الضمانات القانونية لحماية حُرْمة الاتصالات الشخصية

"دراسة مقارنة"

(مصر، فرنسا، الولايات المتحدة الأمريكية)

د. أحمد رجب سيد صميده

قاضي بمجلس الدولة

حاصل على درجة الدكتوراه تخصص القانون العام- كلية الحقوق

جامعة بني سويف

(ISSN: 2537- 0758)

الضمانات القانونية لحماية حُرْمة الاتصالات الشخصية

"دراسة مقارنة"

(مصر، فرنسا، الولايات المتحدة الأمريكية)

د. أحمد رجب سيد صميده

ملخص الدراسة

يهدف البحث إلى عقدَ مقارنة بين موقف التشريعات المقارنة من الضمانات القانونية التي اتخذتها كل منها لحماية حُرمة الاتصالات الخاصة لبيان ما إذا كان المشرع المصري قد حقق الحماية الكافية لحرمة هذه الاتصالات أم أن هناك قصورا في تلك الحماية وأوجه علاجه لتحقيق الموازنة بين حق الفرد في الخصوصية وحق الدولة في الحفاظ على أمنها وسلامتها، ولتحقيق ذلك الهدف اعتمد البحث على المنهج الوصفي الذي يعتمد على جمع المعلومات عن الضوابط التي اتخذتها التشريعات المقارنة لحماية حُرمة الاتصالات الخاصة ثم تفسيرها، كما اعتمد– كذلك– على المنهج التحليلي بإجراء تحليل متعمق لتلك المعلومات، وكذلك المنهج المقارن؛ إذ تتطرق الدراسة إلى مقارنة التنظيم التشريعي لتلك الضوابط في تشريعات الدول المقارنة.

وقد خلص البحث إلى عدد من النتائج أهمها: أجاز المُشرِّع المصري أن يكون إجراء المراقبة أول إجراء من إجراءات التحقيق دون اشتراط أن يكون مسبوقًا بأي إجراءات تحقيق سابقة، خلافا للمشرِّع الأمريكي الذي اشترط لاستصدار أمر بالمراقبة "ثبوت عدم جدوى استخدام إجراءات التحقيق الأخرى عند إجرائها أو أن يكون من المرجح فشلها أو أن يترتب على استخدامها نتائج خطيرة"، كما اعتمد المُشرِّع المصري– فيما يتعلق بإصدار الأمر بمراقبة الاتصالات الخاصة– على "معيار جسامة العقوبة"؛ حيث اشترط لإصدار الأمر بمراقبة المراسلات الخاصة والمحادثات الهاتفية أن تكون الجريمة محَلّ التحقيق من الجرائم المعاقب عليها بالحبس مدة لا تقل عن ثلاثة أشهر، بينما عمد المشرع الأمريكي إلى تحديد جرائم محدَّدة يجوز إصدار الأذن بالمراقبة بشأنها، أخذًا في الاعتبار طبيعة الجريمة، الآثار التي يمكن تخلفها، العقوبة المقرَّرة لها، بما يبرِّر انتهاك حُرْمة الاتصالات الخاصة.

كلمات مفتاحية: حرمة الاتصالات الخاصة– مراقبة الاتصالات الخاصة– المراسلات الخاصة– المحادثات الهاتفية– رسائل الاتصال الإلكتروني– المحادثات الإلكترونية.

Abstract:

The research aims to make a comparison between the position of comparative legislation in (Egypt, France, and the United States of America) regarding the legal guarantees taken by each of them to protect the sanctity of private communications, indicate whether the Egyptian legislator has achieved adequate protection for the sanctity of these communications, or whether there is a deficiency in that protection, and the aspects of its treatment to achieve a balance between the individual's right to privacy and the right of the state to maintain its security and safety, and to achieve this goal, the research relied on the descriptive approach, which relies on collecting information on the determinants taken by comparative legislation to protect the sanctity of private communications and then interpreting it. It has also relied on the analytical approach conducting an in-depth analysis of that information, as well as the comparative approach; The study deals with the comparison of the legislative organization of these determinants in the legislation of the comparative countries.

The research has been concluded with a number of results, the most important of which are: The Egyptian legislator permitted the monitoring procedure to be the first investigation procedure without requiring that it be preceded by any previous investigation procedures, unlike the American legislator who stipulated that “the futility of using other investigative procedures when conducted or that it be one of the It is likely that it will fail or that its use will result in serious consequences “to issue a monitoring order, and the Egyptian legislator relied- with regard to issuing the order to monitor private communications- on the “criterion of the gravity of the penalty”; In order to issue the order to monitor private correspondence and telephone conversations, it was stipulated that the crime in question be one of the crimes punishable by imprisonment for a period of no less than three months, while the American legislator intended to specify specific crimes for which permission to monitor may be issued, taking into account the nature of the crime and the effects that can be left behind, the penalty prescribed for it, justifying the violation of the sanctity of private communications.

Keywords: sanctity of private communications- monitoring of private communications- private correspondence- telephone conversations- electronic communication messages- electronic conversations.

(ISSN: 2537- 0758)

مقدمة

حرَص الدُّسْتُور المصري الحالي لعام ٢٠١٤- على تأكيد حُرْمة الاتصالات الخاصة في المادة (٥٧) منه والتي جاء نصّها على أنه "للحياة الخاصة حُرْمة، وهي مَصُونة لا تُمسّ. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حُرْمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبَّب، ولمدة محدَّدة، وفي الأحوال التي يبيّنها القانون. كما تلتزم الدولة بحماية حقّ المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسُّفي، وينظم القانون ذلك".

وتتجلّى حكمة هذا النصّ في جسامة المخاطر الناتجة عن الانتهاك الواقع على الاتصالات الشخصية بصورها المختلفة (رسائل: بريدية، برقية، إلكترونية، أو محادثات: هاتفية، إلكترونية)، وما يشكله هذا الانتهاك من مساسٍ بالحق في الخُصُوصية، واعتداءٍ على حقوق الأفراد وحرياتهم، على أن المُشرّع أورد ضوابط معينة أجاز من خلالها المساس بتلك الحُرْمة عن طريق أمر قضائي مسبَّب، ولمدة محدَّدة، فضلًا عن الضوابط الأخرى التي تكفلت النصوص التشريعية بتحديدها تنفيذًا للتوجيه الدستوري.

ويرجع جواز المساس بتلك الحُرْمة إلى ضرورة تحقيق التوازن بين حق الفرد في الخُصُوصية وبين مصلحة المجتمع المتمثلة في توقّي الجريمة، فليس كل انتهاك لحُرْمة الاتصالات الشخصية مجرَّمًا، لذا كان التنظيم الدُّسْتُوريّ والتشريعي للمساس بها أمرًا محتمًا تحقيقًا لأمن المجتمع وحماية للأفراد من التعسُّف.

أهمية البحث:

الجانب العلمي (النظري):

تكمُن أهمية هذا البحث– في جانبه النظري– في تحديد مفهوم مراقبة الاتصالات الخاصة في التشريعات المقارنة، وتحديد ضوابط المساس بحرمة هذه الاتصالات على وجه الدقة في التشريعات "محل المُقارنة".

الجانب العملي (التطبيقي):

التعرف الدقيق على ضوابط المساس بحرمة الاتصالات الخاصة في التشريعات المقارنة (مصر، فرنسا، الولايات المتحدة الأمريكية) مما يساهم في تحديد أوجه القصور الذي شاب التشريع المصري عند تنظيم هذه المسألة، وسبل علاجه حال وجوده.

أهداف البحث:

يهدف البحث إلى عقدَ مقارنة بين موقف التشريعات المقارنة في (مصر، فرنسا، الولايات المتحدة الأمريكية) من الضمانات القانونية التي اتخذتها كل منها لحماية حُرمة الاتصالات الخاصة لبيان ما إذا كان المشرع المصري قد حقق الحماية الكافية لحرمة هذه الاتصالات أم أن هناك قصورا في تلك الحماية وأوجه علاجه لتحقيق الموازنة بين حق الفرد في الخصوصية وحق الدولة في الحفاظ على أمنها وسلامتها.

منهج البحث:

اعتمد البحث على المنهج الوصفي الذي يعتمد على جمع المعلومات عن الضوابط التي اتخذتها لتشريعات المقارنة في (مصر، فرنسا، الولايات المتحدة الأمريكية) لحماية حُرمة الاتصالات الخاصة ثم تفسيرها، كما اعتمد– كذلك– على المنهج التحليلي بإجراء تحليل متعمق لتلك المعلومات، وكذلك المنهج المقارن؛ إذ تتطرق الدراسة إلى مقارنة التنظيم التشريعي لتلك الضوابط في تشريعات (مصر وفرنسا والولايات المتحدة الأمريكية) لتحقيق الأهداف المرجوة من هذا البحث.

وسنعرض هذا البحث في ثلاثة مباحث:

المبحث الأول: ضوابط المساس بحُرْمة الاتصالات الشخصية في القانون المصري.

المبحث الثاني: ضوابط المساس بحُرْمة الاتصالات الشخصية في القانون الأمريكي.

المبحث الثالث: ضوابط المساس بحُرْمة الاتصالات الشخصية في القانون الفرنسي.

المبحث الأول

ضوابط المساس بحُرْمة الاتصالات الخاصة في القانون المصري

سوف نتناول دراسة هذا المبحث في مطلبين على النحو التالي:

المطلب الأول

مفهوم المراقبة في القانون المصري:

عزف المُشرّع المصري– شأنه في ذلك شأن غالبية التشريعات– عن وضع تعريف محدّد للمراقبة تاركًا تلك المسألة لاجتهاد الفقه والقضاء، واكتفى بتنظيم تلك العملية تنظيمًا شاملًا، وتكمُن الحكمة من وراء ذلك في تجنُّب وضع تعريف محدَّد قد لا يتسم بالمرونة الكافية التي تجعله مواكبًا لكافة التطورات التي تنتجها التكنولوجيا الحديثة.

(ISSN: 2537- 0758)

موقف الفقه:

حاول الفقه الاجتهاد في وضع تعريف للمراقبة، فعرفها البعض بأنها "تعمُّد الاتصال والتسجيل للمحادثات الخاصة سواء كانت مباشرة أو غير مباشرة؛ أي: سواء كانت مما يتبادله الناس في مواجهة بعضهم، أو عن طريق وسائل الاتصال السلكية واللاسلكية"[١]. وعرَّفها آخرون بأنها "التنصُّت"، ومحلها المحادثات التي تدور بين أكثر من شخص سواء بواسطة الأجهزة التليفونية أو اللاسلكية أو أجهزة الشفرة، أو كانت مباشرة بين شخصين أو أكثر، وكانت بطريقة يقصد بها أطرافها ألا تكونَ مسموعة للغير"[٢].

ومما يؤخذ على تلك التعريفات أنها قَصَرَتِ المراقبة على المحادثات الصوتية على الرغم من أنها تعدُّ إحدى صور الاتصال، فالاتصال كما سبق أن أوضحنا يمكن أن يتم عن طريق البيانات التي تحمل صورًا وعلاماتٍ ورموزًا وإشاراتٍ دون اقتصار على المحتوى الصوتي للاتصال.

موقف القضاء:

تناولت الأحكام القضائية مفهوم المراقبة من وجهة قانونية مبيِّنةً الغرض منها وضوابط إعمالها، فقد استقر قضاء محكمة النقض على أن "المراقبة هي إجراء من إجراءات التحقيق لا يصح إصداره إلا لجريمة وقعت بالفعل، تباشره سلطة التحقيق المختصة، مباشرةً أو عن طريق ندب أحد مأموري الضبط القضائي لإجرائه"[٣]، كما استقر أيضًا على أن المراقبة تنصبُّ على الأحاديث الشخصية والمحادثات السلكية واللاسلكية[٤].

---

[١] د. يوسف الشيخ، حماية الحق في حُرْمة الأحاديث الخاصة، دراسة مقارنة في تشريعات التصنُّت وحُرْمة الحياة الخاصة، دار الفكر العربي، ط١، ١٩٩٨، ص ٢٦٠ وما بعدها.

[٢] د. حسام الدين محمد أحمد، شرح قانون الإجراءات الجنائية، ج١، دار النهضة العربية، ٢٠٠٢، ص٥٨٠.

مشار إليهما بمرجع د. محمد حسام الدين محمد، "الحماية الجنائية لحق الإنسان في حُرْمة اتصالاته الشخصية رسالة دكتوراه، جامعة القاهرة، ٢٠١٦، ص ٣٠٤".

[٣] حكم محكمة النقض– جنائي– في الطعن رقم ٩٨٩ لسنة ٣١ ق، بجلسة ١٩٦٢/٢/١٢، مكتب فني ١٣، الجزء رقم ١، ص ١٣٥.

[٤] حكم محكمة النقض– جنائي– في الطعن رقم ٦٨٥٢ لسنة ٥٩ ق، بجلسة ١٩٩٦/١/١٤، مكتب فني ٤٧، الجزء رقم ١، ص ٧٢ .

المطلب الثاني
ضوابط صدور أمر قضائي لمراقبة الاتصالات الخاصة

أولًا: المراسلات الخاصة والمحادثات الهاتفية:

نصَّت المادة (٩٥)[٥] من قانون الإجراءات الجنائية على أنه "لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق، وأن يأمر بمراقبة المحادثات السلكية واللاسلكية، أو إجراء تسجيلات لأحاديث جرت في مكان خاصّ، متى كان لذلك فائدة في ظهور الحقيقة في جناية أو في جُنحةٍ معاقَبٍ عليها بالحبس لمدة تزيد على ثلاثة أشهر. وفي جميع الأحوال يجب أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناءً على أمر مسبَّب ولمدة لا تزيد على ثلاثين يومًا قابلة للتجديد لمدة أو مدد أخرى مماثلة".

ويسري هذا الحكم في شأن مراسلات المتهم ومحادثاته الهاتفية، كما يسري في شأن غيره إذا اتضحت من أمارات قوية أنه حائز لأشياء تتعلق بالجريمة.

ويتضح من هذا النص أنه يشترط لمشروعية ضبط المراسلات الخاصة أو المحادثات الهاتفية توافرُ عدة شروط شكلية وأخرى موضوعية:

أولًا: الشروط الشكلية:

١- أن يكون الأمر الصادر بضبط المراسلات أو مراقبة المحادثات الهاتفية مسبَّبًا:

يجب أن يكون الأمر الصادر بضبط المراسلات أو مراقبة المحادثات الهاتفية مسببًا، وهو ما يستلزم بطبيعة الحال وقوع الجريمة بالفعل، وأن تشير دلائل جدية على قيام أحد الأشخاص بارتكابها.

ونظرًا لخطورة هذا الإجراء فإنه يجب أن يتمَّ بناءً على تحرّيات جدّية، كما ينبغي استخدام الوسيلة الأقل اعتداءً على حُرْمة الأفراد طالما كانت كافية للوصول إلى الهدف المنشود، حفاظًا على حقّهم في الخُصُوصية.

وقد استقر قضاء محكمة النقض على أنه "... إذا كان الحكم قد أبان أن القاضي قد أصدر الإذن بمراقبة تليفون الطاعنة بعد أن أثبت اطلاعه على التحرّيات التي أوردها الضابط في محضره وأفصح عن اطمئنانه إلى كفايتها، فإنه بذلك يكون قد اتخذ من تلك

---

[٥] المادة (٩٥) من قانون الإجراءات الجنائية رقم (١٥٠) لسنة ١٩٥٠، المستبدلة بالقانون رقم (٣٧) لسنة ١٩٧٢.

(ISSN: 2537- 0758)

التحريات أسبابًا لإذنه بالمراقبة، وفي هذا ما يكفي لاعتبار إذنه مسببًا حسبما تطلَّبه المُشرِّع..."[٦].

الاختصاص بإصدار الإذن:

قاضي التحقيق:

وفقًا لنص المادة (٩٥) من قانون الإجراءات الجنائية يختصّ قاضي التحقيق بإصدار الإذن بضبط المراسلات أو مراقبة المحادثات الهاتفية إذا كان هو من يباشر إجراءات التحقيق.

القاضي الجزئي:

تنصّ المادة (٢٠٦)[٧] من قانون الإجراءات الجنائية على أنه "لا يجوز للنيابة العامة تفتيش غير المتهم أو منزل غير منزله إلا إذا اتضح من أمارات قوية أنه حائز لأشياءَ تتعلق بالجريمة. ويجوز لها 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 خاصّ متى كان لذلك فائدة في ظهور الحقيقة في جناية أو في جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. ويشترط لاتخاذ أيّ إجراء من الإجراءات السابقة الحصول مقدَّمًا على أمر مسبّب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق. وفي جميع الأحوال يجب أن يكون الأمر بالضبط أو الاطلاع أو المراقبة لمدة لا تزيد على ثلاثين يومًا. ويجوز للقاضي الجزئي أن يجدّد هذا الأمر مدة أو مددًا أخرى مماثلة. وللنيابة العامة أن تطلع على الخطابات والرسائل والأوراق الأخرى والتسجيلات المضبوطة على أن يتم هذا كلما أمكن ذلك بحضور المتهم والحائز لها أو المرسلة إليه وتدون ملاحظاتهم عليها. ولها حَسَبَ ما يظهر من الفحص أن تأمر بضمّ تلك الأوراق إلى ملف الدعوى أو بردّها إلى من كان حائزًا لها أو من كانت مرسلةً إليه".

