ضمانات حرمة الحياة الخاصّة أثناء إجراءات مُراقبة الاتصالات الإلكترونية

Guarantees of Privacy during the Procedures for Monitoring Electronic Communications

روابح فريد*

جامعة سطيف 2، الجزائر، Rouabah19Farid@gmail.com

تاريخ الإرسال: 2020/08/31 **تاريخ القبول: 2020/09/03**

ملخص:

على غرار الكثير من التشريعات في العالم، نظّم المُشرّع الجزائري في قانون الإجراءات الجزائية وقانون مكافحة جرائم تكنولوجيا الإعلام والاتصال إجراء مُراقبة المُراسلات والاتصالات الإلكترونية عبر شبكات الانترنت ووسائل الاتصال عبر الأقمار الصناعية، كأسلوب للتحرّي والتحقيق في بعض الجرائم الخطيرة، مثل الإرهاب والجريمة المنظمة والمخدرات والفساد وتبييض الأموال، والجرائم المعلوماتية التي تتّخذ المنظومة المعلوماتية وشبكات التواصل وسيلة إجرامية أو هدفًا إجراميًا. ومن أجل ضمان عدم انتهاك خصوصية وسرّية الاتصالات الالكترونية، فقد قيّدها بشروط موضوعية تتعلّق بطبيعة الجريمة وضرورات التحرّي والتحقيق وبطبيعة الأشخاص الخاضعين له، وشروط إجرائية لترخيص المُراقبة وتنفيذها، تتعلّق بخضوعها لإشراف ورقابة القضاء واحترام حقوق الدفاع.

الكلمات المفتاحية: الإتصال إلكتروني؛ مُراقبة إلكترونية؛ مُعطيات حركة السير؛ تسرّب رقمي؛ إجرام سيبراني.

Abstract:

Like many legislation in the world, the Algerian legislator in the Criminal Procedures Law and the Law on Combating Media and Communication Technology Crimes has regulated the procedure for monitoring correspondence and electronic communications via the Internet and means of communication via satellite, as a method for investigating some serious crimes, such as terrorism, organized crime, drugs, corruption and money laundering, and information crimes that use the information system and communication networks as a criminal means or a criminal objective.

In order to ensure that the privacy and secrecy of electronic communications are not violated, they have been restricted with objective conditions related to the nature of the crime, the necessities of investigation, the nature of the persons subject to it, and procedural conditions for the licensing and implementation of surveillance related to its subjection to the supervision and control of the judiciary and respect for defense rights.

Keywords: *Electronic Communication, Electronic Monitoring, Traffic Data, Digital Leakage, Cybercrime.*

* المؤلف المراسل

مقدمة

كُل شخص له الحق في أن تكون له دائرة خصوصية خاصّة به، حيثُ يُتركُ ليتمتّع بحياته في هدوء، ولكنّ هذا الحق أصبح اليوم مُهدّدًا أكثر من ذي قبل، بسبب التقدّم العلمي والتكنولوجي الذي حمل معه انتهاكات خطيرة للحياة الخاصّة للإنسان، مثل الحاسبات الإلكترونية ووسائل الاتصال الإلكترونية التي جعلت خصوصيات الانسان عاريةً وشفّافةً أمامها، إذْ أضحت الحواسيب التي غزت حياة الإنسان بكل تفاصيلها مُستودعات رقمية لمعلوماته وبياناته الشخصية وغير الشخصية، في ظل الانتشار الواسع لاستخدام شبكات الإنترنيت كوسيلة للتواصل مع الآخرين محليًا وإقليميًا وعالميًا وذلك من خلال البريد الإلكتروني أو مواقع الدردشة أوشبكات التواصل الاجتماعي، ممّا يجعل حق الخصوصية جديرًا بالحماية القانونية ضدّ المتطفلين والهاكرز، ومحترفي الإجرام الإلكتروني.

ورغم أنّ الحق في الحياة الخاصّة هو عصب الحرّية الشخصية وركيزة أساسية لحقوق الإنسان والحريات العامّة، وينبغي احترامه من قِبل الأفراد والسلطات، وأن تكفل هذه الأخيرة حماية دستورية وقانونية ضد انتهاكها غير المشروع، إلاّ أنّ هذا الحق ليس له الصفة المطلقة، بل تُقيّده اعتبارات المصلحة العامّة متى كانت أولى بالرعاية من مصلحة الفرد[1].

فقانون الإجراءات الجزائية يسعى إلى الكشف عن حقيقة الجريمة ومُرتكبيها بوصول المُحقيقين ورجال القضاء إلى المعلومات المتعلّقة بالوقائع الجرمية وأدلّتها والأشخاص الضالعين فيها، وهو ينظم حسب ما تقتضيه حماية المصلحة العامّة للمجتمع كيفية وحدود المساس بالحقوق والحريات الفردية خاصّة ما يتعلّق بسرّية وخصوصية مراسلاته واتصالاته الالكترونية المضمونة دستوريًا وتشريعيًا. حيث لا تُعتبرُ هذه الحماية مُطلقة، لأنّ إطلاقها قد يكون عائقًا في كشف الجرائم ومرتكبيها، وبالتالي يمكن أن تُقلّص الحماية القانونية لخصوصية الاتصالات الالكترونية إذا استخدمت لأغراض مكافحة الجريمة أو البحث والتحري عنها وعن أدلتها. وقد أكّد خبراء اليونيسكو لدراسة مسألة الخصوصية من أنّه « يقتضي الإعتراف بالحق في الخصوصية ضرورة التضحية بقدر من هذا الحق في كل مرّة تفرض فيها الإعتبارات والمصالح العليا للجماعة مثل هذا الأمر»[2].

ونظرًا لأهمية الإنترنيت كوسيلة تقنية مُتطوّرة ومتسارعة للإتصال وتبادل المعلومات بين بلدان العالم في مُختلف قطاعتها ومؤسساتها وبين الأفراد، فالجرائم المُرتكبة بواسطة الإنترنيت والشبكات الرّقمية في تطوّر مُستمر مع التقدم التكنولوجي فقد أصبح المُجرمون وجماعات الإجرام يستغلون الإنترنيت في مُختلف أنشطتهم، كالإعلان عن المُخدرات، والإتجار بها عبر الإنترنيت والتمويه والتستر على جرائمهم، وكذا تبادل الرسائل فيما بينهم[3].

وتماشيًا مع تطوّر الجريمة والصعوبات التي تطرحُها مسألة البحث عن الجريمة ومُكافحتها استحدث المُشرّع الجزائري أساليب خاصّة للتحرّي، من بينها إجراء مراقبة الإتصالات الإلكترونية، ونظّم أحكامها في قانون الإجراءات الجزائية، وفي قانون الوقاية من جرائم تكنولوجيا الإعلام والإتصال ومكافحتها بشكل يُحاول معه حفظ التوازن بين مصلحة المجتمع في مكافحة الجريمة ومصلحة الفرد في حماية خصوصية مراسلاته واتصالاته الإلكترونية.

يُناقش البحث إشكالية رئيسية تتمحورحول الضمانات الإجرائية لخصوصية الاتصلات الإكترونية أثناء مُراقبتها من أجل التحرّي والتحقيق عن الجريمة ؟ حيث يُقاس مقدار الضمانات الإجرائية لحُرمة الاتصلات الإكترونية بمدى احترام شروط استخدام الإجراء وتنفيذه، وعليه تُناقش الإشكالية من خلال الخطّة الآتية:

المبحث الأوّل: الحماية القانونية لحرمة الحياة الخاصّة

المبحث الثاني: التعريف بمراقبة الإتصالات الإلكترونية كإجراء للتحرّي عن الجريمة

المبحث الثالث: شروط مُراقبة الإتصالات الإلكترونية أثناء التحرّي عن الجريمة.

