تراجع الحق في الخصوصية
في مواجهة الاتصالات الإلكترونية

د. شيماء عبد الغني عطا الله (*)

(*) مدرس القانون الجنائي– كلية الحقوق – جامعة الزقازيق

مقدمة

موضوع البحث:

يُعتبر الحق في الخصوصية من الحقوق الدستورية اللصيقة بالإنسان[1]، ويُعد التقدم التكنولوجي في الاتصالات الإلكترونية من أحد الأسباب التي كان لها عظيم الأثر في المساس بهذا الحق. فعلى الرغم من أن الاتصالات الإلكترونية قد سهَّلت التواصل بين الأفراد إلا أنها مع ذلك تحمل الكثير من المخاطر على الحق في الخصوصية. فنجد الأفراد سواء أكانوا كباراً أم صغاراً يقومون بوضع معلوماتهم الشخصية وصورهم ومقاطع فيديو خاصة بهم وبأسرهم على شبكة الإنترنت، وبصفة خاصة مواقع التواصل الاجتماعي مثل الفيسبوك وتويتر. ويترتب على ذلك وجود خطر لا يستهان به على حرمة الحياة الخاصة ويعرض معلومات الأفراد للانتهاك[2].

فقد أدى التطور التكنولوجي إلى زيادة المخاطر التي يتعرض لها الحق في الخصوصية عند الأفراد. فيعتمد غالبية الأفراد في تعاملهم اليومي على استخدام التكنولوجيا سواء في التواصل مع بعضهم البعض، أو في التعامل مع الجهات الحكومية أو غير الحكومية. وأصبحت الحياة الخاصة للأفراد التي تعتمد في الكثير من مظاهرها على تقنية المعلومات مجالاً لصور متعددة للانتهاك منها على سبيل المثال اختراق البريد الإلكتروني[3].

ونتناول في هذا البحث ما تتعرض له الاتصالات الإلكترونية سواء أكانت صوتية أم مكتوبة (البريد الإلكترونية أو المحادثات الفورية التي تتم عن طريق تشات أو الفيسبوك أو توتير أو الفايبر أو التانجو.....إلخ) من انتهاك لحرمة البيانات

(1) تنص المادة 57 من الدستور المصري 2014 على أنه: «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 قضائي مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك».

(2) انظر سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة عبر الإنترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية – المجلد –29 العدد الثالث – 2014، ص423.

(3) جاسم محمد العنتلي، الجرائم والتكنولوجيا الحديثة – دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، 2014، ص13.

والمعلومات التي يتم تداولها عبر الإنترنت. كما سنعالج الضمانات الأساسية لحرمة الحياة الخاصة وما تتعرض له من انتهاك بسبب تشريعات بعض الدول التي تجيز التفتيش والاعتراض والتسجيل للمحادثات الإلكترونية بدون سبق الحصول على إذن.

خطة البحث:

يمكن تقسيم الدراسة على النحو التالي:

المبحث الأول: صور انتهاك حرمة الحياة الخاصة في الاتصالات الإلكترونية.

المبحث الثاني: تجريم اعتراض وتسجيل الاتصالات الإلكترونية دون إذن مسبق.

المبحث الثالث: حالات تفتيش النظام بإذن ودون إذن.

المبحث الأول

صور انتهاك حرمة الحياة الخاصة

بخصوص البيانات المسجلة في الأجهزة الإلكترونية

أولاً – الاطلاع على البيانات المتعلقة بالحياة الخاصة للأفراد:

تحتوي بعض أجهزة الكمبيوتر على بيانات متعلقة بالحرية الفردية كالحالة الاجتماعية والحالة الصحية والدين والانتماءات السياسية والحالة الوظيفية والحالة الجنائية (وجود أحكام سابقة أو تحقيقات.....إلخ).

وتحرص التشريعات المقارنة على حماية البيانات والمعلومات الشخصية للأفراد والمسجلة لدى الجهات المختلفة سواء أكانت حكومية أم غير حكومية. فتنص المادة (32) من القانون رقم 20 لسنة 2014 بشأن المعاملات الإلكترونية في الكويت على أنه: «لا يجوز في – غير الأحوال المصرح بها قانوناً – للجهات الحكومية أو الهيئات أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية أو العاملين بها الاطلاع دون وجه حق أو إفشاء أو نشر أي بيانات أو معلومات شخصية مسجلة في سجلات أو أنظمة المعالجة الإلكترونية المتعلقة بالشؤون الوظيفية، أو بالسيرة الاجتماعية، أو بالحالة الصحية، أو بعناصر الذمة المالية للأشخاص، أو غير ذلك من البيانات الشخصية المسجلة لدى أي من الجهات المبينة في هذه المادة، أو العاملين بها بحكم وظائفهم، ما لم يتم ذلك بموافقة الشخص المتعلقة به هذه البيانات أو المعلومات، أو من ينوب عنه قانوناً، أو بقرار قضائي مسبَّب. وتلتزم الجهات المبينة في الفقرة الأولى من هذه المادة ببيان الغرض من جمع البيانات والمعلومات المذكورة، وأن يتم جمع تلك البيانات والمعلومات في حدود ذلك الغرض».

كما تنص المادة (35) من قانون المعاملات الإلكترونية الكويتي على أنه: «يحظر على الجهات المذكورة بالمادة (32) ما يلي:

أ– جمع أو تسجيل أو تجهيز أي بيانات أو معلومات شخصية من تلك المنصوص

عليها في المادة (32) بأساليب أو طرق غير مشروعة أو بغير رضاء الشخص أو من ينوب عنه.

ب- استخدام البيانات أو المعلومات الشخصية المشار إليها والمسجلة لديها بسجلاتها، أو بأنظمة معلوماتها في غير الأغراض التي جمعت من أجلها.

وتلتزم تلك الجهات بالآتي:

أ- التحقق من دقة البيانات أو المعلومات الشخصية الوارد ذكرها في المادة (32) والمسجلة لديها بأنظمة معلومات والمتعلقة بالأشخاص واستكمالها وتحديثها بانتظام.

ب- اتخاذ التدابير المناسبة لحماية البيانات والمعلومات الشخصية المشار إليها في المادة (32) من كل ما يعرضها للفقد أو التلف أو الإفشاء، أو استبدالها ببيانات غير صحيحة أو إدخال معلومات عليها على خلاف الحقيقة».

كما تنص المادة (36) على أنه: «أ- يجوز للأفراد أن يطلبوا من الجهات المبينة بالمادة (32) محو أو تعديل أي مما تقدم من البيانات أو المعلومات الشخصية المتعلقة بهم، والتي تختزنها في سجلاتها أو أنظمة المعالجة الإلكترونية الخاصة بها، إذ تبين عدم صحة هذه البيانات أو عدم تطابقها مع الواقع، وكذلك لاستبدالها وفقاً لما طرأ عليها من تعديل. ب- وتحدد اللائحة التنفيذية لهذا القانون الاجراءات والضوابط الواجب اتباعها بخصوص الطلبات التي تقدم من الأفراد لمحو أو تعديل أي من البيانات المشار إليها المسجلة بخصوصهم لدى إحدى الجهات سالفة الذكر".

ويعاقب المشرِّع الكويتي في قانون سنة 2014 على كل صور الاطلاع أو التجسس أو التنصت على الأجهزة الإلكترونية بشكل غير مباشر دون أن ينص على تجريمها بشكل صريح. ولكنه بدلاً من ذلك اختار أن يجرِّمها من خلال تجريم الدخول إلى النظام دون إذن من له صاحب الحق في ذلك. فتنص المادة (37) من القانون رقم 20 لسنة 2014 بشأن المعاملات الإلكترونية الكويتي على أنه: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون آخر يعاقب بالحبس لمدة لا تزيد على ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرين ألف دينار أو

بإحدى هاتين العقوبتين كل من:

أ- تعمَّد الدخول بغير وجه حق إلى نظام المعالجة الإلكترونية، أو عطَّل الوصول إلى هذا النظام، أو تسبَّب في إتلافه، أو حصل على أرقام أو بيانات بطاقات ائتمانية، أو غيرها من البطاقات الإلكترونية لاستخدامها للحصول على أموال الغير.

ب- أصدر شهادة تصديق إلكترونية، أو زاول أي من خدمات التصديق الإلكتروني دون الحصول على ترخيص بذلك من الجهة المختصة.

ج- أتلف أو عيَّب توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً، أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحويل بأي طريقة أخرى.

د- استعمل توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً معيباً أو مزوراً مع علمه بذلك.

هـ- توصَّل بأي وسيلة - بغير حق - على توقيع أو نظام أو مستند أو سجل إلكتروني أو اختراق هذا النظام أو اعترضه أو عطله عن أداء وظيفته.

و- خالف أحكام المادة (32)، والبندين «أ- ب» من الفقرة الأولى من المادة (35) من هذا القانون ويجوز الحكم بمصادرة الأدوات أو البرامج أو الأجهزة التي استخدمت في ارتكاب الجريمة وذلك دون إخلال بحقوق الغير حسني النية.

وفي جميع الأحوال يحكم بنشر ملخص الحكم النهائي الصادر بالإدانة في صحيفتين يوميتين صادرتين باللغة العربية على نفقة المحكوم عليه، كما ينشر على شبكة الاتصالات الإلكترونية المفتوحة وفقاً للقواعد التي تحددها اللائحة التنفيذية. وتضاعف العقوبة في حالة العود إلى ارتكاب أي من هذه الجرائم".

ولهذا السبب أيضاً تضع بعض القوانين المقارنة قواعد خاصة لتفتيش هذا النوع من الأجهزة وذلك لحماية هذه البيانات. من ذلك القانون الهولندي لسنة 1993 الذي ينص في المادة (125) منه على أنه: «إذا أدى تفتيش الأجهزة إلى تسجيل بيانات معينة، فإنه من الواجب إخطار صاحب النظام بقائمة تضم هذه البيانات». ولمزيد من تحقيق حماية البيانات المتعلقة بالحياة الخاصة تقرر المادة (125) من القانون الهولندي

السابق أن يتم محو البيانات التي تنتمي إلى هذا النوع، ويقوم بهذا المحو الشخص الذي سبق أن قام بتسجيل هذه البيانات.

بيد أنه ليس في التعديل الأول أو الرابع للدستور الأمريكي ما يحول دون السماح لرجال الضبط القضائي بتفتيش مكاتب الصحافيين بناء على إذن بضبط أدلة تفيد في كشف الجريمة، وهي كثيراً ما تتعلق بأسماء المشاغبين في المظاهرات. وهذا ما قضت به المحكمة العليا الأمريكية[1].

غير أن المشرِّع الأمريكي سنَّ قانون حماية الحياة الخاصة[2] ليحظر هذا النوع من التفتيش فينص هذا القانون على أنه: «لا يجوز لرجال الضبط القضائي تفتيش أو الضبط للمواد في أحد الفروض الآتية:

1- أن تكون المواد مجهزة أو مقدمة أو مؤلفة أو أنشئت بغرض العرض على الجمهور.

2- أن تتضمَّن المواد الانطباع العقلي أو النتائج أو النظريات لمن قام بإعدادها.

3- أن تكون هذه المواد بغرض النشر للجمهور.

4- أن تكون هذه المواد وثائقية والتي تحتوي على المعلومات».

ثانياً- الاطلاع على بيانات الأفراد لدى الجهات القضائية:

تحوز جهات قضائية كالنيابة العامة والمحاكم - كما تحوز جهات الضبط القضائي - بيانات تتعلق بالقضايا التي تحتوي على بيانات خاصة بالأفراد، سواء أكانوا من المتهمين أم من الشهود. وتنظم كثير من التشريعات هذه البيانات المسجلة في أنظمة تلك الجهات من حيث السلطات التي لها حق الاطلاع أو الدخول إلى تلك الأنظمة. ففي فرنسا على سبيل المثال لا يجوز الدخول إلى تلك الأنظمة للاطلاع على البيانات إلا بمقتضى أمر قضائي، أو عند توافر حالة التلبُّس. كما تجيز بعض التشريعات لرجال الضرائب أن يطلعوا على تلك البيانات وذلك بهدف مكافحة التهرب الضريبي[3].

(1) Zurcher v. Stanford Daily , 436 U. S. 547 (1978) , www.cybercrime. gov/s&smanual2002. htm., p. 36 .

(2) Privacy Protection Act . p.37.

(3) Pascal VERGUCHT , La répression des délits informatiques dans une perspective internationale , Thèse , Montpellier , 1996, p. 378.

كما يتقيد تفتيش البيانات بالحدود التي تنص عليها القوانين بخصوص بعض المعلومات التي يشملها سر المهنة أو قوانين أخرى كتلك التي تتعلق بأسرار الدولة العسكرية والسياسية والاقتصادية.....إلخ. من البيانات السرية التي لا يجوز أن يرد عليها التفتيش تلك المتعلقة بسر المهنة كالأطباء والمحامين.... وقد نصت بعض القوانين على تلك القيود كالقانون الهولندي الذي ينص صراحة على إعفاء أصحاب المهن الذين يعفون أصلاً من الشهادة من أن يخضعوا لإجراءات التفتيش، إن لم يتم التفتيش برضاء من أصحاب تلك الأسرار[1].

ثالثاً- الاطلاع على بيانات الموكلين لدى المدافع عنهم:

تعتبر بيانات الموكلين لدى المدافعين عنهم (المحامون) من البيانات التي وضع المشرع لتفتيشها نظاماً خاصاً، ومن الواضح أن هذا النظام يسري على البيانات المبرمجة في كمبيوترات المحامين. فتنص المادة (51) من قانون المحاماة رقم (17) لسنة 1983 على أنه: «لا يجوز التحقيق مع محام أو تفتيش مكتبه إلاّ بمعرفة أحد أعضاء النيابة العامة، ويجب على النيابة العامة أن تخطر مجلس النقابة الفرعية قبل الشروع في تحقيق أي شكوى ضد محام بوقت مناسب». ويترتب البطلان على مخالفة الفقرة الأولى من المادة السابقة[2]. ومن الواضح أن التفتيش والضبط لا يتم في هذه الحالة إلاّ عندما يكون المحامي هو نفسه متهماً بتهمة معينة.

(1) Pascal VERGUCHT , ibid .

(2) عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، 2011، ص 527.

المبحث الثاني

مدى جواز اعتراض وتسجيل

الاتصالات الإلكترونية بدون إذن مسبق

القاعدة: حرمة الحياة الخاصة للبيانات المعالجة آلياً

من المستقر عليه أنه لا يجوز دخول المساكن بغير سبق الحصول على إذن بذلك من سلطة التحقيق. ويقترب الأمر في ذلك بالنسبة للدخول إلى البيانات الموجودة في داخل النظام الإلكتروني. بيد أن مفهوم الدخول إلى النظام يختلف عن الدخول إلى المساكن؛ فالدخول إلى النظام يتم عن طريق تشغيل الجهاز عن قرب أو عن بعد، أو الدخول إلى البيانات الموجودة في جهاز يعمل بالفعل، وذلك باستعمال برنامج خاص بذلك. وتطبيقاً لذلك قُضي في الولايات المتحدة الأمريكية بأن التعديل الرابع للدستور الأمريكي (الذي يحمي الحق في الخصوصية) يحمي البيانات المعالجة آلياً من التداخل إليها عن بعد، مقيماً التماثل بين الاقتحام المادي (للمنازل) والاقتحام المعنوي (للمعلومات)[1].

فلا يشترط لتسجيل المحادثات الإلكترونية بل والمحادثات الهاتفية الدخول إلى أماكن خاصة ووضع أجهزة التنصت في تلك الأماكن، بل يجوز القيام بذلك عن بعد، وهنا يشملها التنظيم القانوني أي الحظر مادامت توافرت الشروط القانونية اللازمة لذلك. تطبيقاً لذلك قُضي في الولايات المتحدة الأمريكية بأن وضع جهاز تنصت على كابينة تليفون كي يسمح ذلك بالتنصت على مكالمة تليفونية يجريها المتهم مع الغير تعتبر عملاً غير مشروع[2]. فإذا كان من المقرر أن ما يسمح به الشخص للغير أن يراه لا يُعد منتمياً إلى الحق في الحياة الخاصة، فإن ذلك يسري على ما يراه الشخص خارج

(1) Katz .c. U.S , 389 U.S. 352 (1967) : www.cdt.org/digi_tele/19706rpt.html#note_1 cited by : René PEPIN , Le statut juridique du courriel au Canada et aux Etats – Unis , www.lex--electronica.org /articles /v6-2/pepin.htm , 29 déc. 2003 , p.4.

(2) Katz v. United States , 88 S.Ct. 507 (1967) : Joshua DRESSELER, George C. THOMASS III, Criminal procedure , West Group , St. Paul , MINN, 1999, p.82.

كابينة التليفون بالنسبة لما يراه داخل تلك الكابينة إذا كانت هذه الكابينة زجاجية، أما بالنسبة لما يجري فيها من أحاديث تليفونية، فإن ذلك لا يعرض الشخص للغير ومن ثمّ ينسحب عليه الحق في الخصوصية.

كما نستفيد من هذا الحكم أنه لا يلزم دخول المكان الخاص للتنصت، وإنما يمكن أن يحدث ذلك التنصت عن بعد، كما في حالة اعتراض الاتصالات الإلكترونية. هذا الالتقاط عن بعد يعتبر وسيلة غير مشروعة لتجميع الدليل، ويعتبر الدليل الذي تحصَّل بتلك الطريقة دليلاً باطلاً.

