تعطي سلطة التحقيق إجازة القيام "بأي شيء" وهذا يعني أن التحقيق يشمل ضبط البيانات المخزنة أو المعالجة إلكترونيًا، لذا لا توجد أية مشكلة في اليونان في ضبط البيانات الإلكترونية، إذ بمقدور المحقق أن يعطي أمرًا للخبير أن يجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحكمة الجنائية[8].

وسار في هذا الاتجاه، القانون الكندي في المادة (487)، والتي تعطي سلطة إصدار إذن لضبط "أي شيء" طالما تتوافر أسس معقولة للاعتقاد بأن الجرم ارتكب، أو يشتبه في ارتكابه، وأن هناك نية في

5– المصدر السابق – ص 85.
6- انظر: د. عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة- ص 359. ود. هشام محمد فريد رستم – الجوانب الإجرائية – ص 95-96.
7- د. عفيفي كامل عفيفي –مصدر سابق – ص 344.
8- انظر: د. هشام محمد فريد رستم الجوانب الإجرائية – مصدر سابق – ص 95، وهلالي عبدالاه أحمد – التفتيش – مصدر سابق – ص 82. وانظر: د. أحمد السمدان – النظام القانوني لحماية برامج الكمبيوتر – مجلة الحقوق – السنة 11 – العدد 4 – جامعة الكويت – الكويت – ديسمبر - 1987 – ص 35 وما بعدها.

أن يستخدم في ارتكاب الجرم، أو أنه سوف ينتج دليلاً على وقوع الجرم[9]، وكذلك الحال في القانون اللوكسمبورجي، فالضبط يشمل بصفة عامة: (كل الأشياء التي تفيد في إظهار الحقيقة)، فيمكن بالتالي ضبط البيانات الإلكترونية، وفي فرنسا ذهب بعض الفقهاء إلى الاعتراف بأن للبرنامج كيانًا ماديًا ملموسًا يتمثل في نبضات إلكترونية أو إشارات إلكترونية مغناطيسية أو ممغنطة[10]، كما يستند الفقه الأمريكي في تبريره لهذا الاتجاه للتشريع الخاص بما قبل المحاكمة لسنة 1975م، الذي نص على أنه: (إلا إذا حظر في أي ضبط أي أدلة أو معلومات تتعلق بالجريمة المرتكبة أو أي جريمة أخرى وذلك باستثناء المعلومات المحضة)[11].

الاتجاه الثالث: يرى أن مصدر الخلاف بين هذه الاتجاهات السابقة هو الخلط بين طبيعة حق صاحب الشيء على الشيء من حيث أنه نتاج لفكرة من ناحية وطبيعة الشيء في ذاته من ناحية أخرى[12]. وعلى حسب الرأي الغالب في الفقه القانوني فإن البرامج أو الكيانات المنطقية هي عمل ذهني، وهي خلاصة فكر خبير البرمجة الذي صاغه على شكل أوامر مرتبة ترتيبًا منطقيًا موجهة إلى الحاسوب، والبرامج بهذا المفهوم تدخل في نطاق الأحكام الخاصة بحقوق المؤلف[13].

ومن هذا المنطلق نجد أن التشريعات العقابية في معظم دول العالم، مدت نطاق الحماية الجنائية لحقوق المؤلف لتشمل برامج الحاسوب كقوانين حماية تقنية المعلومات أو قوانين جرائم تقنية المعلومات أو قوانين حماية حق المؤلف. ونرى أن الاتجاه المقنع هو ما ذهب إليه أصحاب الاتجاه الأول من أنه لا يمكن إجراء الضبط على الكيانات المنطقية لانتفاء الكيان المادي عنها، وأن بيانات الحاسوب ليست مثل الأشياء المادية المحسوسة وبالتالي لا يقع الضبط عليها، إلا بعد تحويلها إلى

9- وبالإضافة إلى ما تقدم، فقد نصت المادة (79) من قانون الإثبات الكندي على أنه: (ما لم يرد ما يخالف ذلك في أمر التفتيش، فإن تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية (كبنك مثلاً) يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخ من المواد المكتوبة). وينطبق النص سواء أكانت السجلات مكتوبة أم كانت في شكل (سجلات الحاسوب). انظر: د. هشام محمد فريد رستم – الجوانب الإجرائية –مصدر سابق – ص 96.، ود. عفيفي كامل عفيفي – التفتيش - مصدر سابق – ص 358.

10- انظر: د. هلالي عبدالاه أحمد – مصدر سابق – ص 83.

11- انظر: د. عفيفي كامل عفيفي – مصدر سابق – ص 359.

12- انظر: د. هلالي عبدالاه أحمد – التفتيش - مصدر سابق – ص 87-88.

13- انظر: د.خالد حمدي عبد الرحمن- الحماية القانونية للكيانات المنطقية- رسالة دكتوراه- جامعة عين شمس – القاهرة- 1992م– ص 58 وما بعدها.و د.محمد عبد الظاهر حسين – الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية – دار النهضة العربية – القاهرة – 2001/2000م– ص 8 وما بعدها. وانظر: د.رشا مصطفى أبو الغيط – الحماية القانونية للكيانات المنطقية – برامج الحاسب الآلي – وصف البرامج – المستندات الملحقة – ملتقى الفكر – الإسكندرية – 2000م– ص 5 وما بعدها.

كيانات مادية كطباعتها على الورق أو إفراغ البيانات على الأقراص المرنة أو المدمجة وضبطها بعد ذلك.

المطلب الثاني
ضبط المراسلات والبريد الإلكتروني

يقصد بالمراسلات بصورة عامة جميع الرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد، وجميع البرقيات لدى مكاتب البرق، والمحادثات السلكية واللاسلكية، وأكدت على حمايتها إعلانات حقوق الإنسان والمواثيق والاتفاقيات الدولية والإقليمية الحديثة[14]، وأكثر الدساتير المعاصرة[15]، ومنها الدستور البحريني في المادة (26) على أن : (حرية المراسلة البريدية والبرقية والهاتفية والإلكترونية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أو إفشاء سريتها إلا في الضرورات التي يبينها القانون، ووفقًا للإجراءات والضمانات المنصوص عليها فيه). وكذلك الدستور الأردني في المادة (18) والتي نصت على أن: (تعتبر جميع المراسلات البريدية والبرقية والمخاطبات الهاتفية سرية، فلا تخضع للمراقبة أو التوقيف إلا في الأحوال المعينة في القانون).

أما الأحوال المعينة في القانون فتجسدت في نص المادة (93) إجراءات جنائية بحريني: (يجوز للنيابة العامة أن تضبط لدى مكاتب البريد جميع الخطابات والرسائل والجرائد والمطبوعات والطرود، ولدى مكاتب البرق جميع البرقيات، وأن تراقب المحادثات والمراسلات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية

14- نصت المادة (12) من الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة في 1948/12/10م على أنه: (لا يجوز تعرض أحد لتدخل تعسفي في حياته الخاصة... أو مراسلاته ... ولكل شخص الحق في الحماية القانونية ضد هذا التدخل)، وبهذه الصياغة تقريبًا وردت كذلك المادة (17) من الاتفاقية الدولية بشأن الحقوق المدنية والسياسية الصادرة عام 1976م، وعلى المستوى الدولي الإقليمي، تحظر المادة (2) من الاتفاقية الأوروبية لحقوق الإنسان وحرياته الأساسية في أحوال استثنائية حددتها كل صور التعرض للحق في المراسلة سواء بالرقابة أو غيرها، أما على مستوى الأقطار العربية والإسلامية فقد نصت المادة (18/ب) من إعلان القاهرة لحقوق الإنسان في الإسلام في عام 1990م، أن للإنسان الحق في الاستقلال بشؤون حياته الخاصة في مسكنه وأسرته وماله واتصالاته، ولا يجوز التجسس أو الرقابة عليه أو الإساءة إلى شخصه، ويجب حمايته من كل تدخل تعسفي). انظر: د.محمود شريف بسيوني ود.عبد العظيم الوزير – الإجراءات الجنائية في النظم القانونية العربية وحماية حقوق الإنسان – ط1 – دار العلم للملايين – بيروت – 1991م– ص 17-343.

15- انظر: المادة (45) من الدستور المصري لعام 1971.