المبحث الأوّل: الحماية القانونية لحرمة الحياة الخاصّة

يُعتبر حق الخصوصية أو حق الحياة الخاصّة وحرمتها من أهم وأقدس حقوق الإنسان ويتصل بجوانب عدّة، لذلك أكّدت النصوص الدولية والتشريعية والدساتر على ضمان حمايتها.

المطلب الأوّل: التعريف بحق الخصوصية وقيمتها الدستورية:

بتطوّر المجتمعات وما حدث فيها من ثورة تكنولوجيا المعلومات، اتسع نطاق حق الخصوصية وأصبح له مفهوم خاص في مجال الاتصالات الالكترونية والشبكات العنكبوتية.

الفرع الأوّل: التعريف بحق الخصوصية

الحق في الخصوصية قديم قدم الإنسانية وتطوّر مع الزّمن، حيث اهتمّت به الأديان السماوية والمواثيق والإعلانات والمؤتمرات الدولية والدساتير والتشريعات، وعبر التطوّر التاريخي للبشرية وجدت مُقاربات قانونية تعتني بحماية الحياة الخاصّة للأفراد عن طريق قواعد القانون المدني الروماني وفي القرون الوسطى. لكن في القرن 19 بدأت تظهر النصوص الجزائية التي تضمن الخصوصية الفردية بشكل غير مُباشر مثل جنحة انتهاك حرمة المسكن وإفشاء السرّ المهني وانتهاك المراسلات. وإلى اليوم تختلف النظم القانونية المُقارنة في كيفية حماية خصوصية الإنسان، فمنها ما يكتفي بالحماية المدنية، ومنها ما يدعمها بحماية جزائية[4].

الخصوصية في اللُّغة العربية هي ما ينفرد به الإنسان لنفسه دون غيره من الأمور والأشياء، وتكون حرمة الحياة الخاصة هي التي يختصها الإنسان لنفسه بعيدا عن تدخل الغير. وباللغة الإنجليزية بتعبير"

Privacy". وتُرادفها كلمة "*Singularity* " أي حرمة الحياة الخاصة " *the quality of being apart from others* " وتعني كون الشخص بعيدًا عن الآخرين. ويُشتقُّ منها معنى العُزلة "*Seclusion*" وكون الشخص وحيدًا *The being alone of state*[5].

باللغة الفرنسية يُترجم الحق في الحياة الخاصّة" *Droit à la vie privée* " بأن يُترك الشخص وشأنه في هدوء " *Laissez moi tranquille* " وهذا الهدوء الشخصي "*La tranquillité*" الذي هو القيمة النفسية محل الحماية تتعدّد مفاهيمه من الناحية الاصطلاحية، بحسب تعدُّد مجالات الحياة الخاصّة، ولذلك فغياب التعريف القانوني للخصوصية جعل مفهومها نسبيًا ومعقّدًا لدى الفقه والقضاء[6]، حيث لم تتفق القوانين على وضع تعريف لمفهوم الحياة الخاصّة ويرجع ذلك إلى صعوبة حصر جوانبها وعناصرها المتعلّقة بالإنسان, ولم يتفق فقهاء القانون الجزائي مع فقهاء الفروع الأخرى للقانون حول تحديد بعض هذه العناصر[7]، نظرًا لصعوبة التمييز بحدود واضحة بين ما يُعدُّ من الحياة الخاصة للإنسان وما يُعدُّ من حياته العامة، لكن يمكن تحديد عناصر الحق في الحياة الخاصة والتي من بينهاالحياة العاطفية، والزوجية، والعائلية، والحالة الصحية، والرعاية الطبية، والمحادثات الهاتفية والأحاديث الخاصة، والذمة المالية، والآراء السياسية، والمعتقدات الدينية، وموطن الشخص، ومحل إقامته، وحرمة مسكنه، وحرمة مراسلاته، وإسمه، وصورته، وحرمة جسمه، وحياته المهنية والوظيفية، ويسري التعريف على الشخص الاعتباري في حدود ما يتّفق وطبيعته وغرضه[8].

وقد تناولت المواد 690 إلى 712 من القانون المدني الجزائري أحكامًا تحمي خصوصيات الغير، ويتمثل ذلك في أحكام فتح المطلات والمناور والمسافات الفاصلة بين الملكيات. وهي تهدف إلى الحيلولة دون اطلاع الجار على خصوصيات جاره. وهي حماية قانونية وقائية لحرمة الحياة الخاصّة للغير[9].

فمثلاً لا يجوز للجار أن يفتح مطلات أو مناور مقابلة أو منحرفة بمسافات تقل عن تلك المُحدّدة في المواد 709،710،711 بحسب الحالة. فإذا كان القانون يمنع فتح المطلات المقابلة على الجار بغرض منع الإطلاع على الخصوصيات بالعين المجردة أو الأذن المجرّدة، فالمنع يُفترض أن يكون من باب أولى إذا استخدمت الوسائل التقنية التي هي أخطر على حرمة الحياة الخاصّة من الوسائل العادية.

والخصوصية في نطاق المعلوماتية، عُرّفت بأنّها حق الفرد في أن يضبط عملية جمع المعلومات الشخصية عنه، وعملية معاملتها آلياً، وحفظها، وتوزيعها، واستخدامها، فلا ينبغي أن تمس المعلومات بالكرامة الإنسانية، أو بحقوق الإنسان، أو بحياته الشخصية، التي تتم معالجتها بواسطة أجهزة الحاسبات الإلكتروني في قاعدة بيانات أو بنك معلومات، لإخراجها في صورة تفيد مستخدمين مختلفين في أغراض متعددة، أو بوضع هذه المعلومات في البريد الإلكتروني، الذي هو خط مفتوح على أنحاء العالم كّله، والذي يستطيع الفرد من خلاله، إرسال كل ما يريد من رسائل واستقبالها[10].

وتهديد المساس بالحياة الخاصّة قد يثور إذا تمّ الإطلاع على هذه المعلومات المتصلة بأسرار حياته الخاصة أو العائلية من قبل الغير أو أفشيت دون رضاء منه، أو نشرت بإحدى طرائق العلانية دون موافقته، سواء أكانت المعلومات على شكل خبر أو تعليق أو صورة أو مُكالمة أو مراسلة.

وقد وسّعت الشريعة الإسلامية في نطاق حفظ أمن الإنسان وأمانه ليشمل حرمة حياته الخاصّة، ويدخل في حق الشخص في عدم تتبع عورته وعيوبه، قال تعالى في الآية 12 من سورة الحجرات (يا أيّها الذين آمنوا اجتنبوا كثيرً من الظنّ ولا تجسّسوا ولا يغتب بعضكم بعضا)[11].