كما ينسحب التعديل الرابع للدستور الأمريكي على البريد الإلكتروني ويشمله بالحماية. وبناء عليه لا يجوز الاطلاع أو التنصت أو التفتيش إلا بإذن قضائي مسبب وفقاً للقواعد المستقر عليها في مجال التنصت والتفتيش. تطبيقاً لذلك قضت المحكمة العليا الأمريكية – في قضية Berger وفي قضية Katz في سنة 1967 – بأن التعديل الرابع يحمي الاتصالات الإلكترونية من التنصت عليها أو اعتراضها وتسجيلها[1].

تجريم اعتراض الاتصالات الإلكترونية:

تعاقب كثير من التشريعات المقارنة على اعتراض الاتصالات السلكية واللاسلكية الخاصة دون إذن بذلك، باعتبار أن ذلك يتضمن انتهاكاً لحرمة الحياة الخاصة. فتنص المادة (309) مكرر عقوبات مصري على أنه: «يعاقب بالحبس مدة لا تقل عن سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه:

1. استرق السمع، أو سجل، أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون.
2. التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.

(1) Katz v. U.S. , 389 U.S. 347 (1967). Berger v. New York, 388 U.S. 41 (1967), Katz v. U.S. , 389 U.S. 347 (1967) ; cited by : René PEPIN , Le statut juridique du courriel au Canada et aux Etats – Unis , www.lex-electronica.org /articles /v6-2/pepin.htm.

3. فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضاً.

4. ويُحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها».

غير أن قانون الجزاء الكويتي لم يتضمن نصاً مماثلاً للعقاب على مثل تلك الأفعال من استراق السمع والتسجيل للمحادثات الخاصة والتقاط الصور التي تجري في مكان خاص، وهو الأمر الذي يتعين تداركه. ولكن نص على جريمة التداخل في النظام في المادة (37) من القانون رقم 20 لسنة 2014 في شأن المعاملات الإلكترونية، كما نظَّم هذا القانون جمع البيانات الشخصية عن الأفراد وحظرها إلاّ بموافقتها، كما حظر الاطلاع عليها إلاّ بإذن أصحابها أو بأمر قضائي (مادة 32 ومادة 33).

كما تدخل المشرِّع الكويتي بالنص على جريمة انتهاك حرمة الحياة الخاصة في مجال الاتصالات وذلك بمقتضى قانون الاتصالات رقم (28) لسنة 2014 التي تنص المادة (46) منه على أنه: «يحظر تداول أجهزة التنصت بأنواعها كما يحظر بيعها أو عرضها للبيع، ولا يجوز لغير الجهات الرسمية المختصة والتي يصدر بتحديدها مرسوم حيازة أجهزة التنصت بأنواعها، كما لا يجوز لأي من هذه الجهات استعماله دون الحصول على إذن مسبق من النيابة العامة وذلك في الحالات ووفقاً للإجراءات والأحكام المنصوص عليها في قانون الإجراءات والمحاكمات الجزائية الكويتي». ويعاقب القانون كل شخص يحوز أو يستعمل أجهزة تنصت فتنص المادة (78) على أنه: «كل من حاز أو استعمل أجهزة التنصت أياً كان نوعها يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على خمسة آلاف دينار كويتي ولا تقل عن خمسمائة دينار». كما تنص المادة (51) من القانون السابق على أنه: «تعتبر المكالمات الهاتفية والاتصالات الخاصة من الأمور السرية التي لا يجوز انتهاك حرمتها، وإلا وقع المخالف تحت طائلة المسؤولية القانونية». وتعاقب المادة (70) كل شخص أساء عمداً استعمال وسائل الاتصالات الهاتفية بقولها: «كل من أساء عمداً استعمال وسائل

الاتصالات الهاتفية يعاقب بالحبس مدة لا تزيد على سنة، وبغرامة لا تزيد على ألفي دينار كويتي .....».

ويلاحظ أن النص السابق في القانون المصري يخص المحادثات الشفوية التي تجري في مكان خاص، كما يخص المحادثات الشفوية التي تتم عن طريق التليفون. وبالتالي فإن النص ينحسر دون المحادثات التي تتم عن طريق الكمبيوتر، والتي تتخذ شكل البريد الإلكتروني أو شكل «المحادثة الفورية»، ويُعد ذلك تطبيقاً لمبدأ الشرعية الذي يقضي بأنه لا جريمة ولا عقوبة إلاّ بناء على قانون[1]. كما أن النص يسري على المحادثات التي تجري في مكان خاص، ولا تعتبر شبكة الإنترنت مكاناً خاصاً حتى بالنسبة للمحادثات الفورية بنظام «التشات». غير أن هناك من قال بسريان النص السابق على هذا النوع من المحاثات استناداً إلى أنها تتم عن طريق خط تليفوني[2]. غير أننا لا نؤيد هذا الرأي استناداً إلى أن هذا النوع من المحادثات يتم عن طريق شبكة الإنترنت، وما استخدام الخط التليفوني إلاّ وسيلة للدخول على الشبكة فقط. لذا فإن هناك محاثات تجري بطريق التليفون مباشرة، ومحادثات تجري بطريق الشبكة التي يستخدم في الدخول عليها خط تليفوني.

لذلك تُعنى التشريعات الحديثة بإدخال من النصوص الخاصة ما يسري على الاتصالات الإلكترونية أي تلك التي تتم عن طريق الكمبيوتر بالإضافة إلى الاتصالات السلكية واللاسلكية.

من تلك التشريعات ما تضمنه القانون الجنائي الفيدرالي الأمريكي (Title 18 Sec.2511 ، Part 1، Chapter 119 ،) من عقاب من قام باعتراض المراسلات الإلكترونية، مساوياً في ذلك بينها وبين الاتصالات السلكية، بنصه على عقاب كل من اعترض أو حاول اعتراض أو ساعد غيره على أن يعترض أو يحاول اعتراض أي اتصال سلكي أو شفوي أو إلكتروني. بل إن القانون الأمريكي يعاقب – احتراماً لحرمة الحياة الخاصة – كل من أفشى أو حاول أن يفشي محتوى اتصال هاتفي

(1) عبد الرؤوف مهدي، شرح القواعد العامة لقانون العقوبات، دار النهضة العربية، 2011 ، ص 89 .
(2) محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية 2003، ص 138.

أو إلكتروني إذا كان الفاعل عالماً أو كان هناك من الأسباب ما يدعو إلى الاعتقاد أن المعلومات تم الحصول عليها من خلال ذلك الاعتراض المخالف للقانون.

كما يعاقب القانون الأمريكي على الدخول إلى معلومات مخزنة إلكترونياً دون تصريح أو تجاوزاً لتصريح سابق. كما يعاقب على تعديل طريقة الدخول لصاحب الحق فيه، وتُشدد العقوبة إذا توافر قصد خاص يتمثل في الرغبة في الحصول على مزايا تجارية أو مادية (TITLE 18 > PART I > CHAPTER 121 > Sec. 2701Sec. 2701 .

وقد عرّف القانون الجنائي الفيدرالي الأمريكي الاتصالات السلكية في المادة(Title 18، Part 1، Chapter 119، Sec.2510) بأنها[1]: «نقل للكلمات المنطوقة بصفة كلية أو بصفة جزئية من خلال استعمال معدات لنقل الاتصالات عن طريق أسلاك أو كوابل أو أي وسيلة أخرى مشابهة بين نقطة الاتصال الأصلية ونقطة الاستقبال (بما فيها استعمال هذه الوسائل في محطة تحويل الاتصالات)، والتي يتم تقديمها أو تشغيلها من جانب شخص يعمل في تقديم أو تشغيل هذه المعدات لنقل هذه الاتصالات بين الولايات، أو مع الخارج، أو يقدم خدمة الاتصالات التي تؤثر في التجارة داخل الدولة أو التجارة الخارجية».

وتؤكد المحاكم الأمريكية على المفهوم السابق، حيث قضت بأن: «الأصل أن الاتصال يكون اتصالاً إلكترونياً إذا لم يكن محمولاً بواسطة الموجات الصوتية ولا يتضمن صوتاً إنسانياً»[2]. وخلاصة القول هنا أن الإشارات الكهربية والإلكترونية التي لا تعتبر اتصالاً سلكياً تعتبر من قبيل الاتصالات الإلكترونية، إذن نخلص من ذلك إلى أن كل اتصالات الإنترنت بما فيها البريد الإلكتروني تعتبر من الاتصالات الإلكترونية.

كما أن الأصل في القانون الكندي أن تسجيل المحادثات التليفونية دون موافقة طرفيها يوصف الدليل المستمد منها بالبطلان وذلك لمخالفته لمبدأ مشروعية الدليل.

(1) http://www4.law.cornell.edu/uscode/18/2701.html

(2) United States v. Herring, 993 F.3d 784, 787 (11th Cir. 199), www.cybercrime.gov/s&smanual2002.htm. , p. 79 .

وقد أيدت المحكمة العليا الكندية هذه القاعدة في قضية Shacter c. Birks[1]. ومع ذلك فإن القضاء الكندي يجيز لرب العمل أن يتنصت على المحادثات التليفونية التي تجرى بين المستخدمين في شركته وبين عملاء الشركة، وذلك استناداً إلى أن تلك الأجهزة التليفونية تنتمي إلى العمل ومخصصة لمتابعة سير العمل. لذلك قضت محكمة الاستئناف الكندية بصحة الدليل المستمد من تلك المراقبة[2]. ويتفق هذا القضاء مع ما سبق أن أقرته أحكام المحاكم الأمريكية.

غير أنه يبدو من أحكام للقضاء الكندي أنها تتجه إلى قبول التسجيلات التليفونية بوصفها دليلاً في الإثبات، وذلك على الرغم من مخالفتها لحرمة الحياة الخاصة إذا وافق عليها أحد أطراف المحادثة. بل أكثر من ذلك فإن المحاكم الكندية تميل إلى القول بمشروعية الدليل حتى ولو تم التسجيل بغير علمٍ من كلا الطرفين[3]. ونحن لا نتفق مع هذا الاتجاه الذي يخالف ما هو مستقر عليه من بطلان الدليل المستمد من الإجراء الباطل.

وتنص المادة (3) من القانون المدني في مقاطعة الكيبيك بكندا على أن: كل شخص من حقه احترام سمعته واعتباره وحياته الخاصة، ولا يجوز المساس بحرمة حياته الخاصة إلاّ برضاء منه أو من ورثته أو كان القانون يجيز ذلك. وقد عددت المادة (36) من القانون المدني في الكيبيك صور المساس بالحياة الخاصة في التالي:

1. الدخول إلى مسكن الشخص أو ضبط أشياء منه.
2. اعتراض أو استعمال اتصال خاص.
3. التقاط أو استعمال صورته عن عمد عندما يتواجد في مكان خاص.
4. مراقبة حياته الخاصة بأي وسيلة كانت.

(1) Shacter c. Birks , 1985 . C.S 343 ; cité par , David G. Masse , www.masse.org/preuve_courriel.htm , p.13 .
(2) Roy c. Saulnier , 1992 . R.J.Q. 2419 ; cité par , David G. Masse , www.masse.org/preuve_courriel.htm .
(3) Roy c. Saulnier , 1992 R.C.Q. 2419 (C.A.) , David G. Masse , www.masse.org/preuve_courriel.htm , p.14 .

5. استعمال اسمه أو صورته أو ملامحه المتشابهة مع شخص أو صوته لغرض آخر

6. بخلاف إعلام الجمهور.

7. استعمال مراسلاته الخاصة أو مكاتيبه أو مستنداته الشخصية.

وقد أوردت المادة (2858) من القانون المدني لمقاطعة الكيبيك الجزاء المترتب على مخالفة تلك النصوص وهو استبعاد الدليل بقولها: «يجب على المحكمة – من تلقاء ذاتها – أن ترفض كل عناصر الإثبات التي تم الحصول عليها في ظروف تشكل مساساً بالحقوق والحريات الأساسية والتي يكون من شأن استعمالها الإضرار بحسن سير العدالة».

وعلى الرغم من النصوص الحديثة السابقة، فإن أحكام القضاء الكندي مازالت تتجه إلى أن الأمر لا يتعلق بحرمة الحياة الخاصة عندما يقوم أحد أطراف المحادثة التليفونية بتسجيل محتواها.

وقد ذهب القانون الأمريكي إلى أبعد من ذلك عندما عُني بوضع تنظيم للمحادثات الإلكترونية، غير مكتفٍ في ذلك بالقواعد العامة في المحادثات التليفونية؛ فقد ميَّز القانون الأمريكي بين الاتصالات الإلكترونية والمحادثات الشفوية على الرغم من أنهما محل للحماية ضد التنصت بقوله في المادة (Title 18 ، Part 1، Chapter Sec 2510 ، 119) : «إن الاتصالات الشفوية تعني أي اتصال شفوي يصدر عن شخص يتوافر لديه توقع – يستند إلى تبرير مقبول – أن مثل ذلك الاتصال ليس محلاً للاعتراض أو التنصت، ولكن هذا المصطلح لا يشمل الاتصالات الإلكترونية».

ومع ذلك فقد عرّف القانون الأمريكي الاعتراض بقوله» «إن كلمة (يعترض) تعني الحصول على محتوى الاتصال السلكي أو الإلكتروني أو الشفوي وذلك باستعمال أي وسيلة إلكترونية أو ميكانيكية أو أي وسيلة أخرى. كما عُني هذا القانون بتحديد المقصود بالوسائل الإلكترونية المستخدمة في الاتصالات محل التنظيم القانوني بأنها تعني أي من المعدات أو الأجهزة التي يمكن أن تُستعمل في اعتراض اتصال سلكي أو إلكتروني أو شفوي بخلاف ما يلي: – أي تليفون أو تليغراف أو معدات أو أدوات أو أي عناصر مكونة منها.

ومؤدى ما سبق أنه إذا تمت مراقبة الاتصالات الإلكترونية، فإن الدليل يُعد باطلًا. وقد عُني القانون الأمريكي بالنص على ذلك صراحة، مع أن ذلك لا يعدو أن يكون تطبيقاً للقواعد العامة في البطلان.

المبحث الثالث

حالات تفتيش النظام بإذن وتفتيشه دون إذن

سوف نتناول في هذا المبحث القواعد المنظمة لتفتيش النظام بناء على إذن (المطلب الأول) وتفتيش النظام دون إذن (المطلب الثاني).

المطلب الأول

تفتيش النظام بناء على إذن

من المستقر عليه أن التشريعات المقارنة – كالقانون الأمريكي – لا تجيز تفتيش جهاز الكمبيوتر إلا بناء علي إذن وفقاً للأصل العام. ولا يصدر الإذن إلا بعد تحريات جدية. ومع ذلك فإن هناك حالات يجوز فيها التفتيش دون سبق الحصول على إذن. لذا سوف نميز بين التفتيش دون إذن والتفتيش بناءً على إذن.

– شروط إذن التفتيش في المواد الإلكترونية:

يلزم توافر شروط معينة لصحة التفتيش في المواد الإلكترونية. من هذه الشروط؛– أن تكون الجريمة على درجة معينة من الخطورة، – شرط جدية التحريات، بالإضافة إلى شرط التحديد.

أولاً– شرط خطورة الجريمة:

تشترط بعض التشريعات لصحة التفتيش – بوجه عام – أن يكون ذلك في جريمة ذات خطورة معينة، وذلك كالقانون الفنلندي الذي يستلزم أن تكون الجريمة معاقباً

عليها بالحبس مدة تزيد على ستة أشهر، ولا يتوافر ذلك في الجرائم المعلوماتية[1]. أما القانون المصري فإنه لم يشترط درجة معينة من الجسامة إلا فيما يتعلق بضبط الرسائل البريدية، وتسجيل المحادثات الهاتفية، حيث يتعين أن يكون ذلك في جناية أو جنحة معاقباً عليها بالحبس لمدة تزيد على ثلاثة أشهر (مادة 95 و 206 إجراءات جنائية). وبتطبيق ذلك على الجرائم الإلكترونية يتبين لنا أنه يلزم توافر هذا الشرط في التشريعات التي تستلزم ذلك فقط.

ثانياً – شرط جدية التحريات:

من المستقر عليه في التشريعات المقارنة أن الإذن بالتفتيش يلزم أن يصدر بناءً على تحريات جدية[2]. بل إن الدستور الأمريكي عُني – في التعديل الرابع منه – بالنص على أن الإذن «تفتيشاً أو قبضاً» يجب أن يكون صادراً بناء على دلائل كافية[3]. وبالمثل فإن قواعد الإجراءات الجنائية الأمريكية الفيدرالية في الفقرة (–41 جـ) تتطلب هذا الشرط.

ومن التطبيقات على الدلائل الكافية التي يلزم أن يستند الإذن بتفتيش المعلومات عليها ما قُضي به من توافر تلك الدلائل بين نقل الصور الفاضحة وعنوان إنترنت بروتوكول، وارتباط ذلك مع رقم حساب المتهم لدى مزوِّد الخدمات، ووجود رقمين للتليفون لديه يستخدمان في ذلك[4].

ثالثاً – شرط التحديد في الإذن:

يتجه الرأي في تشريعات مقارنة – كما هو الحال في القضاء الأمريكي – إلى تطلب شرط التحديد[5] اللازم لصحة الإذن والتفتيش. ويعتبر تنفيذ الإذن مخلا بشرط التحديد إذا قام رجل الضبط القضائي بضبط الجهاز، مع أن الإذن كان لضبط

(1) Pascal VERGUCHT , op. cit., p. 363.