ووفقًا لهذا النصّ، إذا تولّت النيابة العامة التحقيق يكون القاضي الجزئي هو المختصّ بإصدار الإذن، وإلا وقع الإذن باطلًا.

---

[٦] حكم محكمة النقض– جنائي– في الطعن رقم (٩٥٣) لسنة ٤٣ ق بجلسة ١٩٧٣/١١/٢٥، مكتب فني ٢٤، الجزء رقم ٣، ص ١٠٥٣.

[٧] المستبدلة بالقانون (٣٧) لسنة ١٩٧٢.

وتجدر الإشارة إلى أنّ سلطة القاضي الجزئي تقتصر على إصدار الإذن أو رفض إصداره دون أن تستطيل تلك السلطة إلى القيام بتنفيذه، فقد استقر قضاء محكمة النقض على أنه "... سلطة القاضي الجزئي في هذا الإجراء محدودة بمجرد إصدار الإذن أو رفضه دون أن يخلع عليه القانون ولاية القيام بالإجراء موضوع الإذن بنفسه؛ إذ إنه من شأن النيابة العامة –سلطة التحقيق– إن شاءت قامت به بنفسها أو ندبت له من تختاره من مأموري الضبط القضائي كما سلف البيان، وليس للقاضي الجزئي أن يندبَ أحدَ هؤلاء مباشرة لتنفيذ الإجراء المذكور. ولا يصحّ القول كذلك بأن مجرّد عرض النيابة العامة لمحضر التحرّيات– الذي قام به الضابط الذي أجراها– على القاضي الجزئي لاستصدار الإذن بالمراقبة التليفونية يُعدُّ بمثابة ندب ضمني لذلك الضابط بإجراء المراقبة المطلوبة، ذلك بأنه فضلًا عن أن الندب يجب أن يكون صريحًا ومحدّدًا كما سلف القول، فإن النيابة العامة لم تكن تملك الندب قبل صدور إذن القاضي الذي يعيد إليها سلطتها في ممارسة هذا الإجراء من إجراءات التحقيق..."[٨].

النيابة العامة:

تُصدِر النيابة العامة الأمر بضبط المراسلات أو مراقبة المحادثات الهاتفية في عدة حالات تتمثل في:

١– قضت المحكمة الدُّسْتُورية العليا بعدم دُسْتُورية نص المادة (٨) من أمر رئيس الجمهورية رقم ١ لسنة ١٩٦٧ الخاص بالرقابة الذي صدر استنادًا إلى حكم البند الثاني من المادة الثالثة من القرار بقانون رقم ١٦٢ لسنة ١٩٥٨ بشأن حالة الطوارئ[٩]، الذي أجاز لرئيس الجمهورية إصدار الأوامر بمراقبة الرسائل والصحف

---

[٨] حكم محكمة النقض– جنائي– في الطعن رقم (٩٨٩) لسنة ٣١ ق بجلسة ١٩٦٢/٢/١٢، مكتب فني ١٣، الجزء رقم ١، ص ١٣٥.

[٩] "..... وحيث إنه يبين من أمر رئيس الجمهورية رقم ١ لسنة ١٩٦٧ الخاص بالرقابة أنه صدر استنادًا إلى حكم البند الثاني من المادة الثالثة من القرار بقانون رقم ١٦٢ لسنة ١٩٥٨– بشأن حالة الطوارئ– الذي يجيز لرئيس الجمهورية إصدار الأوامر بمراقبة الرسائل والصحف والمطبوعات والمحررات وكافة وسائل التعبير قبل نشرها وضبطها ومصادرتها– وذلك عند إعلان حالة الطوارئ– التي تم إعلانها بموجب القرار الجمهوري رقم ١٣٣٧ لسنة ١٩٦٧. وينص أمر رئيس الجمهورية رقم ١ لسنة ١٩٦٧ في مادته الأولى على أنه "تفرض من الآن وإلى حين صدور أوامر أخرى من أجل سلامة الوطن رقابة عامة في جميع أنحاء البلاد ومياهها الإقليمية على الكتابات والمطبوعات والصور والطرود التي ترد إلى مصر أو ترسل منها إلى الخارج أو تمر بها أو تتداول داخل البلاد.....".

(ISSN: 2537- 0758)

وفى مادته الثانية على أن "يتولى الرقيب العام ومن يندبه من الموظفين التابعين– في سبيل الدفاع الوطني والأمن العام– فحصَ ومراقبة جميع المواد والرسائل والأخبار التي تسرى عليها أحكام الرقابة وفقًا لما نص عليه في المادة (١)، وله أن يؤخر تسليمها أو يوقفها أو يمحو فيها أو يصادرها أو يعدمها أو يتصرف فيها على أي وجه إذا كان من شأنها الإضرار بسلامة الدولة...". كما نصت مادته الثامنة– محَلّ هذه الدعوى– على أنه "لا تترتب أية مسئولية ولا تقبل أية دعوى على الحكومة المصرية أو أحد مصالحها أو موظفيها أو الرقيب العام أو أي موظف تابع له أو أي شركة أو أي فرد بسبب أي إجراء اتخذ تنفيذًا لأعمال الرقابة وفى حدود اختصاصها المبين في هذا الأمر". ومؤدَّى ذلك أن المشرِّع قصد بحكم هذه المادة الأخيرة أن يحصّن كافة القرارات والأعمال التي يتخذها القائمون على شئون الرقابة– في حدود اختصاصهم– ضد أيّ طعن بإلغائها أو أي مطالبة بالتعويض عن الأضرار المترتبة عليها ولو كانت هذه القرارات والأعمال معيبة– فجاء النص بإعفائهم هم والحكومة والجهات التي يتبعونها إعفاء مطلقًا من كل مسئولية تترتب عليها، فحظر قبول أية دعوى بشأنها، كاشفًا بذلك عما تغيَّاه المشرِّع من هذه المادة برمَّتها من إغلاق باب كل منازعة في تلك القرارات والأعمال وحجب حق التقاضي بصددها .

وحيث إن المادة ٦٨ من الدستور تنص على أن "التقاضي حق مصون ومكفول للناس كافة، ولكل مواطن حق الالتجاء إلى قاضيه الطبيعي... وبحظر النص في القوانين على تحصين أي عمل أو قرار إداري من رقابة القضاء". وظاهر من هذا النص أن الدستور لم يقف عند حد تقرير حق التقاضي للناس كافة كمبدأ دُسْتُوريّ أصيل،، بل جاوز ذلك إلى تقرير مبدأ حظر النص في القوانين على تحصين أي عمل أو قرار إداري من رقابة القضاء، وقد خص الدستور هذا المبدأ بالذكر رغم أنه يدخل في عموم المبدأ الأول الذي يقرر حق التقاضي للناس كافة وذلك رغبة من المشرِّع في توكيد الرقابة القضائية على القرارات الإدارية وحسمًا لما ثار من خلاف في شأن عدم دستورية التشريعات التي تحظر حق الطعن في هذه القرارات، وقد ردَّد النص المشار إليه ما أقرته الدساتير السابقة ضمنًا من كفالة حق التقاضي للأفراد، وذلك حين خوّلتهم حقوقًا لا تقوم ولا تؤتى ثمارها إلا بقيام هذا الحق باعتباره الوسيلة التي تكفل حمايتها والتمتع بها ورد العدوان عليها.

وحيث إن الدساتير سالفة الذكر قد تضمن كل منها نصًّا على أن المواطنين لدى القانون سواء، وأنهم متساوون في الحقوق والواجبات العامة، كما ورد في الدستور القائم هذا النص في المادة ٤٠ منه. ولما كان حق التقاضي من الحقوق العامة التي كفلت الدساتير المساواة بين المواطنين فيها، فإن حرمان طائفة معينة من هذا الحق مع تحقق مناطه– وهو قيام المنازعة في حق من حقوق أفرادها– ينطوي على إهدار لمبدأ المساواة بينهم وبين غيرهم من المواطنين الذين لم يحرموا من هذا الحق.

وحيث إن القرارات والأعمال التي تتخذها الجهة القائمة على تنفيذ شئون الرقابة– المنصوص عليها في المادة الأولى من أمر رئيس الجمهورية رقم ١ لسنة ١٩٦٧– إنما هي قرارات وأعمال تصدر عن تلك الجهة باعتبارها سلطة عامة بقصد إحداث مركز قانوني معين ابتغاء مصلحة عامة، فتكون لها صفة القرارات والأعمال الإدارية وتنبسط عليها رقابة القضاء، ومن ثم فإن المادة الثامنة من هذا

والمطبوعات قبل نشرها وضبطها ومصادرتها، كما حصنَ أيَّ عمل أو قرار إداري تم اتخاذه تنفيذًا لأعمال الرقابة، وذكرت المحكمة الدُّسْتُورية العليا في حكمها: "... إن حرمان طائفة معينة من هذا الحقّ مع تحقّق مناطه- وهو قيام المنازعة في حقّ من حقوق أفرادها- ينطوي على إهدار لمبدأ المساواة بينهم وبين غيرهم من المواطنين الذين لم يحرموا من هذا الحق...".

وقد نصّت المادة (٢٠٦) مكرر[١٠] من قانون الإجراءات الجنائية على أنه "يكون لأعضاء النيابة العامة من درجة رئيس نيابة على الأقل- بالإضافة إلى الاختصاصات المقرّرة للنيابة العامة- سلطات قاضي التحقيق في تحقيق الجنايات المنصوص عليها في الأبواب الأول والثاني والثاني مكرّرًا والرابع من الكتاب الثاني من قانون العقوبات. ويكون لهم فضلًا عن ذلك سلطة محكمة الجنح المستأنفة منعقدة في غرفة المشورة المبيَّنة في المادة (١٤٣) من هذا القانون في تحقيق الجرائم المنصوص عليها في القسم الأول من الباب الثاني المشار إليه بشرط ألا تزيد مدة الحبس في كل مرة عن خمسةَ عشرَ يومًا. ويكون لهؤلاء الأعضاء من تلك الدرجة سلطات قاضي التحقيق فيما عدا مُدد الحبس الاحتياطي المنصوص عليها في المادة (١٤٢) من هذا القانون، وذلك في تحقيق الجنايات المنصوص عليها في الباب الثالث من الكتاب الثاني من قانون العقوبات".

وبناءً عليه أضحى صدور الإذن بضبط الرسائل أو مراقبة المحادثات الهاتفية بالنسبة لجرائم أمن الدولة الخاضعة لقانون الطوارئ (١٦٢) لسنة ١٩٥٨ من اختصاص

الأمر إذ تقضى بعدم ترتيب أية مسئولية وعدم قبول أية دعوى على الحكومة أو موظفيها أو الرقيب العام بسبب أي إجراء اتخذ تنفيذًا لأعمال الرقابة المشار إليها- وهى أعمال وقرارات إدارية على ما سلف بيانه- تكون قد انطوت على مصادرة لحق التقاضي وإخلال بمبدأ المساواة بين المواطنين فى هذا الحق مما يخالف المادتين ٤٠، ٦٨ من الدستور.

وحيث إنه لما تقدم، يتعين الحكم بعدم دستورية نص المادة الثامنة من أمر رئيس الجمهورية رقم ١ لسنة ١٩٦٧الخاص بالرقابة..." (حكم المحكمة الدستورية العليا في الدعوى (٧) لسنة (٢) دستورية بجلسة ١٩٨٣/٢/٥، مكتب فني ٢، الجزء رقم ١، ص ٨٦).

[١٠] المعدلة بالقانون (١٤٥) لسنة ٢٠٠٦.

(ISSN: 2537- 0758)

النيابة العامة، ومن ثم لم يَعُدِ الأمر حكرا على القاضي الجزئي، كما يجوز لها– أيضًا– أن تندب أحد مأموري الضبط القضائي لتنفيذه[١١].

فقد استقر قضاء محكمة النقض على أنه "... لما كان ذلك، وكانت الفقرة الثانية من المادة ٧ من القانون رقم ١٠٥ لسنة ١٩٨٠ بإنشاء محاكم أمن الدولة قد نصَّت على أنه ((يكون للنيابة العامة– بالإضافة إلى الاختصاصات المقرَّرة لها– سلطاتُ قاضي التحقيق في الجنايات التي تختصّ بها محكمة أمن الدولة العليا)). كما نصّت المادة الثالثة من القانون ذاته على أن ((تختص محكمة أمن الدولة العليا دون غيرها بنظر الجنايات المنصوص عليها في الأبواب الأول والثاني مكرّر والثالث والرابع من الكتاب الثاني من قانون العقوبات)). فقد نصَّت أيضًا المادة ٩٥ من قانون الإجراءات الجنائية على أن ((لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاصّ متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحةٍ معاقَبٍ عليها بالحبس لمدة تزيد على ثلاثة أشهر)).

ومفاد النصوص المتقدِّمة أن القانون خوَّل للنيابة العامة سلطاتِ قاضي التحقيق– في أمور معينة من بينها الأمر بإجراء التسجيلات في الجنايات التي تختص بها محكمة أمن الدولة العليا ومنها جناية الرشوة– موضوع الدعوى الجنائية الماثلة– لما كان ذلك، فإن ما ردّ به الحكم وأطرح به الدفع ببطلان الإذن بالتسجيل لصدوره عن وكيل النيابة يكون قد أصاب صحيح القانون..."[١٢].

٢– **للنيابة العامة– في الجرائم الإرهابية**[١٣] المنصوص عليها في القانون (٩٤) لسنة ٢٠١٥ بشأن مكافحة الإرهاب– أن تصدر أمرًا مسبَّبًا بضبط المكاتبات والرسائل

---

[١١] تنص المادة (٢٠٠) من قانون الإجراءات الجنائية على أنه "لكل من أعضاء النيابة العامة في حالة إجراء التحقيق بنفسه أن يكلف أي مأمور من مأموري الضبط القضائي ببعض الأعمال التي من خصائصه".

[١٢] حكم محكمة النقض– جنائي– في الطعن رقم (٢٣٠٧) لسنة ٦١ ق بجلسة ١٩٩٣/١١/١٥، مكتب فني ٤٤، الجزء رقم ١، ص ٩٨٨.

[١٣] عرفها المشرّع المصري في المادة الأولى من القانون رقم ٩٤ لسنة ٢٠١٥ بشأن مكافحة الإرهاب، والمعدلة بالقانون رقم ١٥ لسنة ٢٠٢٠ على أنها "... كل جريمة منصوص عليها في هذا القانون،

العادية والمطبوعات والطرود والبرقيات بجميع أنواعها، وكذلك مراقبة وتسجيل المحادثات والرسائل التي ترد على وسائل الاتصال السلكية واللاسلكية وغيرها من وسائل الاتصال الحديثة(١٤).

وكذا كل جناية أو جنحة ترتكب باستخدام إحدى وسائل الإرهاب، أو بقصد تحقيق أو تنفيذ غرض إرهابي، أو بقصد الدعوة إلى ارتكاب أية جريمة مما تقدم أو التهديد بها، وذلك دون إخلال بأحكام قانون العقوبات.....".

كما عرف العمل الإرهابي في المادة الثانية منه على أنه "... كل استخدام للقوة أو العنف أو التهديد أو الترويع في الداخل أو الخارج، بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع أو مصالحه أو أمنه للخطر، أو إيذاء الأفراد أو إلقاء الرعب بينهم، أو تعريض حياتهم أو حرياتهم أو حقوقهم العامة أو الخاصة أو أمنهم للخطر، أو غيرها من الحريات والحقوق التي كفلها الدستور والقانون، أو الإضرار بالوحدة الوطنية أو السلام الاجتماعي أو الأمن القومي، أو إلحاق الضرر بالبيئة، أو بالموارد الطبيعية أو بالآثار أو بالأموال أو الأصول الأخرى أو بالمباني أو بالأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها، أو منع أو عرقلة السلطات العامة أو الجهات أو الهيئات القضائية أو مصالح الحكومة أو الوحدات المحلية أو دور العبادة أو المستشفيات أو مؤسسات ومعاهد العلم، أو البعثات الدبلوماسية والقنصلية، أو المنظمات والهيئات الإقليمية والدولية في مصر، من القيام بعملها أو ممارستها لكل أو بعض أوجه نشاطها، أو مقاومتها، أو تعطيل تطبيق أي من أحكام الدستور أو القوانين أو اللوائح.