الفرع الثاني: القيمة الدستورية لحرمة الحياة الخاصّة:

يقع على الدّولة واجب دستوري يتمثل في ضمان عدم انتهاك حرمة الإنسان ومنع أي عنف معنوي أو بدني أو مساس بالكرامة الإنسانية، حيث تُرسي المادّة 35 من الدستور الجزائري الحالي دستور 28 نوفمبر 1996[12]مبدأ العقاب على كلّ مساس بالسلامة المعنوية وعلى كل المخالفات ضدّ الحقوق والحرّيات، ومن ضمنها ما نصّت عليه المادّة 2/39 من الدستور وهو ضمان سرّية المراسلات والإتصالات الخاصّة للأفراد بكلّ أشكالها، ويجعل من أهمّ ضماناتها كفالة الحماية الجزائية حينما يُقرّر الجزاء العقابي على انتهاكها. بالإضافة إلى الحماية العامّة في الفقرة الأولى من نفس المادّة والمتمثلة في عدم جواز انتهاك حرمة الحياة الخاصّة للمواطن وتقرير حماية القانون لها.

وأضاف التعديل الدستوري لسنة 2016[13] إضافة مُهمّة في هذه المادّة، وهي ضرورة تسبيب الأمر القضائي في الإجراءات التي تتضمّن المساس بحرمة الحياة الخاصّة. وهو مضمون الفقرة الثالثة التي أضافها التعديل المادّة 3/39 « لا يجوز بأيّ شكل المساس بهذه الحقوق دون أمر معلّل من السلطة القضائية. ويُعاقب القانون على انتهاك هذا الحكم».

كما أضاف التعديل فقرة رابعة لهذه المادّة تتضمّن حماية خصوصيات الفرد في البيانات الشخصية ضمن منظومة المُعالجة الآلية للمُعطيات تحت طائلة العقاب.

كما أضاف هذا التعديل الدستوري لسنة 2016 أنّ حق الحصول على المعلومة مُقيّد بضابط عدم المساس بالحياة الخاصّة للغير، هذا ما نصّت عليه المادّة المُضافة وهي المادة41 مكرر3.

ويمنع الدستور بموجب المادّة 2/38 القيام بحجز أي مطبوع أو تسجيل أو وسيلة أخرى للتبليغ والإعلام إلا بأمر قضائي، كما يكفل الدستور الجزائري أيضًا عدم انتهاك حرمة المسكن في المادّة 1/40. ويضمن حرّية التنقل والإقامة عبر التراب الجزائري والدخول إليه والخروج منه بموجب المادّة 44.

المطلب الثاني: الحماية الجزائية لحرمة الحياة الخاصّة:

على الرغم من أهمية وسائل تقنية المعلومات الحديثة، ومالها من آثار إيجابية سبق بيانها، الا أن هنالك مخاطر عديدة تواجه الحق في حرمة الحياة الخاصة بالنظر لإمكانية انتهاكه عبر وسائل تقنية المعلومات

الحديثة، ذلك أن سهولة عمليات التخزين والمعالجة الالكترونية وازدياد تدفق المعلومات التي تتم عبر وسائل تقنية المعلومات الحديثة، تضعف قدرة الفرد على التحكم في تدفق المعلومات الخاصة به.كما أن شبكات المعلومات أدّت الى ازدياد التهديدات لحرمة الحياة الخاصة إذ اصبحت المعلومات الشخصية في ظل الشبكه العالمية متوفرة، وقد أصبح الوصول إلى المعلومات الشخصية بصورة غير مشروعه أكثر من ذي قبل، وازدادت فرص إساءة استخدامها.

على سبيل المثال يتمّ تسجيل وتخزين كل المكالمات الهاتفية الصادرة من أوروبا إلى العالم بحج خمسين مليار دقيقة من الاتصالات الصوتية في السنة، وخطر المساس بالمعطيات الشخصية يبدأ من تقنية تخزين المعلوات في وحدات مادّية صغيرة، وصعوبة مراقبة معالجتها[14].

الفرع الأوّل: حماية حرمة الحياة الخاصّة في قانون العقوبات

ترتبط حماية حقوق الإنسان ارتباطًا وثيقًا بالقانون الجنائي، فالحماية الجنائية هي امتداد وتكريس للحماية التي يكفلها الدستور صيانةً لقيم المجتمع ومبادئه الأساسية. فقانون العقوبات ينظم السلوك الاجتماعي بما يتوافق مع هذه المبادئ، ويقرر العقوبات على المساس بحقوق الإنسان وحريته الشخصية. وقد أصبحت وسائل التنصت الإلكترونية تشكل خطرًا مستمرًا على هذه الحقوق والحريات، مصدره أجهزة السلطة أو الأفراد أو عصابات الجريمة.

كان قانون العقوبات يقتصر على تجريم أفعال الإعتداء على المُراسلات الكتابية إلى الغير عبر البريد أو البرق بسوء نية، بموجب المادّة 303 من ق ع ج، و يُعاقب عليها بالحبس والغرامة أو بإحداهما. وكان يُشدّد العقوبات إذا وقع فضّ أو تسهيل فضّ الرسائل أو البرقيات المسلّمة للبريد من طرف مُستخدمي أو مندوبي مصلحة البريد أو البرق، أو من أي مُوظف في الدولة، بموجب المادّة 137 من ق ع ج، وتكون الدولة مسؤولاً مدنيًا.

وتُعاقب المادّة 301 بالحبس والغرامة فعل إفشاء السرّ المهني من طرف جميع الأشخاص المُؤتمنين على أسرار أدلي بها إليهم بحكم وظيفتهم أو مهنتهم وخاصّة الأطبّاء والصيادلة والقابلات. بالإضافة إلى تجريم انتهاك حرمة المسكن بالمادة 295 ق ع ج، ومعاقبة من يدخل فجأة أو خدعة أو يقتحم منزل مواطن، بالحبس و الغرامة.

وفي سنة 2004 وبموجب القانون 04- 15 أدرج المشرّع في قانون العقوبات جريمة لها انعكاس على الحق في الخصوصية وهي جنحة انتهاك المعطيات المعالجة آليًا نصّت عليها المادّة 394 مكرّر.

بتعديل قانون العقوبات في 23 ديسمبر2006 بالقانون 06-23، مدّد المُشرّع الجزائري هذه الحماية الجنائية بالنص على جريمة التعدي على حرمة الحياة الخاصّة للأشخاص باستخدام الوسائل التقنية، وذلك عن طريق التقاط الأحاديث الشفوية الخاصّة وتسجيلها ونقلها. والتنصت على المراسلات التي تتم

بوسائل الإتصال السلكي واللاسلكي، والتقاط أو تسجيل أو نقل صور الأشخاص. فعاقب بموجب المادة 303مكرر بالحبس والغرامة كل من يتعمّد المساس أو يشرع في المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك عن طريق التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه. والتقاط أو تسجيل أو نقل صورة شخص في مكان خاص بغير إذنه أو رضاه. وعاقبت المادة 303 مكرر1 بنفس العقوبات على جرائم الإحتفاظ والإفشاء والإستخدام للتسجيلات المُتحصلة عن طريق جرائم التنصت والتصوير الخفي المنصوص عليها بالمادّة 303 مكرر. ويُعاقب على الشروع فيهابنفس العقوبة. إلا أنّ صفح الضحية يضع حدًّا للمُتابعة الجزائية.

وبموجب المادة 303 مكرر3 يمكن أن تُقام المسؤولية الجزائية للشخص المعنوي عن هذه الجرائم طبقا للشروط المنصوص عليها في المادة 51 مكرر.

وذكرت المادّتان 144مكرّر و146مكرّر استخدام الوسائل التقنية للمراقبة في جنحة الإساءة لمؤسسات الدولة، فعاقبت على الإهانة أو السب أو القذف باستعمال أية آلية لبث الصورة أو الصوت أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى، ضدّ رئيس الجمهورية أو ضدّ البرلمان أو إحدى غرفتيه أو ضدّ الجهات القضائية أو ضدّ الجيش الشعبي الوطني، أو أيّة هيأة نظامية عمومية أخرى.