أو جنحة معاقب عليها بالحبس، ويشترط لاتخاذ أي من الإجراءات السابقة الحصول مقدمًا على إذن بذلك من قاضي المحكمة الصغرى، ويصدر القاضي هذا الإذن بعد اطلاعه على الأوراق، وفي جميع الأحوال يجب أن يكون الضبط أو المراقبة أو التسجيل بناء على أمر مسبب ولمدة لا تزيد على ثلاثين يومًا قابلة للتجديد لمدة أو مدد أخرى مماثلة).

ويقابلها نص المادة (88) أصول أردني والتي جاء فيها: (للمدعي العام أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود، ولدى مكاتب البرق كافة الرسائل البرقية كما يجوز له مراقبة المحادثات الهاتفية متى كان لذلك فائدة في إظهار الحقيقة)[16].

وإذا كان قانون الإجراءات الجنائية البحريني وقانون أصول المحاكمات الجزائية الأردني قد أوردا نصوصًا تجيز ضبط الرسائل ومراقبة المحادثات الهاتفية، فهل تسري هذه الأحكام الإجرائية على المراسلات الإلكترونية المستحدثة كالبريد الإلكتروني، وما مدى مشروعية التنصت والمراقبة الإلكترونية لشبكات الحاسوب والإنترنت؟

تتشابه – إلى حد ما – الرسائل الإلكترونية المرسلة عبر البريد الإلكتروني مع الرسائل التقليدية المرسلة عبر البريد العادي، من حيث أن البريد الإلكتروني يحتوي على برامج متخصصة لكتابة وإرسال واستعراض وتخزين الرسائل الإلكترونية، ومن الخدمات التي تقدمها هذا البرامج ما يعرف باسم الإمضاء أو التوقيع الإلكتروني، فبدلاً من أن يكتب المستخدم اسمه في نهاية كل رسالة يقوم البرنامج ببيان إمضائه ومعلومات عنه، أما بخصوص ما يتعلق بالمحافظة على سرية البريد الإلكتروني، فقد عالجت نظم البريد الإلكتروني هذا الموضوع بابتكار برامج تشفير خاصة بحيث لا يمكن الإطلاع على أية رسالة إلا ممن يعرف تلك الشفرة[17]، والتعامل مع الرسالة الإلكترونية لا يختلف عن التعامل مع الرسالة الورقية إذ بمقدور المستخدم أن يطرحها جانبًا أو يرد عليها أو ينقلها

16- انظر: المادة (95) إجراءات مصري، والمادة (96) أصول سوري، والمادة (79) من القانون الليبي.

17- هناك عدد من البرامج التشفيرية مثل البرنامج المعروف باسم البريد بالغ السرية، وبرنامج سري جدًا، وهو من أكثر برامج تشفير البريد شيوعًا في الولايات المتحدة الأمريكية وأوروبا – انظر: بهاء شاهين – شبكة الإنترنت –ط1- الدار العربية لعلوم الحاسب – القاهرة – 1996م – ص 59. ومع التوسع المتزايد لطريق المعلومات السريع سوف تطبق خدمات الأمن على كل أشكال المعلومات الرقمية: المكالمات الهاتفية، والملفات، وقواعد البيانات، وأي شيء آخر يمكن أن يخطر ببال الإنسان، وما دام الشخص قد احتفظ لنفسه (بكلمة السر – المرور) فإن المعلومات المخزنة يمكن أن تظل محمية، في ظل أقوى قفل ومفتاح وجدا على الإطلاق، وهو ما يؤمن أقصى قدر من الخصوصية المعلوماتية يمكن أن يتوافر لأي إنسان، انظر: بيل جيتس وآخرون – المعلوماتية بعد الإنترنت (طريق المستقبل) – ترجمة أ. عبد السلام رضوان – سلسلة عالم المعرفة – المجلس الوطني للثقافة والفنون والآداب – العدد 231 – الكويت – مارس 1998 – ص 428.

إلى شخص آخر أو يحفظها في ملف خاص[18]، أما عن كيفية ضبط البريد الإلكتروني، فعلى المحقق الذي يريد ضبط الرسائل الإلكترونية الموجودة في البريد الإلكتروني أن يحدد صندوق البريد الخاص بالمتهم - محل التفتيش والضبط - والمبين في قائمة البرنامج الرئيسة، فتظهر القائمة المسدلة و بها خيارات ثلاث : الوارد (In)، والصادر (Out)، والحفظ و المهملات (Trash)، فإذا كان المحقق يريد ضبط الرسائل الإلكترونية التي وصلت إلى المتهم مثلاً فعليه أن يختار (In)، ويتم ذلك عن طريق تشغيل برامج البريد الإلكتروني في جهاز المشتكى عليه، ومراجعة قائمة الرسائل الجديدة التي وصلته ليلتقط من بينها الرسالة المطلوبة، أما قراءة هذه الرسالة أو الإطلاع عليها، فعلى المدعي العام تحريك المؤشر وتثبيته على الرسالة المطلوب قراءتها والضغط على زر الإدخال، فتظهر الرسالة كاملة أمام المدعي العام على الشاشة، وإذا كان المدعي العام يريد ضبط الرسائل التي أرسلها المشتكى عليه فعليه اختيار الصادر، أما إذا كان يريد ضبط رسالة كان قد ألغاها المشتكى عليه من قبل فعليه اختيار ملفات الحفظ أو سلة المهملات[19]، وفي كل الحالات للمدعي العام طباعة الرسائل الإلكترونية التي يتم إرسالها أو استقبالها أو تلك المحفوظة في ملفات خاصة، بيد أنه يؤخذ في الاعتبار أحكام المادة (89) من قانون أصول المحاكمات الجزائية الأردني والتي تنص على أنه: (1- إذا اقتضت الحال البحث عن أوراق فللمدعي العام وحده أو لموظف الضابطة العدلية المستناب وفقًا للأصول أن يطلع عليها قبل ضبطها.2-لا تفض الأختام ولا تفرز الأوراق بعد ضبطها إلا في حضور المشتكى عليه أو وكيله أو في غيابهما إذا دعيا وفقًا للأصول ولم يحضرا ويدعى أيضًا من جرت المعاملة عنده لحضورها، يتبع هذا الأصول بقدر الإمكان ما لم يكن هناك ضرورة دعت لخلاف ذلك.3-يطلع المدعي العام وحده على الرسائل والبرقيات المضبوطة حال تسلمه الأوراق في غلافها المختوم فيحتفظ بالرسائل والبرقيات التي يراها لازمة لإظهار الحقيقة أو التي يكون أمر اتصالها بالغير مضرًا بمصلحة التحقيق ويسلم ما بقي منها إلى المشتكى عليه أو إلى الأشخاص الموجهة إليهم.

18- ويستطيع المستخدم أن يحفظ بريده الإلكتروني بعدة طرق منها: الحفظ في صناديق بريد خاصة، أو الحفظ في ملفات أو طباعة الرسائل وحفظها في ملفات خاصة مع البريد الورقي التقليدي، وبذلك يمكن لعضو الضابطة العدلية أن يستخدم هذه الطرق لضبط الرسائل عبر البريد الإلكتروني.

19- انظر: د. هلالي عبداله أحمد – التفتيش - مصدر سابق – ص 215.

4-ينبغي أن ترسل أصول الرسائل والبرقيات المضبوطة جميعها أو بعضها أو صور عنها إلى المشتكى عليه أو إلى الشخص الموجهة إليه في أقرب مهلة مستطاعة إلا إذا كان أمر اتصالها بهما مضرًا بمصلحة التحقيق.5-أما الأوراق النقدية فتطبق عليها أحكام الفقرة الثانية من المادة (35)).وتطبيقًا لهذا النص فقد قامت سلطة التحقيق الأردنية في جريمة قتل الدكتور عوني سعد والمحامي حنا نده، بضبط جهاز الحاسوب الموجود في عيادته وعدد من الأقراص المرنة، ثم قامت السلطة المختصة بالتحقيق بقراءة وطباعة المعلومات المخزنة على (الهارد دسك) والأقراص المرنة وعددها (61) قرصًا، والمعلومات عبارة عن اتفاقيات ومحاضر اجتماعات ومراسلات عادية تتعلق بعمل المغدور، وتمت طباعة كل المعلومات وسلمت لسلطة التحقيق، ثم تم ضبط جميع المراسلات الإلكترونية **(E-MAIL)** الخاصة بالدكتور عوني سعد لبيان ما إذا كان قد تلقى أية رسائل تهديد أو أية معلومات من أشخاص مقربين ولم تجد سلطة التحقيق أي دليل على ذلك، وكانت المراسلات عادية، وتم ضبط جميع المحادثات الهاتفية أيضًا، فوجدت السلطة المختصة بالتحقيق محادثات تتضمن تهديد المغدور وردت إلى هاتف منزله وهاتف مكتبه وهاتفه النقال من مجهول يطلب فيه ترك قضية معينة، وبعد معرفة تاريخ التهديد ورقم هاتف المتصل تمت معرفة الفاعل، ثم قامت بإلقاء القبض عليه بعد إجراءات طويلة ومعقدة[20].