وكذلك كل سلوك يرتكب بقصد تحقيق أحد الأغراض المبينة بالفقرة الأولى من هذه المادة، أو الإعداد لها أو التحريض عليها، إذا كان من شأنه الإضرار بالاتصالات أو بالنظم المعلوماتية أو بالنظم المالية أو البنكية، أو بالاقتصاد الوطني أو بمخزون الطاقة أو بالمخزون الأمني من السلع والمواد الغذائية والمياه، أو بسلامتها أو بالخدمات الطبية في الكوارث والأزمات".

(١٤) تنص المادة (٤٦) من القانون رقم (٩٤) لسنة ٢٠١٥ بشأن مكافحة الإرهاب على أنه " للنيابة العامة أو سلطة التحقيق المختصة، بحسب الأحوال، في جريمة إرهابية أن تأذن بأمر مسبَّب لمدة لا تزيد على ثلاثين يومًا، بمراقبة وتسجيل المحادثات والرسائل التي ترد على وسائل الاتصال السلكية واللاسلكية وغيرها من وسائل الاتصال الحديثة، وتسجيل وتصوير ما يجري في الأماكن الخاصة أو عبر شبكات الاتصال أو المعلومات أو المواقع الإلكترونية وما يدون فيها، وضبط المكاتبات والرسائل العادية أو الإلكترونية والمطبوعات والطرود والبرقيات بجميع أنواعها. ويجوز تجديد الأمر المشار إليه في الفقرة الأولى من هذه المادة مدة أو مددًا أخرى مماثلة".

(ISSN: 2537- 0758)

رئيس المحكمة الابتدائية:

ورد هذا الاختصاص بنص المادة (٩٥) مكرّر[١٥] من قانون الإجراءات الجنائية، التي جاء نصها على أنه "لرئيس المحكمة الابتدائية المختصة في حالة قيام دلائل قوية على أن مرتكب إحدى الجرائم المنصوص عليها في المادتين ١٦٦ مكررًا و٣٠٨ مكررًا من قانون العقوبات قد استعان في ارتكابها بجهاز تليفوني معيّن أن يأمر بناءً على تقرير مدير عام مصلحة التلغرافات والتليفونات وشكوى المجني عليه في الجريمة المذكورة بوضع جهاز التليفون المذكور تحت الرقابة للمدة التي يحددها".

وتتعلق الجرائم المنصوص عليها في المادتين ١٦٦ مكررًا[١٦] و٣٠٨ مكررًا[١٧] من قانون العقوبات بجرائم إزعاج الغير باستخدام أجهزة الاتصالات التليفونية وجرائم القذف باستخدام التليفون على الترتيب، ونظرًا لامتداد الإذن بمراقبة المحادثات الهاتفية في هاتين الحالتين لكافة المحادثات دون ثمة تحديد مما يشكل اعتداءً جسيمًا على خُصُوصية الطرف الآخر بخلاف مقدم الشكوى، لذا أناط المُشرِّع برئيس المحكمة الابتدائية إصدار الأمر بالمراقبة في هاتين الحالتين، وهو ما يشكل ضمانًا هامًّا لحماية حقوق الأفراد وحرياتهم.

٣- أن يكون الأمر الصادر بضبط المراسلات أو مراقبة المحادثات الهاتفية لمدة محدّدة:

أكد المُشرِّع الدُّسْتُوريّ الحالي في نص المادة (٥٧) منه ضرورةَ أن يكون الإذن الصادر بضبط المراسلات أو مراقبة المحادثات الهاتفية لمدة محدَّدة باعتبار الإذن

---

[١٥] المضافة بالقانون (٩٨) لسنة ١٩٥٥.

[١٦] تنص المادة (١٦٦) مكرر من قانون العقوبات (٥٨) لسنة ١٩٣٧، المضافة بالقانون (٩٧) لسنة ١٩٥٥ على أن "كل من تسبب عمدًا في إزعاج غيره بإساءة استعمال أجهزة المواصلات التليفونية يعاقب بالحبس مدة لا تجاوز سنة وبغرامة لا تزيد على مئة جنيه أو بإحدى هاتين العقوبتين".

[١٧] تنص المادة (٣٠٨) مكرر من قانون العقوبات، المضافة بالقانون (٩٧) لسنة ١٩٥٥ على أن " كل من قذف غيره بطريق التليفون يعاقب بالعقوبات المنصوص عليها في المادة ٣٠٣. وكل من وجه إلى غيره بالطريق المشار إليه بالفقرة السابقة سبًّا لا يشتمل على إسناد واقعة معينة، بل يتضمن بأي وجه من الوجوه خدشًا للشرف أو الاعتبار يعاقب بالعقوبة المنصوص عليها في المادة ٣٠٦.

وإذا تضمن العيب أو القذف أو السب الذي ارتكب بالطريق المبين بالفقرتين السابقتين طعنًا في عِرض الأفراد أو خدشًا لسمعة العائلات يعاقب بالعقوبة المنصوص عليها في المادة ٣٠٨".

الصادر في هذا الشأن إجراءً من إجراءات التحقيق المقيّدة بغايتها، فلا يجوز أن يمتدَّ الإذن إلى مدة غير محدَّدة حمايةً لحريات الأفراد وحقّهم في الخُصُوصية.

وهذه المدة لا تختلف سواء كان مصدر الإذن النيابة العامة أو قاضي التحقيق أو القاضي الجزئي، كما تعدُّ حدًّا أقصى لا يمكن تجاوزه عند إصدار الأمر، وقد قدَّر المُشرِّع تلك المدة في قانون الإجراءات الجنائية- المادتين (٩٥، ٢٠٦)- وكذلك قانون مكافحة الإرهاب- المادة (٤٦)- بثلاثين يومًا.

ويقتضي تطبيق هذا الشرط أن يكون تنفيذ الإذن تحت رقابة القاضي سواءٌ كان القاضي الجزئي أم قاضي التحقيق، وهو ما يستلزم إعداد تقرير يومي من القائم بتنفيذ الإذن حتى يمكن الوقوف على حقيقة الأمر، والتحقق من أن الغرض من تنفيذ الإذن قد تحقق قبل انتهاء المدة المحدّدة به[١٨].

ويتعين أيضًا عدم تجديد الأمر إلا إذا وجدت مبرِّرات ضرورية تقتضي هذا التجديد وتختلف عن الأسباب التي برَّرت صدوره في المرة الأولى.

ثانيا: الشروط الموضوعية:

١- أن تكون الجريمة المسندة إلى المتهم جناية أو جنحة معاقب عليها بالحبس مدة لا تقل عن ثلاثة أشهر:

الأمر بضبط المراسلات أو مراقبة المحادثات الهاتفية من إجراءات التحقيق التي لا يجوز مباشرتها إلا بمناسبة وقوع جريمة، تلك الجريمة التي يجب أن يكون معاقبًا عليها بالحبس مدة لا تقلّ عن ثلاثة أشهر، وهو ما يستفاد من نص المادتين (٩٥، ٢٠٦) من قانون الإجراءات الجنائية.

وتبدو الحكمة التي توخَّاها المُشرِّع من تقييد صدور الإذن في جرائم بعينها في أنه نظرًا لخطورة ذلك الإجراء الذي يُعدُّ عدوانًا على خُصُوصية الأفراد، فقد حرَص المُشرِّع على عدم اللجوء إليه إلا في الجرائم ذات القدر العالي من الجسامة، إلا أن هذا المعيار كان عرضة للانتقاد من جانب البعض لشموله معظم الجنح التي نصّ عليها قانون العقوبات، والتي قد لا تستدعي اللجوء إلى هذا الإجراء، كما أن مقدار العقوبة، وإن كان أحد المعايير الدالة على خطورة الجريمة وجسامتها، إلا أنه ليس المعيار الوحيد، فهناك معايير أخرى ينبغي أخذها في الاعتبار كالأثر الاجتماعي للجريمة أو الآثار الاقتصادية لها وغيرها من صور الانتهاك المؤثرة التي لا يجوز اختزالها في مقدار العقوبة.

---

[١٨] د. رمزي رياض عوض، الحق في الخصوصية، دار النهضة العربية، القاهرة، ٢٠١٦، ص١٤٣.

(ISSN: 2537- 0758)

ويتطلَّب هذا الشرط وجوب أن يكون الأمر مستندًا إلى تحريات جدية، فقد استقر قضاء محكمة النقض على أن "... الإذن الأول الصادر بالمراقبة والتسجيل قد بني على مجرَّد معلومات وردت إلى المأذون له بصورة مرسلة، وأنه لم يجرَ بشأنه أيُّ تحريات حسبما جرت أقواله في تحقيقات النيابة العامة قبل حصوله على الإذن، ومن ثم يبطل هذا الإذن، كما يستطيل هذا البطلان إلى الأذون التالية له، لأنها جاءت امتدادًا له..."[١٩].

٢- أن يكون الإذن مفيدًا في كشف حقيقة الجريمة المرتكبة:

الأمر بضبط المراسلات أو مراقبة المحادثات الهاتفية يجب أن يهدف إلى تحقيق غاية محددة، تلك الغاية التي حدّدتها المادة (٩٥) من قانون الإجراءات الجنائية المتمثلة في "...متى كان لذلك فائدة في ظهور الحقيقة..."، ونصّت عليها أيضًا المادة (٢٠٦) من قانون الإجراءات الجنائية فقد نصّت على أنه "...متى كان لذلك فائدة في ظهور الحقيقة...".

فإذا لم يحقق الأمر تلك الغاية فلا يكون له فائدة في الكشف عن الحقيقة في خصوص الجريمة المرتكبة، ويضحى بالتالي اعتداءً على حريات الأفراد بصورة تنال من حقهم الدُّسْتُوريّ في الخُصُوصية.

إلا أن غاية "ظهور الحقيقة" ليست سندًا مطلقًا يبرر إصدار الأمر، فلا يجوز ضبط المراسلات أو مراقبة المحادثات الهاتفية إذا تعلق الأمر بضمان حق الدفاع في العلاقة بين المتهم والمدافع عنه، فقد نصَّت المادة (٩٦) من قانون الإجراءات الجنائية على أنه: "لا يجوز لقاضي التحقيق أن يضبط لدى المدافع عن المتهم أو الخبير الاستشاري الأوراق والمستندات التي سلمها المتهم لهما لأداء المهمة التي عهد إليهما بها ولا المراسلات المتبادلة بينهما في القضية".

وإذا كانت المادة المشار إليها قد اقتصرت على "المراسلات المتبادلة" إلا أن الفقه ذهب- وبحق- إلى عدم جواز مراقبة المحادثات الهاتفية قياسًا على الأوراق والمراسلات، طالما كانت متعلقة بمهمة الدفاع، كما أعطت محكمة النقض عبارة "المراسلات المتبادلة" مدلولًا واسعًا يندرج تحته المكالمات الهاتفية[٢٠].

---

[١٩] حكم محكمة النقض- جنائي- في الطعن رقم (٨٧٩٢) لسنة ٧٢ ق بجلسة ٢٠٠٢/٩/٢٥، مكتب فني ٥٣، ص ٨٧٦.

[٢٠] د. رمزي رياض عوض، مرجع سابق، ص١٣٣.

ثانياً: رسائل الاتصال الإلكتروني، والمحادثات الإلكترونية:

تنص المادة (٦) من القانون (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات على أن "لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمرًا مسبَّبًا لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين يومًا قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، **بواحد أو أكثر مما يأتي:**

١- ضبط أو سحب أو جمع أو التحفُّظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر، على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتضًى.

٢- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقًا لغرض الضبط.

٣- أن تأمر مقدِّم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو الجهاز التقني. وفي كل الأحوال، يجب أن يكون أمر جهة التحقيق المختصة مسببًا. ويكون استئناف الأوامر المقدّمة أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة، في المواعيد ووفقًا للإجراءات المقرَّرة بقانون الإجراءات الجنائية".

ويستفاد من هذا النص أن يُشترط لضبط رسائل الاتصال الإلكتروني أو مراقبتها، والتي تنطبق كذلك على المحادثات الإلكترونية، **عدةُ شروط تتمثل في:**

أولًا: الشروط الشكلية:

١- أن يكون الأمر الصادر بضبط المراسلات أو مراقبة المحادثات الإلكترونية مسبَّبًا:

يقتضي هذا الشرط أن يكون صدور الأمر بمناسبة جريمة وقعت بالفعل، وأن تتوافر دلائل جدية على قيام أحد الأشخاص بارتكابها.

٢- أن يكون الأمر الصادر بضبط المراسلات أو مراقبة المحادثات الإلكترونية لمدة محددة:

يجب أن يكون الأمر الصادر بالضبط أو المراقبة مؤقتًا بمدة محدّدة تكفّلت بتحديدها المادة (٦) من القانون (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات بثلاثين يومًا قابلة للتجديد مرة واحدة فقط، حماية لحق الأفراد في الخُصُوصية.

(ISSN: 2537- 0758)

ثانياً: الشروط الموضوعية:

١- أن تكون الجريمة المسندة إلى المتهم من الجرائم المنصوص عليها في القانون (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات:

يجب أن تكون الجريمة الصادر بشأنها الأمر بضبط المراسلات أو المحادثات الإلكترونية من الجرائم المنصوص عليها في الفصل الأول من الباب الثالث من القانون (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، المعاقب على أدناها بالحبس مدة لا تقل عن شهر.

ويؤخذ على هذا القانون، أنه قصر اللجوء إليه عند ارتكاب إحدى الجرائم المنصوص عليها فيه، فلم يمدَّ أحكامه إلى الجرائم المنصوص عليها في قانون العقوبات، والتي قد تعدُّ في أغلب الأحوال أشدَّ جسامة من تلك الجرائم بشكل يبرِّر اللجوء لهذا الإجراء بهدف كشف الحقيقة في أمر الجريمة المرتكبة.

٢- أن يكون الأمر مفيدًا في كشف حقيقة الجريمة المرتكبة:

يجب أن تكون غاية الأمر الصادر بالضبط أو المراقبة باعتباره من إجراءات التحقيق- وَفْقًا لما نصَّت عليه المادة (٦) من القانون (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات- هي الوصول إلى الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكامه.

فإن لم يكن اتخاذ هذا الإجراء مرهونًا بتحقيق تلك الغاية، فقد غدا إجراءً تعسفيًّا ينال بصورة تحكُّمية من حقِّ الفرد في الخُصُوصية.

الجرائم الإرهابية:

تنص المادة (٤٦) من القانون رقم (٩٤) لسنة ٢٠١٥ بشأن مكافحة الإرهاب على أن "للنيابة العامة أو سلطة التحقيق المختصة، بحسب الأحوال، في جريمة إرهابية- أن تأذن بأمر مسبَّب لمدة لا تزيد على ثلاثين يومًا، بمراقبة وتسجيل المحادثات والرسائل التي ترد على وسائل الاتصال السلكية واللاسلكية وغيرها من وسائل الاتصال الحديثة، وتسجيل وتصوير ما يجري في الأماكن الخاصة أو عبر شبكات الاتصال أو المعلومات أو المواقع الإلكترونية وما يُدوَّن فيها، وضبط المكاتبات والرسائل العادية أو الإلكترونية والمطبوعات والطرود والبرقيات بجميع أنواعها. ويجوز تجديد الأمر المشار إليه في الفقرة الأولى من هذه المادة مدة أو مددًا أخرى مماثلة".

ووَفقًا لهذا النص فإن المُشرّع أجاز لسلطة التحقيق المختصة في الجرائم الإرهابية إصدارَ أمر بضبط أو مراقبة المراسلات أو المحادثات الإلكترونية بذات الشروط الشكلية أو الموضوعية التي سبق تناولها، ومن ثم فإننا نكتفي بالإحالة إليها منعًا للتكرار.

وتتمثل الحكمة من هذا النصّ في أنه نظرًا لخطورة الجرائم الإرهابية وتأثيرها الجسيم على أمن المجتمع وسلامته، الأمر الذي يبرر انتهاك خُصُوصية الأفراد على النحو الوارد به.

المبحث الثاني
ضوابط المساس بحُرْمة الاتصالات الخاصة في القانون الأمريكي

ينقسم قانون خُصُوصية الاتصالات الإلكترونية (ECPA) إلى ثلاثة أقسام: **القسم الأول:** قانون مراقبة الاتصالات السلكية واللاسلكية[٢١] والذي حدَّد الإجراءات القضائية الواجبة الاتباع لاعتراض هذا النوع من الاتصالات بهدف تطبيق أحكام القانون، **القسم الثاني:**ويطلق عليه قانون الاتصالات الإلكترونية المخزنة(SCA Act)[٢٢]تناول الحماية الموضوعية لجميع الاتصالات الإلكترونية في مرحلة التخزين الإلكتروني، مثل البريد الإلكتروني، كما عُني ببيان آلية الكشف عن محتوى تلك الاتصالات في هذه المرحلة، **القسم الثالث:** ويطلق عليه قانون التسجيل والتقصي(Register Act–Pen)[٢٣] حرَص من خلاله على بيان الإجراءات القانونية اللازمة لاستخدام أجهزة التتبُّع.

