ضوابط وإجراءات مراقبة الاتصالات الإلكترونية في التشريع الجزائري

Controls and Procedures of Monitoring Electronic Communications in Algerian Legislation

لحسن ناني

LAHCENE Nani

طالب دكتوراه، تخصص قانون جنائي، كلية الحقوق، جامعة غليزان.

عضو باحث بمخبر التشريعات الدولية للبحار واثارها على المنظومة القانونية البحرية في الجزائر.

PhD student, Faculty of law, Relizane University.

*A member researcher of international seas legislation Laboratory and its impact on the
Maritime legal system in Algeria.*

lahcene.nani@univ-relizane.dz

بغشام زقاي

BEGHACHEME Zeggay

أستاذ محاضر قسم أ، كلية الحقوق، جامعة غليزان.

عضو باحث بمخبر التشريعات الدولية للبحار واثارها على المنظومة القانونية البحرية في الجزائر.

Lecturer Class A, Faculty of law, Relizane University.

*A member researcher of international seas legislation laboratory and its impact on the
Maritime legal system in Algeria.*

beghacheme.zeggay@univ-relizane.dz

تاريخ النشر: 2023/06/11

تاريخ القبول: 2023/06/09

تاريخ إرسال المقال: 2023/05/19

ملخص:

في ظل التوسع الهائل لوسائل الاتصال الإلكترونية في الجزائر، إذ بلغ عدد مستخدمي الانترنت 32,09 مليون مستخدم خلال السنة الجارية، وكذا تفشي الاجرام المعلوماتي، سواء باتخاذ الأنظمة الآلية لمعالجة للمعطيات كهدف أو باستغلال شبكات الاتصال لتنفيذ جرائم تقليدية، أضحي اللجوء الى إجراء مراقبة الاتصالات الإلكترونية أمر ضروريا للحيلولة دون إلحاق أضرار بمصالح الدولة وكذا محاربة شتى أنواع الجرائم الإلكترونية، وعليه، ومن خلال هذه الورقة البحثية نعمل على الإحاطة بالدراسة والبيان لمختلف النصوص القانونية التي نصت على إجراء مراقبة الاتصالات الإلكترونية وكيف وازن المشرع الجزائري بين المصلحة العامة وحرية الافراد، على اعتبار أن هذا الإجراء يشكل تهديدا

على الحريات الفردية من جهة، ومن جهة أخرى تتطلبه ضرورة ومقتضيات التحريات، وبالتالي كان لزاما وضع ضوابط وفرض قيود و ضمانات للحفاظ على الحريات الخاصة للأفراد، محترما بذلك أحكام الدستور وكذا نصوص الاتفاقيات الدولية في هذا الشأن، فيما تعلق بالحقوق في حرمة الحياة الخاصة والحقوق في الحصول على المعلومة وحرية الإعلام.

كلمات مفتاحية:

مراقبة الاتصالات الإلكترونية، جرائم إلكترونية، المصلحة العامة، حقوق وحرية الافراد.

Abstract:

In view of the enormous expansion of electronic means of communication in Algeria, as the number of Internet subscribers reached 32.09 million users during the current year (2023), as well as the spread of cybercrime, whether by Taking automated data systems as a target, or by exploiting communication networks for traditional crimes to be committed. Resorting to electronic communications surveillance is necessary to prevent harm to the interests of the state as well as to combat different types of electronic crimes. Therefore, and through this research paper we work to take note of the study and statement of the various legal texts which provided for a monitoring electronic communications procedure and how the Algerian legislator funded a balance between the public interest and the freedoms of individuals, on Considering that this procedure constitutes a threat to individual freedoms on the one hand, and on the other it is required by the necessity and requirements of investigations, and therefore it was necessary to set controls and impose restrictions and guarantees to preserve the private freedoms of individuals, respecting the provisions of the Constitution as well as the provisions of international agreements in this regard, concerning the right to respect for private life and expression, the right to information and freedom of the media.

Keywords:

Monitoring Electronic Communications, Cybercrimes, Public Interest, Individuals' Rights and Freedoms.

مقدمة

لقد ظهرت أنماط من الجرائم المستحدثة زادت في عدد الضحايا وحجم الخسائر على كافة المستويات، حيث تنامي الإجرام بسبب استغلال المجرمين لامتيازات الشبكات الرقمية، التي تسمح لهم بارتكاب جرائم على أوسع نطاق بإمكانات مادية ضئيلة مع القليل من الخطر، فالكثير من الجرائم التي تتم عبر وسائل إلكترونية يتعذر اكتشاف مرتكبيها حال وقوعها، لذلك استلزم الحال إنشاء جهات متخصصة في كشف هذا الصنف من الجرائم والتحقيق فيها، مع إدراج التكوين المتخصص لرجال القضاء الذين سيعرض عليهم هذا الصنف من الجرائم في إطار هيئات قضائية متخصصة للفصل فيها، لا سيما ما تعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

وإذ نظرنا الى الحواسيب التي غزت حياة الإنسان بكل تفاصيلها، وكيف أضحت مستودعات رقمية لمعلوماته وبياناته الشخصية وغير الشخصية، في ظل الانتشار الواسع لاستخدام شبكات الإنترنت كوسيلة للتواصل، سواء على الصعيد الشخصي أو المهني، مما يجعل حق الخصوصية جديرا بالحماية القانونية ضد المتطفلين والهاكرز، ومحترفي الإجرام الإلكتروني.

إنه وفي ظل التفوق المهول لتكنولوجيات الإعلام والاتصال على مختلف التشريعات، فإن محاولات استغلال الإجراءات التقليدية المنصوص عليها في قانون الإجراءات الجزائية لمحاربة الجريمة المعلوماتية باءت بالفشل، بسبب عدم انسجامها مع طبيعة هذه الجرائم وعدم نجاعتها في كشف مرتكبيها، ما اضطر المشرع الجزائري إلى استحداث تدابير إجرائية استثنائية خاصة على أمل ضمان مكافحة فعالة لهذا النوع الإجرامي المستجد، ولعل من أبرز الإجراءات الحديثة التي استعان بها المشرع الجزائري في هذا الصدد هو إجراء المراقبة الإلكترونية، والذي نصت عليه المادة 04 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المؤرخ في 14 شعبان 1430 الموافق 05 غشت 2009، جريدة رسمية عدد 47.

يُعد إجراء مراقبة الاتصالات الإلكترونية من أخطر الإجراءات، لتقاطعها مع الحق في حرمة الحياة الخاصة، فكل شخص له الحق في أن تكون له دائرة خصوصية لا يمكن لأي كان انتهاكها، ليتمتع بحياته في هدوء، ولكن هذا الحق أصبح اليوم مهددا أكثر من ذي قبل، بسبب التقدم العلمي والتكنولوجي الذي حمل معه انتهاكات خطيرة للحياة الخاصة للإنسان، بسبب التقدم المهول لتكنولوجيات الاتصال التي جعلت خصوصياته قاب قوسين أو أدنى، فإن تراجع سلطان القانون انتهكت من طرف المجرمين، وأن زاد سلطانه كُتبت وحُطت.

غالبية التشريعات، بما في ذلك المشرع الجزائري قد تبنت مصطلح المراقبة الإلكترونية، حيث أستمد ذلك من نص الإتفاقية المتعلقة بمكافحة الجريمة المنظمة عبر الحدود الوطنية، والتي سنتها منظمة الأمم المتحدة في إطار مكافحة الجريمة المنظمة، إذ تنص المادة 20 منها على أنه: "تقوم كل دولة طرف ضمن حدود إمكانياتها ووفقا للشروط المنصوص عليها في قانونها الداخلي، إذا كانت المبادئ الأساسية لنظامها القانوني الداخلي تسمح بذلك، باتخاذ ما يلزم من تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم المراقب، وكذلك ما تراه مناسبا من استخدام أساليب تحري خاصة أخرى، مثل المراقبة الإلكترونية أو غيرها من أشكال المراقبة".

ولكون إجراء مراقبة الاتصالات الإلكترونية إجراء خطير، فإن المشرع الجزائري تدخل وأحاطه بجملته من الاعتبارات والضوابط التي تسمح بالقيام به والحدود التي يمكن أن نقف عندها حتى لا نصطدم بمسألة حقوق الإنسان وحرياته، وبناءً على ما سبق سنحاول معالجة الإشكالية الآتية:

ما مدى كفاية الضمانات القانونية التي أقرها المشرع الجزائري إزاء إجراء مراقبة الاتصالات الإلكترونية؟

تهدف هذه الورقة بالدرجة الأولى الى تناول أهم الضمانات الموضوعية والإجراءات تعتبر بمثابة قيود ترد على السلطة القضائية التي تأمر بإجراء مراقبة الاتصالات الإلكترونية وتحول دون تعسفها والأجهزة الأمنية والهيئات التي تتولى التنفيذ.