وبالنسبة للإساءة إلى رئيس الجمهورية تباشر النيابة العامة إجراءات المتابعة تلقائيًا. وبتعديل المادّتين 144مكرّر و146 ق ع في 2 أوت 2011، بالقانون 11-14 ألغي منها الحبس ورفع مبلغ الغرامة.

الفرع الثاني: حماية حرمة الحياة الخاصّة في قانون الإجراءات الجزائية:

كضمانة لمبدأ الشرعية الإجرائية، ينظم قانون الإجراءات الجزائية كيفية وحدود المساس بالحقوق والحريات الفردية عندما تقتضيه حماية المصلحة العامّة للمجتمع في العدالة والأمن والنظام العام والأخلاق والصحة العامّة والمصالح التي تكون أولى بالرعاية من مصلحة الفرد في حياته الخاصّة.

ففي التحقيق كان المشرّع الجزائري يُكرّس الحماية الإجرائية للحياة الخاصّة من خلال حق الدفاع في المادّة 11 من ق إ ج بالنصّ على عدم الإضرار بحقوق الدفاع، وبعد تعديل المادّة في 23 جويلية 2015 بالأمر 15- 02 أضاف فقرة تنصّ على وجوب مُراعاة قرينة البراءة وحُرمة الحياة الخاصّة.

واحترامًا لحقوق الدفاع كذلك نصّ المُشرّع عند تعديل ق إ ج في 2015 في المادّة 51 مُكرّر1 على حق المُشتبه فيه المحتجز تحت النظر بسبب الجريمة المنظمة أن يتلقى زيارة المحامي له في حالة تمديد الاحتجاز، وأكّدت هذه المادّة بأنّ هذه الزيارة تكون في غُرفة خاصّة تُضمن فيها سرّية المُحادثات بين المشتبه فيه ومحاميه.

المبحث الثاني: التعريف بمراقبة الإتصالات الإلكترونية كأسلوب خاصّ للتحرّي والتحقيق

يُجيز القانون في حالات مُعيّنة، التدخل في الحياة الخاصّة بصفة مشروعة من أجل تحقيق مصلحة عامّة، مثل إجازته التصدّي للمراسلات والاتصالات الإلكترونية والتقاط الأحاديث والصور بمبرّرالكشف عن نوع مُعيّن من الجرائم الخطيرة. حيث نُبيّن في هذا المبحث مفهوم التراسل والاتصال الإلكتروني، ومفهوم المُراقبة الإلكترونية المُنصبّه عليه ومدى مشروعية ذلك.

المطلب الأول: تعريف مراقبة الإتصالات الإلكترونية وتقنياتها

تتميز المراقبة الإتصالات الإلكترونية بطابعها التقني ومصطلحاتها العلمية الدقيقة في مجال المعلوماتية وتكنولوجيا الاتصال، واستخدامها كإجراء من إجراءات التحري يجعلها مرتبطة من جهة أخرى بمفاهيم ومصطلحات قانونية، لذي يتعين توضيح تلك المفاهيم والمصطلحات التقنية من الناحية القانونية.

الفرع الأوّل: تعريف مُراقبة الاتصالات الإلكترونية:

أوّلاً: مفهوم الاتصالات الإلكترونية:

أ) في بعض الدول الأوربية:

1- في فرنسا حسب مفهوم المادّة 32 من قانون البريد والمواصلات، فالإتصالات الإلكترونية هي كل وسيلة تُستعمل في إرسال أو استقبال أو نقل لإشارات أو علامات للكتابة أو الصورة أو الصوت، أو تسجيل مهما كانت طبيعته، عبر الأسلاك أو الألياف البصرية أو الراديو كهربائية أو أيّة وسيلة كهرومغناطيسية[15]. وحُدّدت طبيعة المراسلات السلكية واللاسلكية في المادّة 226-15 من قانون العقوبات، بأنّها كل أنواع الإتصالات التي تتمّ عن بُعد سواء كانت عن طريق الهاتف أو الفاكس أو البريد الإلكتروني والإنترنت والأقمار الصناعية[16].

2- في بلجيكا يأخذ قانون العقوبات في المواد 259 مُكرّر فقرة1 و314 مُكرّر فقرة1 من بالمفهوم الواسع لمحكمة النقض، بأنّه يشمل كل ما يتمّ ذكره سواء شفاهة أو ليس شفاهة، وسواء مباشرةً أو عن بُعد وجميع الأشكال الحديثة لخدمات الإتصال عبر شبكة الإعلام الآلي، ووسائل الإتصال السلكي واللاسلكي التي تشمل أجهزة الإرسال المُتمثلّة في العناصر الصوتية من خلال هاتف ثابت أو خلوي أو الحاسوب، والإشارات الإلكترونية للنصوص أو الصور مثل البريد الإلكتروني وغيره[17].

ب) في الجزائر: يتضح مفهوم المراسلات والاتصالات الإلكترونية من خلال عدّة قوانين:

1- في قانون البريد والاتصالات الالكترونية 18-04[18] عرّف المشرّع الاتصالات الإلكترونية في المادّة 10 منه بقوله " يُقصد بالاتصالات الإلكترونية في مفهوم هذا القانون، 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". وكان يُصطلح عليها "الإتصالات السلكية واللاسلكية" في قانون

قانون البريد والمواصلات السابق المُلغى 03.2000[19]. وهو ذاته التعريف الذي ورد ضمن المادّة الثالثة من قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي18-07 المُؤرّخ في 10 يونيو 2018[20].

وعرّفت المادّة 10/ 16المذكورة أعلاه، خدمة الإتصال الإلكتروني للجمهور بأنّها " كل خدمة تتمثّل كليا أو أساسا في تزويد الجمهور بالاتصالات الإلكترونية، وكذا الخدمات التي تستعمل قدرات شبكات الاتصالات الإلكترونية والتي تتطلّب زيادة على خدمة الاتصالات الإلكترونية القاعدية وظائف المُعالجة أو التخزين". كما عرّفت "الإنترنت" الفقرة5 من نفس المادّة بأنّها شبكة معلوماتية عالمية تتشكل من مجموعة شبكات وطنية وإقليمية وخاصة، موصولة فيما بينها عن طريق بروتوكول الاتصال(IP) لتُقدم واجهة موحدة لمستعمليها.

2- في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها رقم 09-04[21]عرّفتُ الفقرة (د) من المادة الثانية منه "الإتصالات الإلكترونية" بأنّها " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صورة أو أصوات أو معلومات مُختلفة بواسطة أية وسيلة إلكترونية". وأظيفت عبارة " بما في ذلك وسائل الهاتف الثابت والنقّال" بموجب المادّة 5 من المرسوم الرئاسي15.261 يُحدّد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المُتصلة بتكنولوجيا المعلومات والإتصال[22].