وسوف نتناول فيما يلي تحديد مفهوم المراقبة في القانون الأمريكي، ونُتبعه ببيان الضوابط التي وضعها لمراقبة الاتصالات الخاصة.

المطلب الأول
مفهوم المراقبة في القانون الأمريكي

عرَّف قانون خُصُوصية الاتصالات الإلكترونية (ECPA) "المراقبة" الاعتراض– intercept في الفقرة (٤) من المادة (٢٥١٠)– بأنها "الحصول على المحتويات السمعية أو المحتويات المتعلقة بأي أنواع مختلفة من الاتصالات عن طريق الأجهزة الإلكترونية أو الميكانيكية أو بواسطة أي وسيلة أخرى"[٢٤].

---

(21) 18 U.S.C. 2510-2522. This part of ECPA was originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510-2520 (1964 ed,) (Supp. IV).

(22) 18 U.S.C. 27-1-2712.

(23) 18 U.S.C. 3121-3127.

(24) 18 U.S.C. 2510(4) "“intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device"

(ISSN: 2537- 0758)

كما تناولت الفقرة (٥) من ذات المادة تحديد مفهوم الوسيلة بأنها "أي وسيلة أو أداة يمكن أن تستخدم لمراقبة الاتصالات السلكية أو الشفهية أو الإلكترونية"[٢٥].

وبرغم أن المنطق يفترض حدوث المراقبة أو الاعتراض يحدث في المكان الذي يتم فيه التقاط الاتصال، إلا أن التطبيقات القضائية أشارت إلى إمكانية حدوث الاعتراض في المكان الذي يبدأ منه الاتصال أو ينتقل أو عند استقباله[٢٦].

وبناءً على هذا التعريف، فإن المراقبة أو الاعتراض لا تشمل الحالة التي يقرأ الفرد فيها أو يستمع إلى ملف اتصال تم اعتراضه مسبقًا[٢٧].

ونستخلص مما تقدّم، أن هناك نوعًا من الإجماع حول وقت حدوث الاعتراض "المراقبة"، فالاعتراض هو الاستحواذ الخفي الذي يحدث إما في وقت متزامن مع وقت الإرسال أو في الوقت الذي يسبق وصول الاتصال بالمرسل إليه[٢٨].

---

(25) 18 U.S.C. 2510(5) "“electronic, mechanical, or other device” means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—..."

(26) United States v. Luong, 471 F.3d 1107, 1109 (9th Cir. 2006) (“an interception occurs where the tapped phone is located and where the law enforcement officers first overheard the call) "

"يحدث الاعتراض؛ حيث يوجد الهاتف وحين يقوم الضباط القائمين على تنفيذ القانون بسماع المكالمة لأول مرة".

United States v. Ramirez, 112 F.3d 849, 852 (7th Cir. 1997) (concluding that an Interception occurs in the jurisdiction where the tapped phone is located, where the second phone in the conversation is located, and where the scanner used to overhear the call is located)

"يحدث الاعتراض؛ حيث يوجد الهاتف المُرسل، أو المُستقبل أو الجهاز المستخدم لسماع الاتصال".

(27) Noel v. Hall, 568 F.3d 743, 749 (9th Cir. 2009)(“In reaching this conclusion, we join a number of other circuits that have held that replaying of tapes containing recorded phone conversations does not amount to a new interception in violation of the Wiretap Act”), citing inter alia, United States v. Hammond, 286 F.3d 189, 193 (4th Cir. 2002)

"أجمعت المحاكم على أن إعادة تشغيل الأشرطة التي تحتوي على محادثات هاتفية مسجلة لا يمكن أن تعد من قبيل الاعتراض في تطبيق قانون التنصت على المكالمات الهاتفية".

(28) United States v. Councilman, 418 F.3d 67, 79-80(1st Cir. 2005) (en banc)(service provider’s access to email “during transient storage” constitutes “interception”; without deciding whether “interception is limited to acquisition contemporaneous with transmission”).

المطلب الثاني
ضوابط إصدار الأمر بمراقبة الاتصالات الخاصة:

أولًا: مراقبة الاتصالات السلكية أو الإلكترونية:

تسمح المادة (٢٥١٨) من قانون خُصُوصية الاتصالات الإلكترونية (ECPA) بمراقبة الاتصالات السلكية أو الإلكترونية بعد الحصول على موافقة مسئول قضائي عالي المستوى (النائب العام، نائب المدّعي العام، المدّعي العام المساعد، أو أي مساعد للمدعي العام...)[٢٩]، يُقدَّم الطلب إلى قاضي ذي سلطة قضائية مختصة، إلا أن المُشرِّع قد فرق في تحديد صفة من يُقدَّم إليه الطلب، وذلك بحسب نوع الجريمة التي يجري التحقيق بشأنها سواء تم ارتكابها أو انعقدت النية على ارتكابها.

"يعد وصول مزود الخدمة إلى البريد الالكتروني في مرحلة " التخزين المؤقت " اعتراضا دون الإشارة إلى ضرورة أن يكون هذا الوصول متزامنا مع الإرسال "

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) (fraudulent access to stored communication does not constitute an"interception"; interception requires access contemporaneous with transmission)

"الوصول الاحتيالي إلى الاتصالات المخزنة لا يشكل اعتراضا فالاعتراض يتطلب وصولا متزامنا مع الإرسال".

United States v. Jones, 451 F.Supp.2d 71, 75 (D.D.C. 2006) (government's acquisition from the phone company of text messages was no interception because there was no contemporaneous access)

"وصول الحكومة إلى الرسائل النصية من خلال شركة الهاتف لا يشكل "اعتراض" لعدم وجود وصول متزامن"

(29) "The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of [the predicate offenses]..."

(ISSN: 2537- 0758)

فإذا كانت تلك الجريمة جريمة فيدرالية– على النحو المبيَّن بالمادة (٢٥١٦) من ذات القانون– فإن طلب الاعتراض والمراقبة يُقدَّم إلى القاضي الاتحادي، أما إذا كانت الجريمة من الجرائم المشار إليها وَفْقًا لقانون الولاية فإن طلب الاعتراض يُقدَّم إلى قاضي الولاية المختص.

ويَشترط القانون لإصدار هذا الطلب أن يكون هناك سببٌ محتملٌ يدعو للاعتقاد بأن التنصت على الاتصالات الهاتفية أو الإلكترونية سوف يؤدي إلى الوصول إلى دليل في شأن جريمة فيدرالية مرتكبة[٣٠] أو يرشد عن أماكن الأشخاص الهاربين من الملاحقة القضائية في إحدى الجنايات الأصلية[٣١].

ويجب أن يتضمن الإذن البيانات الآتية[٣٢]:

---

(30) The list appears in 18 U.S.C. 2516(1).

(31) 18 U.S.C. 2516(1)(l).

(32) 18 U.S.C. 2518 " (1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

١- هوية مقدِّم الطلب، وكذلك المسئول الذي أذِن بتقديمه.
٢- البيان الكامل للحقائق بما في ذلك (تفاصيل الجريمة، وصف خاص لطبيعة وموقع ومكان الاعتراض[٣٣]، وصف خاص للاتصالات التي سيتم اعتراضها، هوية مرتكب الجريمة وهوية الأشخاص الذين سوف يتم اعتراض اتصالاتهم).
٣- البيان الكامل حول أساليب التحقيق الأخرى التي تم استخدامها، توصلًا لأسباب عدم فاعليتها أو خطورتها.
٤- بيان الفترة الزمنية التي يحدث فيها الاعتراض، وإذا لم يُسفر هذا الاعتراض عن الوصول للهدف المنشود يجب بيان الوقائع التي يمكن أن تشكل سببًا محتملًا يدعو للاعتقاد بأن اتصالات من ذات النوع سوف تحدث مستقبلًا.
٥- البيان كامل بشأن كافة عمليات الاعتراض التي تمت في ذات الأماكن أو بالنسبة لنفس الأشخاص.
٦- عندما يتعلق الطلب بتجديد إذن الاعتراض، يجب إيضاح النتائج التي تم الوصول إليها خلال مدة الاعتراض، أو تفسير معقول للفشل في الحصول على هذه النتائج.
٧- يجوز للقاضي أن يطلب من مقدِّم الطلب تقديم بعض الأدلة لدعم الطلب.

ومما لا شكَّ فيه أن تضمن الإذن بهذه البيانات يكفل عدم استخدام هذا الإجراء بما يتضمنه من انتهاك خطير للحق في الخُصُوصية، إلا لتحقيق الغرض المنصوص عليه قانونًا.

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and
(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.
(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application….."

(33) Identification of the place where, or facilities over which, the targeted communications are to occur may be excused where the court finds that the suspect has or will take steps to thwart interception, 18 U.S.C. 2518(11), (12); United States v. Oliva, 686 F.3d 1106, 1109-110 (9th Cir. 2012).

"قد يتعذر تحديد الأماكن التي تجري فيها الاتصالات المستهدفة إذا وجدت المحكمة أن المشتبه فيه سوف يتخذ إجراءات من شأنها إحباط عملية المراقبة"

(ISSN: 2537- 0758)

كما يجب على المحكمة قبل إصدار الأمر أن تتحقق من[٣٤]:

١- وجود سبب محتمل يدعو للاعتقاد بأن أحد الأفراد قد ارتكب جريمة من الجرائم المنصوص عليها في المادة (٢٥١٦) من هذا القانون، أو على وشك ارتكابها.

٢- وجود سبب محتمل يحمل الاعتقاد بأن اتصالات معينة متعلقة بتلك الجريمة سوف يتم الحصول عليها من جراء هذا الاعتراض.

٣- ثبوت عدم جدوى استخدام إجراءات التحقيق الأخرى عند إجرائها أو أن يكون من المرجَّح فشلها أو أن يترتب على استخدامها نتائج خطيرة.

وقد استقر قضاء المحكمة العليا الأمريكية على أنه "يجب على مقدِّم الطلب كما يجب على المحكمة كذلك، أن تجد أن إجراءات التحقيق المعتادة التي تم استخدامها قد باءت بالفشل في كشف غموض الجريمة أو كان من المرجَّح أن يترتب على استخدامها نتائج خطيرة يتعذر تداركها"[٣٥].

---

(34) 18 U.S.C. 2518 "….(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction ofthe court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be

obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person…."

(35) "the applicant must state and the court must find that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous. §§2518(1)(c) and (3)(c)," United States v. Giordano, 416 U.S. 505, 515 (1974).

٤- وجود سبب محتمل يدعو للاعتقاد بأن المكان الذي يتم اعتراض الاتصالات السلكية أو الشفوية أو الإلكترونية منه يستخدم أو يرجّح أن يستخدم في أعمال ذات صلة بالجريمة، أو أن تكون تلك الأماكن مؤجَّرة لهذا الشخص أو مدرجة باسمه أو شائعة الاستخدام من خلاله.

وقد استقر القضاء الأمريكي على أنه "يقصد بشرط الضرورة": "ضمان عدم استخدام الاعتراض كإجراء أولي في التحقيق، إلا أن ذلك لا يعني استنفاذ كافة إجراءات التحقيق الأخرى قبل اللجوء إلى إجراء التنصُّت على الاتصالات الخاصة"[٣٦].

تجدر الإشارة هنا إلى أنّ بعض المواقف العاجلة قد تبرِّر تأجيل الامتثال لتلك الإجراءات إلى ما بعد إجراء المراقبة بالفعل، بشرط موافقة كبار مسئولي وزارة العدل وتحقُّق إحدى الحالات الطارئة[٣٧] **المتمثلة في:**

---

(36) "[t]he necessity requirement was intended to ensure that wiretaps are not used as the initial step in a criminal investigation. However, officials need not exhaust every conceivable investigative technique before obtaining a wiretap." United States v. Forrester, 616 F.3d 929, 944 (9th Cir. 2010) (internal citations omitted); see also, United States v. Long, 639 F.3d 293, 301 (7th Cir. 2011).

(37) 18 U.S.C. 2518 "...(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists that involves—

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such

(ISSN: 2537- 0758)

(أ) وجود خطر حالة أن يترتب عليه وفاة أو إصابة جسدية خطيرة.
(ب)أي نشاط مخالف للقانون من شأنه أن يهدِّد الأمن القومي.
(ت)أي نشاط مخالف للقانون يتعلق بالجريمة المنظمة.

وفي حالة تحقُّق أيٍّ من تلك الحالات يجب أن يتم تقديم طلب لاستصدار أمر بالاعتراض في غضون (٤٨) ساعة من تاريخ حدوث الاعتراض الذي ينتهي فور الحصول على الاتصال المنشود أو حال رفض المحكمة إصدار الأمر أيهما أسبق.

وفي تلك الحالة الأخيرة يُعدُّ سلوك الاعتراض مخالفًا لصحيح حكم القانون مما يحول دون الاستناد إلى تلك الاتصالات المعترضة أو الدليل المستمد منها.

مدة الأمر بالاعتراض[٣٨]:

يتم تنفيذ أمر الاعتراض للمدة اللازمة لتحقيق الهدف منه والتي يجب ألا تتجاوز بأي حال من الأحوال (٣٠) يومًا، ويجوز تجديد تلك المدة عن طريق اتخاذ ذات الخطوات المتبعة في إصدار الأمر الأصلي.

تنفيذ الأمر بالاعتراض:

<u>يجب أن يراعى في تنفيذ هذا الأمر:</u>

١- أن ينفذ بطريقة تقلل من مراقبة الاتصالات "البريئة" غير الخاضعة للاعتراض.

وقد أرست المحكمة العليا الأمريكية عددًا من الضوابط[٣٩] لتفادي مراقبة الاتصالات البريئة حتى يكون تنفيذ أمر الاعتراض متسقًا مع التعديل الدُّسْتُوريّ الرابع، ومن تلك

application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communicationintercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall beserved as provided for in subsection (d) of this section on the person named in the application..."

(38) 18 U.S.C. 2518(5).

(39) we consider the factors identified by the Supreme Court (1) whether a large number of the calls are very short, one-time only, or in guarded or coded language; (2) the breadth of the investigation underlying the need for the wiretap; (3) whether the phone is public or private; and (4) whether the non-minimized calls occurred early in the surveillance. 436 U.S. at 140-41. It is also appropriate to consider (5) the extent to which the authorizing judge supervised the ongoing wiretap. United States v. Lopez, 300 F.3d 46, 57 (1st Cir. 2002); United States v. Daly, 535 F.2d 434, 442 (8th Cir. 1976); United States v. Vento, 533 F.2d 838, 853 (3d Cir. 1976).

الضوابط (ما إذا كان عدد كبير من المكالمات تتم لمدد قصيرة جدًّا أو تتم لمرة واحدة فقط أو تتم بلغة محمية أو مشفَّرة، ما إذا كان الهاتف عامًّا أو خاصًّا، حدوث مكالمات مطوَّلة في وقت مبكر من عملية المراقبة...).

٢- أن ينتهي تنفيذه عند الوصول للهدف المصرَّح به.

انتهاء الأمر بالاعتراض:

بعد الانتهاء من تنفيذ أمر الاعتراض يجب أن يتم تسجيل الاتصالات التي تم اعتراضها وتأمين الأدلة وختمها مع الاحتفاظ بنسخ إضافية ضرورية لتطبيق القانون وتنفيذ أمر المحكمة[٤٠].

كما يجب إخطار الأشخاص الذين تم اعتراض الاتصالات الخاصة بهم في موعد غايته (٩٠) يومًا من تاريخ تقديم الطلب حالَ رفضه أو من تاريخ انتهاء الاعتراض حال الموافقة عليه[٤١].

كما لا يجوز تقديم الأدلة الناتجة عن عملية الاعتراض أو الكشف عنها في أي محاكمة إلا بعد مرور (١٠) أيام من إخطار كافة أطراف عملية الاعتراض بنسخة من أمر المحكمة الصادر بالاعتراض مرفقًا به الطلب الذي تم بموجبه إصدار هذا الأمر.

وللقاضي التجاوز عن هذا الإجراء إذا لم يكن الإخطار ممكنًا بالإضافة إلى عدم تأثر الطرف صاحب المصلحة من جراء التأخير[٤٢].