للإجابة عن الاشكال سالف الذكر وتحقيق أهداف هاته الورقة البحثية، تم استخدام المنهجين الوصفي والتحليلي عن طريق جمع بيانات ومعلومات النصوص القانونية المتاحة، وتصنيفها وتحليلها واخضاعها للدراسات الدقيقة بهدف الوصول الى المعرفة التفصيلية حول مشكلة البحث، الأمر الذي حتم علينا تناول موضوع الحال ضمن محورين أساسيين الأول نتطرق فيه الى الضمانات الموضوعية لإجراء مراقبة الاتصالات الإلكترونية، أما المحور الثاني سيخصص لدراسة الضمانات الشكلية لإجراء مراقبة الاتصالات الإلكترونية.

طبقا لنص المادة الثانية من القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سالف الذكر، يُقصد بالاتصالات الإلكترونية: "اي تراسل أو ارسال أو استقبال علامات أو اشارات أو كتابات أو صور أو اصوات أو معلومات مختلفة بواسطة اي وسيلة الكترونية." وتعرف أيضا بأنها: "كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية."، وهو ما ورد ضمن المادة العاشرة من القانون رقم 04-18 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، جريدة رسمية عدد 27، لسنة 2018.

يُقصد بمراقبة الاتصالات الإلكترونية: "هي ذلك العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية، لجمع المعلومات عن المشتبه فيه، سواء اكان شخص ام مكانا ام شيئا، وذلك لتحقيق غرض امني" (موسى، المراقبة الإلكترونية عبر شبكة الأنترنت (دراسة مقارنة)، 2003، صفحة 192)

يقصد بالجريمة الإلكترونية: وتسمى أيضا بالجريمة المتصلة بتكنولوجيا المعلوماتية والجريمة ذات التقنية العالية، يُعرفها د. مارتن بأنها "الجريمة التي تغطي جميع الأفعال غير المشروعة للاهتمام بتكنولوجيا المعلومات والاتصالات من حيث الأجهزة والبرمجيات." (Mohamed, 2006)

يقصد بالمصلحة العامة: "وهي ما فيه صلاح عموم الأمة أو الجمهور، ولا التفتات منه الى أحوال الأفراد إلا من حيث أنهم أجزاء من مجموع الأمة." (سنا، 2019، صفحة 381)

يُقصد بحقوق وحرّيات الأفراد: كل الحقوق والحرّيات، إلا ما ورد بشأنها قيود يُقرّها القانونُ مستهدفاً منها، حصراً، ضماناً الاعتراف الواجب بحقوق وحرّيات الآخرين واحترامها، والوفاء بالعدل من مقتضيات الفضيلة والنظام العام ورفاه الجميع في مجتمع ديمقراطي (هيئة الأمم المتحدة، 1948).

يُعد إجراء مراقبة الاتصالات الإلكترونية من الإجراءات البالغة الأهمية والخطورة في آن واحد، إلا أننا لم نعثر على أحكام أو قرارات قضائية تتضمن الإشارة الى استعمال هذا الإجراء، كما سجلنا شحا في الكُتب المفردة لهذا الإجراء، لا سيما على مستوى المكتبة القانونية الجزائرية، ومن المقالات الأكاديمية التي تناولت هذا الموضوع؛ "مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري"، للأستاذة ثابت دنيا زاد، منشور بمجلة العلوم الاجتماعية والإنسانية، جامعة تبسة، عدد 06، ديسمبر 2012، وهو مقال جدير بالاطلاع لسببين، أولهما أخذ نظرة شاملة حول

الموضوع، وثانيهما التدقيق وتصويب الأخطاء التي يقع فيها البعض بسبب الخلط بين إجراء مراقبة الاتصالات الإلكترونية وما يشابهه.

أولاً: الضمانات الموضوعية لإجراء مراقبة الاتصالات الإلكترونية

لقد أباح المشرع الجزائري اللجوء إلى استعمال تقنية مراقبة الاتصالات، بشأن الكشف عن الحقيقة في الجرائم الماسة بتكنولوجيات الإعلام والاتصال، عن طريق إجراءات وقواعد خاصة نظمها هذا القانون، وفي سبيل الحيلولة دون مساسها بحقوق وحرية الأفراد، فقد أدرج مجموعة من الضوابط الموضوعية كضمانات.

تنص المادة 03 من القانون 04-09 سالف الذكر على أنه: "مع مراعاة الاحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية ووفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية." وقد تطرق في الفصل الثاني من ذات القانون المعنون بمراقبة الاتصالات الإلكترونية وضمن مادة وحيدة وهي المادة الرابعة الى الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية، مدرجا معها ضمانات خاصة بالإجراء على النحو الآتي:

- لا يجوز اجراء عمليات المراقبة إلا بإذن مكتوب من السلطات القضائية المختصة،
 - تكون الترتيبات التقنية الموضوعية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من هذه الأفعال، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.
- الجدير بالذكر أن القانون رقم 05-20 مؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، جريدة رسمية عدد 25 صادر في 6 رمضان عام 1441 الموافق 29 أبريل سنة 2020، كان قد تطرق ضمن المادتين 26 و 27 منه الى مراقبة الاتصالات الإلكترونية تحت مسمى التسرب الإلكتروني إلى منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أكثر، قصد مراقبة الأشخاص المشتبه فيهم، إلا أنه قيد ذلك بضرورة عدم إتيان أي فعل أو تصرف، بأي شكل من الأشكال، من شأنه تحريض المشتبه فيهم على ارتكاب الجريمة بغرض الحصول على دليل ضدهم، تحت طائلة بطلان الإجراءات.
- باستقراء ما سبق، نستنتج الضمانات الموضوعية لإجراء مراقبة الاتصالات الإلكترونية، وهي كما يلي:

1- الضمانات المتعلقة بمقتضيات ممارسة إجراء مراقبة الاتصالات الإلكترونية

لا ينبغي اللجوء إلى إجراء مراقبة الاتصالات الإلكترونية إلا إذا كان له مقتضى مبرر، أي أنه يستلزم القيام بالإجراء لعدم وجود بديل، وغالبا ما يتعلق الأمر بمكافحة الجرائم التي يتم ارتكابها عبر الوسائط الإلكترونية أو ان تكون هاته الأخيرة هدفا لها، سواء للوقاية منها أو لردع مرتكبيها في حال وقوعها أو الشروع فيها، متى كان الشروع معاقبا عليه طبقاً لأحكام قانون العقوبات والقوانين العقابية الخاصة.

إن الجرائم التي يجوز التحقيق فيها بالاستعانة بإجراء مراقبة الاتصالات الإلكترونية بالنظر الى موضوعها محددة على سبيل الحصر، إلا أن الأمر مفتوح إذا تعلق بجرائم وإن كانت تقليدية إذا كان من الصعب الوصول الى نتيجة دون الاستعانة بهذا الإجراء، وهو ما سنفصله في شكل نقاط.

أ- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة

على غير العادة، عرف المشرع الأفعال المصنفة كجرائم إرهاب أو تخريب ضمن أحكام المادة 87 مكرر من قانون العقوبات، حيث جاء في نص المادة أنه: "يعتبر فعلا إرهابيا أو تخريبيا، في مفهوم هذا الأمر، كل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيورها العادي عن طريق أي عمل غرضه ما يأتي:

- بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء المعنوي أو الجسدي على الأشخاص أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو المس بممتلكاتهم.
- عرقلة حركة المرور أو حرية التنقل في الطرق والتجمهر أو الاعتصام في الساحات العمومية،
- الاعتداء على رموز الأمة والجمهورية ونبش أو تدنيس القبور،
- الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مسوغ قانوني،

- الاعتداء على المحيط أو إدخال مادة أو تسريبها في الجو أو في باطن الأرض أو إلقائها عليها أو في المياه بما فيها المياه الإقليمية من شأنها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر،

- عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام،

- عرقلة سير المؤسسات العمومية أو الإعتداء على حياة أعوانها أو ممتلكاتهم أو عرقلة تطبيق القوانين والتنظيمات." يستقرأ من المادة أن المشرع أجاز اللجوء إلى إجراءات التحقيق المنصوص عليها في هذا القانون متى وصل إلى علم النيابة العامة أن هناك شكوك حول أشخاص يمكن أن يقوموا بارتكاب جرائم متعلقة بالإرهاب أو التخريب أو تمس بأمن الدولة، فالمشرع الجزائري لم ينص على إمكانية اللجوء إلى المراقبة بعد ارتكاب الجريمة والبحث عن حقيقة الوصول إلى مرتكبيها فقط، بل أقر أيضا اللجوء إلى استعمال هذه التدابير كوسيلة وقائية للحماية من وقوع جرائم معينة هي الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة.

قد يتبادر الى أذهاننا أن ممارسة إجراء كمراقبة الاتصالات الإلكترونية بمجرد الشك هو اعتداء صارخ على الحريات وعلى سرية المراسلات، لكن بالمقابل فإن اللجوء الى هذا الإجراء تبرره ضرورة التحقيقات وكذا الحفاظ على أمن واستقرار الدولة، نظرا لخطورة هذه الجرائم على المجتمع ككل، فنية المشرع هي استباق أي جريمة من هذا القبيل لأنه في حال ارتكابها فإن نتائجها تكون وخيمة.