ومن الأمثلة على كشف الجرائم بواسطة البريد الإلكتروني، ما وقع في عام 1997م،وفي (قرين فيلد)، كاليفورينا – الولايات المتحدة الأمريكية – حيث قام المتهم (رونالد ريفا)، وصديقه (ملتون ريفا)، بالتقاط صور فاضحة لفتاة وصديقتها تتراوح أعمارهن (10-11) عامًا، خلال حفل ترفيهي نظمته ابنته لأصدقائها وصديقاتها، وبعدها قام بالاتجار بالصور الفاضحة لهن ولأطفال آخرين، فقدمت شكوى ضدهما من قبل أهل الفتاتين، وقادت التحقيقات مع المتهمين إلى حلقة دولية تعرف باسم "أورشيد" تعمل في الاتجار بالصور الفاضحة للأطفال واستغلالهم جنسيًا عبر الإنترنت، وذلك من خلال غرف النقاش، ونتج عن التحقيق توجيه تهم إلى (16) رجلاً من فنلندا وكندا والولايات المتحدة الأمريكية وأستراليا، وبفحص المعلومات الرقمية المخزنة في البريد الإلكتروني تم العثور على اعترافات للمتهمين يصفون فيها نشاطاتهم تجاه الأطفال وطريقة إغوائهم للأطفال، والتقاط الصور العارية لهم، وبعد عامين من التحقيق توصل المحققون إلى مجموعات من المجرمين تعمل

20-للمزيد من التفاصيل عن القضية انظر: نصوح محي الدين صالح مرزوقة– ص 126 وما بعدها.

في حلقة دولية تطلق على نفسها نادي "الوندرلاند"، وتعمل في (40) دولة، تم تبادل الأدلة الجنائية الإلكترونية في أجهزة الحاسوب وصناديق البريد بين الأجهزة المختصة لمحاكمة (200) شخص[21].

أما عن مدى مشروعية التنصت والمراقبة الإلكترونية لشبكات الحاسوب والإنترنت [22]، فيثور التساؤل عن إمكانية تطبيق القواعد العامة المتعلقة بمراقبة المحادثات الهاتفية وتسجيلها على ما تم ذكره سالفًا.

فالمحادثات الهاتفية تُعد من أخطر الوسائل التي تقررت استثناءً على حق الإنسان في الخصوصية، كتفتيش المنازل أو ضبط المراسلات والإطلاع عليها، لأن مراقبة المحادثات الهاتفية تتم دون علم الإنسان وتتيح سماع وتسجيل أدق أسرار حياته الخاصة، على نحو لا يستطيع التفتيش أو الإطلاع على الرسائل أن يصل إليها، فالأصل هو احترام حق الإنسان في الخصوصية ومشروعية المراقبة هي استثناء يرد على الأصل العام[23]، والغرض من مشروعية المراقبة هي تحقيق نوع من التوازن بين حق الأفراد في الخصوصية والسرية وحق المجتمع في مكافحة الجريمة بوسائل فعالة ليعيش آمنًا مطمئنًا[24].

وتتم مراقبة المحادثات الهاتفية بوسائل فنية مختلفة بقصد كشف الحقيقة، وغالبًا ما يتم بعد ذلك تسجيلها للوقوف على ما تحويه من تفصيلات وأقوال يعول عليها بوصفها دليلاً من أدلة إدانته بعد التأكد من صحة نسبتها إلى قائلها وعدم إدخال أي تغير أو تعديل عليها[25]، وفي فرنسا، فإن المواد (80 و 81) من قانون الإجراءات الجنائية، تجيز لقاضي التحقيق اتخاذ الإجراءات التي يرى فائدتها

21-انظر: اللواء د. محمد الأمين البشري – الأدلة الجنائية الرقمية – مفهومها ودورها في الإثبات – المجلة العربية للدراسات والتدريب – المجلد 17 – العدد 33 – السنة 17- الرياض – أبريل 2002 – ص 135-136.

22 -لقد أنشأت المخابرات العسكرية البريطانية مركز المساعدة الفنية الحكومية (GTAC)،وهو جهاز للتنصت الالكتروني لمراقبة الرسائل الالكترونية الخارجة من بريطانيا والمرسلة إليها، فنتساءل عن مدى مشروعية مثل هذا المركز قانونيًا، للمزيد من المعلومات انظر: د.مصطفى محمد موسى،الجهاز الالكتروني لمكافحة الجريمة، دار الكتب القانونية، مصر،2006م،ص130-131.

23- سمير الأمين – مراقبة التلفون والتسجيلات الصوتية والمرئية – ط3 – دار الكتاب الذهني – القاهرة 2000م – ص 15.

24- انظر: د. أحمد فتحي سرور – مراقبة المكالمات التلفونية – المجلة الجنائية القومية – العدد 1 – مارس 1963م – ص 146.

25- هناك أجهزة تنصت دقيقة على درجة كبيرة من الحساسية يمكنها تسجيل المحادثات الخاصة من مسافات بعيدة، وهناك أجهزة تنصت أخرى تسمح بالتنصت على المحادثات الهاتفية من خلف الحواجز أو الجدران دون الحاجة لتثبيتها في المبنى مراد التنصت على المحادثات فيه، وهناك أجهزة وأدوات عديدة، وللمزيد من المعلومات انظر: سمير الأمين – مصدر سابق – ص 8 وما بعدها.

في إظهار الحقيقة في التحقيق، ولكن ثار الجدل الفقهي حول التسجيلات المتعلقة بالأحاديث الخاصة، سواء تمت من قبل السلطة العامة أو من قبل الأفراد العاديين[26].

ولقد اختلف الفقه الجنائي في تكييف التنصت والمراقبة[27]، فيرى جانب من الفقه أن ضبط المراسلات والتنصت على المحادثات الهاتفية يعتبر تفتيشًا لأنه ينطوي على المساس بحق السر إذ من حق أي إنسان صيانة آرائه وأفكاره التي يعبر عنها في رسائله التي يبعث بها للآخرين، وعدم اطلاع أحد على هذه الأفكار أو الآراء فإذا جرى ضبط هذه المحادثات أو المراسلات والاطلاع على مضمونها، فإن ذلك يشكل مساسًا بحق السر الذي يصونه القانون[28].

والغاية من مراقبة المحادثات الهاتفية هي البحث عن دليل وهي نفس الغاية من التفتيش، ويعد هذا الرأي هو الغالب في الفقه[29].

أما الجانب الآخر من الفقه، فيرى أن مراقبة المحادثات الهاتفية وتسجيلها هي من قبيل الملاحظة القضائية المباشرة، إذ يشترط لمباشرتها أن تكون هناك فائدة من ظهور الحقيقة في جريمة تحقق فيها السلطة المختصة بالتحقيق، وهو إجراء مماثل في طبيعته للتفتيش ولكنه ليس بحقيقته تفتيشًا، وأحاطه المشرع بالضمانات التي تحيط بتفتيش الرسائل لأنه أقرب للتفتيش[30]، وقد حاول جانب من الفقه الأمريكي التوفيق بين خصوصية الأفراد، وإمكانية استعمال الأجهزة العلمية الحديثة من قبل العدالة، توخيًا للكشف عن الحقيقة والتعرف على مرتكبيها، فقالوا بإمكانية اللجوء إلى تسجيل الأحاديث والتنصت متى توافرت الشروط التالية[31]:

1-أن يتعلق الأمر بجريمة خطيرة مع وجود حاجة ماسة إلى اللجوء إلى هذا الأسلوب.