ثانيا: الوصول إلى الاتصالات في مرحلة التخزين الإلكتروني:

أثارت مسألة اتساع عملية المراقبة لتشمل الاتصالات غير المتزامنة، خلافًا في القضاء الأمريكي- وَفْقًا لما سبق بيانه- لذا فإننا نرى أنه من الضروري التعرض للضوابط التي وضعها المُشرِّع الأمريكي للوصول إلى ذلك النوع من الاتصالات.

نظمت المادة (٢٧٠٣) من قانون خُصُوصية الاتصالات الإلكترونية (ECPA) الحالات التي يطلب فيها من مزوِّدي الخدمة الكشف عن محتوى الاتصال وما يتصل به من بيانات، والتي ميزت بين الاتصالات المخزنة لمدة (١٨٠) يومًا على الأقل، وبين الاتصالات المخزنة لمدة تجاوز هذه المدة.

---

(40) 18 U.S.C. 2518(8)(a),(b).
(41) 18 U.S.C. 2518(8)(d).
(42) 18 U.S.C. 2518 (9).

(ISSN: 2537- 0758)

بالنسبة للحالة الأولى (الاتصالات المخزنة لمدة (١٨٠) يومًا على الأقل)[٤٣]: يصدر أمر قضائي لمزوِّد خدمة الاتصالات الإلكترونية وَفْقًا للقواعد الفيدرالية للإجراءات الجنائية.

أما الحالة الثانية (الاتصالات المخزنة لمدة تجاوز "١٨٠" يومًا)[٤٤]: وَفْقًا للفقرة (د) من المادة (٢٧٠٣) من ذات القانون يصدر الأمر القضائي عن المحكمة الاتحادية أو محكمة المقاطعة أو أيّ محكمة استئناف داخل الولايات المتحدة ذات اختصاص بشأن الجريمة قيد التحقيق[٤٥].

(43) 18 U.S.C. 2703 "(a) Contents of wire or electronic communications in electronic storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in a wire or electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction..."

(44) 18 U.S.C. 2703 "(a)….. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section….."

(45) 18 U.S.C. 2703(d)("A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction..."); 18 U.S.C. 2711(3)("As used in this chapter... (3) the term 'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation"); 18 U.S.C. 3127(2)(emphasis added) ("As used in this chapter... (2) the term "court of competent jurisdiction" means—(A) any district court of the United States (including a magistrate of such a court) or a United States Court of Appeals having jurisdiction over the offense being investigated..."), with, 18 U.S.C. 2516(3)("Any attorney for the Government... may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant... an order authorizing or approving the interception of electronic communications..."); 18 U.S.C. 2510(9)(" As used in this chapter... 'Judge of competent jurisdiction' means—(a) a judge of a United States district court or a United States court of appeals").

ولا يشترط إصدار الأمر من المحكمة التي يقع في دائرتها مزوِّد الخدمة، وإنما تختلف المحكمة "مصدرة الأمر" باختلاف الولاية القضائية على الجريمة محَلّ التحقيق(٤٦).

ويشترط لإصدار الأمر أن توضّح الجهةُ الحكومية طالبة الأمر وجودَ أسباب معقولة للاعتقاد بأن محتويات الاتصال أو السجلات والمعلومات المتعلقة به ذات صلة بتحقيق جنائي جارٍ(٤٧).

وقد ارتأت بعض المحاكم أن معيار "الأسباب المعقولة "يعادل معيار" تيري– Terry" الذي يتطلب ضمانات أقلَّ من تلك التي يتطلبها القانون في معيار "السبب المحتمل" وبالتالي فإنه– في بعض الحالات– قد يكون غير كافٍ من الناحية الدُّسْتُورية لتبرير وصول الحكومة إلى البريد الإلكتروني مخزَّنًا.

فقد ذهبت الدائرة السادسة لمحكمة استئناف الولايات المتحدة إلى أنّ التعديل الدُّسْتُوريّ الرابع يحظر وصول الحكومة إلى محتويات الاتصالات الإلكترونية المخزَّنة في حالة عدم وجود مذكرة أو موافقة صريحة من المشترك أو أي إشارة أخرى تفيد تنازل المشترك عن توقعاته بشأن الخُصُوصية(٤٨).

كما أجاز القانون للمحكمة– بناء على اقتراح من مزوِّد الخدمة– إلغاءَ الأمر أو تعديلَه إذا كانت البيانات أو المعلومات المطلوبة ذات طبيعة ضخمة أو حالَ كون الامتثال للأمر سوف يرتب أعباء لا قِبل لمزوِّد الخدمة بها.

---

(46) United States v. Berkos, 543 F.3d 392, 397 (7th Cir. 2008), quoting 18 U.S.C. 2703(a), ("[W]hen 'a court with jurisdiction over the offense' issues an out-of-district warrant for the seizure of electronic communications, it must do so 'using the procedures described in the Federal Rules of Criminal Procedure'"); see also, 18 U.S.C. 2711(3).

(47) 18 U.S.C. 2703(d) " Requirements for court order.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider….."

(48) United States v. Warshak, 631 F.3d 266, 283, 290 n.21 (6th Cir. 2010).

(ISSN: 2537- 0758)

وتلتزم الجهة الحكومية بإخطار المشترك أو العميل الذي يتم الكشف عن اتصالاته في الحالات المنصوص عليها في المادة (٢٧٠٣)[٤٩]، ما لم تأذن المحكمة– بناء على شهادة من كيان حكومي– بتأجيل هذا الإخطار لمدة تصل إلى (٩٠ يومًا) لما قد يسبِّبه الإشعار المعاصر للكشف من أثر سلبي على مجرى التحقيق[٥٠].

وقد عددت المادة (٢٧٠٥) الحالات التي تبرّر تأجيل الإخطار، والتي تتمثل في[٥١]:

١– تعريض حياة الفرد أو سلامته الجسدية للخطر.

٢– إتلاف الأدلة أو التلاعب بها.

٣– الهروب من المحاكمة.

٤– تهديد الشهود المحتملين.

٥– تعريض التحقيق للخطر أو تأخير المحاكمة دون مقتضى.

ثالثا: أجهزة المراقبة والتتبع:

سمح القانون الأمريكي لمدَّعي الحكومة الفيدرالية أو ضباط التحقيق وكذلك ضباط الشرطة المحليّين أن يتقدموا بطلبٍ إلى المحكمة المختصة للحصول على إذن تثبيت جهاز "قلم التسجيل"[٥٢]، أو "جهاز تتبع"[٥٣]، **ويجب أن يتضمن هذا الطلب البيانات الآتية[٥٤]:**

---

(49) 18 U.S.C. 2703 (b) (2) (B).

(50) 18 U.S.C. 2705(a)(1)(B), (4) " …. Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section……"

(51) 18 U.S.C. 2705(a) "….. (2) An adverse result for the purposes of paragraph (1) of this subsection is—
(A) endangering the life or physical safety of an individual;
(B) flight from prosecution;
(C) destruction of or tampering with evidence;
(D) intimidation of potential witnesses; or
(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial….."

(52) 18 U.S.C. 3127 " As used in this chapter—……. (3) the term “pen register” means a device or process which records or decodes or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication, but

١- هوية مقدمه، وهوية الجهة القائمة على التحقيق.
٢- شهادة من مقدم الطلب تفيد بأن المعلومات التي يحتمل الحصول عليها ذات صلة بتحقيق جنائي جارٍ تجريه تلك الجهة.

ويجب أن يتضمن الأمر الصادر بتثبيت الجهاز عدة بيانات تتمثل في:

١- هوية الشخصِ صاحب الهاتف إذا تم الوصول إليها، أو المدرجِ باسمه هذا الهاتف، والمنشأة التي يتم فيها تركيب الجهاز.
٢- هوية الشخص الخاضع للتحقيق إذا تم الوصول إليها.
٣- رقم خط الهاتف المستهدف والنطاق الجغرافي للجهاز.
٤- بيان الجريمة التي تتعلق بها المعلومات التي يحتمل الحصول عليها من خلال الجهاز (٥٥).

---

such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;……"

"قلم التسجيل" هو جهاز يقوم على تسجيل أو فك شفرة بيانات الاتصال أو إرسال بيانات هذا الاتصال عن طريق أداة بشرط ألا تتضمن تلك البيانات محتوى هذه الاتصالات، كما لا تشمل الأجهزة التي يستخدمها مزود خدمة الاتصالات لحساب تكلفة الخدمة أو القيام بأي مهمة أخرى في سياق العمل.

(53) 18 U.S.C. 3127 " As used in this chapter—…….(4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;……"

"جهاز التتبع" هو جهاز أو عملية من شأنها التقاط النبضات الالكترونية الواردة أو النبضات الأخرى التي تحدد رقم الاتصال الأصلي أو البيانات الأخرى المتعلقة بالاتصال بشرط ألا تتضمن تلك البيانات محتوى هذه الاتصالات .

(54) 18 U.S.C. 3122.
(55) 18 U.S.C. 3123.

(ISSN: 2537- 0758)

كما أجاز للمحكمة أن تصدر أمرًا بتثبيت جهاز تتبُّع دون حاجة إلى القيام بتقديم طلب لاستصدار هذا الأمر، إذا أقرَّ ضابط التحقيق للمحكمة أن المعلومات التي يحتمل الوصول إليها من خلال هذا الإجراء ذات صلة بتحقيق جنائي جارٍ.

وفي هذه الحالة الأخيرة تلتزم الجهة القائمة على تنفيذ هذا الأمر بالاحتفاظ بسجل يقدَّم إلى المحكمة خلال مدة قدرها (٣٠) يومًا، تبدأ من تاريخ انتهاء تنفيذ الأمر، **على أن يتضمن البيانات الآتية:**

١- هوية الضباط الذين قاموا بتركيب الجهاز.

٢- تاريخ ووقت تثبيت الجهاز، تاريخ ووقت إلغاء تثبيت الجهاز، وكذلك تاريخ ووقت ومدة كل مرة يتم فيها الوصول إلى الجهاز للحصول على البيانات.

٣- تكوين الجهاز وقتَ تركيبه وأي تعديل لاحقٍ على هذا التركيب.

٤- أي معلومات تم جمعها بواسطة هذا الجهاز[٥٦].

مدة الأمر:

يصدر الأمر بتثبيت جهاز تتبع لمدة لا تجاوز (٦٠) يومًا يجوز مدُّها لمدة أخرى مماثلة، كما يلتزم مزوِّد خدمة الاتصالات بعدم الإفصاح عن وجود أجهزة تتبُّع ما لم تأمر المحكمة بخلاف ذلك.

وقد أجاز المُشرِّع للمدَّعِين العموم أو نوّابِهم أو مساعديهم أو ضباطِ التحقيق في أيّ ولاية أو مقاطعة أن يأذنوا بتركيب جهاز تتبُّع دون الحاجة إلى صدور أمر من المحكمة بذلك، عند تحقق إحدى الحالات الطارئة التي عدَّدتها المادة (٣١٢٥)، **والتي تتمثل في**[٥٧]:

١- وجود خطر حاليّ يمكن أن يترتّب عليه وفاة أو إصابة جسدية خطيرة.

٢- أيّ نشاط مخالف للقانون يتعلق بالجريمة المنظمة.

٣- أيّ نشاط مخالف للقانون من شأنه أن يهدِّد الأمن القومي.

٤- الهجوم الجديّ على حاسب آليّ محميّ.

ويجب على الجهة القائمة على تثبيت الجهاز أن تبادر خلال مدة أقصاها (٤٨) ساعة من تاريخ تثبيته بتقديم طلب لاستصدار أمر قضائي بتثبيت هذا الجهاز، وينتهي هذا الإجراء فور الحصول على البيانات المطلوبة أو في حال رفض المحكمة إصدار أمر بذلك، أيهما أسبق.

---

(56) Id.

(57) 18 U.S.C. 3125.

وفي تلك الحالة الأخيرة يُعدُّ إجراءً مخالفًا للقانون، مما يبرِّر إلغاء تثبيت الجهاز على الفورِ، كما يتم استبعاد ما يترتب عليه من أدلة.

رابعا: مراقبة الاتصالات الخاصة لحماية الأمن القومي:

تملك الحكومة صلاحيات قانونية واسعة تمكِّنها من مراقبة الاتصالات الإلكترونية- دون الحاجة إلى استصدار أمر قضائي- إذا تعلق الأمر بتحقيق يتعلق بأجهزة الاستخبارات الأجنبية أو الأمن القومي للبلاد، وقد تناول قانونًا: مراقبة الاستخبارات الأجنبية (FISA)، وقانون الوطنية (patriot Act) هذه الصلاحياتِ، وهو ما سوف نبيّنه على النحو التالي:

قانون مراقبة الاستخبارات الأجنبية (FISA)- (Foreign Intelligence Surveillance Act):

صدر قانون مراقبة الاستخبارات الأجنبية عام ١٩٧٨ لتنظيم جمع المعلومات المتعلقة بالاستخبارات الأجنبية داخل الولايات المتحدة الأمريكية، ويسمح هذا القانون بمراقبة القوى الأجنبية[٥٨]، وعملاء القوى الأجنبية داخل الولايات المتحدة بموافقة المدعي العام.

وَفقًا لأحكام هذا القانون، تشمل المراقبة الحصول على محتوى الاتصال وكذلك البيانات المتعلقة به وبأطرافه، ويتطلب القانون لإصدار أمر المراقبة ضرورةَ توافر سبب محتمل يدعو للاعتقاد بأن هدف المراقبة هو قوة أجنبية أو أحد وكلائها[٥٩].

---

(58) 50 U.S.C. § 1801."

أ) القوى الأجنبية: ١- الحكومات الأجنبية أو أي عنصر من عناصرها سواء تم الاعتراف بها أم لم يتم الاعتراف بها من قبل الولايات المتحدة. ٢- فصيل من أمة أجنبية لا يتكون من أفراد ينتمون للولايات المتحدة. ٣- كيان تابع وخاضع لسيطرة إحدى الدول الأجنبية، ومعترف به من تلك الدول. ٤- جماعة ضالعة في أنشطة تتعلق بالإرهاب الدولي. ٥- منظمة سياسية أجنبية لا تتألف من أشخاص ينتمون للولايات المتحدة. ٦- كيان تابع وخاضع لسيطرة إحدى الدول الأجنبية. ٧- كيان يتألف من أشخاص لا ينتمون للولايات المتحدة وينخرط في نشاط يتعلق بالانتشار الدولي لأسلحة الدمار الشامل".

(59) 50 U.S.C. § 1805 (requiring probable cause for electronic surveillance); 50 U.S.C. § 1824(requiring probable cause for physical surveillance).

(ISSN: 2537- 0758)

وقد ألزم هذا القانون المدعيَ العامَّ باعتماد إجراءات من شأنها تقييد الحصول على المعلومات غير المتاحة للجمهور والاحتفاظ بها وحظر نشرها في ضوء الهدف من المراقبة وبما يتفق مع مصلحة الدولة[٦٠].

كما أجاز القانون أيضًا للحكومة تثبيت أجهزة تتبُّع للحصول على معلومات تتعلق بالاستخبارات الأجنبية والتي تخصّ أجانب من غير مواطني الولايات المتحدة أو للحماية من الأنشطة الإرهابية الدّولِيّة أو الاستخبارات السرية[٦١].

ويتطلب القانون لإصدار هذا الأمر أن يتوافر سبب معقول يدعو للاعتقاد بأن الأمر يستهدف قوة أجنبية أو أحد وكلائها، وأن يكون ذا صلة بتحقيق مصرَّح به[٦٢].

ومع ذلك، فإنه– تطبيقًا لقانون الحرية الأمريكية الصادر عام ٢٠١٥– يتعيَّن على الحكومة أن تحدِّد الشخص المستهدَف أو الحساب أو العنوان أو الجهاز الشخصي للحدِّ من البيانات المطلوبة واقتصارها على البيانات الضرورية التي تتوافق مع الغرض من البحث[٦٣]، مما يشكل ضمانًا هامًّا لحماية حريات الأفراد.

ويخضع تطبيق تلك القواعد لرقابة محكمة الاستخبارات الأجنبية (Foreign Intelligence Surveillance Court) (FISC).

تعديل قانون مراقبة الاستخبارات الأجنبية (FISA):

عُدِّل قانون مراقبة الاستخبارات الأجنبية عام ٢٠٠٨، وسمح هذا التعديل بجمع محتوى الاتصالات عن طريق إجراءات تختلف عن الإجراءات التقليدية المتبعة في هذا القانون بصورته التقليدية.

فقد سمحت المادة (٧٠٢) منه بالمراقبة الإلكترونية لاتصالات الأجانب خارج الولايات المتحدة بغضّ النظر عما إذا كان هناك سبب محتمل للاعتقاد بأن هؤلاء الأشخاص جزء من قوى أجنبية أو وكلاء لتلك القوى.