ثانيًا: الحماية القانونية للاتصالات الإلكترونية:

أ) في فرنسا: من بين أنواع الحماية القانونية في فرنسا نذكر الحماية الجزائية بنصّ المادّة 226-15 من قانون العقوبات، للإتصالات الإلكترونية الهاتفية السلكية منها واللاسلكية، والإتصالات التي تتمّ عبر شبكات الإعلام الآلي. وذلك ضدّ كافّة أنواع أفعال الإعتراض لهذه الإتصالات، حيث يُمكن أن تكون الجريمة قائمة عند بداية المكالمة أو عند إرسال المراسلة أو عند وصولها، مثلاً عن طريق الدخول في الخط عبر خط آخر، أو بالتطفل على صندوق البريد الإلكتروني المؤمّن بالرقم السرّي[23]

ب) في الجزائر: تتظافر عدّة قوانين لحماية سرية وخصوصية الإتصالات الإلكترونية من بينها:

1- خصوصية الإتصالات الإلكترونية في قانون البريد والاتصالات الإلكترونية: تُلزم المادّة119 مُتعاملي الاتصالات الإلكترونية باتخاذ التدابير التي من شأنها أن تضمن سرّية المكالمات والمعلومات التي يحوزونها عن مشتركيهم، وألاّ يسمحوا بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مُراقبة المكالمات الهاتفية والوصلات والمحادثات والمبادلات الإلكترونية دون إذن مسبق من السلطة القضائية. ويجب عليهم أن يُطلعُوا أعوانهم على التزاماتهم والعقوبات التي يتعرضون لها عند عدم احترامهم لهذه الأحكام.

وتُنظم المادّة 164 أحكام جريمة التنصّت على الإتصالات السلكية واللاسلكية. والمادّتان 165 و166 من نفس القانون تنصّ على جريمة تحويل مضمون الإتصالات السلكية واللاسلكية، بإفشائها أونشرها واستعمالها. وحسب المادّة 187 يُتعتبر الشخص المعنوي مسؤولاً جزائيا عن هذه الجرائم طبقًا ببقواعد المنصوص عليها في قانون العقوبات.

2- **خصوصية الإتصالات الإلكترونية في قانون العقوبات:** يكفل المُشرّع لهذا النوع من المُراسلات والاتصالات حمايةً جزائية في سريتها وخصوصيتها، حيث أنّ اعتراضها أو الاطلاع عليها أوتحويلها يُعتبر جنحة اعتداء على حرمة الحياة الخاصّة طبقًا للمواد 303 مُكرّر. 303مُكرّر3، ويُمكن أن تُشكّل جنحة المساس بأنظمة المُعالجة الآلية للمُعطيات بالمواد 394 مُكرّر إلى 394 مُكرّر7 من ق ع. حيث عُرِّفت جرائم تكنولوجيا الإعلام والإتصال في المادّة2 (أ) من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بأنّها جرائم المساس بأنظمة المعالجة الآلية للمُعطيات المُحدّدة في قانون العقوبات، وأي جريمة أخرى تُرتكب أو يُسهّلُ ارتكابُها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية. وكذلك يُجرّم عدم قيام مُقدّم خدمات الإنترنيت، لالتزامه بالتدخل وسحب أو تخزين أو حجب مُحتويات تُشكّل جرائم، وعدم وضع الترتيبات التقنية التي تسمح بالسحب والتخزين(المادة 394مُكرر8). وجريمة الإرهاب الإلكتروني في المواد87 مُكرّر11 و87 مُكرّر12 ق ع[24].

3- **حماية خصوصية الإتصالات الإلكترونية في قانون الوقاية من جرائم تكنولوجيات الإعلام والإتصال ومكافحتها**[25] يتضمّن هذا القانون الكثير من الأحكام التي فيها حماية لسرّية وخصوصية الأفراد، مثل المادّة3 منه التي نصّت على أنّه يجب مراعاة الأحكام القانونية التي تضمن سرّية المراسلات والإتصالات عند وضع الترتيبات التقنية لمراقبة الإتصالات الإلكترونية وتسجيلها وتجميعها عندما يقتضيها ضرورات التحريات والتحقيقات القضائية الجارية، أو يقتضيها الحفاظ على النظام العام. والمادّة 4 التي أوجبت أن تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة (أ) في إطار احترام الحياة الخاصّة للغير تحت طائلة العقوبات. كما أنّ المادّة 27 من المرسوم الرئاسي 15-261 المُنظم الهيئة الوطنية للوقاية من الجرائم المُتصلة بتكنولوجيا الإعلام والإتصال، ألزمت مُستخدمي الهيئة بالسرّ المهني وواجب التحفظ، حيث يؤدّون اليمين على كتمان سرّية المعلومات التي يُحصّلونها أثناء مراقبة الاتصالات الإلكترونية.

ثالثًا: مفهوم مُراقبة المراسلات والاتصالات الإلكترونية

يتمّ هذا النوع من المُراقبة عن طريق اعتراض المراسلات والاتصالات الإلكترونية بالتقاطها أوالاطلاع عليها أو تسجيلها أو نقلها، حيثُ يُعرّف اعتراض الاتصالات هنا بأنّه إدخال تدابير تقنية مُمغنطة في خط أحد المُشتركين لتسجيل المكالمات عن طريق البحث عن مصدر الإتصال من خلال عنوان(*IP*) في جهاز

الحاسب الآلي الذي يجري منه الإتصال بالموقع ولا يُعتبرُ اعتراضًا للمراسلة الإلكترونية مُجرّد ربط الإتصال بشبكة الإنترنت(*Se connécter*) وقراءة ما يمكن لأي مُتصل قراءته دون إحداث تعديلات مُسبقة بتدابير تقنية مُمغنطة، وهو يُشبه اعتراض المكالمات الهاتفية ولذلك اتفق الفقه والقضاء على تطبيق أحكام هذا الأخير على الإتصالات والمُراسلات بواسطة الإنترنيت[26].

وتناولت اتفاقية بودابست لجرائم الإنترنت 23 نوفمبر2001 في المادّتين 20 و21 أحكام تجميع ومراقبة البيانات أثناء الزمن الفعلي، وهي البيانات التي تتم أثناء التراسُل وتبادل الاتصالات من خلال نظام المعالجة الآلية للمعطيات، حيث تشير عبارة "مراقبة الإتصالات" إلى شبكات الإتصالات التقليدية التي تكون بنيتها الأساسية هي الكابل بما في ذلك نظام الهاتف أو الألياف البصرية والهاتف النقال وشبكات الأقمار الصناعية الخاصّة، وشبكات الحاسوب العالمية[27].

الفرع الثاني: تقنيات مُراقبة المراسلات والاتصالات الإلكترونية:

أوّلاً: حفظ مُعطيات حركة السير

في إطار الانترنت يكون مُزوّد خدمات الانترنت (*ISP*) هو المُسيطر على مُخرجات حركة البرامج فهو الذي يسمح بدخولنا إلى الإنترنت (*Log in*) والتمتع بخدماتها. ولمعرفة زمن الدخول إلى الإنترنت من قبل مرتكب الجريمة لا يتم اللجوء إلى حاسوب المستخدم في العادة، وإنما يتم اللجوء إلى مزود خدمات الانترنت. وتفيد مُخرجات حركة البرامج في إطار جرائم الانترنت كونها تُساهم في ربط السلطات بالمجرم المعلوماتي بالسرعة الكافية.

يُعتبرُ حفظ البيانات أداة تحقيق جديدة في إطار جرائم الحاسوب والجرائم المرتبطة بها، حيث تكون البيانات محلاً للتلاعب، ممّا يؤدّي بالدليل إلى الضياع بسهولة من خلال الإهمال في التخزين، أو التلاعب العمدي أو الحذف المُصمّم بتدمير الدليل، أو الحذف الروتيني للمعلومات التي لم تعد لها حاجة. ولذلك يجب أن يكون المسؤول عن حفظ البيانات جديرًا بالثقة يُمكن معه تأمين مصداقية البيانات استنادًا إلى أمر حفظ البيانات. كما أنّ الكم الهائل من التراسل والإتصالات يمكن أن يؤدي إلى تداخل المعطيات، فيُصبح تحديد مصدر الإتصال أو جهة إرساله مهم جدًّا لمعرفة هوية مرتكبي الجريمة، ولهذا فحفظ حركة البيانات المتعلقة بالإتصال هو أمر لازم لأنه هو الذي يسمح بتتبع الإتصال ومعرفة مصدره، فيكون الإجراء أفضل من التفتيش والضبط المعلوماتي[28].