ب- في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام

أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني

وهو ما أكدته الفقرة (ب) من المادة 04 من القانون 04-09 السالف الذكر، ذلك أن عملية الاعتداء على المنظومة المعلوماتية الوطنية قد تأخذ عدة صور وأشكال، وتتم أساسا عبر وسائل والاتصالات الإلكترونية ما يعطيها طبيعة الجرائم الإلكترونية ومن أهم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال نجد التجسس على الاتصالات والرسائل الإلكترونية التلاعب بحسابات العملاء أو ببطاقات انتمائهم، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية وما الى ذلك.

إن صورة الجرائم المتمثلة في الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني هي من أبرز أوجه الوقائي التي تستدعي تنفيذ إجراء مراقبة الاتصالات الإلكترونية وفقا لما نصت عليه المادة 4 (ب) من القانون 04-09 سالف الذكر.

ج- مكافحة جرائم التمييز وخطاب الكراهية

اعتبرت هيئة الأمم المتحدة في توصيتها العامة رقم 35 (مكافحة خطاب التحريض على الكراهية العنصرية) المؤرخة في 26 سبتمبر 2013، أن سن تشريعات شاملة ضد التمييز العنصري، بما في ذلك القانون المدني والإداري وكذا الجنائي، أمراً لا غنى عنه لمكافحة خطاب التحريض على الكراهية العنصرية مكافحة فعالة (هيئة الامم المتحدة، 2013)، لذا جرم المشرع الجزائري مجموعة من الأفعال ذات الصلة بمكافحة خطاب التحريض على الكراهية العنصرية ضمن أحكام القانون 05-20 سالف الذكر؛ منها:

- إرتكاب فعلا من أفعال التمييز وخطاب الكراهية المادة 30 من القانون فقرة أولى،
- التحريض علنا أو الإشادة أو القيام بأعمال دعائية من أجل إرتكاب فعلا من أفعال التمييز وخطاب الكراهية المادة 30 من القانون فقرة ثانية،
- إرتكاب أحد الأفعال التي تعتبر تمييزا وخطاب كراهية بإستعمال تكنولوجيات الإعلام والاتصال، وهنا فإن إستعمال تكنولوجيات الإعلام والاتصال يُعتبر ظرف تشديد الى جانب ظروف أخرى معدد في المادة 31،
- إرتكاب أحد الأفعال التي تعتبر تمييزا وخطاب كراهية مع الدعوة لاستعمال العنف، المادة 32،
- إرتكاب أحد الأفعال التي تعتبر تمييزا وخطاب كراهية عن طريق إنشاء أو إدارة أو الإشراف على موقع إلكتروني أو حساب إلكتروني، المادة 32،
- إنتاج أو صنع أو بيع أو عرض للبيع أو التداول منتجات أو بضائع أو مطبوعات أو تسجيلات أو أفلام أو أشرطة أو أسطوانات أو برامج للإعلام الآلي أو أي وسيلة تحمل أي شكل من أشكال التعبير التي من شأنها أن تؤدي إلى إرتكاب إحدى الجرائم المكيفة على أنها تشكل تمييزا أو خطابا للكراهية، المادة 35.

د- مقتضيات التحري والتحقيق

نصت المادة الثالثة من القانون 04-09 سالف الذكر بأنه لا يتم اللجوء إلى مراقبة الاتصالات الإلكترونية إلا إذا استدعت ذلك مقتضيات ومستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، هذا وقد حصرت المادة 4 من نفس القانون مراقبة الاتصالات الإلكترونية بحالات

محددة من بينها في الفقرة (ج) حالة مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهمة الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

إذ تكون أن عملية مراقبة الاتصالات الإلكترونية ضرورية لإظهار الحقيقة، وهذا الشرط نصت عليه المادة 2/8 من الاتفاقية الأوروبية لحقوق الإنسان، وفي فرنسا يشترط مبدأ الضرورة بالنسبة لمراقبة الاتصالات صراحة بنص المادة 706-95 فقرة 1 من قانون الإجراءات الجزائية الفرنسي (République Française, 2021)، حيث يتعين على قاضي الحريات والحبس أن يقوم بتقديره والتأكد منه في طلب وكيل الجمهورية، ومسألة تقدير الضرورة لاتخاذ إجراء مراقبة الاتصالات السلكية واللاسلكية ترجع إلى قاضي الحريات والحبس، حيث يجب أن يتضمن الإذن جميع العناصر التي تسمح بالتعرف على الاتصال، والجريمة التي تبرر الإجراء، والمدة التي يجري فيها المادة 100 الفقرة الأولى (GUINCHARD & Jaque, 2010)، والجدير بالذكر نجد أن المشرع الفرنسي اشترط بأن يكون اللجوء إلى تنفيذ المراقبة ضروري لمصلحة التحقيق وتحقق حالة الضرورة حين يكون من الصعب معرفة الجناة وضبط أدلة الجريمة بوسائل البحث والتحري العادية حسب ما جاء ضمن المادة 1-100 من قانون الإجراءات الجزائية الفرنسي سالف الذكر.

هـ - في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة

يتم اللجوء أيضا إلى إجراء مراقبة الاتصالات الإلكترونية إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة في حالة الجرائم التي ترتكب خارج الإقليم الوطني، ومن شأن عملية مراقبة الاتصالات الإلكترونية في الإقليم الجزائري أن تفيد الدولة المعنية بنتائج تتعلق بمعاينة هذه الجرائم الماسة بتكنولوجيات الإعلام والاتصال وكشف مرتكبيها، بشرط أن يتم ذلك في إطار تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة، أي أن يكون ذلك في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل، وهو ما نصت عليه المادة 16 وما يليها من القانون 09-04 وكذا المادة 43 وما يليها من القانون 20-05، سالف الذكر.

2- الضمانات المتعلقة بتوافر أسباب إجراء مراقبة الاتصالات الإلكترونية

الاتصالات الإلكترونية هي نوع من المكالمات التي يهدأ فيها المتحدث إلى محدثه، حيث تتبادل الأسرار ويتم بسط الأفكار الشخصية دون حرج أو خوف من تنصت الغير، وفي مأمّن من فضول استراق السمع، ويعد هذا صورة من صور ممارسة الأفراد لحياتهم الخاصة (شاهين، 2018، صفحة 325)، لذلك كان من الضروري وضع مجموعة من الضوابط كضمانات تصون حرمة الحياة الخاصة للأفراد عند استغلالهم لوسائل الاتصالات الإلكترونية، إذ لا بد من وجود سبب ضروري يبرر اللجوء لمراقبة الاتصالات الإلكترونية، كما يتعين أن يتحقق من خلال الإجراء الغرض من عملية اللجوء إليه، هذا ويتعين أن يفيد الإجراء في عملية التحقيق والتحري.

أ- مبرر اللجوء لإجراء مراقبة الاتصالات الإلكترونية

لقد نصت المادة الثالثة من القانون رقم 09-04 على أنه "مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية

وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية، وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية ". فمراقبة الاتصالات الإلكترونية ليس إجراء آلي نستعين به كلما كنا أمام تحقيقات قضائية، وإنما يجب تقييده وحصره بأسباب محددة، فالمادة 04 من القانون 09-04 الفقرة (ج) اشترطت أن يتم اللجوء إلى مراقبة الاتصالات الإلكترونية متى كان ذلك ضروريا، أي حينما تواجه التحقيقات القضائية صعوبة للوصول إلى نتيجة محددة. تبرر الضرورة في اللجوء إلى إجراء مراقبة الاتصالات الإلكترونية ضمن تقرير مفصل يُعرض على الجهة القضائية صاحبة الاختصاص في منح الإذن، ونرى بضرورة إدراج النقاط الآتية ضمن هذا التقرير؛

- تحديد السياق العام للأحداث التي كونت لدى الجهة طالبة الإذن قناعة بضرورة اللجوء إلى هذا الإجراء، إذا تعلق الأمر بمراقبة الاتصالات الإلكترونية كإجراء وقائي مذكور في المادة الرابعة من القانون 09-04 سالف الذكر، الفقرة "أ"، أو تقديم قرائن من شأنها تكوين قناعة لدى الجهة المانحة للإذن باحتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، وفق ما هو منصوص عليه في الفقرة "ب"، أو سرد الوقائع والإجراءات السابقة لطلب الإذن بمراقبة الاتصالات الإلكترونية، مع التأكيد على عدم نجاعة باقي السبل المتاحة قانونا، إذا تعلق الأمر بالحالات المذكورة في الفقرة "ج"، أو ذكر مراجع طلبات المساعدة القضائية الدولية إذا تعلق الأمر بالحالة المنصوص عليها في الفقرة "د".
- عرض الوسائل التكنولوجية المقترحة لتنفيذ المراقبة الإلكترونية، مع تبرير أسس اختيارها وحدود إستعمالها و/أو إستعمال مخرجاتها في إثبات الجرائم موضوع الإجراء، وهنا يجب التنويه إلى أن اختيار الوسيلة يتوقف على طبيعة الاتصال موضوع المراقبة، فإن كان صوتيا يمكن الاستعانة بمعدات تسجيل الأصوات (التنصت وليس التنصت كون الأولى تعني استراق السمع والثانية تعني إمعان السمع) وإن كان مرئيا تُستخدم وسائل التصوير، كما قد يحدث وأن يتم اللجوء إلى عدة تجهيزات مدعمة ببرامج خاصة، وذلك إذا تنوعت قنوات الاتصال وتشعبت، الأمر الذي قد يُحتم على الجهة المراقبة أن تسخر أكثر من مورد للخدمة، وأن تستنفر مواردها البشرية بمختلف التخصصات بهدف الحصول على نتائج متكاملة تكون أدلة واضحة.
- تحديد جدول زمني أولي للعملية، إذا تعلق الأمر بالحالات المذكورة في الفقرات "ب"، "ج" و "د" من المادة 04 من القانون 09-04 سالف الذكر.