كما سمح للحكومة بإجبار مزوِّدي خدمة الاتصالات الإلكترونية بتمكينها من مراقبة اتصالات الأشخاص الأجانب المتواجدين في الخارج، دون تقييدها بضرورة أن يتم هذا الإجراء لتحقيق هدف محدَّد.

(60) 50 U.S.C. § 1801(h) (defining minimization procedures).
(61) 50 U.S.C. § 1842(a)(1).
(62) Id. at (c)(2).
(63) USA FREEDOM Act of 2015, Pub. L. 114-23, Sec. 201.

إلا أن القانون ألزم الحكومة سنويًّا بضرورة تقديم شهادة خطية مقرونة بحلف اليمين إلى محكمة الاستخبارات الأجنبية (FISC) تشهد بأن "إجراءات المراقبة" يتم تطبيقها بحذر لضمان تطبيقها على أشخاص خارج الولايات المتحدة، وبطريقة تتجنب الحصول عمدًا على اتصالات يكون كافة أطرافها متواجدين داخل الولايات المتحدة(٦٤).

قانون الوطنية (Patriot Act):

سمحت المادة (٢١٥) من هذا القانون للحكومة بضبط أشياءَ ملموسة " بما في ذلك الكتب والسجلَّات والأوراق والوثائق وغيرها من العناصر" للحصول على معلومات استخبارية أجنبية لا تتعلق بمواطن أمريكي أو للحماية من الإرهاب الدّولِيّ أو أنشطة الاستخبارات السرية(٦٥).

كما سمح هذا القانون للحكومة بالاحتفاظ بكافة البيانات المتعلقة بالاتصالات بشكل مستمر دون اشتباه، إلا أن هذا الوضع ما لبث أن تغير بصدور قانون الحرية عام ٢٠١٥ الذي أوجب على الحكومة تحديد الشخص المستهدف أو الحساب أو العنوان أو الجهاز الشخصي للحد من البيانات المطلوبة واقتصارها على البيانات الضرورية التي تتوافق مع الغرض من البحث.

المبحث الثالث

ضوابط المساس بحُرْمة الاتصالات الخاصة في القانون الفرنسي

ميز المُشرِّع الفرنسي بين نوعين من مراقبة الاتصالات الشخصية: **النوع الأول:** الاعتراض القضائي الذي يتم أثناء التحقيق القضائي بهدف الكشف عن غموض إحدى الجرائم، والذي نظمه المُشرِّع في المواد (١٠٠ حتى ١٠٠- ٧ من قانون الإجراءات الجنائية)، **النوع الثاني:** الاعتراض الإداري والذي يطلق عليه "الاعتراض الأمني" والذي يتم عن طريق تفويض من السلطة التنفيذية لأهداف تتعلق بالأمن القومي (نظمه المُشرِّع بقانون الأمن الداخلي "Code de la sécurité intérieure "CSI بموجب التعديل الذي أدخل عليه بموجب قانون المراقبة رقم ٩١٢- ٢٠١٥ "Surveillance Law").

وسوف نتناول فيما يلي تحديد مفهوم المراقبة في الفقه الفرنسي، ونتبعه ببيان الضوابط التي وضعها لمراقبة الاتصالات الخاصة.

---

(64) 50 U.S.C. § 1881a(d).
(65) 50 U.S.C. § 1861(a)(1).

(ISSN: 2537- 0758)

المطلب الأول
مفهوم المراقبة في التشريع الفرنسي

عرَّف الفقه الفرنسي وظيفة المراقبة بأنها "رصد الأنشطة البشرية باستخدام التقنية، وقد تكون المراقبة خفية أو ظاهرة"[٦٦].

كما عرَّفها الفقيه "GUIDICELLI" أنها "فكرة الدخول في محادثة بين شخصين من خلال وسائل تكنولوجية، ولكن هذه المحادثات تنتمي إلى الحياة الخاصة للأفراد، المشمولة بالحماية القانونية في جميع النظم القانونية، لذا فإن التعارض بين المراقبة وبين الحق في الخُصُوصية متواجد بصفة دائمة"[٦٧].

المطلب الثاني
ضوابط إصدار الأمر بمراقبة الاتصالات الخاصة
الفرع الأول
الاعتراض القضائي
أولًا: شروط اللجوء للاعتراض القضائي:

وفقًا لنص المادة (١٠٠)[٦٨] من قانون الإجراءات الجنائية الفرنسي، فلا يجوز إصدار الأمر القضائي باعتراض الاتصالات إلا في جرائم معينة قدَّرَ المُشرِّع خطورتها، وقد اعتمد المُشرِّع معيار العقوبة المقرَّرة للجريمة، وعدَّه دليل على خطورتها، لذا لم يجزِ اللجوء إلى هذا الإجراء إلا في الجرائم المعاقَب عليها بالحبس مدة لا تقلّ عن ثلاث سنوات.

ويختص بإصدار هذا الأمر "قاضي التحقيق" حتى لو كان القائم بالتحقيق النيابة العامة، وقد عبر القانون عن ذلك فيما نصَّت عليه المادة (١٠٠) بلفظ: "تحت سلطته ورقابته"، وبناء عليه فلا يجوز لمأمور الضبط القضائي أن يصدر هذا الأمر.

---

[٦٦] د. بسمة صلاح الدين عبد السلام، سلطات مأمور الضبط القضائي في الجرائم المعلوماتية في مرحلة الاستدلال– دراسة مقارنة، رسالة دكتوراه، جامعة بني سويف، ٢٠١٨، ص ٧٩ .

[٦٧] د. بسمة صلاح الدين عبد السلام، مرجع سابق، ذات الموضع.

[68] Art. 100 " En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à trois ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques. Ces opérations sont effectuées sous son autorité et son contrôle..."

وقد استقر قضاء محكمة النقض الفرنسية على أن "مفاد نصوص المواد ١٠٠ و١٠٠-٤ و١٠٠-٥ من قانون الإجراءات الجنائية، أن قاضي التحقيق وحده هو الذي يملك سلطة الأمر بالتنصُّت على المكالمات الهاتفية ونصوص المحادثات التي يتم اعتراضها، ويتم ذلك في إطار تحقيق قضائي"[٦٩].

"alors qu'il résulte des articles 100, 100-4 et 100-5 du code de procédure pénale que seul le juge d'instruction détient le pouvoir d'ordonner des écoutes téléphoniques et des retranscriptions des conversations ainsi interceptées dans le cadre d'une information judiciaire".

كما أوجبت المادة (١٠٠-١)[٧٠] من قانون الإجراءات الجنائية أن يكون الأمر ضروريًّا، ويقصد بذلك ضرورة وجود أسباب واقعية وقانونية تفرض اللجوء إلى هذا الإجراء، ولعل الحكمة من وراء هذا الشرط تتمثل في خطورة هذا الإجراء وما يترتب على إجرائه من مساس بالحق في الخُصُوصية.

كما أوجبت كذلك ضرورة تحديد بيانات الاتصال الذي سوف يتم اعتراضه، والجريمة التي تستدعي اتخاذ هذا الإجراء، وكذلك مدة الأمر الصادر به.

مدة الأمر[٧١]:

يصدر الأمر بالمراقبة لمدة (٤) أشهر قابلة للتجديد باتباع ذات الشروط والضوابط المعمول بها في إصداره.

ولا يجوز أن يتجاوز إجمالي تلك المدة سنة واحدة أو سنتين في حالة ارتكاب إحدى الجرائم المنصوص عليها في المواد ٧٠٦- ٧٣ و٧٠٦- ٧٣- ١.

---

(69) Cour de cassation, criminelle, Chambre criminelle, 24 septembre2019, 18-85.736, Inédit.

(70) Art 100-1 "La décision prise en application de l'article 100 est motivée par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires. Elle comporte tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci".

(71) Art. 100-2 "Cette décision est prise pour une durée maximum de quatre mois. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée, sans que la durée totale de l'interception puisse excéder un an ou, s'il s'agit d'une infraction prévue aux articles 706-73 et 706-73-1, deux ans".

(ISSN: 2537- 0758)

ثانياً: تنفيذ الأمر بالاعتراض:

أوجب قانون الإجراءات الجنائية الفرنسي– في المادة ١٠٠– ٤ منه[٧٢]– على قاضي التحقيق أو مأمور الضبط القضائي المنوط به تنفيذ الأمر، أن يحرِّر محضرًا بكل عملية اعتراض يدوِّن فيه (تاريخ بدء العملية، تاريخ انتهائها)، ويتم ختم التسجيلات بعد انتهاء العملية.

كما أوجب كذلك– وَفْقًا للمادة ١٠٠– ٥ منه[٧٣]– على القائم بتنفيذ الأمر أن يقوم بتسجيل الاتصال، ولا يحتفظ سوى بالأجزاء الضرورية منه، التي تفيد في كشف الحقيقة.

وإذا كان الاتصال يتم بلغة أجنبية يتم الاستعانة بمترجم فوري مؤهَّل لهذا الغرض.

وقد استقرَّ قضاء محكمة النقض الفرنسية على أن "التنصُّت على المكالمات الهاتفية إجراء يتطلب القيام به ضرورة تدوين الملاحظات والمراجع قبل نسخ محتوى الاتصال في النماذج المنصوص عليها في المواد ١٠٠–٤ و١٠٠–٥ من قانون الإجراءات الجنائية، التي تتطلب اختيار المراسلات المفيدة فقط في إظهار الحقيقة، والتي يشترط ألا تقعَ ضمن ممارسة حقوق الدفاع أو حماية المصادر في المسائل المتعلقة بحرية الصحافة، كما يتطلب القانون أيضًا ضرورة ختم التسجيلات المتحصَّلة من عملية الاعتراض"[٧٤].

---

(72) Art. 100-4 " Le juge d'instruction ou l'officier de police judiciaire commis par lui dresse procès- verbal de chacune des opérations d'interception et d'enregistrement. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée.

Les enregistrements sont placés sous scellés fermés."

(73) Art. 100-5 " Le juge d'instruction ou l'officier de police judiciaire commis par lui transcrit la correspondance utile à la manifestation de la vérité. Il en est dressé procès-verbal. Cette transcription est versée au dossier.

Les correspondances en langue étrangère sont transcrites en français avec l'assistance d'un interprète requis à cette fin.

A peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense.

A peine de nullité, ne peuvent être transcrites les correspondances avec un journaliste permettant d'identifier une source en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse."

(74) Cour de cassation, criminelle, Chambre criminelle, 31 octobre2012, 12-84.220, Inédit.

"que les écoutes téléphoniques font l'objet d'enregistrements téléphoniques dont l'exploitation impose la prise de notes et de repères préalables à leur retranscription dans les formes exigées par les articles 100-4 et 100-5 du code de procédure pénale laquelle nécessite une sélection des seules correspondances utiles à la manifestation de la vérité et ne relevant pas de l'exercice des droits de la défense ou de la protection des sources en matière de presse ainsi que la mise sous scellés des enregistrements".

كما يحظر القانون اعتراض الاتصالات الخاصة بالمحامي أثناء ممارسة الحق في الدفاع، وكذلك الاتصالات الخاصة بأحد الصحفيين على النحو الذي يسمح بالتعرُّف على مصادر معلومات الصحفي لمخالفة هذا الإجراء للمادة (٢) من قانون ٢٩ يوليو ١٨٨١ الخاص بحرية الصحافة، ويترتب البطلان على مخالفة هذا الحظر.

وقد استقر قضاء محكمة النقض الفرنسية على أن "السلطة الممنوحة لقاضي التحقيق بموجب المادة ١٠٠ من قانون الإجراءات الجنائية، تنطبق عندما تقتضي ضرورة الحصول على المعلومات، اعتراض وتسجيل ونسخ المراسلات الصادرة عن الاتصالات السلكية واللاسلكية، إلا أن هذه السلطة لا تمتدُّ إلى المراسلات المتبادلة بين الشخص الخاضع للتحقيق والمحامي الذي عيَّنه للدفاع عنه؛ فلا يمكن نسخُ المحادثات الهاتفية المتبادلة بينهما ووضعُها في الملف إلا في حالة ما إذا كان محتواها وطبيعتها مناسبينِ لافتراض مشاركة هذا المحامي في إحدى الجرائم"[٧٥].

"que le pouvoir, conféré au juge d'instruction par l'article 100 du Code de procédure pénale, de prescrire, lorsque les nécessités de l'information l'exigent, l'interception, l'enregistrement et la transcription de correspondances émises par voie de télécommunication trouve sa limite dans le respect des droits de la défense qui commande notamment la confidentialité des correspondances entre la personne mise en examen et l'avocat qu'elle a désigné ; qu'une conversation téléphonique intervenant entre eux ne peut être transcrite et versée au dossier que si son contenu et sa nature sont propres à faire présumer la participation de cet avocat à une infraction".

(75) Cour de Cassation, Chambre criminelle, du 1 octobre 2003, 03-82.909, Publié au bulletin.

(ISSN: 2537- 0758)

وبعد انتهاء عملية الاعتراض، يتم إتلاف الأدلة بناءً على أمر من المدَّعي العام أو النائب العام بعد انتهاء مدة تقادم الدعوى الجنائية، على أن يتمَّ تحرير محضر بتلك العملية[٧٦].

وتجدر الإشارة إلى أنّ الأحكام الخاصة باعتراض الاتصالات والمراسلات لا تمتدُّ إلى رسائل البريد الإلكتروني المخزَّنة في وقت سابق على صدور أمر الاعتراض، واعتبر قضاء محكمة النقض الفرنسية امتداد تنفيذ الأمر لتلك الرسائل انتهاكًا للحق في الخُصُوصية، وقد عبَّرت المحكمة عن ذلك بقولها: "أيُّ تدخُّل في الحق في احترام الحياة الخاصة يجب أن يقوم على أساس قانوني يمكن التنبؤ به؛ فالمواد ١٠٠ وما يليها من قانون الإجراءات الجنائية، والتي تنصّ فقط على اعتراض الرسائل في المستقبل، لا يمكن أن تشكل أساسًا قانونيًّا دقيقًا يكفي لتنظيم ضبط رسائل البريد الإلكتروني المخزَّنة في وقت سابق على صدور أمر الاعتراض؛ حيث إنّ الوصول إلى تلك الرسائل يخضع لقواعد قانونية خاصة خلافًا للأحكام المنظمة لاعتراض المراسلات"[٧٧].

"le droit au respect de la vie privée doit reposer sur une base légale suffisamment accessible et prévisible ; que les articles 100 et suivants du code de procédure pénale, qui ne prévoient l'interception de messages que pour l'avenir, ne sauraient constituer une base légale suffisamment précise pour encadrer la saisie d'un stock de mails ; que la chambre de l'instruction ne pouvait, pour écarter le moyen tiré d'un défaut de base légale de l'ingérence litigieuse, se borner à considérer qu'un mail entre dans le champ des «correspondances» visées à l'article 100 du code de procédure pénale; qu'en effet, une intrusion dans une boite de messagerie électronique, susceptible de conduire à la récupération de données stockées, nécessite un encadrement particulier que n'assurent pas les dispositions relatives à l'interception des correspondances".

(76) Art. 100-6 "Les enregistrements sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique.
Il est dressé procès-verbal de l'opération de destruction."
(77) Cour de cassation, Chambre criminelle, arrêt du 8 juillet 2015.

الفرع الثاني:
الاعتراض الإداري "الأمني":

أجاز قانون الأمن الداخلي الفرنسي"Code de la sécurité intérieure"CSI[٧٨]– وَفْقًا للتعديل الذي أدخل عليه بموجب قانون المراقبة رقم ٩١٢– ٢٠١٥ "Surveillance Law"[٧٩]– لوكالات الاستخبارات مراقبة الاتصالات الإلكترونية– دون الحصول على إذن قضائي– في الأحوال المتعلقة بتهديد الأمن القومي، وكذلك المصالح الأساسية المتعلقة بالأمة الفرنسية.