أ) في الجزائر وبهدف مُساعدة السلطات القضائية المكلفة بالتحري والتحقيق، يقوم مقدّمو الخدمات بحفظ مُعطيات حركة السير بتسجيلها والإحتفاظ بالتسجيلات لمُدّة سنة من تاريخ التسجيل. وهي

المُعطيات التي عرّفتها الفقرة (ه) من المادّة2 من قانون الوقاية من جرائم تكنولوجيا الإعلام والإتصال،بأنّها " أي مُعطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تُنتجها هذه الأخيرة باعتبارها جُزءًا من حلقة اتصالات، توضح مصدر الإتصال، والوجهة المُرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومُدة الإتصال ونوع الخدمة". ونصّت المادّة 11 على الالتزام المفروض على مُقدّمي خدمات الإنترنيت بحفظ معطيات حركية السير وبيّنت أنواعها.

ب) وفي فرنسا تفرض المادّة 34 من قانون البريد والإتصالات الإلكترونية على مُورّدي خدمات الإنترنيت التزامًا بحفظ المُعطيات غير المشروعة من أجل تقديمها عند الحاجة إلى السلطات القضائية والمصالح المُكلّفة بمحاربة الإرهاب، دون أن يُنشئوا ملفات أو قوائم إسمية لمُستخدمي الشبكة، ولا القيام بحفظ الإتصالات التي تتم بواسطة الرسائل القصيرة الـ (*SMS*) أو عن طريق الـ (*e-mail*). كما أنّ قانون مكافحة الإرهاب 2006-64 المؤرّخ 23 جانفي 2006 يوسّع هذا الإلتزام بالحفظ إلى مقاهي الإنترنيت والأشخاص الذين يُورّدون لزبائنهم خدمة الإنترنيت كالفنادق وشركات الطيران بصفة مجانية أو بمقابل عبر اللاسلكي (WIFI). وصدر في فرنسا أيضًا مرسوم خاص بهذا الإجراء وهو المرسوم 2006-358 في 24مارس2006 يتعلّق بحفظ مُعطيات الإتصال الإلكتروني، يُحدّد بالتفصيل أنواع المعطيات التي يجب حفظها، وهي محصورة بالمادّة (1.L34)من هذا القانون[29].

ج) وفي اتفاقية بودابست لجرائم الإنترنيت لسنة 2001، نصّت على هذا الإجراء المادّة 16 وكيفية الحصول على حفظ مُعجّل لبيانات حاسوب مُحدّدة أثناء قيام إجراء جنائي مُحدد ضمن الإختصاص الوطني للسلطات القضائية. حيث عرّفت الاتفاقية في المادّة الأولى فقرة(*b*) حركة البيانات (*Traffic data*) بأنّها: " صِنفٌ من بيانات الحاسوب التي تُشكل محلاً لنظام قانوني مُحدّد، حيث يتم توالد هذه البيانات من الحواسيب عبر تسلسل حركة الإتصالات لتحديد مسلك وشكل الإتصالات من مصدرها إلى الجهة المقصودة". وتشمل حركة البيانات خاصّةً " المصدر" الذي يُشير إلى رقم الهاف أو عنوان الـ(*IP*) بروتوكول الإنترنيت(*Internet Protocol*)، و" الوجهة المقصودة " أي الإشارة التي يتم إرسال الإتصال إليها، و"نوع الخدمة التي يحتويها" أثناء الإتصال مثل البريد الإلكتروني أو المراسلات الفورية.

ويتطلب حفظ البيانات أن توضع هذه البيانات في هيأة مخزنة ومحمية من أي شيء يمكن أن يتسبّب في تغيير أو تعييب معالمها الفعلية والإستمرار في تأمينها من التعديل والتدمير والحذف. لكن لا يعني حفظ البيانات تجميدها بخاصية منع الدخول إليها مثلا، وأن لا يكون هناك مجال لنسخها، وأن لا يتم الإستعانة بها ولو بشكل مشروع. وتُحدّد المادّة 2/16 من اتفاقية بودابست الحد الأقصى لمدة الحفظ ب 90 يومًا للسماح للسلطات المختصة باتخاذ الإجراءات الضرورية للكشف عنها[30].

ثانيًا: التسرّب الرقمي

التسرُّب الرقمي هو تسلّل معلوماتي يسمح بالدخول بطريقة احتيالية مُخادعة في مُنتدى حوار، أو على المواقع. وهو يُعدُّ من تقنيات التحري الإستثنائية التي لا يجب أن تُستخدم إلاّ من طرف مُحققين مؤهلين خصيصًا مركزيين أو جهويين، في إطار التحري والتحقيق عن الجريمة المنظمة المنصوص عليها في المادّة 73-706 من ق إ ج ف وفقط. وفي القانون رقم 2007-297 المؤرّخ في5 مارس2007 المُتعلّق بالوقاية من الإجرام، عدّلت المادّة (III35) منه قانون الإجراءات الجزائية الفرنسي من أجل السماح لضباط الشرطة القضائية المُؤهلين خصيصًا للقيام بالتسرّب بغرض تسهيل مُعاينة بعض الجرائم التي تُرتكب بواسطة وسائل الإتصال الإلكتروني وجمع أدلتها وكشف مرتكبيها. وتُتيح المادّة 1/35-706 من ق إ ج ف لضباط الشرطة القضائية المتخصصين أثناء التحريات أو بموجب إنابة قضائية، باتخاذ إجراء التسرب الإلكتروني لمعاينة وكشف الجرائم المقرّرة بالمواد225-4-1 إلى225-4-9 والمواد 225-5 إلى225-12 والمواد 225-12-1 إلى 225-12-4 من قانون العقوبات الفرنسي خاصّة منها الجرائم المتعلقة بتصوير مشاهد الشذوذ الجنسي الخليعة وجرائم الدعارة، واستخدام القصر لأغراض جنسية والإتجار بالرقيق عبر الإنترنيت. وكذلك تسمح المادّة 3-47-706 من ق إ ج ف، بالتسرّب المعلوماتي من أجل المعاينة وجمع الأدلة وكشف مرتكبي الجرائم المنصوص عليها في المواد 227-8 إلى 227-24 من قانون العقوبات الفرنسي عندما تُرتكب هذه الأخيرة باستعمال وسائل الإتصال الإلكتروني. فهذه الأحكام تسمح لضابط الشرطة القضائية أثناء التحريات أو التحقيق الإبتدائي أن يُشارك بإسم مُستعار في التراسلات الإلكترونية، وأن يكون في اتصال إلكتروني مع الأشخاص المُشتبه فيهم ارتكابهم جرائم جنسية. أو بناءًا على طلب استعجالي في جريمة استخراج أو حيازة أو حفظ مضمون غير شرعي للمعطيات، بشرط أن لا تُشكل هذه الأعمال تحريضًا على الجريمة. و تُحدّد المواد (D47-8,9,11) من ق إ ج ف، إطارًا لضباط الشرطة القضائية المؤهلين لاستخدام التسرّب في شبكات الإنترنيت. بوجوب إذن قضائي مُسبب لتنفيذه تُذكر فيه الجريمة وهوية المتسرّب والضابط المسؤول عن العملية، ومُدتها[31].