ب- تحقيق أغراض إجراء مراقبة الاتصالات الإلكترونية

إن إجراءات المراقبة عموما تهدف إلى الوقاية ومكافحة الجرائم ذات الصلة بالمعلوماتية وجرائم التمييز وخطاب الكراهية، وكذا تعزيز التعاون الدولي في مجال مكافحة الإجرام المنظم في مجال المعلوماتية، ذلك أن هذه الجرائم تُعد من الجرائم العابرة للحدود الوطنية ولا ترتبط في كثير من الأحيان بمكان معين، ويكون ذلك في إطار المساعدة الدولية المتبادلة وفقا لما نص عليه القانون والاتفاقيات الدولية في هذا المجال.

فلقد أقر المشرع الجزائري إجراء اللجوء إلى مراقبة الاتصالات الإلكترونية وتفتيش المنظومة المعلوماتية في حالات استثنائية فقط لما لها من اعتداء على حق الإنسان في سرية حياته الخاصة واتصالاته الشخصية لغرض معين وهو الوصول إلى حقيقة الجريمة والكشف عن مرتكبيها خلال مرحلتي جمع الاستدلالات والتحقيق الابتدائي، ولم يتم التوصل إلى ذلك عن طريق اللجوء إلى الإجراءات التقليدية، إذ تنص المادة 03 من القانون 09-04 بأن يتم اللجوء إلى هذا الإجراء متى تطلبت مستلزمات التحريات أو التحقيقات القضائية الجارية.

كما تجدر الإشارة إلى أنه يمكن اللجوء إلى إجراءات المراقبة قبل وقوع جريمة الاعتداء المعلوماتي على منظومة معلوماتية، وذلك بمجرد وصول معلومات إلى السلطة القضائية بشرط أن تكون هذه المعلومات تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، وتلعب أيضا هذه الإجراءات في هذه الحالة دورا وقائيا من شأنها الحيلولة دون وقوع مثل هذه الجرائم الخطيرة، والتي تستهدف على وجه الخصوص أمن الدولة.

فاللجوء إلى المراقبة يكون بعد ارتكاب الجريمة وأثناء مرحلة جمع الاستدلالات أو التحقيق القضائي، ويكون الغرض من ذلك هو التوصل إلى معرفة مرتكبي الجريمة، وذلك في حالة عدم جدوى الإجراءات التقليدية في الوصول إلى الحقيقة المنشودة.

3- السلطة المختصة بتنفيذ إجراء مراقبة الاتصالات الإلكترونية

بوجه عام، أجاز المشرع الجزائري لوكيل الجمهورية أو لضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينييه، تسخير جهات مختصة للتكفل بالجوانب التقنية بموجب أحكام المادة 49 من قانون الإجراءات الجزائية، كما نصت المادة 65 مكرر 08 من قانون الإجراءات الجزائية على تمكين وكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، أو قاضي التحقيق أو ضابط الشرطة القضائية الذي ينييه قاضي التحقيق، من أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المتعلقة باعتراض المراسلات، تسجيل الأصوات والتقاط الصور، وهي الإجراءات الخاصة الواردة ضمن المادة 65 مكرر 05 وما يليها من قانون الإجراءات الجزائية الجزائري.

أما وفيما يخص مراقبة الاتصالات الإلكترونية، فيقصد بالجهة المختصة بالدرجة الأولى بأنها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وهذا ما جاءت به المادة 04 في فقرتها الرابعة من المرسوم الرئاسي 15-261 ممضى في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 53، الصفحة 16، والتي تحيلنا إلى المادة 14 من القانون 09-04، غير أن هاتين المادتين لم تحددتا بدقة تلك الوحدة وأولئك الأشخاص المكلفين تقنيا بمراقبة الاتصالات الإلكترونية.

كما أن ذات المرسوم الرئاسي، أي رقم 15-261، لم يصدر إلا بعد حوالي ست سنوات من صدور القانون 09-04 سالف الذكر، ليتم إلغائه بموجب المرسوم الرئاسي رقم 19-172 الممضى في 06 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها،

بعد أقل من أربع سنوات من تاريخ إصداره، وكذلك الأمر بالنسبة لهذا الأخير، الذي تم إلغائه أيضا بموجب المرسوم الرئاسي رقم 20-183 الممضى في 13 يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ولم يصدر لحد الساعة القرار الوزاري المشترك الذي يعرض القرار الوزاري المشترك الممضى في 17 ديسمبر 2017، الذي يحدد التنظيم الداخلي لهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهو أمر يستدعي البحث والتعمق لا سيما ما تعلق بالشق المرتبط بفكرتي الأمن القانوني والإسهال التشريعي.

بالرجوع الى نص المادة 14 من القانون 09-04 فإنه تُسند الى الوحدة التابعة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ما يلي:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية؛
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

وعليه يجب على مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة) في أقرب الآجال إخطار الهيئة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال فيما تسمح به القوانين—وخاصة منها ما يتعلق بالسر المهني— بما كشفته أو وصل إلى علمها من جرائم متصلة بتكنولوجيات الإعلام والاتصال، هذا ويتم تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات التي تسمح بالتعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم: في هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية.

ومن ثم تشاركها مع المنظمات (الهيئات) المماثلة لها على مستوى الدول، بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل، كما أنها تدرس الروابط العملية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم.

كان المشرع قد أسند مهمة تنفيذ عملية مراقبة الاتصالات الإلكترونية لجهة حصرية وحدد أشخاصا معينين للقيام والإشراف على هذه العملية بموجب المادة 22 من المرسوم الرئاسي 15-261 الملغى، التي نصت على أنه: "يمكن الهيئة لتنفيذ عملية لمراقبة الاتصالات الإلكترونية أن تضع وحدة مراقبة واحدة أو أكثر، تزود بالوسائل والتجهيزات التقنية الضرورية.

تتكون الوحدة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض يساعده ضابط واحد من الشرطة القضائية أو أكثر ينتمي للهيئة، تمثل الوحدة في عملها إلى أحكام التشريع الساري المفعول وشروط الرخصة المسلمة من الشرطة القضائية، وتحرر أشغالها في محضر يعد طبقا لأحكام قانون الإجراءات الجزائية"

ثم خول مراقبة الاتصالات الإلكترونية الى مديرية المراقبة الوقائية واليقظة الإلكترونية التابعة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والتي حددت مهامها ضمن أحكام المرسوم التنفيذي رقم 20-183 الممضى في 13-07-2020، الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

حاليا، وبموجب المرسوم التنفيذي 21-439 المؤرخ في 07-11-2021 الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، لا سيما المادة 14 و 20 وما يليها منه، تم الإبقاء على مديرية المراقبة الوقائية واليقظة الإلكترونية والتي تشكل من مستخدمي الهيئة أو من خارجها إذا اقتضت الضرورة ذلك، ويُستقدم مستخدمي الهيئة من الأسلاك الاتية:

- القضاة،
 - ضباط وأعوان الشرطة القضائية المؤهلين من المصالح العسكرية للأمن والدرك والأمن الوطني،
 - مستخدمي الدعم التقني والإداري للمصالح العسكرية للأمن المختصة والدرك والأمن الوطني.
- بالنسبة للديوان المركزي لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال بفرنسا فإن له مهام أدرجت ضمن المادة الثالثة من المرسوم رقم 2000-405 المؤرخ في 15 ماي 2000 المتضمن إنشاء هذا الديوان، وتتمثل أساسا في (République Française, 2000):
- قيادة وتنسيق التنفيذ العملي لمكافحة الجناة والمتواطئين في الجرائم الخاصة بالجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات، على المستوى الوطني؛
 - القيام، بناء على طلب السلطة القضائية، بجميع أعمال التحقيق والاعمال التحري التقنية لمساعدة الضبطية القضائية المكلفة بالتحقيق في الجرائم المرتكبة و/أو التي يسهل ارتكابها باستخدام بتكنولوجيا المعلومات والاتصالات، دون المساس باختصاص مكاتب الشرطة القضائية المركزية الأخرى؛
 - تقديم يد المساعدة لمصالح الأمن الوطني والدرك الوطني والمديرية العامة للجمارك والحقوق غير المباشرة والمديرية العامة للمنافسة وشؤون المستهلك ومكافحة الغش، وأي مصلحة أخرى، في حالة الجرائم المشار إليها في الفقرة 2 من المادة 2، بناءً على طلبهم، هذه المساعدة لا تجرد المصالح الطالبة من اختصاصها؛
 - التدخل تلقائيا، بموافقة السلطة القضائية المختصة، كلما اقتضت الظروف ذلك، للحصول على معلومات فورا عن الوقائع المتعلقة بالتحقيقات التي تجري.
- يتجلى الفارق الذي يمتاز به النص الفرنسي عما أورده المشرع الجزائري في نقطتين وهما:
- تقديم المساعدة، بعد إذن القضاء، الى المصالح الأمنية والادارية، ودون أن يؤدي ذلك إلى رفع يد هذه المصالح؛
 - التدخل تلقائيا، بعد موافقة السلطات القضائية، من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به.