أولًا: شروط اللجوء للاعتراض الإداري:

حدَّدت المادة L. 811–3[٨٠] من قانون الأمن الداخلي– المضافة بقانون المراقبة رقم ٩١٢– ٢٠١٥– حالات معينة يمكن أن يصدر الأمر الإداري باعتراض الاتصالات الإلكترونية حال تحقُّق إحداها، **وتتمثل هذه الحالات في:**

---

(78) French Internal Security Code is available at http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000025503132&dateTexte=20151111

(79) Law no 2015-912 of 24 July 2015 related to intelligence– Exposé des motifs (available at http://www.legifrance.gouv.fr/affichLoiPubliee.do;jsessionid=AC82D0703DA2374DEF16BEA404A88989.tpdila23v_3?idDocument=JORFDOLE000030375694&type=expose&typeLoi=&legislature=14)

(80) Article L811-3" Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants:

1- L'indépendance nationale, l'intégrité du territoire et la défense nationale;
2- Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère;
3- Les intérêts économiques, industriels et scientifiques majeurs de la France;
4- La prévention du terrorisme;
5- La prévention:
a) Des atteintes à la forme républicaine des institutions;
b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1;
c) Des violences collectives de nature à porter gravement atteinte à la paix publique;
6- La prévention de la criminalité et de la délinquance organisées;

(ISSN: 2537- 0758)

١- حماية استقلال الوطن وسلامة أراضيه والدفاع عنه.
٢- حماية المصالح الأساسية للدولة في السياسة الخارجية، تنفيذ الاتفاقيات الدّولِيّة والأوروبية، ومنع أيّ تدخّل خارجي.
٣- حماية المصالح الاقتصادية، العلمية، الصناعية الرئيسة لدولة فرنسا.
٤- مكافحة الإرهاب.
٥- حماية الدولة من التهديدات التي من شأنها أن تُعرِّض الأمن العام لخطر جسيم.
٦- منع الجريمة المنظَّمة.
٧- منع انتشار أسلحة الدمار الشامل.

وقد ارتأى مجلس الدولة الفرنسي (Conseil d'État) "أن الحالات التي تضمنها هذا القانون التي تسمح باستخدام التقنيات المتعلقة باعتراض الاتصالات الإلكترونية- والتي يشكل بعضُها انتهاكًا شديدًا للخُصُوصية- تُعدُّ الضمانة الأساسية التي تكفل عدم استخدام تلك التقنيات إلا لتحقيق هذه الأغراض المشروعة"(٨١).

التقنيات المستخدمة:

يجوز لوكالات الاستخبارات- بناء على تصريح من السلطة التنفيذية- جمع الاتصالات الإلكترونية، أو المعلومات أو المستندات التي تتم معالجتها بواسطة مشغِّلي خِدْمات الاتصالات، بما في ذلك (البيانات التقنية المتعلقة بأرقام تعريف الاتصال أو الاشتراك، وبيانات موقع الاتصال، ومدد الاتصالات وتوقيتها)(٨٢).

وللأهداف المتعلقة بمكافحة الجرائم الإرهابية، أجاز القانون الحصول على البيانات المتعلقة بـ(حركة مرور الاتصالات في التوقيت الفعلي للاتصال، بيانات سجل الاتصال الخاصة بالأشخاص الذين يشكلون تهديدًا للأمن والذين تم تحديدهم مسبقًا) من مشغلي خِدْمات الاتصالات(٨٣)، كما أجاز كذلك تحليل حركة الاتصالات لاكتشاف التهديدات الإرهابية المحتملة، والوصول إلى بيانات حركة مرور الاتصالات، تسجيل البيانات التي

7- La prévention de la prolifération des armes de destruction massive."
(81) Conseil d'Etat– séance du jeudi 12 mars 2015– avis sur un projet de loi relative au renseignement (available at file:///C:/Users/FPFBenedicte/Downloads/avis_ce_prmx1504410L_cm_19_03_2015.pdf)
(82) Article L. 851-1 of the French Internal Security Code.
(83) Article L. 851-2 of the French Internal Security Code.

يحتفظ بها مقدِّمو خِدْمات الاستضافة على مواقع الإنترنت بما في ذلك خِدْمات وسائل التواصل الاجتماعي(٨٤).

وأكثر تلك التقنيات إثارةً للجدل، تلك المتعلقة بتحليل جميع بيانات حركة مرور الاتصالات، وكذلك سجلات الاتصالات بشكل عشوائي لتحديد النشاط المشبوه، التهديدات الإرهابية المحتملة(٨٥).

إصدار الأمر بالاعتراض:

وفقًا للمادة (L 821-1)(٨٦) من قانون الأمن الداخلي، يصدر الأمر بالاعتراض بناء بناء على تفويض من رئيس مجلس الوزراء، بعد صدور توصية غير ملزمة من اللجنة الوطنية لمراقبة تقنيات الاستخبارات "CNCTR"، **ويمر إصدار أمر الاعتراض ببعض الخطوات:**

١- يقدم وزير الدفاع أو وزير الداخلية أو وزير العدل أو الوزراء المسئولون عن الاقتصاد أو الميزانية أو الجمارك، طلبًا مكتوبًا بهدف اتخاذ الإجراءات اللازمة لاعتراض الاتصالات، على أن يتضمن هذا الطلب عدة بيانات تتمثل في: (التقنية أو التقنيات التي سوف يتم تنفيذها، الجهة التي تقدم هذه التقنية، الهدف المبتغَى منها، سبب اللجوء إلى هذا الإجراء، مدة سريان التفويض، الشخص أو المكان أو المركبة المستهدفة)(٨٧).

---

(84) Articles L. 851-1 to L. 851-7 of the French Internal Security Code.

(85) Article L. 851-3 of the French Internal Security Code.

(86) Art. L821-1 "La mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées au titre V du présent livre est soumise à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement.

Ces techniques ne peuvent être mises en œuvre que par des agents individuellement désignés et habilités."

(87) Art. L821-2 "L'autorisation mentionnée à l'article L. 821-1 est délivrée sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur, du ministre de la justice ou des ministres chargés de l'économie, du budget ou des douanes. Chaque ministre ne peut déléguer cette attribution individuellement qu'à des collaborateurs directs habilités au secret de la défense nationale.

La demande précise:

1- La ou les techniques à mettre en œuvre;

2- Le service pour lequel elle est présentée;

3- La ou les finalités poursuivies;

(ISSN: 2537- 0758)

ولعل الحكمة في اشتراط تضمن الطلب المقدَّم لسبب اللجوء إلى الاعتراض، وكذلك الهدف الذي يرمي إلى تحقيقه يشكّل ضمانًا هامًّا لحماية الحق في الخُصُوصية، ويكفل عدم التعسُّف في استعماله، كما أن وضوح تلك البيانات من شأنه تيسير عمل اللجنة الوطنية لمراقبة تقنيات الاستخبارات "CNCTR" التي تقوم على التحقُّق من الالتزام بالأحكام المتعلقة بإصدار أمر الاعتراض الإداري.

٢- يقدُّم الطلب إلى رئيس اللجنة الوطنية لمراقبة تقنيات الاستخبارات "CNCTR"- التي تتألَّف من: عضوَين من أعضاء البرلمان، عضوَين من أعضاء مجلس الشيوخ، عضوَين من أعضاء مجلس الدولة من درجة مستشار على الأقل، قاضيَين من خارج التسلسل الهرمي لمحكمة النقض، عضو متخصِّص في الاتصالات الإلكترونية[٨٨]- وفي حالة تعذر تقديم هذا الطلب إلى رئيس اللجنة، يتم تقديمه إلى أحد أعضاء اللجنة من بين هؤلاء المنصوص عليهم في الفقرتين ٢، ٣ من المادة L. 831-1، وتصدر رأيها في هذا الطلب خلال (٢٤) ساعة من تاريخ تقديمه، ويبلغ رئيس الوزراء بهذا الرأي خلال (٧٢) ساعة.

وفي حالة عدم إبلاغ رئيس الوزراء بالرد خلال المدة المنصوص عليها، يُعدُّ الردُّ قد تم تسليمه.

٣- يصدر رئيس الوزراء أو مَن ينوب عنه، تفويضًا للوزير الذي طلب تنفيذ أمر الاعتراض لمدة أقصاها (٤) أشهر، على أن يتضمن الأمر الصادر بالاعتراض البيانات الآتية: (التقنية أو التقنيات التي سوف يتم تنفيذها، الجهة التي تقدِّم هذه التقنية، الهدف المبتغى منها، سبب اللجوء إلى هذا الإجراء، مدة سريان التفويض، الشخص أو المكان أو المركبة المستهدفة)، ويمكن تجديد الأمر بإتباع ذات القواعد المنصوص عليها في إصداره.

ويعدُّ حصر المُشرِّع الفرنسي لعدد المسئولين المؤهَّلين لمنح التصريح بالاعتراض، يُعدُّ ضمانة أخرى لحماية الحقِّ في الخُصُوصية حتى لا يُساءَ استخدامُ هذا الإجراء بما يؤدي إلى انتهاك الحق في الخُصُوصية.

4- Le ou les motifs des mesures;
5- La durée de validité de l'autorisation;
6- La ou les personnes, le ou les lieux ou véhicules concernés..."
(88) Article L. 831-1 of the French Internal Security Code.

وفي حالة إصدار أمر الاعتراض بالمخالفة لرأي اللجنة، يجب أن يشير الأمر الصادر بالاعتراض إلى أسباب عدم اتباع هذا الرأي، ويسجل الطلب والأمر الصادر بالاعتراض في سجلات تابعة لمجلس الوزراء توضع تحت تصرّف اللجنة الوطنية لمراقبة تقنيات الاستخبارات "CNCTR"[٨٩].

وفي الحالات الطارئة، يجوز لرئيس الوزراء أو من يُفوّضه إصدارُ أمر بالاعتراض دون الحصول على توصية من اللجنة الوطنية لمراقبة تقنيات الاستخبارات "CNCTR" في الأغراض المنصوص عليها في الفقرات (١، ٤، ٥) من المادة L. 811-3، التي تتعلق بـ(حماية استقلال الوطن وسلامه أراضيه والدفاع عنه، مكافحة الإرهاب، حماية الدولة من التهديدات التي من شأنها أن تعرض الأمن العام لخطر جسيم).

إلا أن القانون قد أوجب على رئيس الوزراء– خلال (٢٤) ساعة من تاريخ صدور الإذن– أن يرسل جميع العناصر التي الاستعجال المشكل لتلك الحالة الطارئة[٩٠].

---

(89) Art. L821-4 "L'autorisation de mise en œuvre des techniques mentionnées au titre V du présent livre est délivrée par le Premier ministre pour une durée maximale de quatre mois. Le Premier ministre ne peut déléguer cette attribution individuellement qu'à des collaborateurs directs habilités au secret de la défense nationale. L'autorisation comporte les motivations et mentions prévues aux 1° à 6° de l'article L. 821-2. Toute autorisation est renouvelable dans les mêmes conditions que celles prévues au présent chapitre.

Lorsque l'autorisation est délivrée après un avis défavorable de la Commission nationale de contrôle des techniques de renseignement, elle indique les motifs pour lesquels cet avis n'a pas été suivi.

L'autorisation du Premier ministre est communiquée sans délai au ministre responsable de son exécution ainsi qu'à la commission.

La demande et l'autorisation sont enregistrées par les services du Premier ministre. Les registres sont tenus à la disposition de la Commission nationale de contrôle des techniques de renseignement."

(90) Art. L821-5 "En cas d'urgence absolue et pour les seules finalités mentionnées aux 1° et 4° et au a du 5° de l'article L. 811-3, le Premier ministre, ou l'une des personnes déléguées mentionnées à l'article L. 821-4, peut délivrer de manière exceptionnelle l'autorisation mentionnée au même article L. 821-4 sans avis préalable de la Commission nationale de contrôle des techniques de renseignement. Il en informe celle-ci sans délai et par tout moyen.

Le Premier ministre fait parvenir à la commission, dans un délai maximal de vingt- quatre heures à compter de la délivrance de l'autorisation, tous les éléments de motivation mentionnés audit article L. 821-4 et ceux justifiant le caractère d'urgence absolue au sens du présent article."

(ISSN: 2537- 0758)

ثانياً: رقابة اللجنة الوطنية لمراقبة تقنيات الاستخبارات "CNCTR":

تُعدُّ اللجنة الوطنية لمراقبة تقنيات الاستخبارات "CNCTR" سلطةً إدارية مستقلة تعمل على ضمان الالتزام بالقواعد القانونية المنظمة لإصدار أمر الاعتراض "الإداري"، وفي سبيل قيامها باختصاصها المنوط بها **فإنها تقوم بما يلي:**

١- تتلقَّى جميع الطلبات التي نصَّ عليها القانون.

٢- لديها وصول دائم وكامل ومباشر إلى كافة البيانات والسجلات والمعلومات التي تجمعها.

٣- لها في أي وقت، أن تطلب كافة البيانات المتعلقة بطريقة تنفيذ أي أمر اعتراض.

٤- لها أن تطلب من رئيس الوزراء أن يمدَّها بكافة البيانات اللازمة لقيامها بمهامها، خاصة تلك المتعلقة بقيام بعض الجهات بتنفيذ إجراءات الاعتراض دون طلب أو صدور تفويض لها بذلك أو بالمخالفة للقواعد القانونية المتبعة في إصداره(٩١).

كما أجاز القانون للجنة توجيه توصية لرئيس الوزراء والوزير المختص بتنفيذ أمر الاعتراض، بوقف تنفيذ عملية الاعتراض وإتلاف المعلومات والبيانات التي تم جمعها نتيجة تنفيذ أمر الاعتراض، وذلك في حالة ما إذا تم تنفيذ عملية اعتراض بالمخالفة لأحكام هذا القانون.

وفي هذه الحالة يتم جمع البيانات التي تم الحصول عليها أو إتلافها(٩٢).

ويكون للجنة سواء من تلقاء نفسها، أو بناء على شكوى من ذوي الشأن، إجراء رقابة على كل عملية مراقبة بهدف مراجعة ما إذا كانت تلك العملية قد أجريت بمراعاة الإجراءات القانونية التي تنظمها من عدمه، ويخطر ذوي الشأن بما يتم من إجراء في تلك الشكوى(٩٣).

---

(91) Article L. 833-2 of the French Internal Security Code.

(92) Art. L 833-6 "La commission peut adresser, à tout moment, au Premier ministre, au ministre responsable de son exécution et au service concerné une recommandation tendant à ce que la mise en œuvre d'une technique soit interrompue et les renseignements collectés détruits lorsqu'elle estime que:
1- Une autorisation a été accordée en méconnaissance du présent livre;
2- Une technique a été mise en œuvre en méconnaissance du présent livre;
3- La collecte, la transcription, l'extraction, la conservation ou la destruction des renseignements collectés est effectuée en méconnaissance du chapitre II du titre II du présent livre."

(93) Art. L833-4 "De sa propre initiative ou lorsqu'elle est saisie d'une réclamation de toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard, la

وقد أجاز القانون للجنة حال عدم الامتثال لتوصياتها أو تجاهل ما تضمنته، يجوز لها– عن طريق ثلاثة على الأقل من أعضائها– أن تتقدَّم بطلب إلى مجلس الدولة (Conseil d'État) بهدف إخضاع إجراءات المراقبة التي أذن بها رئيس الوزراء للرقابة القضائية[٩٤].

ويترتب على التقدّم بهذا الطلب، قيامُ مجلس الدولة بالتحقّق من شرعية عملية المراقبة، فإذا انتهى إلى عدم شرعية تلك العملية، يتم إلغاء أمر المراقبة، وإتلاف البيانات التي تم جمعها عند تنفيذ هذا الأمر.

وإذا تراءى للمجلس أن عدم مشروعية إجراء المراقبة يمكن أن يشكّل جريمة جنائية، يقوم المجلس بإخطار المدّعي العام للجمهورية، كما يتم إخطار اللجنة الوطنية لمراقبة تقنيات الاستخبارات "CNCTR" بعناصر تلك القضية حتى تصدر توصيتها إلى رئيس الوزراء بشأن إمكانية رفع السرية عن تلك العناصر تمهيدًا لتقديمها للمدعي العام[٩٥].

وتجدر الإشارة إلى أنّ إخضاع عمليات المراقبة للرقابة القضائية عن طريق مجلس الدولة يمثل ضمانة هامة لحماية حق الأفراد الخاضعين لتلك العمليات في الخُصُوصية، في ظل اقتصار سلطة اللجنة على إصدار توصيات لا تتمتع بطابع الإلزام.

ويجدر بنا أن ننوّه بأنّ قانون الأمن الداخلي قد تضمّن حكمًا يصرّح بمراقبة الاتصالات الصادرة أو المتسلّمة في الخارج لأغراض تتعلق بحماية المصالح الأساسية للأمة الفرنسية[٩٦]، إلا أن المجلس الدُّسْتُوريّ (Conseil Constitutionnel) ما لبث أن أصدر قراره رقم ٧١٣– ٢٠١٥ بتاريخ ٢٣ يوليو ٢٠١٥– بعدم دُسْتُورية هذا النص لعدم تضمُّنه شروطًا تتعلق باستخدام البيانات المجمَّعة، أو حفظها، أو إتلافها، كما لم

commission procède au contrôle de la ou des techniques invoquées en vue de vérifier qu'elles ont été ou sont mises en œuvre dans le respect du présent livre. Elle notifie à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer leur mise en œuvre."

(94) Art. L833-8 "Le Conseil d'Etat peut être saisi d'un recours prévu au 2° de l'article L. 841-1 soit par le président de la commission lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission ou que les suites qui y sont données sont estimées insuffisantes, soit par au moins trois membres de la commission."