(2) عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، المرجع السابق، ص 447 .

(3) U.S. Const .Amend . IV(« no Warrants shall issue , but upon probable cause, supported by Oath or affirmation «). Department of justice , p.48.

(4) United States v. Cervini , 2001 WL 863559 (10th Cir .Jul.31 ,2001); United States v. Hay , 231 F.3d 630 , 634 (9th Cir.2000); United States v. Grant , 218 F.3d 72 , 76 (1st Cir .2000). Department of justice , p.48 .

(5) Particularity.

المعلومات. ولا يعتبر الإذن مخلاً بشرط التحديد أن ينص على ضبط وتفتيش جهاز الكمبيوتر والديسكات الممغنطة والأقراص الممغنطة وكل البرامج التي يمكن أن تحتوي على أدلة تفيد في كشف الجريمة. وبناء عليه أيضاً فإنه يكفي لصحة الإذن بالتفتيش والضبط أن يقتصر هذا الإذن على ذكر «ضبط جهاز الكمبيوتر الخاص بالمتهم» دون تحديد أكثر من ذلك. وبالمثل لا يفتقر الإذن إلى شرط التحديد إذا ورد هذا الإذن على جميع عناصر الجهاز وملحقاته مع أن الضبط يستهدف بعض الملفات التي تحتوي على صور جنسية خاصة بالأطفال. ويرجع ذلك إلى صعوبة تحديد مواضع تلك الملفات[1].

ولنا أن نتساءل: إذا صدر الإذن بضبط الجهاز، هل يشمل هذا الإذن الديسكات والأقراص الممغنطة التي تتواجد على مقربة منه؟ للإجابة على هذا التساؤل نرى أنه يمكن الرجوع إلى القواعد العامة في تفتيش الأماكن حيث تتجه الأحكام القضائية إلى أن الإذن الصادر بتفتيش المنزل يمتد إلى ملحقاته[2]. ومن ثَمّ فإننا نرى أن الديسكات والأقراص الممغنطة هي من ملحقات الجهاز، بشرط أن تكون متواجدة على مقربة من هذا الجهاز محل التفتيش.

وقد اطردت أحكام القضاء الأمريكي على جواز ضبط الكمبيوتر مع أن الإذن جاء بصيغة عامة مشيراً إلى المستندات بوجه عام دون ما إشارة إلى المستندات المبرمجة[3]. وبالنسبة إلى الملفات فإن الأصل هو ضرورة تحديد تلك الملفات محل الضبط في الإذن.

(1) United States v. Hay , 231 F.3d 630 , 634 (9th Cir .2000) ; United States v. Campos , 221 F.3d 1143 , 1147 (10th Cir .2000) ; United States v. Upham , 168 F.3d 532 , 535 (1st Cir . 1999) ; United States v. Lacy , 119 F.3d 742, 746 (9th Cir. 1997) ; United States v. Henson , 848 F.2d 1374 , 1382-83 (6th Cir. 1988) ; United States v. Albert , 195 F. Supp . 2d 267 , 275-76 (D.Mass.2002); Cf. United States v. Lamb , 945 F. Supp . 441, 458-59 (N.D.N.Y 1996) ; Department of justice , p. 47 .

(2) قضت محكمة النقض بأن: «إيجاب إذن النيابة في التفتيش قاصر على حالة تفتيش مساكن المتهمين وما يتبعها من الملحقات. ولكن هذا الإذن ليس ضرورياً لتفتيش مزارعهم غير المتصلة بالمساكن، لأن القانون إنما يريد حماية حرمة المسكن فقط» :نقض 30 أبريل سنة 1934 مجموعة القواعد القانونية جـ3 ص 325 رقم 243 ؛ 8 أبريل سنة 1968 مجموعة أحكام النقض س 19 ص 398 رقم 75 ؛ 4 نوفمبر سنة 1968 س 19 ص899 رقم 178 ؛ 27 يناير سنة 1974 س 25 ص 58 رقم 13 ؛ 14 يناير سنة 1985 س36 ص 75 رقم 8 .

(3) United States v. Musson , 650 F. Supp . 525 , 532 (D. Colo . 1986) ; United States v. Reyes , 798 F.2d 380 , 383 (10th Cir . 1986) ; Department of justice , p. 48

ولكن هذا الأصل يرد عليه استثناء هو إذا وجدت دلائل كافية على تعدد الملفات المؤثمة في نفس الجهاز[1].

غير أنه يجوز تحديد الأشياء محل الضبط بصياغة شاملة بحيث تشمل البحث عن أدلة جريمة معينة. وعلى سبيل المثال يجوز أن يشمل الإذن بالتفتيش البحث عن معلومات في الكمبيوتر تتعلق بجريمة من جرائم المخدرات. ويستوي أن تكون المعلومات في أي شكل كان إلكترونياً أو مغناطيسياً في صورة ديسك أو أسطوانة أو مسجلة على الهارد ديسك أو في شكل أوراق تم طبعها بناء على ذلك.

- مجال الإذن بالتفتيش:

يمكن أن يصدر إذن بتفتيش الكمبيوتر ليشمل جميع البيانات الشخصية الخاصة بالمشترك والمتعاملين معه، وكذلك محتويات الملفات المخزنة بما فيها تلك التي تم تخزينها مدة أقل من 180 يوماً وفقاً للقانون الأمريكي. ولا يلزم لذلك أن يسبق صدور الإذن توجيه إخطار إلى المشترك[2]. مادة (18 (1) (b) 2703 U.S.C.§ A))) من القانون الأمريكي.

وبناءً على ذلك فإن الإذن بالتفتيش لا يتقيد بنوع معين من المعلومات. غير أنه مشروط في صدوره بضرورة توافر الدلائل الكافية على وقوع جريمة يفيد التفتيش لدى مزود الخدمات في كشف الحقيقة بخصوصها.

- اقتصار صدور الإذن بالتفتيش على الكمبيوتر:

غالباً ما يصدر الإذن بتفتيش مسكن المتهم أو محل عمله بحيث ينصرف هذا الإذن إلى كل ما يتواجد في المسكن أو في مقر العمل. فإذا صدر إذن بتفتيش المسكن أو محل العمل الخاص بالمتهم، فمن حق رجل الضبط القضائي أن يقوم بتفتيش أجهزة الكمبيوتر المتواجدة في المسكن أو محل العمل، ما دام أن ذلك يفيد في كشف الحقيقة عن الجريمة التي صدر الإذن بخصوصها.

(1) United States v. Ford , 184 F. 3d 566 , 576 (6th Cir . 1999) ; United States v. Kow , 58 F. 3d 423 , 427 (9th Cir . 1995) , www.cybercrime.gov/s&smanual2002.htm , ibid , p. 45 .
(2) United States Department of Justice , http://www.justice.gov/.

وبالمثل إذا صدر إذن بتفتيش شخص المتهم وكان هذا الأخير يحمل جهازاً متنقلا للكمبيوتر(لاب توب)، أو كان يقود سيارة بها جهاز الكمبيوتر، فإن الإذن بتفتيش شخص المتهم يشمل تفتيش جهاز الكمبيوتر في الحالتين السابقتين، باعتبار أن الكمبيوتر في هاتين الحالتين من ملحقات الشخص[1]. بيد أن هناك فارقاً في الشروط بين تفتيش مسكن المتهم وشخص المتهم؛ حيث لا تجيز حالة التلبس تفتيش مسكن المتهم بينما تجيز تلك الحالة تفتيش شخص المتهم[2].

ومع ذلك فإنه ليس هناك ما يمنع من صدور إذن بالتفتيش مقتصراً على تفتيش الكمبيوتر فقط دون بقية أجزاء المسكن أو محل العمل أو شخص المتهم. ويحدث ذلك إذا كانت التهمة الموجه إلى المتهم تتعلق بجريمة من جرائم الكمبيوتر فقط مثل حيازة صور جنسية إلكترونية فاضحة خاصة بالأطفال، وهي الجريمة التي تعاقب عليها كثير من التشريعات المقارنة (كالفرنسي والأمريكي) على ما سبق بيانه.

– تفتيش أكثر من ملف في كمبيوتر واحد:

قد يحتوي جهاز الكمبيوتر على أكثر من ملف، فإن التساؤل يثار حول اعتبار كل ملف «صندوقاً مغلقاً» يحتاج كل واحد منها إلى إذن قضائي مستقل عن الآخر. في إجابة على هذا التساؤل صدرت للقضاء الأمريكي أحكام اعتبرت الديسك بما فيه من ملفات وجهاز الكمبيوتر بما يحتويه من ملفات صندوقاً مغلقاً واحداً، أي أن هذه الأحكام لم تعتبر الملف الواحد صندوقاً مغلقاً مستقلاً، ومن ثَمّ فإن هذه الأحكام لا تستوجب صدور إذن قضائي مستقل لكل ملف على حدة[3].

وعلى خلاف ذلك اتجهت أحكام أخرى للقضاء الأمريكي إلى أن كل ملف في الكمبيوتر يتطلب إذناً لتفتيشه. وبناء على ذلك فإنها اعتبرت أن الملف الواحد صندوقٌ

---

(1) قُضي بأن: «تفتيش محل التجارة مستمد من اتصاله بشخص صاحبه»، نقض 6 أبريل سنة 1964، مجموعة أحكام النقض س12 ص246 رقم 49؛ 26 فبراير سنة 1978 س 29 ص 185 رقم 32. كما قضت محكمة النقض بأن: «حرمة السيارة الخاصة مستمدة من اتصالها بشخص صاحبها أو حائزها»، نقض 30 يونيو 1969 س 20 ص 976 رقم 193؛ 26 نوفمبر سنة 1984 س 35 ص 829 رقم187.

(2) حكم المحكمة الدستورية في 2 يونيو سنة 1984، القضية رقم 105 لسنة 4 ق دستورية.

(3) United States v. Runyan , 275 F.3d 449 , 464-65 (5th Cir. 2001) ; United States v. Slanina , 283 F.3d 670 , 680 (5th Cir . 2002) www.cybercrime.gov/s&smanual 2002.htm , p. 9 .

مغلقٌ. فتقول المحكمة: «السبب في اعتبار الملف الواحد صندوقاً مغلقاً هو أن الكمبيوتر يحتوي الكثير والكثير من المعلومات التي تتعلق بالحياة الخاصة لصاحب هذا الجهاز. وإذا أخذنا في الاعتبار أنه يجوز لرجال الضبط القضائي فتح الملفات الأخرى الموجودة في داخل جهاز الكمبيوتر، فإن ذلك سوف يؤدي بالفعل إلى الاعتداء على الحياة الخاصة التي يتمتع بها الفرد»[1].

- مشكلة تحديد السلطة المختصة بإصدار إذن التفتيش:

تقضي القاعدة العامة في كثير من الدول - مثل كندا والولايات المتحدة - بأنه من الضروري توافر الاختصاص للجهة القضائية التي تقوم بإجراء قضائي معين. ويتوافر هذا الاختصاص في الدولتين المشار إليهما عندما توجد بيانات الكمبيوتر محل التفتيش أو الضبط في جهاز، أو على شبكة تتواجد في دائرة اختصاص الجهة التي تأمر بهذا الإجراء. فالقاعدة رقم (41 - أ) من قانون الإجراءات الجنائية الأمريكي الفيدرالي تنص على أن الاختصاص بإصدار إذن التفتيش يؤول إلى الجهة القضائية في الدائرة [2] الفيدرالية التي يتواجد فيها محل التفتيش، شيئاً كان أو شخصاً[3].

وإذا كانت الشبكات التي ترتبط بها أجهزة الكمبيوتر لها خصوصيتها، حيث إنها تتعدى أكثر من مكان أو دائرة اختصاص، فإن تسجيل المكالمات التليفونية بناءً على إذن تفتيش يمكن أن يساعد في إيجاد حل لتلك المشكلة. في هذا الخصوص قُضي في الولايات المتحدة الأمريكية في قضية Etats-Unis v. Rodriguez بتوافر الاختصاص في دائرة منهاتن Manhattan بنيويورك لاعتراض وتسجيل مكالمات تليفونية، مع أنها صادرة من أجهزة تابعة لسنترال واقع في ولاية نيوجرسي Newgersey[4].

ويلاحظ أن الاختصاص ينعقد للجهة التي أصدرت إذن التفتيش ما دام محل

(1) United States v. Walser , 275 F. 3d 981 , 986 (10th Cir. 2001) , www.cybercrime.gov/s&s-manual2002.htm.

(2) district

(3) Pascal VERGUCHT , op. cit., p. 372.

(4) Etats-Unis contre Rodriguez , 968 F.2d 130 (2d Cir.) et 113 S. Ct . 140 (1992) cité par ETATS--UNIS , Département de la Justice , Division criminelle, Federal guidelines for searching and seizing computers , United States Government Printing Office , juill. 1994 , p.94.

التفتيش كان واقعاً في دائرة تلك الجهة، حتى وإن تغير مكانه بعد ذلك قبل تنفيذ الإذن أو الإجراء وانتقل إلى دائرة أخرى (كما لو تعلق الأمر بسيارة المتهم التي غادرت الدائرة التي صدر فيها إذن التفتيش). على ذلك يجري نص القاعدة (41 – أ) من قانون الإجراءات الجنائية الأمريكي الفيدرالي.

وقد يصدر إذن التفتيش لضبط بيانات معينة كانت مسجلة في جهاز معين يقع في دائرة اختصاص الجهاز. هذا الإذن يصلح للتنفيذ على تلك البيانات حتى وإن قام المتهم بنقل تلك البيانات على ذاكرة في جهاز يقع في دائرة اختصاص أخرى ما دام أنها مرتبطة بالجهاز محل التفتيش بحيث يمكن الدخول إليها من هذا الجهاز. ويُعد هذا تطبيقا لما هو مقرر من جواز تفتيش الشبكة التي يرتبط بها جهاز المتهم.

– مدى جواز اعتراض الاتصالات الإلكترونية:

ما المقصود باعتراض الاتصالات؟ يجيب على هذا التساؤل القانون الأمريكي في المادة 18 4) U.S.C.§ 2510) فيعرف التقاط أو اعتراض الاتصالات بأنه: «اكتساب سماعي أو غيره لمحتوى أية اتصالات سلكية أو إلكترونية أو شفوية وذلك من خلال استعمال أي جهاز سواء كان هذا الجهاز آلياً أو إلكترونياً أو غير ذلك». وقد قُضي بأن المقصود بكلمة اكتساب أن يتم الالتقاط أثناء الاتصال نفسه. ويترتب على ذلك أن مراقبة الاتصالات المخزنة لا يعتبر التقاطاً لها. وقد قضت المحاكم الأمريكية بذلك حيث اعتبرت الدخول إلى الاتصالات الخاصة بالبريد الإلكتروني المخزنة مختلفاً عن الالتقاط[1].

كما قُضي بأن الدخول على الاتصالات السلكية المخزنة أيضاً لا يعتبر من قبيل اعتراض الاتصالات[2]. وذهب الرأي الثاني إلى أن الالتقاط يمكن أن يرد على اتصالات مخزنة، واستند في ذلك على حجتين. الأولى أن الاتصالات السلكية تختلف عن

(1) Steve Jackson Games v. United States Secret Service , 36 F. 3d 457 , 460-63 (5th Cir . 1994) « access to stored e-mail communications « ; Wesley College v. Pitts , 974 F. Supp . 375 , 384 – 90 (D. Del . 1997) ; ; United States v. Scarfo , 180 F. Supp . 2d 572 , 582 (D . N . J . 2001) , www.cybercrime.gov/s&smanual2002.htm , ibid , p. 55.

(2) United States v. Moriarty , 962 F. Supp 217 , 220 – 21 (D . Mass . 1997) " access to stored wire communications " , www.cybercrime. gov/s&smanual2002.htm, p. 80 .

الاتصالات الإلكترونية من حيث العبارة التي وردت في تعريف الاتصالات السلكية وهي «تخزين إلكتروني لهذه الاتصالات». والثانية أن اقتصار الالتقاط على الاتصالات السلكية أثناء انتقالها فقط سوف يجعل العبارة السابقة بدون معنى. وحسماً للخلاف السابق ألغى القانون الأمريكي المسمي بـ USA PATRIOT ACT العبارة السابقة من تعريف الاتصالات السلكية. وبذلك تم حسم الخلاف لصالح الرأي الأول والراجح القائل بأن التقاط أو اعتراض الاتصال يكون أثناء الاتصال نفسه فقط وفيما عدا ذلك لا يعتبر اعتراضاً أو التقاطاً للاتصال.

ويجوز وضع المعلومات الموجودة بالكمبيوتر وكذلك تلك التي يتم تبادلها سواء بين جهاز وآخر من خلال شبكة داخلية (مثل تلك التي تتواجد داخل البنك الواحد) أو عدة شبكات محدودة (كتلك التي توجد بين مجموعة من البنوك) تحت المراقبة (التنصت) في شأن تحقيق جنائي قائم. والحقيقة أن ثمة خلافاً في القانون المقارن بخصوص شروط المراقبة (التنصت): هل يشترط أن يتم ذلك عندما تكون الجريمة من الجنايات أم يكفي أن تكون من الجنح؟

يتجه المجلس الأوروبي إلى جواز التنصت بخصوص الجرائم الخطيرة التي تقع على سرية الاتصالات اللاسلكية وكذلك الخاصة بالكمبيوتر والتداخل في هذه الأنظمة (الهاتفية أو الكمبيوتر) الذي من شأنه الاعتداء على الخطوط (بالسرقة) أو من شأنه الإخلال بحسن سيرها. وقد نصت التوصية رقم 13 لسنة 1995 للجنة الوزراء على ذلك.