بالإضافة الى ما سبق فإن المشرع الجزائري وبموجب القانون رقم 20-05 مؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهم، سالف الذكر، قد مكن ضباط الشرطة القضائية باختلاف الاسلاك التابعين لها من تنفيذ إجراء مراقبة الاتصالات الإلكترونية وذلك ضمن المادتين 26 و27 من ذات القانون، إذ تنص المادة 26 على ما يلي: "مع مراعاة أحكام قانون الإجراءات الجزائية، يمكن وكيل الجمهورية أو قاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن، تحت رقابته، لضباط الشرطة القضائية، بالتسرب الإلكتروني إلى منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أكثر، قصد مراقبة الأشخاص المشتبه في ارتكابهم لأي جريمة من الجرائم المنصوص عليها في هذا القانون، وذلك بإيهامهم أنه فاعل معهم أو شريك لهم. يمنع على ضباط الشرطة القضائية، تحت طائلة بطلان الإجراءات، إتيان أي فعل أو تصرف، بأي شكل من الأشكال، من شأنه تحريض المشتبه فيهم على ارتكاب الجريمة بغرض الحصول على دليل ضدهم." كما تنص المادة 27 على ما يلي: "يمكن وكيل الجمهورية أو قاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن، تحت رقابته، لضباط الشرطة القضائية، متى توافرت دوافع ترجح ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون، بتحديد الموقع الجغرافي للشخص المشتبه فيه أو المتهم أو وسيلة ارتكاب الجريمة أو أي شيء آخر له صلة بالجريمة وذلك باستعمال أي وسيلة من وسائل تكنولوجيات الإعلام والاتصال، أو بوضع ترتيبات تقنية معدة خصيصا لهذا الغرض."

ثانيا: الضمانات الشكلية لإجراء مراقبة الاتصالات الإلكترونية

نظرا لخطورة إجراء المراقبة الإلكترونية على حقوق وحرية الأفراد، فقد أورد المشرع العديد من الضمانات الشكلية التي تعتبر بمثابة قيود ترد على السلطة التي تأمر بإجراء المراقبة وتحول دون تعسفها سواء كانت هي أو السلطات التي تتولى تنفيذها، فمن خلال هذه الجزئية سيتم الحديث عن ضرورة وجود أمر قضائي مستوفي الشروط القانونية، كما يتعين تبيان السلطة المختصة في إصدار الإذن، كذا البيانات الواجب توافرها فيه وتسببه، هذا ويتعين تبيان مدة ممارسة إجراء مراقبة الاتصالات الإلكترونية.

1- ضرورة وجود إذن قضائي مستوفي الشروط القانونية

يعتبر الحصول على إذن من السلطة القضائية المختصة لمراقبة الاتصالات الإلكترونية من أهم الضمانات التي وضعها المشرع الجزائري أو غيره من التشريعات المقارنة للأفراد، ويتعلق الأمر كما سبق الشرح بقاضي التحقيق أو وكيل الجمهورية حسب الأحوال أو النائب العام لدى مجلس قضاء الجزائر وفقا لما نصت عليه صراحة نص المادة 04 من القانون 09-04 والتي اشترطت بفقرتها الأخيرة وجوب صدور رخصة عن الجهة القضائية المختصة، ويجب على القضاء قبل أن يصدر الإذن أن يقدر توافر جريمة من الجرائم الواردة على سبيل الحصر في نفس نص المادة، والسابق التعرض لها منعا للتعسف من أي جهة أخرى، ومن ثم فإذا قام ضباط الشرطة القضائية من تلقاء نفسه بهذا الإجراء، تعرض للعقوبات الجزائية المقررة قانونا.

وهو ذات الأمر المطلوب في القانون رقم 20-05 مؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، سالف الذكر، إلا أن الفقرة الثانية من المادة 26 من ذات القانون قد رتبته البطلان صراحة في حال إتيان أي فعل أو تصرف، بأي شكل من الأشكال، من شأنه تحريض المشتبه فيهم على ارتكاب الجريمة بغرض الحصول على دليل ضدهم.

ما يُعاب على المشرع الجزائري في هذه الجزئية، عدم ترتيب البطلان على غياب الإذن بمراقبة الاتصالات الإلكترونية، وهو أثر منطقي كان من الواجب فرضه استنادا إلى مبدأ عدم شرعية الدليل، والحال أنه لا بطلان إلا بنص وفي ظل غياب نص صريح يرتب البطلان، فإن الدعوى العمومية تستمر بغض النظر عن معاقبة ضابط الشرطة القضائية جزائيا، وكذا القاضي الذي أشرف على العملية جزائيا و/أو تأديبيا، سواء وكيل الجمهورية باعتباره مدير الضبطية القضائية، أو كلا من قاضي التحقيق في حال وافق على الإجراء دون وجود أمر ووكيل الجمهورية في حال علمه بذلك.

2- السلطة المختصة في إصدار الإذن

في التشريع الجزائري يمكن اللجوء إلى المراقبة الإلكترونية بجميع أنواعها في كلتا مرحلتَي التحريات الأولية والتحقيق القضائي الابتدائي، ومن ثم يصدر الإذن من قاضي التحقيق في إطار التحقيق الابتدائي، ومن وكيل الجمهورية في إطار التحقيق الأولي وتحقيقات التلبس (عمارة، 2010، صفحة 242)، وإذا تعلق موضوع المراقبة بجرائم الإرهاب والتخريب وأمن الدولة يصدر الإذن عن النائب العام لمجلس قضاء الجزائر إلى الهيئة الوطنية للوقاية من الجريمة الإلكترونية المذكورة في المادة 13 من القانون 09-04، بناء على تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

وتدخل جرائم المعلوماتية والجرائم الأخرى التي يسمح فيها بمراقبة الاتصالات الإلكترونية ضمن اختصاص الأقطاب القضائية الجزائرية بموجب المواد 37، 40 و329 من قانون الإجراءات الجزائية الجزائري، وكذلك الاختصاص الإقليمي الموسع لضباط الشرطة القضائية في المراقبة بالمادة 16 مكرر من نفس القانون.

أما في التشريع الفرنسي وفي ظل قانون 10 جويلية 1991 كانت المادة 100 من قانون الإجراءات الجزائية الفرنسي وما بعدها لا تسمح بهذه الإجراءات إلا أثناء التحقيق الابتدائي، ليأتي بعدها قانون 9 مارس 2004 يسمح بتطبيقه أثناء التحريات الأولية في أفعال الإجرام المنظم عندما تقتضي ذلك ضرورات التحقيق في التلبس أو التحقيق الأولي (المادة 706-95 من قانون الإجراءات الجزائية الفرنسي)، وهي المذكورة على سبيل الحصر في المادة 706-73 من ذات القانون، ويجوز لقاضي التحقيق بموجب أمر مسبب وبعد إخطار وكيل الجمهورية أن يأذن بالالتقاط عن بعد لمعطيات معلوماتية وتسجيلها وحفظها ونقلها، مثلما هي ظاهرة على شاشة الحاسوب أو مثلما تم كتابتها بأحرف الجهاز (المادتين 706 و102 من القانون سالف الذكر).

كما ترجع سلطة اتخاذ إجراء اعتراض المراسلات السلكية واللاسلكية والإلكترونية في الجريمة المنظمة لقاضي الحريات والحبس بالمحكمة ذات الاختصاص الشامل (Le Tribunal de Grande Instance - TGI) بطلب من وكيل الجمهورية المختص، أما بالنسبة للمجالات الأخرى في الجنائيات أو الجنح التي تساوي أو تزيد عقوبتها عن

سنتين حبس، فقاضي التحقيق هو الذي له سلطة اتخاذ الإجراء (المادة 100 من قانون الإجراءات الجزائية الفرنسي) أو في إطار التحقيق التكميلي لقضاة التحقيق أو محكمتي الجرح والجنايات (PRADEL, 2005, p. 151).

3- البيانات الواجب توافرها في الإذن بمراقبة الاتصالات الإلكترونية

يجب أن تثبت إجراءات التحقيق دائما بالكتابة لكي تكون أساسا صالحا لما يبنى عليها من النتائج، فبالرجوع إلى القواعد العامة في قانون الإجراءات الجزائية التي أحالت إليها نصوص هذا القانون، فينطبق عليه ما ينطبق على غيره من الأوامر التي تصدرها الجهات القضائية، وهذه البيانات تتعدد وتتفاوت من حيث الأهمية بين البيانات الجوهرية التي يترتب على عدم وجودها عدم شرعية الإذن، والبيانات غير الجوهرية، فالبيانات الجوهرية هي:

- أن يكون الإذن مكتوبا ومؤرخا وموقعا عليه ممن أصدره ويذكر فيه اسم من أصدره ووظيفته،
- أن يكون صريحا في الدلالة على التفويض، ويتضمن صفة ووظيفة المأذون له بالتنفيذ،
- أن يحدد نوع الجريمة والأشياء و/أو الأفعال التي تجرى من أجلها المراقبة، أي موضوع المراقبة،
- أن يحدد محل المراقبة، أي تحديد الشخص أو قاعدة المعطيات أو النظام الآلي لمعالجة المعطيات أو الشبكة أو الاتصال / الاتصالات الإلكترونية المستهدفة بالإجراء.