2-ألا تكون ثمة بدائل أخرى أقل خطورة من حيث درجة مساسها بالحق في الحياة الخاصة.

26- انظر: ممدوح خليل البحر- حماية الحياة في القانون الجنائي- دراسة مقارنة- رسالة دكتوراه- دار الثقافة عمان- 1996م – ص 543 وما بعدها.

27- د.صالح عبد الزهرة الحسون- أحكام التفتيش وآثاره في القانون العراقي- دراسة مقارنة- رسالة دكتوراه- جامعة بغداد- ط1- مطبعة الأديب – بغداد- 1979م– ص 115 وما بعدها.

28- د.سامي حسني الحسيني- النظرية العامة للتفتيش في القانون المصري والمقارن- رسالة دكتوراه-جامعة القاهرة- ط1- دار النهضة العربية – القاهرة –1972م– ص 345.و د.فاروق الكيلاني – محاضرات في قانون أصول المحاكمات الجزائية الأردني والمقارن – ج2 – دار الفارابي – عمان – 1985م – ص 458.

29- انظر: د. سامي الحسيني – مصدر سابق – ص 344، ود. أحمد فتحي سرور – مصدر سابق – ص 147.

30- انظر: د. ممدوح خليل بحر – الحياة الخاصة - مصدر سابق – ص 614 وما بعدها.

31- المصدر السابق – ص 556.

3-أن يراعي الحذر الشديد في التعويل على هذا الأسلوب والثقة فيه، وهي مسألة بلا شك تتطلب اللجوء إلى إعمال الخبرة الفنية والتدقيق الشديد في صحة هذه الطريقة، وعدم حدوث أي تغيير أو تعديل أو تبديل عليها.

ولما كانت شبكات الحاسوب والإنترنت تستخدم ضمن خطوط الهاتف[32]، وبواسطة جهاز مُعدل الموجات والذي يُعرف اختصارًا بالمودم (Modem)[33]، وهو الجهاز الذي يحول الإشارات الرقمية المستخدمة بواسطة الحاسوب إلى موجات تناظرية، تنقل مع الموجات الصوتية خلال خطوط الهاتف، ولكي تستطيع هذه الخطوط الهاتفية المخصصة أساسًا لنقل الموجات الصوتية حمل الموجات التناظرية، يستخدم مُعدل للموجات، وهذا المُعدل يكون مطلوبًا في محطة الإرسال لتحويل الإشارات الرقمية إلى موجات تناظرية، وفي محطة الاستقبال يكون مطلوبًا لإعادة تعديل آخر لتحويل الموجات التناظرية إلى إشارات رقمية يتم استقبالها بواسطة الحاسوب[34].

ومما تقدم يتضح أن هناك تشابهًا بين التنصت والمراقبة الإلكترونية لشبكات الحاسوب ومراقبة المحادثات الهاتفية وتسجيلها، لكن هل تكفي النصوص الحالية في قانون الإجراءات الجنائية البحريني لمواجهة هذه التقنيات الحديثة؟

يرى الباحث أن نص المادة (93) إجراءات جنائية بحريني يكفي ليعالج هذا الموضوع لنصه على أن" تراقب المحادثات والمراسلات السلكية واللاسلكية"، ويجد سند ما نعتقد من النص الحالي يشمل هذه المراقبات الإلكترونية من بعض التشريعات المقارنة، ففي الولايات المتحدة الأمريكية يجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسوب بشرط الحصول على إذن تفتيش صادر من القاضي، فلقد مكنت أجهزة مراقبة الحاسوب التي تم وضعها في جامعة هارفرد السلطة المختصة بالتحقيق في قضية اختراق شخص أرجنتيني لأنظمة المعلومات في القوات البحرية الأمريكية (NCIS)، من أن تحدد وبنجاح الفاعل الذي قام بالاختراق من بين (16500) مستخدم لشبكة الإنترنت، وبمساعدة المدعي العام الأمريكي في بوسطن قام وكلاء (NCIS)، باختراق اثنين من الاتصالات التي قد لا تكون من فعل الشخص المتطفل، وذلك استنادًا إلى نص القانون الذي يحكم

32- هذا بالإضافة إلى الموجات اللاسلكية أو الأقمار الصناعية.
33- المودم (Modem) مختصر لـ (Modulator Demodulator).
34- د.محمد فهمي طلبة وآخرون – دائرة المعارف/ الحاسب الإلكتروني – مجموعة كتب دلتا – مطابع المكتب المصري الحديث – القاهرة – 1991م.– ص 305.

اعتراض الاتصالات وتطبيقًا للتعديل الرابع للدستور والمتعلق بالحقوق الشخصية السرية للمواطنين الأبرياء، وقد تم تطبيق برنامج خاص في إجراء هذه العملية[35]، أما في فرنسا فأجاز القانون الصادر عام 1991م، اعتراض الاتصالات عن بُعد بما في ذلك شبكات تبادل المعلومات، وفي هولندا يجوز لقاضي التحقيق أن يأمر بالتنصت على شبكات اتصالات الحاسوب، إذا كانت هناك جرائم خطيرة ارتكبها المتهم[36]، ونجد أن المشرع العراقي قد اعتبر مراقبة الرسائل البريدية والبرقية وكافة الاتصالات السلكية واللاسلكية تفتيشًا وذلك في قانون السلامة الوطنية رقم (4) لسنة 1965م، حيث نصت الفقرة (12) من المادة (4) منه على: (مراقبة الرسائل البريدية والبرقية وكافة وسائل الاتصال السلكية واللاسلكية وتفتيشها وضبطها)[37].من هذه التشريعات يمكن القول إنها اعتمدت على نصوصها التقليدية ليمتد سلطانها للتنصت والمراقبة الإلكترونية لشبكات الحاسوب والإنترنت.

ولقد نظمت المادتان (88) و (89) من قانون الأصول الجزائية الأردني أحكام وضوابط مراقبة المحادثات الهاتفية وتسجيلها، ويجد الباحث من خلال هذين النصين وبعض النصوص العربية المقارنة أن هناك شروطًا تطلبها القانون للقيام بالمراقبة أو تسجيلها وهي[38]:-

1-**وقوع جريمة**: إذ لا يجوز مراقبة المحادثات الهاتفية وتسجيلها إلا بعد وقوع الجريمة، ويجوز الضبط في أية جريمة سواء أكانت جناية أم جنحة أم مخالفة. واشترط المشرع البحريني لإمكانية الأمر بالتفتيش أن تكون جناية أو جنحة وأن يكون قد وجه اتهام إلى شخص بارتكابها(انظر المادة 90 إجراءات جنائية بحريني).كما اشترط المشرع البحريني لصحة التفتيش في هذه الحالة الحصول على إذن من قاضي المحكمة الصغرى(انظر المادة 92 إجراءات جنائية بحريني).

2-**وجود فائدة في كشف الحقيقة**: ويشترط لمشروعية الضبط أن يكون مفيدًا في كشف الحقيقة متى كانت المحادثات صادرة عن المشتكى عليه أو موجهة إليه، والمحقق هو الذي يقدر ذلك تحت رقابة

35- The (NCIS) Argentine Computer Interusion. Investigation – FBI- Law Enforcement Bulletin-Oct 1982, vol.67 Issue 10- p.9.

36- د. هلالي عبداله – التفتيش - مصدر سابق – ص 22.

37- د. صالح عبد الزهرة الحسون –مصدر سابق – ص 123.

38-د.سعيد حسب الله عبدالله-الوجيز في قانون الإجراءات الجنائية البحريني-ط1-إصدارات جامعة البحرين-البحرين-2005م-ص189 -191.

محكمة الموضوع[39]، أما الرسائل الموجهة من شخص إلى آخر ولا علاقة لأي منها بالجريمة المرتكبة فلا يجوز ضبطها والإطلاع عليها[40].