وبخصوص اعتراض وتسجيل المعلومات التي يتم تداولها بطريق الكمبيوتر أوصت لجنة الوزراء التابعة للمجلس الأوروبي في سنة 1995 بأن يقتصر هذا الاعتراض على ما هو ضروري للتحقيقات الجنائية، وذلك على غرار ما يتم بالنسبة للتنصت على المحادثات التليفونية. فتنص التوصية رقم 13 على أنه: «إذا أخذنا في الاعتبار التوافق بين تقنية المعلومات والاتصالات اللاسلكية فإن التشريعات المتعلقة بالمراقبة المستخدمة في أغراض البحث الجنائي كاعتراض الاتصالات يتعين عند اللزوم مراجعتها وتعديلها».

- شروط تسجيل الاتصالات الإلكترونية وفقا للقانون الأمريكي والمقارن:

كي يتم تسجيل الاتصالات الإلكترونية أو الهاتفية على الوجه القانوني الصحيح- وفقا للقانون الأمريكي - يلزم أن يصدر به إذن من القاضي المختص بناء على طلب من أحد أعضاء النيابة ممن حددهم القانون الأمريكي بالموافقة على طلب تسجيل المحادثات الإلكترونية الذي يقدمه أحد رجال الضبط القضائي.

وقد حدد القانون الأمريكي الجرائم التي يجوز فيها استصدار إذن بتسجيل الاتصالات، ومن أهمها الجرائم المعاقب عليها بالإعدام أو بالحبس لمدة تزيد علي سنة واحدة. وعلى العموم فإن التشريعات المقارنة تقر مشروعية وضع المحادثات التليفونية تحت المراقبة - بناء على إذن من السلطة المختصة - لتجميع الأدلة عن جريمة معينة متى كان ذلك ضروريا لظهور الحقيقة[1].

وقد أجازت المحكمة الأوروبية لحقوق الإنسان هذا الإجراء تطبيقاً للمادة (8) من الاتفاقية الأوروبية لحقوق الإنسان باعتبار أن له ما يبرره في مجتمع ديموقراطي، وما دام أنه محاط بالضمانات القانونية اللازمة[2]. والجدير بالذكر أن التشريعات المقارنة تتجه إلى استلزام إذن صادر من قاض لتسجيل المحادثات الهاتفية؛ فتنص المادة (206) من قانون الإجراءات المصري على أنه: «ويجوز لها (أي النيابة) أن تضبط لدى مكاتب البريد جميع الخطابات والرسائل والجرائد والمطبوعات والطرود، ولدى مكاتب البرق جميع البرقيات، وأن تراقب المحادثات السلكية واللاسلكية، وأن تقوم بتسجيلات لمحادثات جرت في مكان خاص، متى كان لذلك فائدة في ظهور الحقيقة في جناية أو في جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. ويشترط لاتخاذ أي إجراء من الإجراءات السابقة الحصول مقدماً على أمر مسبب بذلك من القاضي

---

(1) انظر على سبيل المثال المادتين (44 و 45) من الدستور المصري ؛ نقض مصري 11 فبراير سنة 1974 مجموعة أحكام النقض س25 ص 138 رقم 31؛ وانظر كذلك المادتين (81 و151) من قانون الإجراءات الجنائية الفرنسي التي تجيز هذا الإجراء ؛ نقض فرنسي :

Crim 15 mars 1988 , Bull. crim. , nº 128 , p. 327 .

وانظر لمزيد من الأحكام الفرنسية :

Albear MARON , procédure pénale , Juriss – class . Procédure pénale , droit pénal , janv 1992 , p. 15 .

(2) Arrêt Klass c / R .F. Allemagne , 6 sept . 1978 .

الجزئي بعد إطلاعه على الأوراق». ويبرز ذلك ما يجمع بين المراسلات الإلكترونية والمراسلات الهاتفية من تماثل في النظام القانوني لكل منهما.

وجدير بالذكر أن المادة (8) فقرة 2 من الاتفاقية الأوروبية تجيز التدخل في نطاق الحياة الخاصة للأفراد بشروط، إذا كان ذلك منصوصاً عليه بمقتضى القانون وكان إجراءً ضرورياً في مجتمع ديمقراطي للحفاظ على الأمن العام أو الوقاية من الجريمة. وبالتالي فإن المواد (81 و151) من قانون الإجراءات الجنائية الفرنسي تتماشى مع أحكام الاتفاقية الأوروبية لحقوق الإنسان[1]. فقد صدر في فرنسا قانون في 10 يوليو سنة 1991 أدخل المواد من (100 إلى 7–100) إجراءات جنائية لتنظيم تسجيل المحادثات التليفونية. فتنص المادة (100) من قانون الإجراءات الفرنسي على أنه: «في مواد الجنايات وفي الجنح، إذا كانت العقوبة المقررة للجريمة هي سنتين حبس أو أكثر فإن قاضي التحقيق له – عندما تقتضي ذلك ضرورات التحقيق – أن يأمر باعتراض وتسجيل وتدوين المراسلات التي تتم بطريق الاتصالات اللاسلكية. وتتم تلك الإجراءات تحت إشرافه ومراقبته. ويكون قرار الاعتراض مكتوباً، وهو لا يجوز الطعن فيه». وتتلخص تلك الشروط وفقاً للقانون السابق في التالي: «1– يلزم صدور إذن من قاضي التحقيق، فلا يكفي صدور إذن من النيابة العامة في إطار حالة التلبس، 2– أن يكون ذلك في الجنايات والجنح المعاقب عليها بعقوبة الحبس سنتين على الأقل، 3 – يجب أن يكون الإذن الصادر به مكتوباً، كما أنه يلزم أن يحدد هذا الإذن الخط التليفوني الذي يتم وضعه تحت المراقبة»[2].

وقد أدخل المشرِّع الفرنسي ما يسمى بتسجيل المحادثات التليفونية بالطريق الإداري بمقتضى المواد من (3 إلى 19) من القانون الصادر سنة 1991، والذي نظم هذا النوع من التسجيل. ويسري التسجيل الإداري في مجال: – الأمن العام، – الحفاظ على مقدّرات الأمة العلمية والاقتصادية، – الوقاية من الجريمة، – الوقاية من محاولات تكوين مليشيات خاصة. ويشترط لهذا النوع من التسجيل توافر الشروط التالية: – «أن يصدر تصريح من رئيس الوزراء بناء على طلب من الوزير المختص، – تسري

(1) Merle et Vitu , Traité de droit criminel , Procedure pénale , éd. Cujas 2001 , p. 204.

(2) MERLE et VITU , Traité de droit criminel , Procedure pénale , op. cit. p.206 .

تلك الموافقة لمدة أربعة أشهر ما لم يتم التجديد، – يتم التسجيل والتفريغ للتسجيلات والإتلاف وفقاً للأساليب المتبعة في حالة التسجيل القضائي، – تخضع التسجيلات من هذا النوع لرقابة اللجنة الوطنية للرقابة Commission nationale de contrôle. هذه اللجنة الأخيرة تتشكل من شخصية يعينها رئيس الدولة، ومن نائب في البرلمان، وعضو من مجلس الشيوخ، وذلك لفحص شرعية الإجراءات، ويمكن أن تطلب وقفه وتقوم بتبليغ رئيس النيابة عن المخالفات التي تقع للقانون»[1].

ونستطيع أن نوجز أشكال المراقبة الإلكترونية في التالي:

1– استخدام وسائل فنية من خلال ما يسمى بقلم التسجيل أو ما يُسمى بالفخ والمتابعة. في هذه الحالة يتم تسجيل أسماء المتراسلين مع متهم معين أي مع بريده الإلكتروني أو ما يقوم بالمحادثة الفورية معه(تشات).

2– استخدام وسائل للتنصت على محتوى الرسالة الإلكترونية، أو المحادثة الفورية الإلكترونية بوسائل للاعتراض والتنصت.

ويلاحظ أن هناك مشكلة تتعلق بتشفير الرسائل حيث أصبح يتواجد في السوق الأمريكي خاصة برامج تشفير غيرغالية الثمن تسمح بتشفير الرسائل، الأمر الذي يثير مشكلات بالنسبة لرجال الضبط القضائي بعد ضبط الرسائل للتعرف على محتواها.

وقد أسفر التقدم التقني عن ابتكار برامج لمكافحة ما يلجأ إليه المجرمون من تشفير رسائلهم الإجرامية وذلك باستعمال جهاز يُقال له key Logger System، وتسمح تلك الوسيلة بتسجيل ضربات الجهاز على لوحة المفاتيح بعد استعمال الجهاز ومن ثَمّ تسمح بمعرفة كلمة السر. كما ظهر برنامج يُقال له Magic Lantern. تتلخص وسيلة الجهاز الأول في تثبيت قطعة معينة على جهاز الكمبيوتر الخاص بالمتهم، الأمر الذي يستلزم دخول مسكن المتهم لإتمام هذا العمل، أما البرنامج الثاني فإنه لا يستلزم سوى إرسال برنامج معين مختفياً في إعلان مثلاً إلى المتهم كما لو أُرسلت إليه رسالة تقول: «اضغط هنا لتكسب» وعند الضغط

(1) R. MERLE et A. VITU , op.cit., p. 207.

تُفتح الرسالة ويتم زرع برنامج Magic Lantern في جهاز المتهم دون أن يدري. وسواء تعلق الأمر بالوسيلة الأولى أو بالوسيلة الثانية فإن هاتين الوسيلتين تسمحان بمعرفة كلمة السر لجهاز المتهم والدخول إليه لمعرفة الشفرة التي يستعملها المتهم في رسائله.

وجدير بالملاحظة أنه يتعين التمييز بين الوسائل التقنية التي من شأنها الاطلاع على الجهاز وهو مغلق لا يستخدمه المتهم في المراسلة كالوضع بالنسبة لوسيلة Key Logger System، وبين الحالة التي فيها يتم التنصت على رسائل المتهم عند إرساله لها، كما في حالة استعمال برنامج يسمى المفترسcarnivore والذي يتيح التقاط الرسائل عند تداولها[1]؛ في الحالة الأولى يكفي إصدار إذن بالتفتيش. وبالفعل فقد قُضي في قضية United States v. Scarfo بأنه يكفي صدور إذن التفتيش لأن هذه الوسيلة تعمل والجهاز مغلق[2]. أما في الحالة الثانية فإنه يتعين الالتزام بالشروط التي يتطلبها القانون بالنسبة لتسجيل الاتصالات ومن أهمها صدور أمر من قاض وليس من النيابة العامة فقط وهو الأمر الذي يتطلبه القانون الأمريكي أيضا (18 U.S.C. §§ 3122–3123). كما انتقدت وسيلة KLS استناداً إلى أنها تؤدي إلى ضبط مراسلات عديدة للمتهم مع أن إذن التفتيش الصادر باستخدامها قد تضمن أن غرضها هو معرفة كلمة المرور الخاصة بالمتهم. ولم تر المحكمة في استخدام تلك الوسيلة ما يخالف قواعد تنفيذ التفتيش من ضرورة الالتزام بالغرض منه، ذلك أن من يحصل على إذن بتفتيش كتاب معين للحسابات يتعين عليه أن ينظر في كتب أخرى قبل أن يعثر عليه[3].

– عدم جواز اعتراض الاتصالات الإلكترونية بين المدافع والمتهم:

يثار التساؤل عن مدى انطباق أو إعمال القواعد الخاصة باعتراض المحادثات التليفونية على المحادثات الإلكترونية كالرسائل والمحادثات الفورية: هل تسري عليها قاعدة احترام الحق في الدفاع وخصوصاً المحادثات التي تجري بين المتهم والمدافع عنه

(1) Amitai Etzioni , Implications of Select New Technologies for Individual Rights and Public Safety , Harvard Journal of Law & Technology 2002 , p.274

(2) 180 F. Supp. 2d 572 : Amitai Etzioni , ibid , p. 276

(3) Amitai Etzioni , ibid , p. 280 .

بطريق مباشر أو بالتليفون؟ وهل نحتاج إلى قواعد خاصة تحكم المحادثات الإلكترونية ؟ الأصل أن الحق في الدفاع يحول دون تفتيش كمبيوتر المحامي عن المتهم لضبط ملفات خاصة بالدفاع . بيد أنه إذا اشترك المحامي مع المتهم في جريمة معينة، فإنه يصبح هو الآخر متهماً. لذا قُضي في هذه الحالة الأخيرة بأنه لا يجوز التمسك بالحق في الدفاع للدفع ببطلان تسجيل المحادثات التليفونية التي تتم بين المتهم والمدافع عنه ما دام أن المحامي يشترك في جريمة مع المتهم، فيصبح هو الآخر عندئذ متهماً معه[1].

كما أثار هذا الحكم النقاط الثلاث الآتية:

أولاً – صدور إذن بتفتيش مكان معين ينسحب على جهاز الكمبيوتر المتواجد به، ولا يشترط صدور إذن صريح بتفتيش جهاز الكمبيوتر. ويتماشى هذا المفهوم مع ما يتجه إليه القضاء الأمريكي في العديد من أحكامه، حيث يصح التفتيش الواقع على الكمبيوتر ما دام إذن التفتيش قد جاء عاماً بالمكان المتواجد فيه هذا الجهاز. ولكن عندما يقوم رجل الضبط بتفتيش الكمبيوتر فإن عليه أن يلتزم بالبحث عن الحقيقة في التهمة التي صدر الإذن بخصوصها، فإذا كان صادراً للتفتيش عن جريمة مخدرات فلا يصح للقائم بالتفتيش أن يتفرغ للتفتيش عن جرائم استغلال جنسي للأطفال.

ثانياً – إن تفتيش الكمبيوتر الخاص بالمدافع عن المتهم وضع له القانون قواعد خاصة، ما دام أنه متواجد في مكتب المحامي لأنه يأخذ حكم الملفات الورقية.

ثالثاً – يُثار التساؤل عما إذا كان يجوز تفتيش كمبيوتر جماعي وكان أحد أصحاب الحق فيه متهماً دون الآخرين وصدر إذن بتفتيشه، أو بتفتيش المكان الذي يتواجد فيه: هل يصح هذا الإذن أم أنه باطل؟ تقضي القاعدة بأن تفتيش المكان المشترك جائز ما دام أن المتهم يشارك فيه كأن يكون منزلاً مشتركاً أو مكتباً مشتركاً[2]. أما إذا كان أحد المشتركين في الكمبيوتر مدافعاً عن المتهم (ولم يكن هذا المدافع متهماً هو الآخر)، فإننا نرى أن التفتيش يتعين أن يحترم الحق في الدفاع؛ فلا يجوز ضبط ملفات في الكمبيوتر تتعلق بالدفاع عن المتهمين. ويقترب ذلك من تفتيش مسكن أحد أصحاب

(1) Crim ., 14 nov. 2001 ; D. : Juris-Data nº 012110 , JCP .16 janv 2002 nº3 , Edition Générale , Sommaires de Jurisprudence , p. 159 .
(2) Crim ., 14 nov. 2001 , op. cit., p. 159 .

الحصانات (كعضو مجلس الشعب أو أحد القضاة)، إذا كان ابنه متهماً ومقيماً معه في نفس المسكن، فيتجه الرأي إلى عدم جواز ذلك، تأسيسا على أن تفتيش المسكن دون رفع الحصانة يؤدي إلى تفويت الغاية التي من أجلها شُرعت الحصانة[1].

- الخصائص التي تميز تفتيش البريد الإلكتروني:

يتمتع صاحب البريد الإلكتروني بالحق في حرمة الحياة الخاصة بالنسبة للمعلومات المتواجدة داخل البريد الإلكتروني لجهاز الكمبيوتر الخاص به. وتقيم أحكام القضاء التماثل بين مراسلات البريد الإلكتروني والمراسلات التي تتم عن طريق البريد العادي. وبناءً عليه لا يجوز التدخل للاطلاع على البريد الإلكتروني دون إذن صاحبه، ما لم يصدر إذن قضائي بذلك. تطبيقاً لذلك قُضي بعدم مشروعية الدليل (في قضية Maxwell) في الولايات المتحدة الأمريكية بالنسبة للمتهم Maxwell الذي كان يحوز صوراً فاضحة خاصة بالأطفال (الأمر الذي يعاقب عليه القانون الأمريكي)، استناداً إلى أن رجال الضبط القضائي لجأوا إلى مزوِّد الخدمات الخاص بهذا المتهم، ليساعدهم على الدخول إلى بريده الإلكتروني والتعرف على ما يحوزه من تلك الصور، ومعرفة من يتعامل معهم في هذه الصور، وذلك دون سبق الحصول على إذن قضائي بذلك[2].

فالبريد الإلكتروني يتماثل مع المراسلات البريدية في أن كلا النوعين يتمتعان بالحق في الخصوصية الذي يضمنه الدستور والقانون في التشريعات المقارنة. تطبيقاً لذلك قُضي في كندا ببطلان الدليل المستمد من البريد الإلكتروني لأحد الأشخاص دون موافقة هذا الأخير[3].