أ- أن يكون الإذن بمراقبة الاتصالات الإلكترونية مكتوبا

قياسا، وبالرجوع لأحكام الإذن وطبقا للمادة 65 مكرر 7 فإنه: "يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5، كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية".

وعليه، وإلى جانب شرط كتابة الإذن، يجب أن يتضمن هذا الأخير بعض العناصر لاسيما الاتصالات المراد التقاطها، والأماكن المقصودة لهذا الغرض، سواء تعلق الأمر بالمساكن أو غيرها، وذكر الجريمة التي تبرر اللجوء إلى هذه التدابير، مع ضرورة تحديد المدة بأربعة أشهر كحد أقصى قابلة للتجديد.

وهذا ما أخذ به المشرع الجزائري في جميع إجراءات التحقيق تطبيقا للقاعدة العامة المعمول بها في جل التشريعات الإجرائية المقارنة أن إجراءات التحقيق يجب أن تثبت دائما بالكتابة لكي تكون أساسا صالحا لما يبنى عليها من النتائج.

فضلا عما سبق، يُفضل أن يتم إصدار الإذن إنطلاقا من قاعدة بيانات وزارة العدل، أي نظام تسيير الملفات القضائية (SGDG - Le système automatisé de gestion du dossier judiciaire)، بهدف توحيد النموذج، وضبط مضمونه وفق مقتضيات القانون من جهة، ومن جهة ثانية إمكانية تتبع وجرد هذه الأوامر وتوفير إحصائيات دقيقة، وبالتالي ضمان عدم إستغلال هذا الإجراء خارج الغاية المنشودة منه، بشرط أن تتم العملية مع فرض السرية التامة على الوثيقة حتى في مواجهة مصالح الوزارة الوصية الى غاية عرض الملف على جهات الحكم.

ب- أن يكون الإذن بمراقبة الاتصالات الإلكترونية صريحا

فضلا عن شرط الكتابة يجب أن يكون الإذن صريحا يستفاد منه مباشرة نية السلطة القضائية المختصة في اللجوء إلى هذا الإجراء دون غيره، ولا يكفي أن يستنتج منه ضمنا نية السلطة القضائية في أن هذا الإجراء هو المقصود وليس غيره، وبالتالي يجب أن يذكر في الإذن صراحة أن الإذن يتعلق بمراقبة الاتصالات الإلكترونية، وكلما تم مراعاة هذه الضمانات التي قامت بها العديد من التشريعات المقارنة، وعلى وجه الخصوص التشريع الفرنسي تم التأكيد على احترام الحريات الفردية للأشخاص وخاصة الحق في حرمة الحياة الخاصة.

ومن شروط صراحة الإذن، أن يدون في عنوانه عبارة "إذن بمراقبة الاتصالات الإلكترونية" مع ذكر الأسس القانونية وتحديد المدة إذا كانت واجبة التحديد.

ج- أن يكون الإذن بمراقبة الاتصالات الإلكترونية مؤرخا وموقعا

إن الفائدة في تحديد تاريخ الإذن أو الإذن هي معرفة ما إذا كان مصدر الإذن السلطة المختصة به محليا وقت إصداره فعلا أو كانت غير مختصة بذلك، كما يفيد أيضا في حساب المدة التي يجب خلالها تنفيذ عملية المراقبة طالما أن الإذن بالمراقبة يصدر لمدة زمنية معينة لارتباطه بالحياة الخاصة للأفراد التي يجب عدم انتهاكها إلا بالقدر اليسير الذي يجيز الكشف عن حقيقة الجريمة والتوصل إلى مرتكبيها، كما يفيد تاريخ الإذن في حساب مدة تقادم الدعوى العمومية إذا كان آخر الإجراءات التي تم اتخاذها بمناسبة الدعوى العمومية ولم تتبعه إجراءات أخرى، كما أنه يقطع تقادم الدعوى العمومية، علما أن قانون الإجراءات الجزائية لم ينص على هذا الشرط صراحة، لكن يفترض ذلك في أي أمر مكتوب يصدره قاضي التحقيق، ويشمل التاريخ اليوم والشهر والسنة والساعة وحتى الدقيقة إن كانت طبيعة القضية موضوع الإذن تتطلب ذلك.

ويجب أيضا على مصدر أمر اللجوء إلى مراقبة الاتصالات الإلكترونية سواء كان وكيل الجمهورية أو قاضي التحقيق أن يوقع عليه، حيث الغرض من هذا الإجراء بطبيعة الحال التعرف على من أصدر هذا الإذن للقول باختصاصه أو عدم اختصاصه بإصداره، ولا يشترط شكل معين في التوقيع ما دام موقعا عليه فعلا ممن أصدره.

وإذا تعددت صفحات الإذن، فالأصل هو توقيع مصدره على كل صفحة من صفحاته تحرزا من احتمالات استبدال بعض صفحاته أو الإضافة إليها، وذلك وفقا لما جرى عليه العمل ميدانيا، دون أن يؤدي ذلك إلى بطلان الإذن طالما تم التوقيع على الصفحة الأخيرة منه، كما يجب أيضا أن يتضمن الإذن باللجوء إلى مراقبة الاتصالات الإلكترونية المنظومات المعلوماتية بطبيعة الحال اسم مصدره وصفته، أي كونه قاضي تحقيق أو وكيل الجمهورية حتى يمكن التحقق من أن هذا الإذن قد صدر عن السلطة المختصة بإصداره.

بالنسبة للتاريخ، وبالإضافة إلى ما سبق، يُستحسن أن يُدرج التاريخ آليا من قبل نظام تسيير الملفات القضائية (Le système automatisé de gestion du dossier judiciaire - SGDG)، مما يضمن احترام الآجال.

د- ضرورة تحديد الشخص المراد مراقبة اتصالاته

يجب أن يتضمن الإذن اسم الشخص المراد مراقبة اتصالاته الإلكترونية، ويجب أن لا يصدر الإذن عاما لأن في ذلك مساس بحريات الأفراد، ويجب أن يتخذ الإجراء ضد هذا الشخص فقط دون غيره فإذا امتدت المراقبة إلى الغير

غير المذكورين في الإذن عد باطلا، ويتم تحديد الشخص المراد مراقبة اتصالاته الإلكترونية ببيان اسمه ولقبه ومحل إقامته وكل ما يفيد في تعيينه ونفي الجهالة عنه، كما لا يقع إجراء التفتيش صحيحا بتحديد المنظومة المعلوماتية المراد تفتيشها بدقة ومكان وجودها سواء كان مكانا عاما أو خاصا دون حاجة لذكر صاحبها إذا لم يتم التعرف عليه، والعبارة هنا بالمنظومة المعلوماتية محل التفتيش التي يجب أن يتضمنها الإذن بالتفتيش.

يجب تحرير محضر بالعمليات التقنية التي تم القيام بها، فلما كان اللجوء إلى مراقبة الاتصالات الإلكترونية والتفتيش عملا من أعمال التحقيق، فإنه يجب تحرير محضر بها يثبت فيه ما تم من إجراءات بشأنها، وما أسفرت عنه من أدلة حتى ولو لم يشترط ذلك صراحة في نصوص القانون 09-04، ومن ثم يجب على ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عمليات وضع التدابير التقنية لمراقبة للاتصالات الإلكترونية وما أسفرت عنه، كذلك عمليات التفتيش التي تم القيام بها وما أسفرت عنها من أدلة، ويجب أن يذكر في المحضر أيضا تاريخ وساعة بداية هذه العمليات والانتهاء منها، وجميع الشروط الشكلية العامة في جميع المحاضر، كما يجب أن يكون محررا باللغة العربية.

هـ - ضرورة تبيان طبيعة الاتصالات الإلكترونية المطلوب مراقبتها

إن الإذن بإجراء مراقبة الاتصالات الإلكترونية ينصب على محل معين يتمثل في اتصالات الشخص الإلكترونية وتبعاً لذلك فيجب أن يحدد الإذن كل العناصر التي تسمح بالتعرف على الاتصالات الإلكترونية المطلوب تجميعها وتسجيلها، والذي يجب أن يحدد بدقة طبيعة هذه الاتصالات هل هي مراسلات إلكترونية تتعلق برسائل تصل بريده الإلكتروني أو أحاديث خاصة تتم عن طريق شبكة الإنترنت ومن ثم فإن نطاق الإذن من حيث تنفيذه يتحدد بمحله فإذا صدر الإذن بمراقبة اتصالاته الإلكترونية لم يتعداها إلى تفتيش منظومته المعلوماتية إلا ما تعلق منها ببيده الإلكتروني، والذي يرتبط باتصالات الشخص الإلكترونية.