3-**مراعاة حقوق الدفاع**: تتقيد سلطة التحقيق في ضبط الخطابات والمراسلات البريدية بمراعاة حقوق الدفاع، فلا يجوز ضبط الخطابات والرسائل المتبادلة بين المشتكى عليه ومحاميه، فقد نصت المادة (152) أصول أردني على أنه: (لا يجوز إثبات واقعة بالرسائل المتبادلة بين المتهم أو الظنين أو المشتكى عليه ومحاميه)[41]، وتقابلها نص المادة (94) إجراءات جنائية بحريني والتي جاء فيها: (لا يجوز لعضو النيابة العامة أن يضبط لدى المدافع عن المتهم أو الخبير الاستشاري الأوراق والمستندات التي سلمها المتهم لهما لأداء المهمة التي عهد إليهما بها ولا المراسلات المتبادلة بينهما في القضية) فالإطلاع على هذه الخطابات يعيق عمل المحامي في الدفاع عن موكله، فحق الدفاع حق مصون يقتضي حماية الفرد ضد إساءة السلطة[42].

وهناك عدد من الشروط تطلبتها القوانين الإجرائية العربية لم ينص عليها المشرع الأردني مثل تسبب أمر الضبط (انظر المادة 95 إجراءات مصري)، أو تحديد مدة الضبط بمدة لا تزيد على ثلاثين يومًا قابلة للتجديد لمدة أو مدد أخرى مماثلة (انظر المادة 95 إجراءات مصري)، ويرى الباحث أنه من الضروري أن يحدد المشرع الأردني أيضًا مدة للضبط وخصوصًا أن جرائم المعلوماتية تمتاز بسرعتها الفائقة وأدلتها القابلة للمحو والتغيير، ومن الأفضل أن ينص المشرع على تحديد مدة الضبط بثلاثين يوم أسوة بالمشرع المصري وأيضًا لضمان حقوق المشتكى عليه حتى لا تبقى عرضة لمزاج عضو الضابطة العدلية.

ومن المعلوم أن الاتصالات عبر شبكة الحاسوب والإنترنت تحتاج إلى خطوط الهاتف، وبالتالي فإن مراقبة المحادثات عبر الإنترنت وشبكات الحاسوب وتسجيلها لا تتعارض مع هذا الرأي الفقهي، ويمكن لأعضاء الضابطة العدلية المراقبة أو التنصت ضمن الحدود القانونية المنصوص عليها في القانون.

39- د.محمود محمود مصطفى – الإثبات في المواد الجنائية في القانون المقارن – رسالة دكتوراه – جامعة القاهرة - القاهرة – 1978م– ص 88.

40- انظر: د. سامي الحسيني –مصدر سابق – ص 341.

41- يماثلها نص المادة (181) أصول سوري، والمادة (96) إجراءات مصري والتي جاء فيها: (لا يجوز لقاضي التحقيق أن يضبط لدى المدافع عن المتهم أو الخبير الاستشاري الأوراق والمستندات التي سلمها المتهم لهما لأداء المهمة التي يمهد إليهما بها، ولا المراسلات المتبادلة بينهما في القضية).

42- انظر: فاروق الكيلاني –مصدر سابق – ص 462-463.

المطلب الثالث

أحكام ضبط نظم الحاسوب والإنترنت والمراسلات والبريد الإلكتروني

أوجبت التشريعات الإجرائية أن توصف الأشياء المضبوطة وتعرض على المتهم أو من ينوب عنه، ويطلب منه إبداء ملاحظاته عليها، ويكتب بذلك محضر ويوقع عليه المتهم أو يذكر فيه امتناعه، ونصت الفقرة (2) من المادة (32) أصول أردني على أنه: (يستجوب المدعي العام المشتكى عليه عن الأشياء المضبوطة بعد عرضها عليه ثم ينظم محضرًا يوقعه والمشتكى عليه وإذا تمنع هذا الأخير عن التوقيع صرح بذلك في المحضر)، ونصت على ذلك أيضًا الفقرة الثالثة من المادة (36) أصول أردني على أنه: (تعرض الأشياء المضبوطة على المشتكى عليه أو على من ينوب عنه للمصادقة والتوقيع عليها وإن امتنع صرح بذلك في المحضر)[43].

وأوجبت بعض التشريعات أن يوقع المحضر المتهم أو الأشخاص الذين حضروا التفتيش والضبط، ومنها التشريع الأردني في الفقرة (1) من المادة (38) أصول التي نصت على أنه: (يوقع المدعي العام والكاتب والأشخاص المذكورين في المادة (36) على كل صفحة من أوراق الضبط التي ينظمها بمقتضى الأحكام السابقة)[44]، وكذلك نص المادة (**73**) إجراءات جنائية بحريني على أن:

(لمأموري الضبط القضائي أن يضبطوا الأوراق والأسلحة والآلات وكل ما يحتمل أن يكون قد استعمل في ارتكاب الجريمة، أو نتج عن ارتكابها، أو ما وقعت عليه الجريمة، وكل ما يفيد في كشف الحقيقة، وتعرض هذه الأشياء على المتهم ويطلب منه إبداء ملاحظاته عليها، ويحرر بذلك محضر يوقع عليه المتهم أو يذكر فيه امتناعه عن التوقيع).

وإذا كان من بين المضبوطات أوراق أو مستندات فمن حق القائم بالتفتيش والأشخاص الذين حضروا التفتيش الإطلاع عليها قبل اتخاذ قرار بضبطها، ولقد نصت على ذلك المادة 2/34 من الأصول الجزائية الأردني بأن: (ومن حق المدعي العام وحده والأشخاص المعنيين في المادتين (36 و 89) الإطلاع على الأوراق قبل اتخاذ القرار بضبطها)، وكذلك المادة 1/89، (إذا اقتضت الحال

43- انظر: المادة (82) من القانون العراقي، والمادة (55) من القانون المصري، والمواد (2/30 و 2/34) لبناني، والمادة (2/32) سوري، والمادة (2/43) ليبي، والمادة (2/61) إماراتي.

44- انظر: المادة (1/82) من القانون العراقي، والمادة (37) لبناني، والمادة (38) سوري.

البحث عن أوراق فللمدعي العام وحده أو لموظف الضابطة العدلية المستناب وفقًا للأصول أن يطلع عليها قبل ضبطها)[45]. وتعطي بعض التشريعات لمن ضبطت عنده الأوراق أو لصاحبها صورة منها مصدقًا عليها، متى كانت له مصلحة عاجلة فيها ولم يكن في ذلك إضرار بسير أو بصالح التحقيق[46].

ولا تجيز غالبية التشريعات للقائم بالتفتيش إذا كان موظف ضابطة عدلية أن يفض أية أوراق مختومة أو مغلقة بأية طريقة في المنزل الذي يقوم بتفتيشه[47]. ويرى الباحث بأنه يشمل أية مواد أو أدوات تخزن عليها البيانات إلكترونيًا، ذلك لأن فض الأوراق المغلقة والإطلاع عليها وحجز ما يكون لازمًا منها لإظهار الحقيقة مقصور على المحقق وحده[48]، ذلك لأنها تحوي أسرارًا خاصة لا يجوز الإطلاع عليها من غيره، وتكون إنابة عضو الضابطة العدلية في هذه الحالة مقصورة على التفتيش والضبط وليس الإطلاع وكشف الأسرار، إلا إذا كان عضو الضابطة العدلية منابًا للبحث عن الأوراق والمستندات فإنه يجوز له الإطلاع عليها قبل ضبطها سواء كانت ظاهرة أم مغلقة وهذا مستفاد مما نصت عليه صراحة بعض القوانين[49].

ومما تقدم يتضح بأن صلاحيات مأمور الضبط القضائي في ضبط المراسلات والبريد وغيرها تنحصر في حالتين فقط هما:

الحالة الأولى: أن يكون عضو الضابطة العدلية منابًا للتفتيش وضبط الأشياء التي تفيد في كشف الحقيقة، فله الإطلاع على الأوراق والبيانات المكشوفة أو الظاهرة على شاشة الحاسوب قبل ضبطها، أما الأوراق المغلقة أو الملفات المشفرة أو الأقراص الصلبة والمرنة المغلقة فليس له سوى

45- انظر: ما يقابلها: المادة (84/أ) عراقي، والمواد (2/32 و 1/97) لبناني، والمواد (2/34 و 1/97) سوري، والمواد (2/61 و 1/105) مغربي، والمواد (2/49 و 1/87) موريتاني، والمواد (2/45 و1/84)جزائري.