ثالثًا: التقاط المُعطيات:

من ضمن صور الإعتراض والمراقبة في مجال الإتصالات الإلكترونية، توجد المراقبة عن طريق أسلوب الإلتقاط عن بُعد للمعطيات عبر أنظمة المعالجة الآلية، نصّ عليها مشروع قانون التوجيه والبرمجة في الأمن الداخلي الفرنسي. والذي يسمح لضباط الشرطة القضائية المنتدبين في إنابة قضائية أن يقوموا بدون رضا المعني، بوضع تدابير تقنية بغرض الدخول في أي حيّز كان إلى مُعطيات الإعلام الآلي، وتسجيلها والإحتفاظ بها ونقلها مثلما هي معروضة على الشاشة للمستخدم. حيثُ يسمح هذا الإجراء بوضع حصان الطراودة بدون علم المشتبه فيه، حيث يُستعمل بضمانات إجرائية صارمة وخاصّة تحت رقابة القاضي.

وهي لا تُطبّق إلا في الجرائم الخطيرة المرتكبة في إطار العصابات ، وهذه المراقبة يمكن أن تدوم (8) أشهر، أي (4) أشهر قابلة للتجديد مرّة واحدة في أيّة لحظة[32].

ويمكن للسلطة التي تقوم بالتفتيش في منظومة معلوماتية استعمال التقنيات اللازمة لحجز المُعطيات عن طريق منع الوصول إلى المعطيات التي تحتويها منظومة معلوماتية أو نسخها طبقًا المادّة 7 القا 09-04.

رابعًا: فتح المُعطيات المُشفرة:

بصدور القانون2001-62 المؤرّخ في15 نوفمبر2001المتعلّق بالأمن أصبحت المواد 1.230 إلى 230-5 من ق إ ج الفرنسي تُرخّص لقاضي التحقيق استخدام تقنيات فك الرسائل المشفرة. حيث متى كان هذا الإجراء ضروريًا لإظهار الحقيقة، بإمكان قاضي التحقيق تعيين أي شخص طبيعي أو معنوي مُتخصّص مؤهل لتنفيذ العملية التقنية التي تسمح بالحصول على الصيغة المجانية أو المفتوحة (*Claire*) للمعلومات أو مُعادلة فك الشفيرة في حالة استخدام تقنية التشفير(*Cryptage, Chiffrement*) وقرارات قاضي التحقيق بهذا الشأن غير قابلة للطعن. ومن أمثلة هذا الإجراء أنّه عندما يجري التحري أو التحقيق في جرائم مُعاقب عليها بالحبس لمُدّة تُساوي أو تجاوز السنتين، يُمكن لقاضي التحقيق استخدام الوسائل المشمولة بأسرار الدفاع الوطني، بموجب تسخيرة موجهة إلى الديوان المركزي لمكافحة جرائم تكنولوجيا الإعلام (*OCLCTIC*) حيث يقوم هذا الديوان بإحالة الطلب أو التسخيرة إلى هيأة تقنية خاضعة لأسرار الدفاع الوطني ومُعيّنة بموجب مرسوم. ونفس الإجراءات تُتبع في حالة قطع أو توقيف العملية. ويتمّ إرسال نتائج العملية من طرف الديوان إلى السلطات القضائية التي تُحرّر محضرًا بالإستلام يُضم إلى ملف الإجراءات، حيث يُمكن الإطلاع على هذه المعلومات المرتبطة بأسرار الدفاع الوطني من قبل الأطراف لمناقشتها في طعونهم[33].

المطلب الثاني: مشروعية مراقبة الإتصالات الإلكترونية:

نظرًا لمساسها بالحرمة الحيات الخاصّة للأفراد، وتعارضها مع النصوص الدولية والدستورية لحقوق الانسان، فقد أثار الإجراء في البداية جدلاً فقهيًا، ولاقى معارضة من بعض اتجاهات الفقه وتأخرت الكثير من تشريعات الدول في تكريسه. لكن بسبب ضرورته وأهميته في إجراءات التحري، فقد تمّ تكريسه بنصوص قانونية على الدولي والوطني.

الفرع الأوّل: مشروعية مراقبة الإتصالات الإلكترونية في قوانين بعض الدول الأوروبية:

أوّلاً: في بلجيكا:

صدر قانون 30 أفريل 1994 المُعدّل في 10 جوان 1998 يتعلّق بحماية الحياة الخاصّة ضدّ التنصّت والإستخبارات وتسجيل المُحادثات والإتصالات السلكية واللاسلكية الخاصّة وغيرها من الأفعال يُجيز لقاضي التحقيق ووكيل النيابة لدى الملك اتخاذ إجراءات مثل التنصّت والتسجيل بموجب المواد 90*ter* إلى 90*monies* من قانون التحقيقات الجنائية، والتقاط الصور بموجب المادّة 88 مُكرّر، والتعرّف على هوية الإتصالات السلكية واللاسلكية الخاصّة بالمادّة 46 مُكرّر من نفس القانون. وبعد صدور قانون الإجرام المعلوماتي لسنة 2000 أضاف المُشرّع البلجيكي أشكالاً جديدة من الجرائم التي تُبرّر اتخاذ الإجراءات المتعلّقة بالإتصالات السلكية واللاسلكية والإلكترونية بواسطة وسائل الإعلام الآلي. ثمّ صدر قانون6جانفي2003 المتعلّق بأساليب التحري الخاصّة ، فوسّع من سلطات التحقيق وسمح بالتنصت المباشر من طرف قاضي التحقيق[34].

ثالثًا: في فرنسا:

أصبح لتكنولوجيات الحديثة للإعلام والاتصال قيمة إثباتية في المجال الجنائي نظرًا لما للعالم الافتراضي عالم المعلوماتية من آثار وبصمات من خلال تبادل المعطيات، حيث أنّ أحكام قانون1991 المتعلّقة باعتراض المراسلات والاتصالات السلكية واللاسلكية تُطبّق على جرائم المعلوماتية والإنترنيت لكشف مُستخدميها من المجرمين، مثل مُنتديات الدردشة انطلاقًا من العنوان (*IP*) المُرتبط بالحاسوب أو(*URL*) المُرتبط بالموقع، حيث هناك إمكانية للإلتقاط عن بُعد لمُعطيات مُعالجة آليًا سواء الظاهرة على الشاشة أو المكتوبة بلوح الأحرف(*Clavier*) الخاصّين بالشخص المعني أو في إطار إجراءات التفتيش والحجز داخل منظومة معالجة ألية للمعطيات طبقًا للمادّة 97 من ق إ ج[35]

ثمّ ابتداءً من سنة 2000 تدعّمت الإجراءات الجزائية بوسائل وأساليب جديدة للتحرّي والتحقيق للحصول على الأدلّة الرقمية، فصدر قانون التوجيه والبرمجة من أجل الأمن الداخلي في2003، وقانون الإئتمان في الإقتصاد الرقمي في 2004، وقانون تكييف جهاز القضاء مع الإجرام 2004 جاءت بأساليب حديثة لفاعلية وسرعة التحريات. كحفظ المُعطيات غير المشروعة (*Conservation des données de trafic*)، وشرطة الإنترنت(*Cyber patrouilles*)، واعتراض الإتصالات الإلكترونية (*L'interception des communication électronique*)بالإضافة إلى الأساليب الإجرائية التقليدية التي ظلت قابلة للتطبيق في مجال جرائم الإنترنيت[36].