كما يشترط أيضا أن تبقى الإجراءات المتخذة المتعلقة بمراقبة الاتصالات الإلكترونية في إطار المعلومات المبحوث عنها (المجلس الشعبي الوطني الجزائري، 2009، صفحة 22)، وهو الشرط الذي نص عليه المشرع الإجمالي صراحة في نص المادة 4 فقرة أخيرة من القانون 09-04، والتي أوجبت على أن تكون الترتيبات التقنية الموضوعية للأغراض الموجهة للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية منها وعدم الالتزام بذلك يترتب عليه توقيع العقوبات المتعلقة بالمساس بالحق في حرمة الحياة الخاصة، ويكون المشرع قد قصد تطبيق نص المادة 303 مكرر 3 وما يليها من قانون العقوبات الجزائري، وهنا تثار مشكلة التمييز بين الاتصالات التي تتناول موضوع الجريمة وتلك التي تمس بالحياة الخاصة، وبالتالي يتوجب على ضابط الشرطة القضائية الاحتياط أثناء المراقبة والقيام بتسجيل ما يفيد في الوقاية من الأفعال المذكورة دون غيرها.

وإذا تضمن الإذن مراقبة الاتصالات الإلكترونية لشخص في مكان خاص معين فقط، فإن هذا الإذن يستدعي اتخاذ التدابير التقنية اللازمة لذلك في هذا المكان دون غيره، وتبعاً لذلك فيجب أن يتضمن الإذن هذه الأماكن سواء

كانت سكنية أو عامة وتحديد عنوانها تحديدا دقيقا نافيا للجهالة، حيث يسمح الإذن المسلم بغرض وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من قانون الإجراءات الجزائية وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن وفقا لما للقواعد العامة المعمول بها في قانون الإجراءات الجزائية بشأن وضع التدابير التقنية لاعتراض المراسلات، التقاط الصور أو تسجيل الأحاديث طالما أن القانون 04-09 ينص على ضرورة مراعاة الأحكام المنصوص عليها في قانون الإجراءات الجزائية. كذلك إذا حدد الإذن إجراء تفتيش منظومة معلوماتية لا يجوز تفتيش غيرها إلا إذا ارتبطت بها، وكان بالإمكان تفتيشها من المنظومة المعلوماتية الأولى وبعد إعلام الجهة القضائية المختصة، كما لا يجوز بناء على نفس الإذن مراقبة اتصالات الشخص الإلكترونية، وإن كان إجراء التفتيش لا يطرح العديد من المشاكل المتعلقة بصفة الأشخاص لأنه يتعلق بدرجة خاصة بمنظومات معلوماتية.

و- تسبب الإذن بمراقبة الاتصالات الإلكترونية

التسبب هو تبيان الأسانيد الواقعية والقانونية التي أدت إلى إصداره، ومن ثم يجب على السلطة القضائية المختصة ذكر الأسباب التي دفعت بها إلى إصدار الإذن بمراقبة الاتصالات الإلكترونية حتى ولو لم ينص القانون صراحة على ذلك، فالتسبب هو الوسيلة المثلى لتقييد سلطة الجهة القضائية المختصة الذي يجب عليه أن يتثبت من المبررات التي يستند إليها عند لجوئه إلى مثل هذه الإجراءات الماسة بحريات الأفراد وانتهاك حقهم في الحياة الخاصة، زيادة على ذلك تمكين محكمة الموضوع من بسط رقابتها على المبررات التي استند إليها السلطة المختصة في إصدارها الإذن. وعليه فالتسبب هو الأصل المعمول به بمناسبة معظم الأوامر التي تصدر عن السلطة القضائية، ومن ثم يجب أن يؤسس الإذن على إحدى الحالات المنصوص عليها قانونا كأن يكون سببه الوقاية من وقوع جرائم إرهابية أو جرائم ماسة بأمن الدولة أو احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو تكون ضرورات التحري أو التحقيق الابتدائي هي التي دفعت إلى اللجوء إلى هذه الإجراءات، أو كان الإجراء في إطار تنفيذ طلبات مساعدة دولية متبادلة (المادة 04 من القانون 04-09 السالف الذكر).

كما يتعين أن يرافق الإذن بمراقبة الاتصالات الإلكترونية للوقاية من الأفعال الإرهابية والتخريبية والماسة بأمن الدولة تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها، ومن شأن هذا التقرير أن يوضح الأسباب والدوافع التي دفعت بالسلطة القضائية اتخاذ الإذن بمراقبة الاتصالات الإلكترونية وما هو الغرض الذي يريد الوصول إليه، وهذا هو المقصود بعنصر التسبب (المادة 04 فقرة 03 من القانون 04-09 السالف الذكر)، ويجب التأكيد على أن هذا التقرير يجب أن يصحب جميع حالات مراقبة الاتصالات الإلكترونية وتفتيش المنظومات المعلوماتية، إذ ذهب وزير العدل في شرحه للقانون 04-09 أمام البرلمان للمصادقة عليه إلى التأكيد على أن جميع الإجراءات المتخذة بشأن مراقبة الاتصالات الإلكترونية أو تفتيش المنظومات المعلوماتية يجب أن تتخذ تحت ضمانة أن تتم هذه الإجراءات بعد تقديم تقرير يبين طبيعة الترتيبات والمعلومات المبحوث عنها (المجلس الشعبي الوطني الجزائري، 2009، صفحة 26)، فلا بد أن توافر أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأنهى

يمكن الدخول إليها من المنظومة المعلوماتية الأولى لتمديد التفتيش إلى منظومة معلوماتية أخرى، الأمر الذي يستشف منه ضرورة توافر الأسباب لإصدار الإذن منذ البداية، وهذا ما أكدته المادة 5 فقرة 2 من القانون 09-04 السالف الذكر.

وأن تكون أسباب اللجوء إلى إجراءات المراقبة جدية وكافية، وفي هذا الصدد يكفي الإشارة إلى الدلائل والقرائن التي تسوغ إصدار الإذن، واشتراط أن يكون الإذن الصادر من القضاء باللجوء إلى مراقبة الاتصالات الإلكترونية مسببا يرجع إلى أنها تعد من أخطر الإجراءات الماسة بحريات الأفراد وانتهاك حقهم الطبيعي في السرية، ولكونه إجراء استثنائي يرد على الأصل العام المنصوص عليه في الدستور والمتمثل في حرمة الحياة الخاصة للمواطنين وحقهم في سرية اتصالاتهم، وهذا الاستثناء تبرره المصلحة العامة في الوقاية من الجرائم المذكورة أعلاه قبل وقوعها أو بقصد التوصل إلى كشف الحقيقة والقبض على الجناة.

والأصل أن يستمد القاضي تسيبته من الطلب الموجه إليه، بعد إطلاعه على تقرير الجهة التي طلبت الإذن، وبالتالي فإن التقرير الوجوبي المذكور في المادة 04 من القانون 09-04 سالف الذكر، الفقرة 04 والى جانب تبيان طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها، نرى بضرورة سرد الوقائع التي دفعت إلى طلب الإذن.

كما أنه، ومن وجهة نظرنا، لا يمكن فرض التقرير في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، بل يجب أن يمتد ذلك كل الجرائم التي تستدعي اللجوء إلى إجراء مراقبة الاتصالات الإلكترونية بما في ذلك جرائم التمييز وخطاب الكراهية.

4- مدة ممارسة اجراء مراقبة الاتصالات الإلكترونية

لقد حرصت معظم التشريعات على تحديد مدة مباشرة أي إجراءات من إجراءات التحري، لا سيما تلك المرتبطة بالتقنيات الحديثة، منعا للتعسف وإساءة استعمال السلطة وحمايةً للحقوق والحريات، وإن كان الأمر كذلك، فالأجدر أن يُقيد إجراء مراقبة الاتصالات الإلكترونية بآجال صارمة.

في التشريع الجزائري، ووفقا لقانون الإجراءات الجزائية نجد على سبيل المثال أن مدة الإذن فيما تعلق بإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور حددت ضمن المادة 65 مكرر 07 منه بأربعة أشهر قابلة للتجديد، كذلك الأمر بالنسبة لإجراء التسرب إذ يحظر ضمن الإذن الخاص به مدة عملية التسرب والتي لا يمكن أن تتجاوز أربعة (04) أشهر قابلة للتجديد، كما يجوز للقاضي الذي رخص بها ان يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب، فإذا انقضت مدة أربعة أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه يجب إخبار القاضي المرخص الذي يستطيع ان يرخص بتمديدتها لمدة أربعة أشهر أخرى على الأكثر، طبقا لأحكام المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري.

بالإضافة إلى ما سبق، فإن المشرع الجزائري وبموجب أحكام المادة 65 مكرر 17 قد منح للعون المتسرب إمكانية مواصلة النشاطات المذكورة في المادة 65 مكرر 14 المرتبطة بتنفيذ التسرب للوقت الضروري الكافي لتوقيف

عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولاً جزائياً، وذلك لمدة إضافية بغض النظر عن التمديد العادي، تصل الى أربعة 04 أشهر، كما يمكن له ولنفس الأسباب، وإذا انقضت مهلة الأربعة (04) أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه ، أن يستصدر ترخيصاً من القاضي المختص يتضمن تمديد لمدة أربعة (04) أشهر إضافية على الأكثر.