وفي قضية تتلخص وقائعها في أن مأمور الضبط القضائي أثناء قيامه بتفتيش جهاز الكمبيوتر الخاص بالمتهم - عن تهمة تقليد البرامج- دخل على البريد الإلكتروني ووجد فيه رسائل جنسية خاصة بالقُصَّر، ومن المعروف أن هذه الرسائل مما يحظر القانون على الأشخاص حيازتها. وقد طعن المتهم ببطلان الدليل استناداً

(1) د. عبدالرؤوف مهدي، شرح قانون الإجراءات الجنائية، المرجع السابق، ص 465.

(2) U.S c. Maxwell 45 M.J 406 (1996) ; cited by : René PEPIN , Le statut juridique du courriel au Canada et aux Etats – Unis , www.lex-electronica.org /articles /v6-2/pepin.htm, p. 4.

(3) David G. Masse , www.masse.org/preuve- courriel.htm , op. cit., p.11 .

إلى أن مأمور الضبط القضائي قد خالف حق المتهم في حرمة حياته الخاصة، فقضت المحكمة الكندية ببطلان الدليل وذلك استناداً إلى الأسباب الآتية:

1- أن التفتيش من قبل مأمور الضبط القضائي غير قانوني لعدم وجود إذن مسبق بالتفتيش، بالإضافة إلى التعسف في التفتيش الذي يتضح من خلاله قيام مأمور الضبط القضائي بفتح كل الملفات بما فيها ملف الرسم .

2 – أن قيام مأمور الضبط القضائي بقراءة البريد الإلكتروني الخاص بالمتهم حيلة واضحة ومتعمَّدة وهي تمس بحق المتهم في التوقع المعقول للحياة الخاصة.

3 – وأخيراً، إن قيام مأمور الضبط القضائي بالتفتيش بدون الحصول على إذن مسبق بذلك يمثل مخالفة صريحة للمادة الثانية من ميثاق الحقوق والحريات الكندي.

– المقارنة بين الخطاب الورقي والمحادثة التليفونية فيما يتعلق بحرمة الحياة الخاصة:

إذا أرسل شخص إلى أخر خطاباً فإن هذا الخطاب يصبح ملكاً للمرسل إليه من وقت تسليمه إلى مصلحة البريد، ومن باب أولى عند وصوله إلى المرسل إليه. وبالتالي فإنه من الطبيعي أن يكون لهذا الأخير أن يفشي محتواه إلى الغير، فالرضاء ذو أثر فعَّال سواء أكان هذا الرضاء صريحاً أم ضمنياً. ومن التطبيقات على الرضاء الضمني ما قضت به المحاكم الكندية من أن الزوجة التي تلقت خطاباً وسلمته لزوجها دون مظروف خارجي يغلفه كي يقوم بوضعه بين بريدها قد تخلت عن حقها في حرمة الحياة الخاصة[1]. وبالتالي فإن من حق هذا الزوج أن يقرأه.

ويختلف الأمر في حالة المحادثة التليفونية حيث تجري المحادثة في شكل مباشر بين المتحدثين فليس هناك مرسل ومرسل إليه بل تفاعل في الحديث بين طرفين، فالأمر يتعلق بمحادثة وليس بمراسلة. وبالتالي فإنها ملك للاثنين، والأصل أنه لا يجوز الاعتداء على حرمتها إلا بموافقة الطرفين.

(1) L›arrêt Protection de la jeunesse -763 , J.E. 95-1099 (C.S.) , David G. Masse , www.masse.org/preuve_courriel.htm, p.16 .

– مدى التماثل بين الرسائل الإلكترونية والرسائل البريدية من ناحية النظام القانوني للتفتيش:

في حالة عدم وجود نص يحدد النظام القانوني للرسائل الإلكترونية يتعين علينا أن نبحث عما يقترب من الرسائل الإلكترونية، ولا نجد سوى النظام القانوني المعروف والخاص بالرسائل البريدية. والحقيقة أن الاثنين يقتربان من عدة أوجه: 1– كل منهما يشكل اتصالا مكتوبا بين طرفين، 2– كل منهما يستخدم صندوقاً بريدياً خاصاً، 3– تمر مدة بين إرسال واستقبال الرسالة في الحالتين، 4– تتفق الحالتان في أنه عندما يتم إرسال الرسالة لا يمكن للمرسل أن يستردها مرة أخرى، 5 – كما يتفقان أيضا في إمكانية إرسال رسائل إلى المرسل إليه من أشخاص غير مرغوب فيهم كأصحاب الإعلانات للبضائع والخدمات.

بيد أن هناك ما يفرق بين الرسائل البريدية والرسائل الإلكترونية وذلك على الوجه التالي:

هناك وسيط يتمثل في وجود طرف ثالث (أي إنسان) بين المرسل والمرسل إليه في خصوص الرسائل البريدية، الأمر الذي لا يتوافر بالنسبة للرسائل الإلكترونية.

الرسائل البريدية تتميز بالسرية بشكل أكبر من الرسائل الإلكترونية التي تسببت الوسائل التكنولوجية الحديثة في إمكانية التقاطها من الغير بالاستعانة ببرامج خاصة بذلك.

على الرغم من ذلك فإن البريد الإلكتروني يتمتع بحرمة المراسلات الخاصة، مع أن الجهاز الخادم يحتفظ بنسخة من هذا النوع من المراسلات الإلكترونية. وقد قُضي في الولايات المتحدة الأمريكية (في قضية United States v. Maxwell) تطبيقاً لذلك بأنه لا يجوز الإطلاع على المراسلات الإلكترونية لدى الجهاز الخادم إلاّ بعد سبق الحصول على إذن بذلك من الجهة المختصة[1]. على خلاف ذلك، فقد قُضي في قضية United States v. Charbonneau بأن اشتراك الشخص في غرفة

(1) United States v. Maxwell (1996) : Amitai Etzioni , op. cit., p.271

للمحادثات الفورية بين عدة أشخاص لا يجعل لمحادثته حرمة خاصة، ومن ثَمّ فإنه لا يلزم سبق الحصول على إذن للاستماع والتسجيل مادام أن الاشتراك في غرف المحادثات الجماعية مسموحاً به لغيره من الناس[1].

أما بالنسبة لأرقام الأشخاص الطالبين أو المرسلين لرسالة معينة وكذلك أرقام المرسل إليهم، فإن الأمر لا يتعلق بمحتوى الرسالة أو الحديث وبالتالي فإن معرفة تلك الأرقام لا يخالف الحق في الحياة الخاصة ومن ثم فإنه لا يلزم له سبق الحصول على إذن باستخدام برامج معينة، كما أنه يجوز معرفة تلك الأرقام من الجهاز الخادم دون سبق استصدار أمر بذلك. وقد قُضي تطبيقاً لذلك في الولايات المتحدة الأمريكية بأن الفرد ليس له حق في التوقع المعقول لحرمة حياته الخاصة فيما يتعلق بتلك البيانات في قضية Smith v. Maryland[2].

– مدى التماثل بين المحادثات الإلكترونية والمكالمات الهاتفية:

ثمة أوجه للتقارب بين المحادثات الإلكترونية والمكالمات الهاتفية؛ من ذلك ما يلي:1– يعتمد كل منهما على خط تليفوني، 2– يتم الاتصال في كل منهما مباشرة ودون الحاجة إلى وسيط بينهما وذلك على خلاف الوضع بالنسبة للمراسلات البريدية، 3– يحدث تبادل للمحادثات الإلكترونية والمكالمات الهاتفية دون فاصل زمني وهذا على خلاف الرسائل البريدية.

ويتجه الفقه – في غياب النصوص الصريحة أو الأحكام القضائية – إلى إعمال القواعد المتعلقة بالاختصاص في موضوع تفتيش وضبط ومراقبة الاتصالات الهاتفية لكي تسري في مجال الاتصالات الإلكترونية.

وقد تضمنت المادة (2510) من القانون الأمريكي تعريفاً للاتصالات السلكية، حيث تتطلب وجود صوت إنسان كي نكون بصدد اتصال سلكي .وإذا لم تحتوِ الاتصالات على صوت إنساني حقيقي فإنها تخرج عن نطاق الاتصالات السلكية.

(1) United States v . Charbonneau (1997) : Amitai Etzioni , op. cit., p . 271

(2) United States v. Maryland 442 U.S. 735 (1979) , United States Department of Justice , ibid , p. 78 .

ولقد أكدت هذا المعنى المحاكم الأمريكية في العديد من أحكامها[1]. كما تتطلب المادة السابقة بخصوص الاتصال السلكي أن يتم هذا الاتصال أو يمر بأكمله أو في جزء منه خلال سلك أو كابل. ويثار التساؤل عن اعتبار التليفون الهوائي من قبيل الاتصالات السلكية أم لا؟ والرد هنا هو بالإيجاب حيث يعتبر التليفون الهوائي من قبيل الاتصالات السلكية، والسبب في ذلك يرجع إلى أنه في لحظة من لحظات الاتصال تمر المكالمة بمرحلة سلكية تتمثل في محطة السنترال. وأخيراً فإنه يجب القول بأنه إذا وجد السلك داخل جهاز التليفون عند حدوث الإرسال أو الاستقبال للاتصال فإن ذلك لا يكفي لاعتبار الاتصال هنا اتصالاً سلكياً.

غير أن الأمر قد تطور في القانون الأمريكي في اتجاه حماية المحادثات الإلكترونية بحيث أصبح هناك تماثل بين هذا النوع من المحادثات وبين المحادثات الهاتفية: فقد تم التوسع في مفهوم المحادثات محل الحماية ضد الاعتراض والتنصت منذ سنة 1986 بمقتضى قانون حماية الحياة الخاصة (ECPA) والذي عدل القسم الثالث (Title 111 18 U.S.C. 2701–2703. ECPA) من هذا القانون بحيث يسري على البريد الإلكتروني، وعلى الاتصالات بين كمبيوتر وكمبيوتر بوجه عام[2].

ونرى أن المشرِّع يتعين عليه أن يتدخل لسن قوانين لتنظيم الوضع القانوني للمحادثات الإلكترونية ولا يتركها لاجتهاد المحاكم لمعرفة ما إذا كان الوضع القانوني لهذه المحادثات تسري عليه القواعد الخاصة بالاتصالات السلكية. ويرجع ذلك إلى الطبيعة الخاصة للمراسلات الإلكترونية والتي تأخذ بعض الجوانب من المراسلات البريدية على ما سبق بيانه (وخاصة من وجود صندوق بريد خاص ووجود الكتابة). وتضم جوانب أخرى من المحادثات التليفونية حيث يستخدم الخط التليفوني في تبادلها.

(1) United States v. Torres , 751 F.2d 875 , 885-86 (7th Cir. 1984); See S.Rep.No. 99-541.at12 (1986) reprinted in 1986 U.S.C.C.A.N. 3555 ; United States Department of Justice , ibid , p. 78 .
(2) www.cs.ou.edu/disclaimer/disclaimer2.htm . (2004)

– التمييز بين مراقبة وتسجيل المحادثات الإلكترونية وقواعد التفتيش المعتادة:

على الرغم من أن الاتصالات التليفونية تتم في الوقت الحالي عن طريق أجهزة الكمبيوتر في السنترالات المختلفة، فإن هناك ما يميز تسجيل المحادثات التليفونية عن تسجيل المحادثات الإلكترونية أو تفتيش الكمبيوتر ذاته، وعلى الرغم من أن أجهزة الكمبيوتر تعمل على خط تليفوني عندما تكون متصلة بالإنترنت، فإن تسجيل المحادثات التليفونية يخضع لبعض القواعد المختلفة عن قواعد تفتيش المساكن. من ذلك أنه لا يتم إخطار أو حضور صاحب الشأن في أثناء تسجيل المكالمات الهاتفية، بينما يلزم ذلك في حالة تفتيش المساكن (مادة 92 إجراءات مصري).

ومما يميز تسجيل المحادثات التليفونية عن تفتيش أجهزة الكمبيوتر أنه يمكن تتبع المعلومات وصولا إلى الأجهزة الخادمة حيث يتم تخزين تلك المعلومات.

كما أن اعتراض المحادثات الإلكترونية، أو تفتيش أجهزة الكمبيوتر يمكن أن يتم عن بعد وهذا يختلف عن تسجيل المحادثات التليفونية في الوضع المعتاد.

وعلى الرغم من أن أجهزة الكمبيوتر تعمل على خط تليفوني، فإن تفتيشها لا يخضع لنفس النظام الذي يحكم تسجيل المحادثات التليفونية[1].

ويلاحظ أنه بالنسبة لتسجيل المحادثات التليفونية والمراسلات البريدية فإن النصوص التي تجيز ذلك لم تواجه بشكل صريح تسجيل المحادثات والمراسلات التي تتم عن طريق الإنترنت: فهل تخضع هذه المحادثات لنظام المحادثات التليفونية مع أنها لا تتم بطريق التليفون مباشرة ومع أنها أحياناً ليست محادثات ناطقة بل مراسلات مكتوبة؟ أم هل يخضع البريد الإلكتروني لنظام المراسلات المكتوبة (الخطابات) مع أنها وإن كانت مكتوبة ليست على غرار المراسلات البريدية التي يقصدها النص الخاص باعتراض المراسلات البريدية؟ من الواضح أن هذه التساؤلات تثير مشكلة مبدأ الشرعية الإجرائية[2]، أي في مجال الإجراءات الجنائية، ولذا فإنه من الصواب استحداث نصوص خاصة بمراقبة المراسلات الإلكترونية عبر الإنترنت.

(1) Pascal VERGUCHT , op. cit., p. 383.

(2) انظر لمزيد من التفصيل: أحمد فتحي سرور، الشرعية الدستورية وحقوق الإنسان في الإجراءات الجنائية، دار النهضة العربية، 1995، ص 121 وما يليها؛ لنفس المؤلف: القانون الجنائي الدستوري، دار الشروق، 2002، ص 530 .

لذا فإن بعض التشريعات قد عدلت نصوصها لكي تأخذ في الاعتبار هذا التطور التقني، فقد أصبح القانون الصادر في شأن الاتصالات الإلكترونية سنة 1986 في الولايات المتحدة الأمريكية ينظم التنصت على المحادثات الإلكترونية بوصفها: «كل انتقال، بشكل كلي أو جزئي، للإشارات أو الكتابات أو الصور أو الأصوات أو المعطيات أو المعلومات أيّاً كان نوعها، عن طريق الكابل أو الراديو أو النظام الكهرومغناطيسي أو التصوير الكهربائي أو الصور المرئية». وبناءً على هذا النص فقد تم اعتراض وتسجيل المراسلات التي تجري عن طريق الإنترنت في الولايات المتحدة الأمريكية.

ويُلاحظ أنه إذا تعلق الأمر بترددات أو ذبذبات تصدر على مسافة قريبة من الجهاز ويمكن التقاطها وتسجيلها، فإنها تأخذ حكم تسجيل المحادثات الإلكترونية الخاصة. وإلى هذا المعنى اتجهت اتفاقية Málaga–Torremolinos لسنة 1973[1].

– جواز التفتيش لضبط المعلومات:

أصبحت التشريعات الحديثة تجيز تفتيش الأجهزة الإلكترونية لضبط المعلومات المتواجدة فيها والتي تفيد في كشف الحقيقة. من ذلك أن المجلس الأوروبي أكد في التوصية رقم (R. 95 13) على أنه يتعين مراجعة القوانين في مجال الإجراءات الجنائية للسماح باعتراض الرسائل الإلكترونية، وتجميع للبيانات المتعلقة بتداول المعلومات في حالة التحقيقات المتعلقة بجريمة من الجرائم الخطيرة الماسة بسرية أو سلامة الاتصالات أو أنظمة الكمبيوتر.

وتفرض الطبيعة المعنوية للمعلومات قواعد خاصة للتفتيش لكي تتمشى مع تلك الطبيعة، نظرا لأن قواعد التفتيش التقليدية قد صُممت لكي يتم ضبط الأشياء المادية، لذا يتعين الأخذ بعين الاعتبار تلك الطبيعة.

ومراعاة لذلك تنص التوصية رقم (R. 95– 13) الصادرة من المجلس الأوروبي على أنه: «بالنظر إلى تدفق وتطور تقنية المعلومات والاتصالات، يتعين أن تتمشى القوانين المتعلقة بمراقبة الاتصالات في إطار التحقيقات الجنائية كاعتراض الاتصالات

(1) Pascal VERGUCHT , op. cit., p. 388.

مع هذه المعطيات وأن تتم مراجعتها كلما كان ذلك ضرورياً لضمان فعاليتها في التطبيق». كما تتضمن التوصية أنه يتعين أن يسمح القانون لسلطات التحقيق والاستدلال أن يتزودوا بالوسائل الفنية الحديثة التي تمكّنهم من تجميع المعلومات الضرورية لتحرياتهم وتحقيقاتهم.

وقد حرصت التوصية الأوروبية السابق ذكرها على تأكيد أنه عندما يتم تجميع المعلومات في أثناء التحريات والتحقيقات وبصفة خاصة عندما يتم اعتراض الرسائل الإلكترونية، فإن المعلومات التي هي محل للحماية القانونية والتي تتم معالجتها بطريق الكمبيوتر يجب أن يتم التحفظ عليها وصيانتها بطريقة مناسبة. فمما لا شك فيه أن ضبط المعلومات يختلف عن ضبط الأشياء المادية كالمخدرات مثلاً، هذا أمر يقتضي وسائل تقنية خاصة بالمعلومات للحفاظ عليها عند ضبطها من كل عبث يمكن أن يلحق بها.