46- ومن هذه التشريعات: القانون المصري في المادة (59)، والليبي في المادة (47)، والمادة (2/82) من العراقي، والمادة (64) من الإماراتي.

47- انظر المواد: (59) مصري، و(2/82) عراقي، و(47) ليبي، و(64) إماراتي.

48- تنص الفقرة (3) من المادة (89) أصول أردني على أنه: (يطلع المدعي العام على الرسائل والبرقيات المضبوطة حال تسلمه الأوراق في غلافها المختوم فيحتفظ بالرسائل والبرقيات التي يراها لازمة لإظهار الحقيقة أو التي يكون اتصالها بالغير مضرًا بمصلحة التحقيق ويسلم ما بقي منها إلى المشتكى عليه أو إلى الأشخاص الموجهة إليهم). انظر المادة (84/ب) عراقي، والمواد (97و199) مصري، والمادة (3/97) لبناني، والمادة (3/97) سوري، والمادة (1/81)ليبي والمادة (76) إماراتي.

49- انظر المادة (1/89) أردني (سابق ذكرها) والمادة (1/97) لبناني، والمادة (1/97) سوري، والمادة (105) مغربي، والمادة (1/87) موريتاني.

ضبطها، ولا يجوز له فتحها والإطلاع عليها إذ أن ذلك من اختصاص سلطة التحقيق الأصلية وحدها.

الحالة الثانية: أن يكون عضو الضابطة العدلية مستنابًا للبحث عن أوراق أو مستندات أو ملفات أو بيانات إلكترونية، فله حق الإطلاع عليها قبل ضبطها سواء كانت مكشوفة أم مغلقة، لأنه في هذه الحالة يحل محل سلطة التحقيق في حدود ندبه.

ويشترط القانون أن توضع الأشياء أو الأوراق المضبوطة في حرز مغلق وتربط ويختم عليها، ويكتب على شريط داخل الختم تاريخ المحضر المحرر لضبط تلك الأشياء، ويجب أن يشار إلى الموضوع الذي حصل من أجله الضبط، وأكدت ذلك المادة (1/35) أصول أردني ونصت على أنه[50]: (يعنى بحفظ الأشياء المضبوطة بالحالة التي كانت عليها، فتحزم أو توضع في وعاء إذا اقتضت ماهيتها ذلك وتختم في الحالتين بخاتم رسمي)، ويتم ختم الأجسام والمستندات، وبصورة أعم كل دليل مثبت يتم اكتشافه بالشمع الأحمر، ولا بد من جردها جميعًا وضبطها من أجل مطابقة الهوية كتابيًا، ويجب اتخاذ كل التدابير اللازمة للحؤول دون إمكان إجراء أي تعديل على المستندات المضبوطة كوصفها في محضر خطي، ووضعها داخل مغلف إذا لزم الأمر[51].

ولا يجوز فض الأختام الموضوعة على الاحراز ولا الإطلاع على الأوراق إلا بحضور المتهم أو وكيله أو من ضبطت عندهم هذه الأشياء أو بعد دعوتهم لذلك[52]، والهدف من هذه القاعدة درء احتمال القول باستبدال الاحراز نتيجة خطأ أو تعمد أو حدوث تلاعب فيها[53]، أو حتى تسليم المضبوطات للمتهم قبل تقديمه إلى المحكمة المختصة مما يسبب فقدان الدليل على الإدانة، فقد

50-انظر: المادة (56) مصري، والمادة (1/33) لبناني، والمادة (35) سوري، والمادة (44) ليبي، والمادة (4/61) مغربي، والمادة (4/49) موريتاني، والمواد (2/45 و 2/84) جزائري، والمادة (2/97) تونسي.
وفي بعض التشريعات إذا وجدت أوراق نقدية لا يستوجب الأمر الاحتفاظ بها لاستظهار الحقيقة أو لحفظ حقوق الطرفين أو حقوق الغير جاز للمدعي العام أو لقاضي التحقيق أن يأذن بإيداعها في صندوق الخزينة أو صندوق الودائع.
انظر المادة (2/35) من القانون الأردني، والمادة (2/33) لبناني، والمادة (2/35) سوري، والمادة (6/105) مغربي، والمادة (4/84) جزائري.

51- د. مارسيل لوكلير – الوجيز في الشرطة التقنية – تعريب د. بسام الهاشم – ط1 – الدار العربية للموسوعات – بيروت – 1983م – ص 345.

52- انظر: المادة (1/89) أردني، والمادة (83) عراقي، والمادة (57) مصري، والمادة (2/97) لبناني، والمادة (2/97) سوري، والمادة (45) ليبي، والمادة (3/105) مغربي، والمادة (3/84) جزائري، والمادة (62) إماراتي.

53- انظر: د. رؤوف عبيد – مبادئ الإجراءات الجنائية في القانون المصري – ط16 – دار الجيل – القاهرة – 1986م – ص 386.

اشتكت شركة أمريكية إلى الشرطة على محاسب يعمل لديها، سمحت له هذه الشركة بإدارة أعمالها من منزله، وقد تكبدت الشركة خسائر مادية جسيمة، وعلى اثر ذلك قامت الشرطة بتفتيش منزله وضبطت جهاز الحاسوب الخاص به استنادًا إلى نص المادة (19) من قانون الشرطة والأدلة الجنائية، ومن ثم قاموا وحسب المادة (20) من نفس القانون بإصدار وثيقة تتعلق بالاتهام بجريمة الاحتيال، ولكن الدعوى سقطت استنادًا للمادة (78) من قانون الشرطة والأدلة الجنائية؛ لأن الشرطة سمحت للشركة صاحبة الإدعاء أن تأخذ جهاز الحاسوب المضبوط للفحص[54]. ويعد حضور الأشخاص المذكورين في النصوص السابقة شرطًا أساسيًا لصحة إجراء التفتيش والضبط، لذلك لا يجوز للنيابة العامة منع أي منهم من الحضور إذا تواجدوا أثناء التفتيش، إلا إذا اقتضت مصلحة التحقيق خلاف ذلك[55].

وتضمنت غالبية التشريعات نصوصًا صريحة، اشترطت قيام سلطة التحقيق بفض الأختام وفرز الأوراق في حضور المتهم أو من ينوب عنه أو من ضبطت عنده هذه الأوراق، أو بالأقل بعد دعوة هؤلاء الحضور، ومن هذه التشريعات،القانون البحريني في المادة (95) إجراءات جنائية والتي نصت على أن:(لعضو النيابة العامة وحده أن يطلع على الخطابات والرسائل والأوراق الأخرى المضبوطة على أن يتم هذا إن أمكن بحضور المتهم أو الحائز لها أو المرسلة إليه ويدون ملاحظاتهم عليها، وله حسب ما يظهر من الفحص أن يأمر بضم تلك الأوراق إلى ملف الدعوى أو يردها إلى من كان حائزًا لها أو من كانت مرسلة إليه). وكذلك القانون الأردني في المادة (2/89) التي نصت على أنه: (لا تفض الأختام ولا تفرز الأوراق بعد ضبطها إلا في حضور المشتكى عليه أو وكيله أو في غيابهما إذا دعيا وفقًا للأصول ولم يحضرا ويدعى أيضًا من جرت المعاملة عنده لحضورها، تتبع هذه الأصول بقدر الإمكان ما لم تكن هناك ضرورة دعت لخلاف ذلك)[56]، إن قاعدة حضور المتهم أو وكيله عند فض الأختام والإطلاع على الأوراق هي قاعدة مكملة لقاعدة وجوب تحريز المضبوطات وعرضها على المتهم، وغايتها منع العبث بالاحراز المضبوطة، وتفادي ما قد يثيره

54- Hildreth , Jacqwi – The Enemy Withen – Delecting White Cfoller Crime – Intrnational Review of Law Computer and Technology Oct 1997, Vol.11.Issue 2. P.263.

55- د.مأمون محمد سلامة – الإجراءات الجنائية في التشريع المصري – ج1 – دار النهضة العربية – القاهرة – 1988م– ص 618.

56- انظر: المادة (84/ب) عراقي، والمادة (2/97) لبناني، والمادة (2/97) سوري، والمادة (3/84) جزائري، والمادة (3/105) مغربي.