(95) Article L. 773-7 CAJ.

(96) Former Article L. 854-1 of the French Internal Security Code.

(ISSN: 2537- 0758)

يسمح لمن خضع لتلك العملية من المواطنين باللجوء للقضاء بهدف إعمال الرقابة القضائية على مشروعيتها[٩٧].

مدة الاحتفاظ بالبيانات:

يتم إتلاف البيانات التي تم جمعها نتيجة تنفيذ عملية المراقبة[٩٨]:

١- بعد مرور (٣٠) يومًا من اليوم الذي تم جمعها فيه: بالنسبة للبيانات التي تم جمعها حول المشتبه بهم وداخل الدائرة التي يتواجد فيها الشخص الخاضع للمراقبة.

٢- بعد مرور (١٢٠) يومًا من اليوم الذي تم جمعها فيه: بالنسبة للبيانات المتعلقة بالأماكن الخاصة والمركبات، وبعض بيانات سجل الهاتف، باستثناء بيانات سجل الهاتف التي جمعها وَفْقًا للشروط المنصوص عليها في المادة (L851-1).

٣- بعد مرور (٤) سنوات من اليوم الذي تم جمعها فيه: بالنسبة لبيانات حركة مرور الاتصالات التي يحتفظ بها من قدَّموا خدمة الاتصالات، بيانات سجل الاتصال التي يحتفظ بها من قدَّموا خدمة الاستضافة.

وبالنسبة للبيانات المشفَّرة، تبدأ فترة الاحتفاظ اعتبارًا من تاريخ فكّ تشفير البيانات، ولا يمكن الاحتفاظ بتلك البيانات أكثر من (٦) سنوات تبدأ من تاريخ الاستلام.

بالإضافة إلى جميع ما تقدَّم، يجب إتلاف البيانات التي تم جمعها إذا لم تعدْ ضرورية لأيٍّ من الأغراض التي تم جمعها من أجلها[٩٩].

التطور التشريعي:

أقرَّ البرلمان القانون ١٥٥٦- ٢٠١٥ بتاريخ ٣٠ نوفمبر ٢٠١٥، الذي يتعلق بإجراءات مراقبة الاتصالات الإلكترونية الدّولِيّة[١٠٠] أخذًا في اعتباره ما انتهي إليه المجلس الدُّسْتُوريّ من قرارات بشأن دُسْتُورية قانون المراقبة رقم ٩١٢- ٢٠١٥.

---

(97) Decision no.2015-713 of 23 July 2015– Considérant 49 (available at http://www.conseil- constitutionnel.fr/conseil-constitutionnel/root/bank/pdf/conseil-constitutionnel-144138.pdf).

(98) Article L. 822-2 of the French Internal Security Code.

(99) Article L. 822-3 of the French Internal Security Code.

(100) Law n2015-1556 of 30 November 2015 relating to surveillance measures of international electronic measures (available at http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=998EACDA05B79BB46ECB1B480CC1846E.tpdila07v_2?cidTexte=JORFTEXT000031549747&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000031549744).

حظر القانون مراقبة الاتصالات الصادرة أو الواردة التي تحدث في الخارج إلا لأغراض الدفاع وحماية المصالح الأساسية للأمة الفرنسية، كما لم يجزِ استخدام أحكامه لمراقبة الأشخاص ما لم يصدر إجراء فردي ضد شخص بعينه أو تم تحديد أحد الأشخاص باعتباره يمثل تهديدًا للمصالح الأساسية للأمة.

وقد تضمن القانون المذكور عدة أحكام أبرزها:

١- الشروط التي يجوز لرئيس الوزراء بموجبها أن يأذن بعمليات المراقبة الدّولِيّة(١٠١).

٢- شروط الاحتفاظ بالبيانات(١٠٢).

٣- صلاحيات اللجنة الوطنية لمراقبة تقنيات الاستخبارات "CNCTR"(١٠٣).

٤- حق الأفراد في اللجوء للقضاء بشأن الإجراءات التي يتم تنفيذها وَفْقًا لأحكام هذا القانون(١٠٤).

وقد اعتبر المجلس الدُّسْتُوريّ- في قراره رقم "2015-722 DC" الصادر بتاريخ ٢٦ نوفمبر ٢٠١٥- أن ما تضمنه هذا القانون من أحكام جاء متسقًا مع المبادئ الدُّسْتُورية، محترمًا حق الأفراد في الخُصُوصية، وكذلك الحق في حُرْمة الاتصالات الخاصة، كما نظم حق الأفراد في الالتجاء للقضاء بشأن مشروعية الإجراءات المتخذة تطبيقًا لأحكامه"(١٠٥).

النتائج:

بعد استعراض الضوابط التي وضعها المُشرِّع المصري لمراقبة الاتصالات الخاصة، وكذا تلك التي تضمنتها التشريعات المقارنة، خلص **البحث إلى النتائج الآتية:**

١- أجاز المُشرِّع المصري أن يكون إجراء المراقبة أول إجراء من إجراءات التحقيق دون اشتراط أن يكون مسبوقًا بأي إجراءات تحقيق سابقة، بل يصح أن يكون أول إجراء

(101) Article L. 854-2 of the French Internal Security Code.
(102) Article L. 854-5 of the French Internal Security Code.
(103) Article L. 854-9 of the French Internal Security Code.
(104) Individual recourse set forth in article L. 841-1 of the French Internal Security Code applies to these provisions.
(105) Decision no.2015-722 DC of 26 November 2015 (available at http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=998EACDA05B79BB46ECB1B480CC1846E.tpdila07v_2?cidTexte=JORFTEXT000031549759&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000031549744).

(ISSN: 2537- 0758)

تتحرك به الدعوى الجنائية، خلافا للمشرِّع الأمريكي الذي اشترط لاستصدار أمر بالمراقبة "ثبوت عدم جدوى استخدام إجراءات التحقيق الأخرى عند إجرائها أو أن يكون من المرجح فشلها أو أن يترتب على استخدامها نتائج خطيرة "، إلا أن ذلك لا يعني استنفاذ كافة إجراءات التحقيق الأخرى قبل اللجوء إلى إجراء التنصُّت على الاتصالات الخاصة.

٢- جاء التشريع المصري خلوًا من تنظيم عملية استصدار الإذن بالمراقبة تنظيمًا يحدِّد فيه شكل طلب الإذن والبيانات التي يجب أن يتضمنها هذا الطلب خلافًا للتشريعات المقارنة؛ حيث تطلب القانون الأمريكي- على سبيل المثال- في سبيل استصدار إذن بالمراقبة؛ أن يتضمن الطلب عدة بيانات منها: (هُوِيَّة مقدِّم الطلب، تفاصيل الجريمة، طبيعة موقع الاعتراض ومكانه، بيان بالاتصالات التي سيتم اعتراضها، هوية الأشخاص الذين سوف يتم اعتراض اتصالاتهم...) على نحو يمكِّن السلطة المختصَّة بإصدار هذا الإذن من تقدير جدية تلك الأسباب، تحقيقًا للحد الأدنى من الحماية الإجرائية التي تستأهلها حُرْمة الاتصالات الشخصية.

٣- اعتمد المُشرِّع المصري فيما يتعلق بإصدار الأمر بمراقبة الاتصالات الخاصة على "معيار جسامة العقوبة"؛ حيث اشترط لإصدار الأمر بمراقبة المراسلات الخاصة والمحادثات الهاتفية أن تكون الجريمة محَلّ التحقيق من الجرائم المعاقب عليها بالحبس مدة لا تقل عن ثلاثة أشهر، بينما **عمد المشرع الأمريكي إلى تحديد** جرائم محدَّدة يجوز إصدار الأذن بالمراقبة بشأنها، أخذًا في الاعتبار طبيعة الجريمة، الآثار التي يمكن تخلفها، العقوبة المقرَّرة لها، بما يبرِّر انتهاك حُرْمة الاتصالات الخاصة.

٤- حرَص الدُّسْتُور المصري الحالي لعام ٢٠١٤- على تأكيد حُرْمة رسائل الاتصال الإلكتروني، والمحادثات الإلكترونية في المادة (٥٧) منه التي جاء نصها: "... وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حُرْمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها، إلا بأمر قضائي مسبَّب، ولمدة محدَّدة، وفي الأحوال التي يبيِّنها القانون..."، إلا أن المُشرِّع لم يستجب إلى هذا التوجيه بشكل كامل فقد خلا هذا التشريع المصري من أيّ تنظيم لتلك المسألة سوى ما تضمنه القانون رقم (٩٤)

لسنة ٢٠١٥ بشأن مكافحة الإرهاب، وكذلك القانون (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات فيما يتعلق بالجرائم المنصوص عليها فيهما.

التوصيات:

١- **يجب** على المُشرِّع المصري- عند تنظيم مسألة على قدر كبير الأهمية كمراقبة الاتصالات الخاصة- أن يضع عددًا من الشروط الواجب توافرها حتى يمكن اللجوء إلى مثل هذا الإجراء دون أن يكتفي بشرط "لزومه في كشف الحقيقة" الذي يُعدُّ شرطا عاما لا ضابط لإعماله، يمكن أن يؤدي إلى التعسف في استخدام هذا الإجراء الأمر الذي يترتب عليه انتهاك للحق في الخُصُوصية.

٢- يجب أن يتضمن التشريع المصري تنظيما لعملية استصدار الإذن بالمراقبة تنظيمًا يحدِّد فيه شكل طلب الإذن والبيانات التي يجب أن يتضمنها هذا الطلب على غرار ما تضمنه القانون الأمريكي في هذا الخصوص- على سبيل المثال- في سبيل استصدار إذن بالمراقبة؛ يجب أن يتضمن الطلب عدة بيانات منها: (هُوِيَّة مقدِّم الطلب، تفاصيل الجريمة، طبيعة موقع الاعتراض ومكانه، بيان بالاتصالات التي سيتم اعتراضها، هوية الأشخاص الذين سوف يتم اعتراض اتصالاتهم...) على نحو يمكِّن السلطة المختصَّة بإصدار هذا الإذن من تقدير جدية تلك الأسباب، تحقيقًا للحد الأدنى من الحماية الإجرائية التي تستأهلها حُرْمة الاتصالات الشخصية.

٣- اعتمد المُشرِّع المصري- كما سبق أن ذكرنا- فيما يتعلق بإصدار الأمر بمراقبة الاتصالات الخاصة على " معيار جسامة العقوبة "؛ حيث اشترط لإصدار الأمر بمراقبة المراسلات الخاصة والمحادثات الهاتفية أن تكون الجريمة محَلّ التحقيق من الجرائم المعاقب عليها بالحبس مدة لا تقل عن ثلاثة أشهر.

إلا أنه قد يؤخذ على مقدار العقوبة أنه، وإن كان أحد المعايير الدالة على خطورة الجريمة وجسامتها، إلا أنه ليس المعيار الوحيد، فهناك معايير أخرى ينبغي أخذها في الاعتبار كالأثر الاجتماعي للجريمة أو الآثار الاقتصادية لها وغيرها من صور الانتهاك المؤثرة التي لا يجوز اختزالها في مقدار العقوبة.

كما أنه، ومن ناحية أخرى يُعدُّ معيارًا عامًّا لشموله معظم الجنح التي نصَّ عليها قانون العقوبات، والتي قد لا تستدعي اللجوء إلى هذا الإجراء، مما يؤدي إلى تحوُّل إجراء المراقبة من إجراء استثنائي إلى إجراء ذي صفة عادية.

(ISSN: 2537- 0758)

لذا فقد كان من الأجدر على المُشرِّع المصري– على غرار المُشرِّع الأمريكي– أن يحدِّد جرائم محدَّدة يجوز إصدار الأذن بالمراقبة بشأنها، أخذًا في الاعتبار طبيعة الجريمة، الآثار التي يمكن تخلفها، العقوبة المقرَّرة لها، بما يبرِّر انتهاك حُرْمة الاتصالات الخاصة.

٤– أكد الدُّسْتُور المصري الحالي المُعدل لعام ٢٠١٤– على حُرْمة رسائل الاتصال الإلكتروني، والمحادثات الإلكترونية في المادة (٥٧) منه، **إلا أن التشريع المصري** قد خلا– كما سبق أن ذكرنا– من أيِّ تنظيم لتلك المسألة سوى ما تضمنه القانون رقم (٩٤) لسنة ٢٠١٥ بشأن مكافحة الإرهاب، وكذلك القانون (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات فيما يتعلق بالجرائم المنصوص عليها فيهما.

لذا كان من الضروري– استجابةً للنص الدُّسْتُوريّ– أن ينظم المُشرِّع مراقبة رسائل الاتصال الإلكتروني، والمحادثات الإلكترونية تنظيمًا شاملًا يحيط بكافة جوانبها– على غرار الوضع في التشريعات المقارَنة– **على أن يتضمن:**

١– إمكانية تطبيقها على الجرائم المنصوص عليها في قانون العقوبات.

٢– القواعد المتعلقة بإصدار الأمر بالمراقبة، ومدته، وطريقة تنفيذه.

٣– القواعد الخاصة بجمع البيانات وحفظها وإتلافها حال انتهاء الغرض من جمعها على نحو يحقق الحماية القانونية للبيانات الشخصية التي تم جمعها.

٤– إتاحة الفرصة لمن خضع لتلك الإجراءات للجوء للقضاء لمراقبة مشروعية الإجراء المتخذ.

٥– وأخيرًا، فإنه نظرًا لخطورة الجرائم التي تهدِّد الأمن القومي للدولة، أو تلك التي تمسُّ استقلاله وسلامة أراضيه تبدو الحاجة إلى سنِّ تشريع يسمح بمراقبة الاتصالات الخاصة– دون الحصول على إذن قضائي– في جرائم محدَّدة على سبيل الحصر يقدِّر المُشرِّع خطورتها، على أن يكون من شأن إتباع القواعد العامة في إصدار الأمر القضائي بالمراقبة تعريض أمن الدولة وسلامتها للخطر.

غير أنه من المتعيَّن عند إنشاء هذا النظام أن يحاط بالعديد من الضمانات التي تكفل عدم خروجه على الهدف من إنشائه، حماية للحق في الخُصُوصية، **ومن بين تلك الضمانات:**

١- اقتصار سلطة إصدار الأمر على رئيس مجلس الوزراء أو من ينوب عنه، بعد عرض "طلب إصدار الأمر" على لجنة متخصِّصة ذات تشكيل يضمُّ عناصر تنفيذية وقضائية بالإضافة إلى خبراء في مجال الاتصالات.

٢- أن يكون لتلك اللجنة صلاحيات تمكنها من مراقبة تطبيق القواعد القانونية الخاصة بإصدار أوامر المراقبة، ووقف تنفيذ عملية المراقبة وإتلاف المعلومات والبيانات التي تم جمعها نتيجة تنفيذ أمر المراقبة، وذلك في حالة ما إذا تم تنفيذ هذا الأمر بالمخالفة لأحكام هذا القانون.

٣- أن يتضمن الأمر البيانات الآتية: (شخص الخاضع لإجراء المراقبة، الاتصال الخاضع للمراقبة، مدة المراقبة، سبب اللجوء للإجراء، التقنية المستخدمة في المراقبة).

٤- وجود قواعد خاصة بجمع البيانات الناتجة عن هذا الإجراء، وتخزينها، وإتلافها بعد مدة معينة أو في حالة انتهاء الغرض من جمعها.

٥- إتاحة الفرصة للأفراد للجوء إلى القضاء بشأن إجراءات المراقبة التي يتم تنفيذها وَفْقًا لأحكام هذا النظام.

المراجع

أ- مراجع عامة:

١- د. بسمة صلاح الدين عبد السلام، سلطات مأمور الضبط القضائي في الجرائم المعلوماتية في مرحلة الاستدلال– دراسة مقارنة، رسالة دكتوراه، جامعة بني سويف، ٢٠١٨.

٢- د. حسام الدين محمد أحمد، شرح قانون الإجراءات الجنائية، ج١، دار النهضة العربية، ٢٠٠٢.

٣- د. رمزي رياض عوض، الحق في الخصوصية، دار النهضة العربية، القاهرة، ٢٠١٦.

(ISSN: 2537- 0758)

٤- د. محمد حسام الدين محمد، الحماية الجنائية لحق الإنسان في حرمة اتصالاته الشخصية، رسالة دكتوراه، جامعة القاهرة، ٢٠١٦.

٥- د. يوسف الشيخ، حماية الحق في حُرْمة الأحاديث الخاصة، دراسة مقارنة في تشريعات التصنُّت وحُرْمة الحياة الخاصة، دار الفكر العربي، ط١، ١٩٩٨.

ب- مواقع إلكترونية:

1- http://www.legifrance.gouv.fr
2- http://www.conseil- constitutionnel.fr