كما صرحت الاتفاقية الأوروبية في شأن جرائم السيبر بحق الدول الأعضاء في تفتيش أجهزة الكمبيوتر في إطار الإجراءات الجنائية. فتنص المادة (19من القسم الرابع) على أن كل دولة طرف من حقها أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة أن تقوم بتفتيش أو الدخول إلى:

– نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة به.

– الوسائط التي يتم تخزين معلومات الكمبيوتر بها ما دامت مخزنة في إقليمها.

– اختلاف تفتيش وضبط المعلومات المخزنة عن الاتصالات المباشرة:

يختلف تفتيش وضبط المعلومات المخزنة عن اعتراض الاتصالات المباشرة أي أثناء حدوث تلك الاتصالات. هذه الأخيرة يتم اعتراضها ووضعها تحت التنصت وتسجيلها، الأمر الذي لا يتوافر في حالة المعلومات التي تم تخزينها بالفعل. فإذا كان تسجيل المحادثات في أثناء حدوثها يحتاج إلى إجراءات أكثر صرامة، ويتمثل في صدور إذن من القاضي الجزئي بناء على طلب من النيابة العامة وفقاً للقوانين المقارنة (منها القانون المصري: مادة (95) إجراءات جنائية)، فإن التفتيش بغرض ضبط المعلومات المخزنة، بما فيها المحادثات التي انتهت والتي يستمر تخزينها في «الجهاز الخادم»،

يتميز بقواعد أقل صرامة تتمثل في الاكتفاء بإذن من النيابة العامة. ولا يفوتنا أن ننبه إلى أن تفتيش جهاز الخادم يعني تفتيش أماكن العمل، هذا النوع من التفتيش ليس تفتيشا يتعلق بالمنازل والتي قضت المحكمة الدستورية المصرية بتاريخ 2 يونيو سنة 1984[1] بالنسبة له بأنه لا يكفي قيام حالة التلبس لجواز ذلك التفتيش[2]. وبناءً عليه فإن تفتيش جهاز الخادم – مع أنه يقتضي الدخول أي تفتيش المكان – إلاّ أنه تفتيش لأماكن العمل يجوز – في رأينا – قانوناً بناء على توافر حالة التلبس.

وقد كرست التوصية رقم (13 – 95 .R) الصادرة من المجلس الأوروبي هذا المعنى بنصها على أنه يجب إقامة التمييز بين تفتيش المعلومات المخزنة وضبطها وبين اعتراض تلك المعلومات عند انتقالها (ملحق رقم 1 من التوصية السابقة). كما نصت التوصية رقم (2) على أنه: «يجب أن تسمح قوانين الإجراءات الجنائية لسلطات التحقيق أن تقوم بتفتيش أنظمة الكمبيوتر وأن تضبط المعلومات وفقاً لشروط معينة كما هو الحال بالنسبة للسلطات التقليدية في شأن التفتيش والضبط. ويتعين أن يتم إخطار الشخص المسؤول عن النظام بنوع المعلومات التي تم ضبطها، كما يجب أن يُتاح له من وسائل الطعن القضائي ما يتاح في غير ذلك من حالات التفتيش والضبط «. كما عُنيت التوصية السابقة بالنص على أنه: «تُعتبر البيانات المعالجة آلياً بالكمبيوتر في حكم المستندات التقليدية، ويتعين أن يسري على تفتيشها وضبطها ما يسري على غيرها من تفتيش وضبط تلك المستندات».

– التزام مزودي الخدمات بالتعاون مع المحقق:

تتجه التشريعات المقارنة إلى إلزام مزودي الخدمات بالتعاون مع المحقق، بالإضافة إلى التزامهم بالتعاون مع رجال الضبط القضائي. في ذلك تنص التوصية رقم 95/ 13 الصادرة عن المجلس الأوروبي على أنه: «.... –12 يتعين أن يُفرض التزام على مزودي الخدمات الذين يقدمون خدمات الاتصالات اللاسلكية للجمهور،

(1) حكم المحكمة الدستورية العليا في 2 يونيو سنة 1984، القضية رقم 105 لسنة 4 ق دستورية، وبناء عليه قضت محكمة النقض بأن «المادة (44) من الدستور لم تستثن حالة التلبس من ضرورة صدور أمر قضائي مسبب ممن له سلطة التحقيق أو من القاضي المختص بتفتيش المسكن سواء أقام به الآمر بنفسه أم أذن لمأمور الضبط القضائي بإجرائه».
(2) عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، المرجع السابق، ص 274.

إما من خلال شبكة عامة، أو من خلال شبكة خاصة، أن يقدموا لسلطة التحقيق المعلومات اللازمة لتحديد هوية مستعمل الشبكة».

وقد فرضت الاتفاقية الأوروبية لجرائم السيبر التزاماً على مزودي الخدمات بالتعاون مع جهات التحقيق، فتنص المادة (20) من القسم الخامس على أن الدول الأعضاء من حقها أن تلزم مزود الخدمات – في حدود ما تسمح به وسائله الفنية المتاحة – أن يقوم بـ :

– تجميع أو تسجيل البيانات بالوسائل الفنية المناسبة.

– أن يتعاون وأن يساعد السلطة المختصة في تجميع وتسجيل البيانات المتعلقة بحركة التداول في الوقت الحقيقي المتعلقة بالاتصالات التي تجري على إقليمها، والتي تجري بطريق الكمبيوتر.

كما تلزم الاتفاقية مزودي الخدمات أن يحتفظوا بسرية الإجراءات السابقة التي تتخذها السلطة المختصة.

وإذا كانت التشريعات المقارنة تلزم مزود الخدمات بالتعاون مع سلطة التحقيق، فإن هذا التعاون يصبح واجبا في مرحلة المحاكمة، فيجوز للمحكمة أن تصدر أمرا لمزود الخدمات بأن يقدم المعلومات اللازمة لتحديد هوية المشتركين في الاتصالات الإلكترونية أو الذين قاموا بإنشاء موقع معين على الإنترنت وذلك في المواد المدنية والجنائية.

ومن التشريعات التي تسمح للمحكمة بإصدار مثل هذا الأمر القانون الأمريكي الذي يلزم مزودي الخدمات بأن يقدموا ما لديهم من معلومات تخص المشتركين والمتعاملين معهم والتي تنتمي إلى الطائفة الأولى والثانية السابق ذكرها. وتقف سلطة المحكمة عند هذا الحد؛ فلا يجوز لها أن تصدر أمراً يتعلق بمحتوى الملفات نفسها والتي تنتمي إلى الطائفة الثالثة سابقة الذكر.

أما عن الشروط المتطلبة لصدور هذا الأمر، فإنها تتمثل في وجود تحقيق جنائي، وأن يكون هناك ما يدعو إلى الاعتقاد بأن الكشف عن هذه المعلومات لدى مزود

الخدمات يفيد في إظهار الحقيقة. فتنص المادة (18U.S.C.§2703) من قانون الإجراءات الجنائية الأمريكي الفيدرالي على أنه «يجب على رجال الضبط القضائي أن يقدموا معلومات واضحة وكافية على أن محتويات الاتصالات الإلكترونية والسلكية تفيد في الكشف عن الحقيقة في تحقيق جنائي جار».

ويمتد اختصاص المحكمة عند إصدار هذا الأمر إلى خارج دائرة اختصاصها المحلي، بحيث يمكن لها أن تلزم مزود الخدمات الذي يقع مقره في خارج دائرة اختصاصها. ويفترض ذلك بالطبع أن تكون المحكمة مختصة أصلاً بمحاكمة المتهم عن الجريمة[1].

– صعوبات تتعلق بالتعاون الدولي في مجال تحقيق الجرائم الإلكترونية:

يدعو الطابع الدولي لجرائم الكمبيوتر – بسبب وجود شبكة الإنترنت، وكذلك بسبب اتصال أجهزة الكمبيوتر بعضها ببعض عبر حدود الدول – إلى ضرورة التعاون القضائي الجنائي بين الدول، غير أنه توجد صعوبات تحول دون توافر هذا التعاون منها؛ عدم الاهتمام على المستوى الدولي بالكثير من جرائم الكمبيوتر ما عدا جرائم الاستغلال الجنسي للأطفال. كما يحول دون زيادة هذا التعاون انتماء الدول إلى أنظمة قانونية مختلفة؛ فكل دولة لها مفهومها في تحديد أركان الجريمة وفي أنواع العقوبات وفي التحقيق والمحاكمة. يضاف إلى ذلك أن جرائم الكمبيوتر لا تنتمي إلى الجرائم الجسيمة التي تدعو إلى الاهتمام الدولي بها. فالقانون الإنجليزي مثلا لا يعتبر من الجرائم الجسيمة إلا جريمة الدخول وتعديل البيانات (قانون سنة 1990). ومن المعروف أن تسليم المجرمين لا يجوز إلا في الجرائم التي تبلغ درجة معينة من الجسامة[2]. ويرتبط بذلك أن هذه الجرائم لا تمس في غالبيتها قيماً ومصالح ذات صبغة دولية، فالغالبية العظمى من هذه الجرائم – ما عدا الاستغلال الجنسي للأطفال عبر شبكة الإنترنت – لا تجتمع الدول المختلفة على تجريمها. بل إن كثيراً من الدول – مثل مصر ومعظم البلاد العربية – لا تعرف حتى كتابة هذه السطور

(1) United States Department of Justice , ibid , p. 66 .
(2) Pascal VERGUCHT , op. cit., p . 415 .

تجريماً لكثير من جرائم الكمبيوتر. والمعروف أنه حتى يتم تعاون دولي يتعين أن يتوافر تجريم مشترك[1] لفعل معين. ولكن ذلك لم يمنع الدول الأوروبية من وضع اتفاقية أوروبية لتنظيم التعاون الأوربي في مجال العدالة الجنائية بوجه عام الذي يمكن أن تسري على جرائم الكمبيوتر. من ذلك الاتفاقية الأوروبية النافذة في سنة 1993 والتي ضمت ثمانية دول أوروبية. هذه الاتفاقية ترمي إلى تسهيل التحقيقات عبر الحدود بين الدول الأوربية بخصوص الجرائم الخطيرة بوجه عام مثل تهريب الأسلحة والمخدرات والاتجار بالأطفال والرقيق الأبيض والإرهاب، ويمكن أن تسري أحكام هذه الاتفاقية على جرائم الكمبيوتر. وتسمح أحكام هذه الاتفاقية بالمساعدة القضائية[2] بين تلك الدول سواء في مجال تبادل المعلومات أو التحقيق أو المحاكمة أو تنفيذ الأحكام ومنها حكم المصادرة[3].

والحقيقة أنه نظراً لطابع الجرائم المعلوماتية التي تتخطى حدود الدول أصبح من الضروري عقد اتفاقيات دولية للاعتراف بالأدلة التي يتم ضبطها في دولة حتى يكون لها قوة في الإثبات أمام قضاء الدولة الأخرى[4].

(1) double incrimination
(2) entraide judiciaire
(3) Pascal VERGUCHT , op. cit., p . 413 .
(4) Pascal VERGUCHT , op. cit., p . 430 .

المطلب الثاني

تفتيش النظام بدون إذن

– القاعـدة: عدم جواز تفتيش جهاز الكمبيوتر دون إذن

– إذا قام مأمور الضبط القضائي بتفتيش جهاز الكمبيوتر دون أن يحصل مسبقاً على إذن من الجهة المختصة، فإن ما قام به من تفتيش يكون باطلاً، ولا يترتب عليه أي أثر. ولكن هذا الأصل يرد عليه بعض الاستثناءات من أهمها حالة التلبس.

فلا يجوز تفتيش الكمبيوتر – بحسب الأصل – إلاّ بإذن وفقاً للعديد من القوانين، ومنها القانون الفرنسي وكذلك القانون الأمريكي. ويستند ذلك إلى أن تفتيش الكمبيوتر يأخذ حكم تفتيش الشخص في القانون المصري والقانون الفرنسي، ما دام أن الجهاز ليس في منزل المتهم. أما القانون الأمريكي، فإن عدم جواز هذا النوع من التفتيش يستند إلى الدستور الأمريكي في التعديل الرابع منه الذي ينص على: «حق الأفراد في حرمتهم الشخصية وحرمة منازلهم وأوراقهم وأموالهم المنقولة في مواجهة التفتيش غير المعقول والضبط يتعين احترامه ولا يجوز أن يصدر إذن بالتفتيش إلاّ بناءً على أسباب معقولة يؤيدها حلف لليمين، أو بناءً على تحريات جدية ويُحدد في هذا الإذن المكان محل التفتيش والأشخاص وكذلك الأشياء المطلوب ضبطها».

ومقتضى ما تقدم أن الفرد له حرمة الحياة الخاصة بحيث لا يجوز التعدي عليها باتخاذ إجراء يخالف التوقع المعقول للحياة الخاصة. هذا الإجراء الأخير يعتبر تفتيشاً ومن حق الفرد الحماية في مواجهته وذلك بضرورة استصدار إذن قضائي بالتفتيش. وقد صرح التعديل الرابع للدستور عن ذلك بقوله: «ضد التفتيش والضبط غير المعقولين»، وقد فسرت المحاكم الأمريكية معيار الحماية الدستورية للحق في الحياة الخاصة بأن الإجراء يخالف الدستور إذا كان يخالف معيار «التوقع المعقول للحق في الخصوصية»[1].

(1) " reasonable expectation of privacy "; Illinois v. Andreas , 463 U.S. 765 , 771 (1983) ; Illinois v. Rodriguez , 497 U.S. 177 , 185 (1990) cited by : United States Department of Justice , Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations , www.cybercrime.gov/s&smanual2002.htm , op. cit., p. 8 .

وإذا أعملنا المبدأ السابق في مجال جرائم الكمبيوتر فإنه من الواجب أن نعتبر الكمبيوتر من قبيل «الصندوق المغلق»؛ وبناءً عليه فإن المعلومات التي تتواجد داخل جهاز الكمبيوتر تعتبر أموالاً منقولة لحائز الكمبيوتر، ويُقبل منه أن يتمسك بالتوقع المعقول للحياة الخاصة. وقد انحاز القضاء الأمريكي إلى هذا الرأي في العديد من أحكامه[1].

الاستثناء: جواز تفتيش جهاز الكمبيوتر دون إذن

تقضي القواعد العامة في التفتيش بأنه إذا توافرت حالة من الحالات التي يجوز فيها التفتيش دون إذن، فإن التفتيش يكون على الرغم من ذلك صحيحاً. من هذه الاستثناءات في مجال المعلومات في كثير من التشريعات وبصفة خاصة القانون الأمريكي ما يلي:

1- التفتيش لا يخالف التوقع المعقول للحياة الخاصة.

2- حالة الرضاء.

3- التفتيش على أثر الضبط الصحيح.

4- حالة الضرورة.

5- حالة التلبس عند وجود الكمبيوتر في خارج المسكن.

7- التفتيش في حالة جرد الأشياء المضبوطة.

8- تفتيش الجمارك.

9- تفتيش شبكة الإنترنت .

حرمة التعاملات الإلكترونية واعتبارات مكافحة الإرهاب:

تأثر حرمة الحياة الخاصة باعتبارات مكافحة الإرهاب:

(1) see United States v. Barth , 26 F. Supp . 2d 929 , 936-37 (W. D .Tex .1998) ; United States v. Reyes , 922 F. Supp . 818 , 832-33 (S.D.N.Y. 1996); United States v. Lynch , 908 F. Supp . 284 , 287 (D.V.I. 1995) ; United States v. Chan, 830 F.Supp .531 , 535 (N.D.Cal . 1993) ; United States v. Blas , 1990 WL 265179 , at 21 (E. D. Wis .Dec. 4, 1990) , www.cybercrime.gov/s&smanual2002.htm , ibid , p. 9 .

كان لهجمات الإرهابيين في السنوات الأخيرة سواء في الولايات المتحدة الأمريكية، أو في البلاد الأوروبية الأثر الواضح في إدخال نصوص تخالف ما تقرره القوانين من ضمانات إجرائية لاحترام الحق في حرمة الحياة الخاصة للمشتبه في علاقتهم بالإرهاب والإرهابيين على وجه الخصوص.

وقد انعكس ذلك على السياسة الجنائية التي اتبعها المشرع الأمريكي في مكافحة الإرهاب بعد هجمات الحادي عشر من سبتمبر وذلك بإصداره للقانون الوطني Patriot Act الذي تبنى فلسفة التشدد في معاملة المشبته فيهم بعلاقتهم بالإرهابيين. من ملامح التشدد في هذا القانون: التوسع في مفهوم الإرهاب، تجريم دعم الإرهاب، تشديد العقوبات المقررة للجرائم الإرهابية، زيادة سلطات موظفي وزارة العدل في مراقبة الدخول إلى البلاد وتقوية سلطتهم في التفتيش الإداري سواء تفتيس الأشخاص أو التفتيش الإلكتروني للأشخاص المشتبه فيهم بالإرهاب وإلغاء القيود التي تم وضعها على التعاون بين القائمين بالتحقيقات الجنائية وجهاز المخابرات العامة. وقد تم تعديل ذلك القانون عدة مرات في نفس الاتجاه في سنة 2002 وسنة 2004 وسنة 2005[1].