المتهم حول ضبط هذه الأشياء لديه مما قد يضعف الدليل المستمد منها، ولذلك لا مجال للتفرقة في شأن وجوب الالتزام بهذه القواعد أيًا كانت السلطة القائمة بالتفتيش والضبط.

ومن التحديات المثارة في حقل الأدلة الرقمية والتعامل معها[57]:

من السهل الادعاء بوجود قفاز ملطخ بالدماء في منزل مشتبه به معين ولكن إثبات ذلك مسألة أخرى، فعندما يتم الحديث عن البراءة أو الإدانة فإن إثبات أصالة الأدلة وسلامتها يصبح غاية في الأهمية، لذلك فإن الدليل يجب أن يتناغم مع قواعد الأدلة، ومن منظور العلم الجنائي هناك العديد من النواحي لمعالجة وفحص الأدلة الرقمية ومنها[58]:

تمييز الأدلة الرقمية : وهي عملية تتكون من عنصرين، أولاً: يجب على المحقق أن يميز الأجهزة Hardware مثل جهاز الحاسوب والأقراص المرنة وكوابل الشبكات والتي تحتوي على المعلومات الرقمية، وثانيًا: يجب على المحقق أن يميز بين المعلومات غير المهمة والمعلومات المرتبطة بالجريمة.

جمع وحفظ الأدلة الرقمية والأجهزة: يجب حفظ الأدلة الرقمية بحالتها الأصلية لأن القانون يطلب أصالة الأدلة وعدم تغيير الحالة الأصلية لها ومن هنا يجب طباعة الدليل وفي هذه الحالة فإن للنسخة المطبوعة قيمة قانونية كدليل إلا إذا كان الدليل الأصلي محل شك. ومن المهم جمع الأدلة بطريقة لا تتغير معها وعلى أن تكون مقبولة في المحكمة ومن الضروري عدم ترك أي دليل وهنا قد يقوم المحقق بأخذ كل شيء أو قد يأخذ ما هو متعلق فقط بالقضية أي الأشياء الأساسية.

توفير الوقت والجهد وتجنب تدمير أو مقاطعة عمل فرد أو مؤسسة ما: فبعض أجهزة الحاسوب حساسة لإدارة مؤسسات وقد يؤدي أخذ الجهاز إلى توقف عمل المؤسسة، مثل أجهزة المستشفيات فإن أخذ مثل هذه الأجهزة قد يعرض حياة الناس للخطر.

توثيق الأدلة الرقمية والأجهزة: إن التوثيق مهم لعدة أسباب لأن هذا يثبت أن الدليل أصيل ولم يتغير، فأحيانًا يتم استدعاء الأشخاص الذين جمعوا الأدلة للتأكيد على أن دليلاً معينًا هو نفسه الذي جمع منذ البداية، كذلك يستخدم التوثيق للتفريق بين الدليل الأصلي والنسخة المأخوذة عنه، أما إذا لم

---

[57] -انظر: كمال أحمد الكركي، التحقيق في جرائم الحاسوب،بحث منشور على موقع www.ArabLawInfo.com

[58] : أنظر (Eoghan Casey, Digital Evidence and Computer Crime, Academic Press, 1 st edition, 2000, pages 41-73.

يستطع المحقق التفريق بين الأصل والنسخة فقد يكون لذلك آثار سيئة بالنسبة للمحقق، والتوثيق مهم لدى محاولة إعادة بناء الجريمة فمثلاً عند جمع حاسوب يجب تعليم جميع الكوابل لمعرفة من أين جاءت فيما بعد، وأيضًا يلزم التوثيق وبالذات توثيق هوية الأشخاص الذين جمعوا الدليل وتعاملوا معه من أجل الحفاظ على سلسلة الوصاية.

هـ- **تصنيف ومقارنة وإفراد الدليل الرقمي:** وهذه المرحلة هي عملية إيجاد الخصائص التي تصف الأدلة بشكل عام وتميزها عن غيرها، فمثلاً أكثر الأشخاص يعرفون رسائل البريد الإلكتروني ولكن تصنيفها بدقة يتم من قبل المحققين المدربين مثل تحديد نوع التطبيق المستخدم، وهناك أيضًا أنواع مختلفة من ملفات الصور مثل jpg, gif, tiff والمقارنة مهمة عند فحص الدليل الرقمي باستخدام عينة قياسية Control Specimen بحيث يؤدي ذلك إلى إظهار النواحي الفريدة من الدليل الرقمي، ويمكن استخدام هذه النواحي لربط القضية مع جهاز معين.

و. الدليل الرقمي وإعادة البناء:

1. **إعادة بناء الدليل الرقمي المشطوب أو المخفي أو المشفر:** ويعتمد ذلك على نوع الدليل الرقمي ونوع الحاسوب ونظام التشغيل وإعدادات الحاسوب. عندما يتم شطب ملف فعادة يبقى موجودًا على القرص ويمكن استرجاعه باستخدام برامج خاصة، وحتى عند إعادة الكتابة على الملفات المشطوبة فإن جزءًا منها يبقى ويمكن قراءتها مرة أخرى باستخدام برامج خاصة، ومن التحديات الأخرى الملفات المشفرة حيث أن برامج التشفير أصبحت شائعة وأصبح بإمكان المجرمين بعثرة الدليل الذي يدينهم باستخدام شفرة غير مقروءة وبالتالي يصبح فك التشفير مسألة صعبة ويتطلب فك التشفير كلمة سر خاصة ويمكن في عدة حالات فك التشفير باستخدام الخبرة والأجهزة المناسبة ولكن محاولة فك التشفير غير عملية في بعض التحقيقات.

2. **إعادة بناء الجريمة:** ويشمل ذلك إصلاح الأدلة المتلفة واستخدامها لتحديد الأعمال المحيطة بجريمة ما، والهدف هنا هو صيانة كيفية ووقت حصول الأحداث، فلا يكفي معرفة أنه قد حصل اختراق بل يجب معرفة كيف ومتى وأين حصل ذلك وعند إعادة بناء ظروف الجريمة سوف تسد الفجوات في القضية ويتم فهم ما حصل بالتحديد، ومن المهم عدم الاعتماد كليًا على الدليل الرقمي حيث يجب النظر إلى الدليل المادي.

ومما تقدم لا ضير في أن تطبق القواعد الإجرائية السالفة على ضبط أجهزة الحاسوب وشبكاته ونظمه والإنترنت، لكن يجب أن يراعى في تحريز الاسطوانات الصلبة والأقراص المرنة، مجموعة من القواعد المهمة للمحافظة عليها من التلف أو اختفاء البيانات المسجلة عليها، يمكن إجمالها بما يأتي[59]:

1-يجب حمل الاسطوانات أو الأقراص من الجزء العلوي لها عند علامة الشركة وإدخالها أو إخراجها من مشغل الاسطوانات أو الأقراص برفق للمحافظة على القرص والمشغل.

2-عدم ثني القرص لأن ذلك يؤدي إلى تلفه وفقدان البيانات المسجلة عليه.

3-عدم لمس الأجزاء المكشوفة من الأقراص حتى لا يؤدي إلى تلفه وفقد المُسجل عليه.

4-عدم الضغط على القرص بوضع أشياء ثقيلة عليه كالكتب مثلاً.

5-عدم تعريض القرص للضوء الشديد أو لأي سائل من السوائل.

6-عدم تعريض القرص لدرجات الحرارة العالية أو المنخفضة جدًا، ويجب أن تكون الحرارة المسموح بها تتراوح ما بين (10-52) درجة مئوية، لأن تمدد أو انكماش الأقراص يؤدي إلى تلفها وفقد ما عليها من بيانات.

7-يجب القيام بتوثيق الدليل من خلال الاحتفاظ بالنسخة الأصلية وعمل نسخة دقيقة (صورة المرآة)، مع حفظ الملف الأصلي أو الوثيقة الأصلية في مكان داخل ذاكرة الحاسوب بحيث يكون المحقق هو الشخص الوحيد الذي يحتفظ بها أو يتوصل إليها[60].

8-ويجب عدم تعريض القرص للأتربة وذرات الغبار والدخان لأن في ذلك تأثير على السطح المغناطيسي مما يجعله غير قابل للقراءة أو الكتابة، ولذا يجب وضعه في غلافه الورقي الذي يغطي الأجزاء المكشوفة بعد الاستعمال.