أما القانون 09-04 فلم يشترط المدة في غير حالة جرائم الإرهاب والتخريب وأمن الدولة، فقد حددت المادة 04 فقرة 05 منه مدة الإذن الذي يمنحه النائب العام لمجلس قضاء العاصمة للهيئة الوطنية للوقاية من الجريمة الإلكترونية بستة (6) أشهر قابلة للتجديد، وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها، وهي مدة طويلة نسبياً، إضافة الى ذلك جعلها قابلة للتجديد دون ان يحدد عدد مرات التجديد، ويُمكن تبرير ذلك بالنظر الى درجة خطورة هذا النوع من الإجرام وكذا طبيعته، على إعتبار أنه منظم وعابر للحدود الوطنية في كثير من الأحيان، حيث لا يتم الكشف عنه بسهولة إلا إذا استغرقت التحريات مدة زمنية معينة تمكن من الكشف عن حقيقته والتوصل إلى عناصر تنظيماته المنتشرة عبر العالم.

إلا أنه وفي المقابل، نسجل فراغاً فيما تعلق بمدة الإذن بإجراء مراقبة الاتصالات الإلكترونية، عدى الحالات المتعلقة بالوقاية من جرائم الإرهاب والتخريب وأمن الدولة، لا سيما إذا قارنا هذا الإجراء مع إجراءات مُشابهة له كالتسرب الذي قد تمتد مدته الى ستة عشر 16 شهراً كاملة.

وعليه يجب أن تكون هذه الإجراءات الاستثنائية مؤقتة احتراماً للحريات الفردية، وطالما لم ينص القانون 09-04 على ذلك نرجع إلى القواعد العامة في قانون الإجراءات الجزائية، ومن ثم فإننا نقترح أن يُتخذ هذا التدبير لمدة لا تتجاوز أربعة (04) أشهر يمكن تجديدها إذا دعت لذلك مقتضيات البحث والتحري والتحقيق قياساً بما نصت عليه المادة 65 مكرر 07 من نفس القانون، وبزوال حالة الضرورة يجب أن ينتهي الإذن باللجوء إلى هذه المراقبة لأن الحاجة إلى وجوده لم تعد قائمة، وبالتالي فيمكن أن يستمر باستمرار التحقيق بشرط أن يكون اللجوء إلى هذه الإجراءات نافعا ومجدياً.

أما في التشريع الفرنسي نجد المادة 706-95 من قانون الإجراءات الجزائية قد حددت مدة المراقبة ب 15 يوماً قابلة للتجديد مرة واحدة وفق نفس الشروط الشكلية والزمنية، على أن تتم عملية الاعتراض تحت إشراف الأمانة العامة لوزارة العدل التي تتكفل بالتنسيق بين مختلف الإدارات المختصة في مجال اعتراض المراسلات، فلقد حدد المشرع الفرنسي الحد الأقصى لمثل هذه الإجراءات بمدة أربعة (04) أشهر أيضاً قابلة للتجديد بنفس الشروط التي صدر بناء عليها أمر المراقبة الأول حسب نص المادة 100-2 من قانون الإجراءات الجزائية الفرنسي.

خاتمة

نظراً لارتباط إجراء مراقبة الاتصالات الإلكترونية بالحق في حرمة الحياة الخاصة، فإنه من الواجب إحاطته بضمانات تكفل حماية هذا الحق، وهذا لن يتأتى إلا إذا كان له مقتضى أي أنه يستلزم القيام بمجموعة من التحريات

- والتحقيقات وفقا لما هو مقرر قانونا ناهيك عن مباشرة هذا الإجراء وفقا لأشكال معينة، بحيث إذا ما تركت هذه الشكليات كلها أو بعضها كان اللجوء إلى هذه الإجراءات باطلا، وعلى العموم قد خلصنا إلى عدة نتائج أهمها الآتي:
- يجب مكافحة الجرائم الإلكترونية وفقا لما هو مقرر من أحكام قانونية، فبقدر ما تكون هذه الأحكام القانونية محددة وواضحة بقدر ما تكون مباشرة المراقبة مقيدة وفقا للهدف منها، وعلى العكس من ذلك فإن عدم تحديد هذه الأحكام أو قصورها يفسح المجال لوجود سلطة تقديرية واسعة في اللجوء إلى المراقبة تختلف ممارستها من سلطة إلى أخرى مما يمثل خطرا كبيرا على حرمة الحياة الخاصة، فالغاية من تقرير تلك الأحكام القانونية هو خلق نوع من التوازن بين حق المجتمع في إقامة العدالة وكشف غموض الجرائم وضبط الجناة وبين حق الأشخاص في حرمة حياتهم الخاصة فلا تستباح الحرمات ولا تهدر الحريات.
 - يتعين أن يكون الإذن بمراقبة الاتصالات الإلكترونية مكتوبا يتضمن جميع العناصر التي تبين حقيقة الاتصال المعترض، بحيث ينبغي التحديد الدقيق لنوع الجريمة التي تيرر الإجراء، والتحديد الواضح والمفصل للاتصال الخاضع للمراقبة وطبيعة المعطيات المراد التقاطها أو اعتراضها ومدة ذلك، وطريقة حفظ الأدلة المستقاة من الاجراء.
 - لا بد من تسبب الإذن احتراماً لمبدأ الضرورة والملاءمة في اتخاذ هذا الإجراء عن طريق اشتراط أن يكون الإذن المرخص للإجراء مسببا، لأن الملاءمة لا تنتج فقط عن توافر الشروط القانونية لتطبيق الإجراء، بل تخضع للسلطة التقديرية للقاضي بحالة بحالة فعندما يكون الإذن بالاعتراض غير مسبب يصعب مراقبة مدى توافر هذا الشرط، وتجاهل هذا الشرط ينبغي أن يرتب البطلان، وهو الأمر الذي أغفله المشرع الجزائري.
- وبناء على ما سبق، نوصي بالآتي:
- ضرورة تدعيم مضمون النصوص القانونية التي تنص على هذا الإجراء بالتفاصيل اللازمة التي تمكن من تنفيذه بالشكل المطلوب، وعلى وجه الخصوص تبيان الوسائل المستخدمة، وطريقة حفظ الأدلة المستقاة، وترتيب البطلان على مخالفة الإجراءات، كما نوصي بجمع النصوص القانونية التي تتضمن هذا الإجراء وإدراجها ضمن قانون الإجراءات الجزائية.
 - ضرورة تبيان الترتيبات بشكل أكثر وضوح في النصوص القانونية، وتحديد الآجال في كل حالات مراقبة الاتصالات الإلكترونية، مع توضيح كيفية وآجال تجديدها الأمر الذي من شأنه خلق حماية للحريات.
 - اقتراح إصدار الإذن انطلاقا من قاعدة بيانات وزارة العدل، أي نظام تسيير الملفات القضائية (Le système automatisé de gestion du dossier judiciaire - SGD) ، بهدف توحيد النموذج، وضبط مضمونه وفق مقتضيات القانون بما يضمن عدم استغلال هذا الإجراء خارج الغاية المنشودة منه.

قائمة المصادر والمراجع

1. المجلس الشعبي الوطني الجزائري. (06, 07, 2009). جريدة رسمية للمناقشات الصادرة عن بتاريخ 6 جويلية 2009، السنة الثالثة رقم 122، ص.22. الجريدة الرسمية لمناقشات المجلس الشعبي الوطني الجزائري، صفحة 22.
2. رحمانى سناء. (09, 2019). القاعدة الفقهية "المصلحة العامة مقدمة على المصلحة الخاصة" ودورها في مكافحة الفساد. مجلة الإحياء (22)، الصفحات 377-402.
3. فوزي عمارة. (06, 2010). إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية. مجلة العلوم الإنسانية (33)، الصفحات 235-254.
4. محمد كمال شاهين. (2018). الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي. الإسكندرية: دار الجامعة الجديدة.
5. مصطفى محمد موسى. (2003). المراقبة الإلكترونية عبر شبكة الأنترنت (دراسة مقارنة). سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية (العدد الخامس)، صفحة 192.
6. هيئة الأمم المتحدة. (10, 12, 1948). الإعلان العالمي لحقوق الانسان. تم الإسترداد من [هيئة الأمم المتحدة](#).
7. هيئة الأمم المتحدة. (26, 09, 2013). هيئة الامم المتحدة. تم الاسترداد من [لجنة القضاء على التمييز العنصري](#).
8. GUINCHARD, S., & Jaque, B. (2010). Procédure Pénale (Vol. N°06). Paris : LITEC.
9. Mohamed, C. (2006, 10 17). Essai sur la notion de cybercriminalité. Récupéré sur www.cybercrime-fr.org
10. PRADEL, J. (2005). Le crime organisé après la loi française du 09 Mars 2004 dite loi de Perben II. Revue de droit pénal et de criminologie (2), p. 151.
11. République Française. (2000, 05 15). Décret n°2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Récupéré sur [Légifrance](#).
12. République Française. (2021, 12 22). Code de procédure pénale. Récupéré sur [Légifrance](#).