التوسع في سلطة التفتيش في قضايا الإرهاب:

أصبحت عديد من التشريعات تسمح بالتوسع في حالات التفتيش عندما يتعلق الأمر بالإرهاب ؛ فلم يعد القانون الأمريكي لسنة 2001 يشترط الدلائل الكافية لتفتيش المتهم في جرائم الإرهاب. فلا يلزم لرجل الشرطة سبق توافر إذن بالتفتيش أو حالة تلبس أو حتى مجرد الدلائل الكافية لكي يقوم بتفتيش من يشتبه في أنه يحمل في حقيبته أو في ملابسه أو سيارته ما يتعلق بجرائم الإرهاب (الفصل 215 من القانون الوطني). وقد وسع القانون الإنجليزي سلطات الشرطة في تفيتش المتهم بدون اشتراط الدلائل الكافية، مما يشكل افتئاتاً على الحياة الخاصة. هذا الافتئات يمكن أن يوجه إلى جنسيات معينة (عربية أو مسلمة) أكثر من غيرها.

(1) Julien Cantegreil ,La doctrine du « combattant ennemi illégal »Revue de science criminelle 2010 p. 81

صحيح أن ظاهرة الإرهاب وخطورته أمر حديث نسبيا بالنسبة للولايات المتحدة، غير أن بلاداً أخرى قد سبق أن ضربها الإرهاب بسبب الحركات الانفصالية مثل انجلترا (أيرلندا الشمالية) وأسبانيا (بلاد الباسك) منذ فترة السبعينات). فتنص المادة (16) من التشريع الأسباني لسنة 1984 لقوات أمن الدولة تفتيش الأماكن التي يقيم فيها المشتبه بتورطهم بجرائم إرهابية. كما تجيز لهم مصادرة الأدوات والأمتعة بدون سبق الحصول على إذن أو تكليف قضائي، ويقوم وزير الداخلية، أو مدير أمن الدولة عند الضرورة بإخطار القاضي المختص بما تم إجراؤه من تفتيش[1].

ومن ناحية طريقة تنفيذ التفتيش، يسمح القانون الوطني الأمريكي لمأمور الضبط القضائي أن يقوم بتنفيذ إذن التفتيش للمسكن ومكاتب العمل دون إخطار سابق (sneek and peer) على عكس ما يتطلبه التعديل الرابع من الدستور الأمريكي. وبذلك فإن مأموري الضبط القضائي يصبح من حقهم في التحقيقات الخاصة بالإرهاب الدخول إلى المنازل وأماكن العمل دون سابق إنذار والتقاط الصور وضبط الأشياء والاتصالات الإلكترونية دون إخطار صاحب المكان[2]. فإذا كان قانون الإجراءات الجنائية المصري (مادة 92) يستلزم وجود صاحب المسكن أو شاهدين عند تفتيشه فإن هذا الإجراء لا يترتب على مخالفته البطلان[3][4]. ويعرف القانون الأمريكي قاعدة اطرق الباب وأعلن عن نفسك knoch and announce rule عند تفتيش المسكن، تلك القاعدة تجد أساسها في السوابق القضائية common law باستثناء حالة الضرورة، الأمر الذي لا يعرفه القانون المصري[5].

(1) راجع: فتيحة بن ناصر، الحد من الضمانات الإجرائية للمتهمين بالجرائم الإرهابية، دار الجامعة الجديدة بالإسكندرية، 2011، ص89.

(2) American Civil Liberties Union , Surveillance Under the Patriot Act , http://www.aclu.org/national-security/surveillance-under-patriot-act

(3) نقض 25 مايو سنة 1959، مجموعة أحكام محكمة النقض س 10 ص 568 رقم 126؛ 30 ديسمبر 1952، س 4 ص 314 رقم 122؛ 14 نوفمبر 1960 س 11 ص 782 رقم 150؛ أول ديسمبر 1958 س 9 ص 1006 رقم244؛ 8 يونيو 1980 س 31 ص 723 رقم 140 ؛ 17 مارس 1988 س 39 ص 435 رقم 63.

(4) عوض محمد عوض، التفتيش في ضوء أحكام النقض، دراسة نقدية، مطابع السعدني، سنة 2007، ص279.

(5) Wilson v. Arkansas , 514 US 927 (1995), www.law.cornel.ed/wex/knoch-and-announce rule.

– مراقبة الاتصالات الهاتفية والإلكترونية في جرائم الإرهاب:

من مظاهر المساس بحرمة الحياة الخاصة في مكافحة الإرهاب ما تضمنه القانون الوطني Patriot Act من نصوص تسمح لهيئة الأمن الوطني National Security Agency أن تلتقط الاتصالات الهاتفية التي تجري بين طرفين يتورط أحدهما في جريمة إرهابية استناداً إلى توافر أسباب مقبولة تقدر الحكومة أنها تكفي لكي تقوم بهذا الالتقاط. ويسمح الفصل رقم (218) من القانون الوطني الأمريكي لهيئة الاستخبارات أن تقوم بالتنصت وتسجيل جميع المحادثات والاتصالات السلكية واللاسلكية.

فيسمح قانون الاستخبارات الأجنبية FISA: Foreign Intelligence Surveillance Act لسنة 1978 المعدل لسلطات التحقيق العادية بالتنصت والتسجيل للمحادثات، يكفي في ذلك أن يثبت رجال الاستخبارات أن المقصود بجمع المعلومات عنه هو عميل لجهة أجنبية. كما أنه يكفي أن تثبت سلطة التحقيق أن غرضاً من أغراض ذلك التنصت والتسجيل هو تجميع معلومات عن جهة أجنبية، وليس شرطاً أن يكون الغرض الرئيسي هو ذلك التجميع لتلك المعلومات. ومن ثَمّ فإن التحقيقات التي تجريها سلطات التحقيق أصبحت تقترب من التحقيقات التي تجريها هيئة الاستخبارات في الشروط والمدى[1].

وكان قانون الاستخبارات الأجنبية FISA قد أوجد محكمة تجتمع في سرية كي تعطي الإذن الخاص بالمراقبة والتسجيل للمحادثات السلكية واللاسلكية والإلكترونية، إذا تعلق الأمر بجهة أجنبية ولو كانت تتصل بعميل داخل الولايات المتحدة. ومع ذلك فإن القانون ذاته يسمح لرئيس الدولة من خلال المحامي العام وذلك دون إذن من المحكمة الخاصة التي أنشئت لتعطي ذلك الإذن (الفصل 50 U.S.C.$1801(a)(1)،(2)) . وقد تم تعديل قانون FISA كي يسمح بالمراقبة والتنصت على محادثات الإرهابي الفرد (كلب الولف الوحيد Lone wolf) دون اشتراط أن يتعلق الأمر بمنظمة إرهابية أجنبية أو جهة إرهابية أجنبية[2].

(1) http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act
(2) http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act

وقد أثير أمام القضاء الأمريكي مدى دستورية قانون FISA في قضية United States v. Duggan 743 F.2d 59 (2nd Cir.، 1984)، وقُضي بدستورية ذلك القانون الذي يسمح بالمراقبة والتنصت على الأشخاص الأجانب في جرائم الإرهاب دون الوطنيين، على سند من أن ذلك لا يشكل تمييزاً في المعاملة بين الوطني وغير الوطني، لأن هناك مصلحة ملحة تتعلق بالأمن القومي عند مكافحة الإرهاب.

ومن مظاهر الإخلال بحرمة الحياة الخاصة ما أجازه الفصل (206) من القانون الوطني الأمريكيPatriot Act الذي يسمح بوضع الاتصالات الهاتفية تحت المراقبة دون شرط تحديد الهواتف محل المراقبة (roving wiretap). فمن المبادئ المستقرة في القانون المقارن أنه يلزم تحديد الهاتف محل المراقبة عند صدور الإذن بمراقبة متهم معين وتسجيل محادثاته. ويؤكد ذلك التعديل الرابع من الدستور الأمريكي[1]. وقد تضمن القانون الوطني لمكافحة الإرهاب في أمريكا نصا يسمح بوضع الاتصالات الهاتفية لمتهم معين من أي جهاز يستخدمه دون تحديد رقم معين لوضعه تحت المراقبة.

يضاف إلى ما سبق من المساس بالحياة الخاصة ما تضمنه الفصل (6001) من قانون الوقاية من الإرهاب لسنة 2004 من نص أخر يسمح بمراقبة الأشخاص غير الأمريكين المقيمين في الولايات المتحدة وتسجيل محادثاتهم على الرغم من أنهم لا يرتبطون بمنظمات أجنبية. ويعطى الإذن بذلك بشكل سري الأمر الذي يفتح الباب للعسف بالحريات الفردية. وقد جاء هذا تعزيزاً لما تضمنه القانون الوطني لمكافحة الإرهاب من نصا يسمح بـ(خطابات الأمن القومي NSLs : National Security Letters). هذه الخطابات تعتبر إذناً يسمح بمراقبة التعاملات المالية والاطلاع على سجلات البنوك إذا تعلق الأمر بتحقيق في جرائم الإرهاب حتى ولو كانت التعاملات تخص شخصاً غير متهم بجرائم الإرهاب. وقد صدر حتى الآن عشرات الآلاف من

(1) Amendment IV: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. http://www.scn.org/ccapa/pa-vs-const.html

الخطابات في أمريكا كل عام لجمع المعلومات التي تتعلق بالأشخاص[1].

وقد أدخل القانون الإيطالى تعديلات إجرائية بغرض تقوية سلطات جمع الاستدلالات بشأن الإرهاب. وقد سمح هذا القانون بتسجيل المكالمات التليفونية بترخيص من المدعي العام لدى محكمة الاستئناف في المنطقة التي وضع فيها الشخص تحت المراقبة. ولا شك في أن ذلك يتعارض مع المبادئ الدستورية وخاصة أن الشروط التي تبيح تسجيل المكالمات التليفونية ليست محددة بشكل دقيق[2].

ولا يختلف الأمر بالنسبة للقانون الألماني الصادر في سنة 2003 والذي يخوِّل الأجهزة الأمنية صلاحية مراقبة الأحاديث التليفونية وتسجيلها للمشتبه بارتكابهم جرائم إرهابية، وذلك دون إذن قضائي مسبق. كما يجيز لهم سلطة الاطلاع على المراسلات وأرصدة البنوك بالنسبة للمشتبه بارتكابهم أعمال إرهابية[3].

– السماح بتبادل المعلومات بين أجهزة الدولة المختلفة بخصوص جرائم الإرهاب:

يسمح الفصل رقم (203/ أ و ب) من التقنين الأمريكي لسلطات التحقيق الاطلاع على المعلومات التي هي بحوزة وكالة الاستخبارات (CIA). فقد ثبت أن هيئة الاستخبارات كان لديها معلومات عن إرهابيين معيينين بأنهم موجودون في الولايات المتحدة قبيل هجمات الحادي عشر من سبتمبر، بينما لم يكن لدى مكتب البحث الجنائي الفيدرالي (FBI) تلك المعلومات. وجواز هذا الاطلاع محل للانتقاد، ذلك أنه يفتح الباب لإنشاء قاعدة بيانات تخص أشخاصا عديدين منهم أبرياء ليسوا متورطين في جرائم الإرهاب.

وبشكل تبادلي مع ما سبق يجيز الفصل (203/ أ و ب) اطلاع هيئة الاستخبارات CIA على ملفات التحقيق الجنائي. ويؤدي ذلك إلى إفشاء سرية التحقيقات وأسرار المتهمين. صحيح أن ذلك يزيد من قدرة الهيئة على تتبع المتهمين بارتكاب جرائم

(1) American Civil Liberties Union, Reform the Patriot Act, http://www.aclu.org/reform-patriot-act.

(2) مشار إليه في: فتحي سرور، المرجع السابق، ص 194.

(3) راجع: فتيحة بن ناصر، الحد من الضمانات الإجرائية للمتهمين بالجرائم الإرهابية، المرجع السابق، ص89.

إرهابية ولكن ذلك يتحقق على حساب حرمة الحياة الخاصة لهؤلاء المتهمين. هذه الحرمة يبدو أن المشرع الأمريكي أصبح يوليها أهمية أقل في ميزان أولوياته عند مكافحة الإرهاب، خاصة وأن التحقيقات الجنائية لا تخص أسرار المتهمين بالجرائم الإرهابية فحسب، ولكنها تحتوي على أسرار أشخاص عاديين وردت أسماؤهم في تلك التحقيقات. وقد حدا ذلك بالبعض إلى اعتبار أن ذلك يشكل افتئاتا واضحا على الحق في حرمة الحياة الخاصة[1].

يضاف إلى ما سبق أن الفصل رقم (215) من هذا القانون يسمح لهيئة الاستخبارات عندما تجري تحقيقاتها بالاطلاع على الملفات الخاصة بالشركات وجهات العمل المختلفة[2].

ويسمح الفصل رقم (215) من القانون الوطني لسلطات التحقيق الاطلاع على جميع الملفات والأوراق والمستندات التي تخص الجهات العامة والخاصة بل والمكتبات العامة، وذلك في التحقيقات المتعلقة بجرائم الإرهاب. وقد كان ذلك محلاً للانتقاد لأنه يشكل تغولا من السلطات العامة في مجال الحياة الخاصة للأفراد حيث يمكنهم هذا الحق من تجميع معلومات عن كل الأفراد.

وقد كان الفصل رقم (18 U.S.C. $ 2709) من قانون الإجراءات الأمريكي يجيز إصدار خطابات الأمن القومي (NSLs) والتي بمقتضاها لمكتب المباحث الفيدرالي أن يفرض على مزودي خدمات الهواتف والإنترنت أن تزودوها بملفات بعض المتعاملين معهم أي عملائهم. طعن أحد مزودي خدمات الإنترنت بعدم دستورية هذه الأوامر على سند من أنها تخالف التعديل الأول والرابع والخامس من الدستور الأمريكي. فتلك الأوامر – وفقا لرافعي الدعوى – تفرض عليهم إفشاء أسرار العملاء لديهم وتلزمهم بهذا الالتزام دون تمكينهم من وسائل الطعن القانونية عليها. قضت المحكمة العليا للولايات المتحدة الأمريكية – في قضية Doe v. Ashcroft سنة 2004 بأن تلك الخطابات تخالف الدستور الأمريكي في تعديله الرابع الذي يضمن

(1) www.npr.org/news/specials/patriotact/patriotactprovisions.html
(2) www.npr.org/news/specials/patriotact/patriotactprovisions.html

الحق في دعوى عادلة، ذلك أنه لا يسمح بالطعن أمام القضاء في تلك الأوامر الصادرة إلى مزودي الخدمة[1].

ونظرا لأهمية الاتصالات في مجال الإرهاب وخاصة الاتصالات الدولية، فإن قانون حرية الاتصالات الفرنسي la liberté de communication الصادر في 30 سبتمبر سنة 1986، في المادة (43 . 7) يلزم مزودي الخدمات، بالحفاظ على بيانات الاتصالات الإلكترونية، ومحتوى الاتصال نفسه لمدة لاتزيد عن سنة. كما أنه يجيز الكشف عن أطراف تلك الاتصالات بناءً على أمر بذلك من رجال الضبط القضائي، ولكن بعد الحصول على إذن بذلك من النيابة العامة، وبعد استئذان قاضي الحريات والحبس Le juge des libertés et de detention.

وقد أكد هذا الالتزام القانون الفرنسي بمقتضى القانون رقم (719) لسنة 2000 في شأن حرية الاتصالات، حيث ألزم مزودي خدمات الدخول fournisseurs d'accés والمسكنين fournisseurs d'hébergement بالمحافظة على بيانات مستعملي هذه الخدمات، تمهيداً لطلب السلطات القضائية منهم تلك البيانات، لكشف الحقيقة بصدد جريمة ارتكبت بالفعل.

وقد ألزم قانون الأمن اليومي الفرنسي la sécurité quotidienne الصادر في 15 نوفمبر 2001، مزودي الخدمات بتسجيل البيانات المتعلقة بالاتصالات لمدة سنة، والحفاظ عليها. ذلك أنها قد تساعد في كشف الحقيقة بصدد تقرير أو متابعة تحقيقات جنائية، كما ألزمهم بالحفاظ على البيانات المتعلقة بشخصية المتراسلين عبر شبكة الإنترنت، وكذلك أسماء المواقع التي رجعوا إليها (المادة 29).

ولكن المشرِّع الفرنسي قد عدَّل هذا النص بمقتضى قانون الأمن الداخلي الفرنسي la sécurité intérieure الصادر سنة 2003، لكي يشمل محتوى المراسلات نفسها، والتي كان القانون السابق يحظر الاحتفاظ بها.

(1) http://www.masslib.org/IFC/LawForLibraries/Case_Law/NSLAshcroft334FSupp2d471.pdf

ومن الجدير بالذكر أن المادة (60.1) من قانون الإجراءات الجنائية الفرنسي قد تم تعديلها سنة 2004 وسنة 2010 لكي تسمح لمأموري الضبط القضائي ولرئيس النيابة بالاطلاع على المستندات والمعلومات التي هي في حوزة أي شخص أو جهة أو إدارة عامة أو منشأة أو شركة. كما نصت على عدم جواز التمسك بسر المهنة في مواجهة طلب الاطلاع من مأموري الضبط القضائي. غير أنه إذا تعلق الأمر بمستندات لدى محام أو طبيب أو لدى مؤسسة صحفية فإن الاطلاع لا يتم إلاّ برضائهم.