9-ويشترط عدم تعريض الأقراص للمجالات المغناطيسية، بعد وضعها على الأجهزة أو السطوح المعدنية حتى لا يفقد ما عليها لأن التسجيل على الأسطوانة أو القرص يتم مغناطيسيًا.

59- للمزيد من المعلومات انظر: د. هشام محمد فريد رستم – الجوانب الإجرائية –مصدر سابق – ص 129 وما بعدها، وانظر: د. هلالي عبداله أحمد – التفتيش - مصدر سابق – ص 210، ود. جميل عبد الباقي الصغير – أدلة الإثبات الجنائي والتكنولوجيا الحديثة (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية) - دراسة مقارنة – دار النهضة العربية - القاهرة – 2001م – ص 121-122.وانظر: د. عفيفي كامل عفيفي –مصدر سابق – ص 337. وانظر: د.عبد الفتاح بيومي حجازي- مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دراسة قانونية متعمقة في القانون المعلوماتي- دار الكتب القانونية و دار شتات والبرمجيات-مصر-2007م– ص 61 وما بعدها.

60- Bort , Julie – To Catch a thief – Infoworld 21/7/1997- Vol.19.Issue.29-P.2.

10-ويجب عدم كتابة بيانات على اللاصقة الورقية المخصصة للمستخدم بعد لصقها على القرص لأن الضغط بالقلم قد يفسد سطح القرص.

11-ويقتضي تأمين البرامج المضبوطة قبل تشغيلها ويتم ذلك بعمل نسخ سليمة وكاملة منها[61].

12-ويجب تمييز المادة المضبوطة[62]، ويكون بوضع علامة مادية خاصة عليها من قبل كل من كانت في حيازته، فإذا ما اقتضى التحقيق – مثلاً – يكون متعينًا على المحقق ومُشغل النظام أن يسجل كل منهما اسمه وبياناته التعريفية على كل من أسطوانة الحاسوب والأقراص أو الأشرطة ذاتها، ولا بد من ختم الأشرطة بعد إتمام عملية التسجيل ووضع الاسم والتوقيع وتدوين البيانات اللازمة، وإذا كان التسجيل قد جرى على أقراص ممغنطة فيوضع الاسم والتوقيع على قاعدتها على أن يتم بعد ذلك وضعها في علب مغلقة وتحريزها[63].

61- محمد محمد شتا – فكرة الحماية الجنائية لبرامج الحاسوب – دار الجامعة الجديدة – الإسكندرية – 2001م – ص 131.

62- Welch , Thomas – Computer Crime Investigationj and Computer forensics – Information Systems Security – Summer 19 97 , Vol.6.Issue.2. P50.

63- Jeffrey , Sassinsky – Computer Forensics – OP – Cit . P.9-10.

مراجع البحث:

1. د. محمد زكي أبو عامر – الإجراءات الجنائية – ط2 – منشأة المعارف الإسكندرية – 1990م.
2. د.هشام محمد فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – 1994م.
3. د.هلالي عبداللاه أحمد – تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – دراسة مقارنة – ط1 – دار النهضة العربية – القاهرة – 1997م.
4. د.عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون - دراسة مقارنة – (د.ت).
5. د. أحمد السمدان – النظام القانوني لحماية برامج الكمبيوتر – مجلة الحقوق – السنة 11 – العدد 4 – جامعة الكويت – الكويت – ديسمبر – 1987.
6. د.خالد حمدي عبد الرحمن- الحماية القانونية للكيانات المنطقية- رسالة دكتوراه- جامعة عين شمس – القاهرة- 1992م.
7. د.محمد عبد الظاهر حسين – الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية – دار النهضة العربية – القاهرة – 2001/2000م.
8. د.رشا مصطفى أبو الغيط – الحماية القانونية للكيانات المنطقية – برامج الحاسب الآلي – وصف البرامج – المستندات الملحقة – ملتقى الفكر – الإسكندرية – 2000م.
9. د.محمود شريف بسيوني ود.عبد العظيم الوزير – الإجراءات الجنائية في النظم القانونية العربية وحماية حقوق الإنسان – ط1 – دار العلم للملايين – بيروت – 1991م.
10. بهاء شاهين – شبكة الإنترنت –ط1- الدار العربية لعلوم الحاسب – القاهرة – 1996م.
11. أ. عبد السلام رضوان – سلسلة عالم المعرفة – المجلس الوطني للثقافة والفنون والآداب – العدد 231 – الكويت – مارس 1998.
12. اللواء د. محمد الأمين البشري – الأدلة الجنائية الرقمية – مفهومها ودورها في الإثبات – المجلة العربية للدراسات والتدريب – المجلد 17 – العدد 33 – السنة 17- الرياض – أبريل – 2002.

13. د.مصطفى محمد موسى، الجهاز الالكتروني لمكافحة الجريمة، دار الكتب القانونية، مصر، 2006م.
14. سمير الأمين – مراقبة التلفون والتسجيلات الصوتية والمرئية – ط3 – دار الكتاب الذهني – القاهرة 2000م.
15. د. أحمد فتحي سرور – مراقبة المكالمات التلفونية – المجلة الجنائية القومية – العدد 1 – مارس –1963م.
16. ممدوح خليل البحر- حماية الحياة في القانون الجنائي- دراسة مقارنة- رسالة دكتوراه- دار الثقافة عمان- 1996م.
17. د.صالح عبد الزهرة الحسون- أحكام التفتيش وآثاره في القانون العراقي- دراسة مقارنة- رسالة دكتوراه- جامعة بغداد- ط1- مطبعة الأديب – بغداد- 1979م.
18. د.سامي حسني الحسيني- النظرية العامة للتفتيش في القانون المصري والمقارن- رسالة دكتوراه-جامعة القاهرة- ط1- دار النهضة العربية – القاهرة –1972م.
19. د.فاروق الكيلاني – محاضرات في قانون أصول المحاكمات الجزائية الأردني والمقارن – ج2 – دار الفارابي – عمان – 1985م.
20. د.محمد فهمي طلبة وآخرون – دائرة المعارف/ الحاسب الإلكتروني – مجموعة كتب دلتا – مطابع المكتب المصري الحديث – القاهرة – 1991م.
21. محمد محمد شتا – فكرة الحماية الجنائية لبرامج الحاسوب – دار الجامعة الجديدة – الإسكندرية – 2001م.
22. د.سعيد حسب الله عبدالله -الوجيز في قانون الإجراءات الجنائية البحريني-ط1-إصدارات جامعة البحرين-البحرين-2005م.
23. د.محمود محمود مصطفى – الإثبات في المواد الجنائية في القانون المقارن – رسالة دكتوراه – جامعة القاهرة - القاهرة – 1978م.
24. د. مارسيل لوكلير – الوجيز في الشرطة التقنية – تعريب د. بسام الهاشم – ط1 – الدار العربية للموسوعات – بيروت – 1983م.

25. د. رؤوف عبيد – مبادئ الإجراءات الجنائية في القانون المصري – ط16 – دار الجيل – القاهرة – 1986م.

26. د.مأمون محمد سلامة – الإجراءات الجنائية في التشريع المصري – ج1 – دار النهضة العربية – القاهرة – 1988م.

27. د. جميل عبد الباقي الصغير – أدلة الإثبات الجنائي والتكنولوجيا الحديثة (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية) - دراسة مقارنة – دار النهضة العربية - القاهرة – 2001م.

28. د.عبد الفتاح بيومي حجازي- مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دراسة قانونية متعمقة في القانون المعلوماتي- دار الكتب القانونية و دار شتات والبرمجيات-مصر-2007م.

29. Bort , Julie – To Catch a thief – Infoworld 21/7/1997- Vol.19.Issue.29.

30. Welch , Thomas – Computer Crime Investigationj and Computer forensics – Information Systems Security – Summer 19 97 , Vol.6.Issue.2.

31. Hildreth , Jacqwi – The Enemy Withen – Delecting White Cfoller Crime – Intrnational Review of Law Computer and Technology Oct 1997, Vol.11.Issue 2.

32. Eoghan Casey, Digital Evidence and Computer Crime, Academic Press, 1 st edition, 2000.

33. The (NCIS) Argentine Computer Interusion. Investigation – FBI- Law Enforcement Bulletin-Oct 1982, vol.67 Issue 10.