– اتساع سلطات النيابة في التفتيش والاطلاع والتنصت في جرائم الإرهاب في القانون المصري:

وسَّع المشرِّع المصري من سلطة النيابة العامة في تحقيق الجرائم الواردة في القسم الأول من الباب الثاني من الكتاب الثاني من قانون العقوبات ويدخل ضمنها جرائم الإرهاب؛ فأصبح لها نفس السلطات المخولة لقاضي التحقيق[1]. ومؤدى ذلك أن للنيابة العامة بالإضافة سلطة تفتيش غير المتهم وكذلك تفتيش منزله والاطلاع على الرسائل والخطابات المضبوطة (مادة 92 ومادة 94 إجراءات) وسلطة ضبط جميع الخطابات والرسائل والمطبوعات والطرود لدى مكتب البريد، وسلطة مراقبة المحادثات السلكية واللاسلكية وتسجيل المحادثات التي تجري في مكان خاص (مادة 95 إجراءات) وسلطة توجيه الأمر لحائز الشيء لضبطه أو الاطلاع عليه ويسري حكم المادة 284 إجراءات على من يخالف ذلك الأمر (الحكم بالغرامة) (مادة 99 إجراءات).

(1) محمود صالح العادلي، السياسة الجنائية لدرء جرائم العنف الإرهابي، دار النهضة العربية، 1997، ص121؛ إبراهيم عيد نايل، السياسة الجنائية في مواجهة الإرهاب، دار النهضة العربية، 1996، ص 165؛ محمد محمود سعيد، جرائم الإرهاب، أحكامها الموضوعية وإجراءات ملاحقتها، المرجع السابق، ص183.

– اتساع سلطة النيابة العامة في الكشف عن سرية الحسابات بالبنوك في القانون المصري:

وسَّع المشرِّع المصري أيضاً من سلطة النيابة العامة في الكشف عن سرية الحسابات بالبنوك، وذلك وفقاً لتعديل المادة الثالثة من القرار بقانون رقم 205 لسنة 1990 بالمادة السادسة من القانون رقم 97 لسنة 1992 بشأن سرية الحسابات بالبنوك، فأصبح للنيابة العامة هذه السلطة بدلاً من رئيس محكمة استئناف القاهرة في الجرائم المنصوص عليها في القسم الأول من الباب الثاني من الكتاب الثاني من قانون العقوبات. وتدخل جرائم الإرهاب في عداد تلك الجرائم[1].

(1) أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة، التجريم وسبل المواجهة، دار الطلائع، 2006 ص97.

النتائج والتوصيات

أولاً – النتائج:

– يعد التقدم التكنولوجي في الاتصالات الإلكترونية من أحد الأسباب التي كان لها عظيم الأثر في المساس بالحق في الخصوصية.

– تحرص التشريعات المقارنة على حماية البيانات والمعلومات الشخصية للأفراد والمسجلة لدى الجهات المختلفة سواء أكانت حكومية أم غير حكومية.

– تنظم كثير من التشريعات كيفية الاطلاع على بيانات الأفراد والمسجلة في الأجهزة الإلكترونية لدى الجهات القضائية أو جهات الضبط القضائي. ففي فرنسا على سبيل المثال لا يجوز الدخول إلى تلك الأنظمة للاطلاع على البيانات إلا بمقتضى أمر قضائي أو عند توافر حالة التلبس.

– يحمي التعديل الرابع للدستور الأمريكي البيانات المعالجة آليا من التداخل إليها عن بعد، مقيما التماثل بين الاقتحام المادي (للمنازل) والاقتحام المعنوي(للمعلومات). فلا يجوز الإطلاع أو التنصت أو التفتيش على الاتصالات الإلكترونية إلا بإذن قضائي مسبب وفقا للقواعد المستقر عليها في مجال التنصت والتفتيش.

– تعاقب كثير من التشريعات المقارنة – منها قانون العقوبات المصري (م 309 مكرر) –وقانون الاتصالات الكويتي لسنة 2014 (مادة 70) على اعتراض الاتصالات السلكية واللاسلكية الخاصة دون إذن بذلك، باعتبار أن ذلك يتضمن انتهاكاً لحرمة الحياة الخاصة.

– تشترط بعض التشريعات – كالقانون الفنلندي – لصحة التفتيش عن البيانات المبرمجة بوجه عام أن يكون ذلك في جريمة ذات خطورة معينة.

– يسمح القانون الأمريكي أن يصدر إذن بتفتيش الكمبيوتر ليشمل جميع البيانات الشخصية الخاصة بالمشترك والمتعاملين معه وكذلك محتويات الملفات المخزنة بما فيها تلك التي تم تخزينها مدة أقل من 180 يوماً.

- ليس هناك ما يمنع من صدور إذن بالتفتيش مقتصرا على تفتيش الكمبيوتر فقط دون بقية أجزاء المسكن أو محل العمل أو شخص المتهم. ويحدث ذلك إذا كانت التهمة الموجه إلى المتهم تتعلق بجريمة من جرائم الكمبيوتر فقط مثل حيازة صور جنسية إلكترونية فاضحة خاصة بالأطفال، وهي الجريمة التي تعاقب عليها كثير من التشريعات المقارنة (كالفرنسي والأمريكي).

- يتجه المجلس الأوربي إلى جواز التنصت بخصوص الجرائم الخطيرة التي تقع على سرية الاتصالات اللاسلكية وكذلك الخاصة بالكمبيوتر والتداخل في هذه الأنظمة (الهاتفية أو الكمبيوتر) الذي من شأنه الاعتداء على الخطوط (بالسرقة) أو من شأنه الإخلال بحسن سيرها.

- يتمتع صاحب البريد الإلكتروني بالحق في حرمة الحياة الخاصة بالنسبة للمعلومات المتواجدة داخل البريد الإلكتروني لجهاز الكمبيوتر الخاص به. ولا يجوز التداخل للاطلاع على البريد الإلكتروني دون إذن صاحبه، ما لم يصدر إذن قضائي بذلك.

- تتجه التشريعات المقارنة إلى إلزام مزودي الخدمات بالتعاون مع المحقق بالإضافة إلى التزامهم بالتعاون مع رجال الضبط القضائي.

- أصبحت عديد من التشريعات تسمح بالتوسع في حالات التفتيش عندما يتعلق الأمر بالإرهاب؛ فلم يعد القانون الأمريكي لسنة 2001 يشترط الدلائل الكافية لتفتيش المتهم في جرائم الإرهاب. وبذلك فإن مأموري الضبط القضائي يصبح من حقهم في التحقيقات الخاصة بالإرهاب الدخول إلى المنازل وأماكن العمل دون سابق إنذار والتقاط الصور وضبط الأشياء والاتصالات الإلكترونية دون إخطار صاحب المكان.

- من مظاهر المساس بحرمة الحياة الخاصة في مكافحة الإرهاب ما تضمنه القانون الوطني Patriot Act من نصوص تسمح لهيئة الأمن الوطني National Security Agency أن تلتقط الاتصالات الهاتفية التي تجري بين طرفين يتورط أحدهما في جريمة إرهابية استنادا إلى توافر أسباب مقبولة تقدر الحكومة أنها تكفي لكي تقوم بهذا الالتقاط.

- من مظاهر الإخلال بحرمة الحياة الخاصة ما أجازه الفصل 206 من القانون الوطني الأمريكيPatriot Act الذي يسمح بوضع الاتصالات الهاتفية تحت المراقبة دون شرط تحديد الهواتف محل المراقبة (roving wiretap).
- يخول القانون الألماني الصادر في سنة 2003 الأجهزة الأمنية صلاحية مراقبة الأحاديث التليفونية وتسجيلها للمشتبه بارتكابهم جرائم إرهابية وذلك بدون إذن قضائي مسبق.

ثانياً - التوصيات

- ندعو المشرِّع الكويتي إلى إدخال نص يعاقب على اعتراض والتقاط المحادثات التي تتم في مكان خاص.
- ندعو المشرِّع الكويتي والمشرِّع المصري إلى التسوية بين المراسلات الإلكترونية والملاسلات البريدية أو إيجاد وضع قانوني محدد لها.
- ندعو المشرِّع الكويتي والمشرِّع المصري إلى وضع نظام قانوني لتفتيش وضبط البيانات المبرمجة في الكمبيوتر.

المراجع:

المراجع العربية:

- سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة عبر الإنترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية – المجلد –29 العدد الثالث – 2014.
- جاسم محمد العنتلي، الجرائم والتكنولوجيا الحديثة – دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، 2014.
- عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، 2011.
- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية 2003.
- أحمد فتحي سرور، الشرعية الدستورية وحقوق الإنسان في الإجراءات الجنائية، دار النهضة العربية، 1995.
- أحمد فتحي سرور، القانون الجنائي الدستوري، دار الشروق، 2002.
- فتيحة بن ناصر، الحد من الضمانات الإجرائية للمتهمين بالجرائم الإرهابية، دار الجامعة الجديدة بالإسكندرية، 2011.
- عوض محمد عوض، التفتيش في ضوء أحكام النقض، دراسة نقدية، مطابع السعدني، سنة 2007.
- محمود صالح العادلي، السياسة الجنائية لدرء جرائم العنف الإرهابي، دار النهضة العربية، 1997،
- إبراهيم عيد نايل، السياسة الجنائية في مواجهة الإرهاب، دار النهضة العربية، 1996.
- أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة، التجريم وسبل المواجهة، دار الطلائع، 2006.

مصادر قانونية وقضائية:

- فقرات من الدستور المصري 2014 .
- نقض 30 أبريل سنة 1934 مجموعة القواعد القانونية جـ3 ص 325 رقم 243 ؛ 8 أبريل سنة 1968
- مجموعة أحكام النقض س 19 ص 398 رقم 75 ؛ 4 نوفمبر سنة 1968 س 19 ص899 رقم 178 ؛ 27 يناير سنة 1974 س 25 ص 58 رقم 13 ؛ 14 يناير سنة 1985 س36 ص 75 رقم 8 .نقض 6 أبريل سنة 1964.
- مجموعة أحكام النقض س12 ص246 رقم 49؛ 26 فبراير سنة 1978 س 29 ص 185 رقم 32. كما قضت محكمة النقض بأن: «حرمة السيارة الخاصة مستمدة من اتصالها بشخص صاحبها أو حائزها»، نقض 30 يونيو 1969 س 20 ص 976 رقم 193؛ 26 نوفمبر سنة 1984 س 35 ص 829 رقم187.
- حكم المحكمة الدستورية في 2 يونيو سنة 1984، القضية رقم 105 لسنة 4 ق دستورية.
- المادتان (44 و 45) من الدستور المصري.
- نقض مصري 11 فبراير سنة 1974 مجموعة أحكام النقض س25 ص 138 رقم 31؛
- حكم المحكمة الدستورية العليا في 2 يونيو سنة 1984، القضية رقم 105 لسنة 4 ق دستورية، وبناء عليه قضت محكمة النقض بأن «المادة (44) من الدستور لم تستثن حالة التلبس من ضرورة صدور أمر قضائي مسبب ممن له سلطة التحقيق أو من القاضي المختص بتفتيش المسكن سواء أقام به الآمر بنفسه أم أذن لمأمور الضبط القضائي بإجرائه».
- نقض 25 مايو سنة 1959، مجموعة أحكام محكمة النقض س 10 ص 568 رقم 126؛ 30 ديسمبر 1952، س 4 ص 314 رقم 122؛ 14 نوفمبر 1960 س 11 ص 782 رقم 150؛ أول ديسمبر 1958 س 9 ص 1006 رقم 244 ؛ 8 يونيو 1980 س 31 ص 723 رقم 140 ؛ 17 مارس 1988 س 39 ص 435 رقم 63.

مصادر أجنبية:

- Zurcher v. Stanford Daily , 436 U. S. 547 (1978) , www.cybercrime.gov/s&smanual2002.htm.
- Privacy Protection Act.
- Pascal VERGUCHT , La répression des délits informatiques dans une perspective internationale , Thèse , Montpellier , 1996, p. 378.
- Katz .c. U.S , 389 U.S. 352 (1967) : www.cdt.org/digi_tele/19706rpt.html#note_1 cited by : René PEPIN , Le statut juridique du courriel au Canada et aux Etats – Unis , www.lex-electronica.org /articles / v6-2/pepin.htm , 29 déc. 2003 , p.4.
- United States v. Herring, 993 F.3d 784, 787 (11th Cir. 199), www.cybercrime.gov/s&smanual2002.htm. , p. 79 .
- Shacter c. Birks , 1985 . C.S 343 ; cité par , David G. Masse , www.masse.org/preuve_courriel.htm , p.13 .
- Roy c. Saulnier , 1992 . R.J.Q. 2419 ; cité par , David G. Masse , www.masse.org/preuve_courriel.htm .
- U.S. Const .Amend . IV(« no Warrants shall issue , but upon probable cause, supported by Oath or affirmation «). Department of justice , p.48.
- United States v. Cervini , 2001 WL 863559 (10th Cir .Jul.31 ,2001); United States v. Hay , 231 F.3d 630 , 634 (9th Cir.2000); United States v. Grant , 218 F.3d 72 , 76 (1st Cir .2000). Department of justice , p.48 .
- United States v. Hay , 231 F.3d 630 , 634 (9th Cir .2000) ; United States v. Campos , 221 F.3d 1143 , 1147 (10th Cir .2000) ; United States v. Upham , 168 F.3d 532 , 535 (1st Cir . 1999) ; United States v. Lacy

, 119 F.3d 742, 746 (9th Cir. 1997) ; United States v. Henson , 848 F.2d 1374 , 1382-83 (6th Cir. 1988) ; United States v. Albert , 195 F. Supp . 2d 267 , 275-76 (D.Mass.2002); Cf. United States v. Lamb , 945 F. Supp . 441, 458-59 (N.D.N.Y 1996) ; Department of justice , p. 47 .

- United States v. Musson , 650 F. Supp . 525 , 532 (D. Colo . 1986) ; United States v. Reyes , 798 F.2d 380 , 383 (10th Cir . 1986) ; Department of justice , p. 48
- United States v. Ford , 184 F. 3d 566 , 576 (6th Cir . 1999) ; United States v. Kow , 58 F. 3d 423 , 427 (9th Cir . 1995) , www.cybercrime.gov/s&smanual2002.htm , ibid , p. 45 .
- United States Department of Justice , http://www.justice.gov/.
- United States v. Runyan , 275 F.3d 449 , 464-65 (5th Cir. 2001) ; United States v. Slanina , 283 F.3d 670 , 680 (5th Cir . 2002) www.cybercrime.gov/s&smanual 2002.htm , p. 9 .
- United States v. Walser , 275 F. 3d 981 , 986 (10th Cir. 2001) , www.cybercrime.gov/s&smanual2002.htm.
- Etats-Unis contre Rodriguez , 968 F.2d 130 (2d Cir.) et 113 S. Ct . 140 (1992) cité par ETATS-UNIS , Département de la Justice , Division criminelle, Federal guidelines for searching and seizing computers , United States Government Printing Office , juill. 1994 , p.94.
- Steve Jackson Games v. United States Secret Service , 36 F. 3d 457 , 460-63 (5th Cir . 1994) « access to stored e-mail communications « ; Wesley College v. Pitts , 974 F. Supp . 375 , 384 – 90 (D. Del . 1997) ; ; United States v. Scarfo , 180 F. Supp . 2d 572 , 582 (D . N . J . 2001) , www.cybercrime.gov/s&smanual2002.htm , ibid , p. 55.
- United States v. Moriarty , 962 F. Supp 217 , 220 – 21 (D . Mass . 1997

) « access to stored wire communications « , www.cybercrime. gov/s&smanual2002.htm, p. 80 .
- Albear MARON , procédure pénale , Juriss – class . Procédure pénale , droit pénal , janv 1992 , p. 15 .
- Arrêt Klass c / R .F. Allemagne , 6 sept . 1978 .
- Merle et Vitu , Traité de droit criminel , Procedure pénale , éd. Cujas 2001 , p. 204.
- Amitai Etzioni , Implications of Select New Technologies for Individual Rights and Public Safety , Harvard Journal of Law & Technology 2002 , p.274
- David G. Masse , www.masse.org/preuve- courriel.htm , op. cit., p.11 .
- L›arrêt Protection de la jeunesse -763 , J.E. 95-1099 (C.S.) , David G. Masse , www.masse.org/preuve_courriel.htm, p.16 .
- United States v. Barth , 26 F. Supp . 2d 929 , 936-37 (W. D .Tex .1998) ; United States v. Reyes , 922 F. Supp . 818 , 832-33 (S.D.N.Y. 1996); United States v. Lynch , 908 F. Supp . 284 , 287 (D.V.I. 1995) ; United States v. Chan, 830 F.Supp .531 , 535 (N.D.Cal . 1993) ; United States v. Blas , 1990 WL 265179 , at 21 (E. D. Wis .Dec. 4, 1990) , www.cybercrime.gov/s&smanual2002.htm , ibid , p. 9 .
- Julien Cantegreil ,La doctrine du « combattant ennemi illégal »Revue de science criminelle 2010 p. 81
- American Civil Liberties Union , Surveillance Under the Patriot Act , http://www.aclu.org/national-security/surveillance-under-patriot--act
- Wilson v. Arkansas , 514 US 927 (1995), www.law.cornel.ed/wex/knoch-and-announce rule.

- Amendment IV: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. http://www.scn.org/ccapa/pa-vs-const.htm
- American Civil Liberties Union, Reform the Patriot Act, http://www.aclu.org/reform-patriot-act.
- www.npr.org/news/specials/patriotact/patriotactprovisions.html
- www.npr.org/news/specials/patriotact/patriotactprovisions.html
-http://www.masslib.org/IFC/LawForLibraries/Case_Law/NSLAshcroft334FSupp2d471.pdf