الفرع الثاني: مشروعية مُراقبة الاتصالات الإلكترونية في القانون الجزائري:

أوّلاً: في قانون الإجراءات الجزائية:

عند تعديل قانون الإجراءات الجزائية بالقانون 06-22، كرّس المُشرّع ضمن المواد 65 مُكرّر5 إلى65مُكرّر10 المراقبة الإلكترونية عن طريق اعتراض ونقل وتسجيل المراسلات التي تتم بواسطة وسائل

الإتصال السلكية والسلكية وتشمل إتصالات الهاتف الثابت والهاتف النقال والإتصالات الإلكترونية عبر الشبكة الرقمية والإنترنيت وتسجيل والتقاط ونقل الأحاديث والصور، ونظّم شروط استخدامها في التحقيات الجنائية. وهي التي أشار إليها قانون الوقاية من الفساد ومكافحته[37] بموجب المادّة 56 « من أجل تسهيل جمع الأدلّة المتعلّقة بالجرائم المنصوص عليها في هذا القانون يمكن اللجوء إلى أساليب التحرّي الخاصّة كالترصّد الإلكتروني...على النحو المناسب بإذن من السلطة القضائية المختصّة ...».

ثانيًا: في قانون الوقاية من جرائم تكنولوجيات الإعلام والإتصال ومكافحتها[38] :

بهذا القانون نظّم المُشرّع مُراقبة الإتصالات الإلكترونية التي تتم عبر الإنترنيت والشبكات الرقمية، حيث جعلت المادّة 3 من بين مجالات تطبيقه مُراقبة الإتصالات الإلكترونية عن طريق وضع الترتيبات التقنية وتجميع وتسجيل محتواها في حينها. وخصّص في المادّة 4 فصلاً مُستقلاً لمراقبة الإتصالات الإلكترونية والحالات التي تسمح بها. وأنشأ في فصله الخامس بموجب المادّتين 13 و14 الهيئة الوطنية للوقاية من الجرائم المُتصلة بتكنولوجيا المعلومات والإتصال. وبيّن المرسوم 15-261 تشكيلة وتنظيم وكيفية سير الهيئة. حيثُ نصّت المادّة 4 منه على مهام الهيئة ومن أهمّها ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة. ونصّت المادّة 21 « بأنّه تُكلّف الهيئة حصريًا بمراقبة الإتصالات الإلكترونية وتسجيل مُحتواها في حينها والقيام بإجراءات حجز وتفتيش داخل منظومة معلوماتية تحت سُلطة قاض مُختصّ، ووفقًا لأحكام المادّة 4 من القانون 09-04»

وتُكلّف بتنفيذ عمليات مراقبة الإتصالات الإلكترونية مصلحة داخل هذه الهيئة تُسمّى مُديرية المُراقبة والوقاية واليقظة الإلكترونية. حيث طبقًا للمادّة11 من المرسوم الرئاسي تُكلّف مُديرية المُراقبة والوقاية واليقظة الإلكترونية على الخصوص بتنفيذ عمليات المُراقبة الوقائية للإتصالات الإلكترونية من أجل الكشف عن الجرائم المُتصلة بتكنولوجيا الإعلام والاتصال بناءً على رُخصة مكتوبة من السلطة القضائية وتحت رقابتها طبقًا للتشريع الساري المفعول، وإرسال المعلومات المُحصّل عليها من خلال المُراقبة الوقائية، إلى السلطات القضائية ومصالح الشرطة القضائية، المُختصّة، وتنفيذ طلبات المُساعدة القضائية الأجنبية في هذا المجال.

المبحث الثالث: شروط مُراقبة الاتصالات الإلكترونية

حتى يكون أسلوب مُراقبة الاتصالات الإلكترونية مُنتجًا وفعّالاً في تحقيق أهدافه الإجرائية بالكشف عن حقيقة الجريمة ومُرتكبها، دون أن ينطوي على تعسف وانتهاك لسرّيّة وخصوصية الاتصالات الالكترونية ينبغي أن يستجيب لشروطه القانونية من ناحية إجراءات ترخيصه وتنفيذه.

المطلب الأوّل: شروط ترخيص مُراقبة الاتصالات الإلكترونية

يمكن تقسيم هذه الشروط إلى شروط موضوعية تتصل بالجريمة والمجرم، وشروط إجرائية تتصل بكيفيات الترخيص ومدّته والسلطات المختصّة بذلك.

الفرع الأوّل:الشروط الموضوعية لترخيص المراقبة الإلكترونية:

أوّلاً: الجريمة موضوع الإجراء:

أ) أنواع الجرائم موضوع المراقبة الإلكترونية: تكرّست تدابير المراقبة الإلكترونية في القانون الجزائري كأسلوب من أساليب التحرّي والتحقيق على أنواع مُحدّدة على سبيل الحصر من الجرائم الخطيرة في المادّة 65 مُكرّر5 من قانون الإجراءات الجزائية وهي جرائم نظم المعالجة الآلية للمعطيات وجرائم والإرهاب، والمُتاجرة بالمُخدرات، وتبييض الأموال وجرائم الفساد وجرائم الصرف، والجريمة المنظمة عبر الوطنية. ويرجع للقاضي مُصدر الإذن، تقدير مدى توفر الوصف الجنائي في الأفعال محل التحرّي والتحقيق كمبرّر وشرط موضوعي لاتخاذ إجراء المراقبة الإلكترونية.

وتُحدَّد حالات اللجوء إلى مُراقبة الإتصالات الإلكترونية كذلك بموجب المادّة 4 من قانون الوقاية من جرائم تكنولوجيا الإعلام والاتصال 09-04 في قسمين، أوّلهما كمراقبة إدارية تدخل في إطار الضبط الإداري للوقاية من جرائم الإرهاب والتخريب والمساس بأمن الدولة والنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني. والثاني يدخل في إطار الإجراءات الجزائية للضبط أو التحقيق القضائي وله حالتان: حالة مُقتضيات التحرّيات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة في الأبحاث الجارية دون اللجوء إلى المُراقبة الإلكترونية. وحالة تنفيذ طلبات مُساعدة قضائية دولية مُتبادلة.

وبموجب المادّة 26 من المرسوم الرئاسي15-261 المُنظم الهيئة الوطنية للوقاية من الجرائم المُتصلة بتكنولوجيا المعلومات والإتصال، يجب تحت طائلة العقوبات الجزائية ألاّ تُستخدم التسجيلات والمُعطيات لأغراض أخرى غير تلك المُتعلّقة بالوقاية من الجرائم المُتصلة بتكنولوجيا الإعلام والاتصال ومُكافحتها وذلك وفقًا للأحكام المنصوص عليها في القانون 09-04. ولهذا الغرض رخّصت المادّة 30 من نفس المرسوم للقضاة القيام بتفتيش مكان أو هيكل بلغ إلى علمهم أنّه يحوز أو يستعمل تجهيزات موجهة لمراقبة الإتصالات الإلكترونية، وفي حالة مُعاينة أفعال جزائية تُخطر النائب العام المُختص للقيام بالمُتابعة المحتملة.

ب) مُقتضيات وضرورات التحرّي والتحقيق: مثل أي إجراء تطفلي يجب أن يكون إعتراض المراسلات الالكترونية ضروريًا لإظهار الحقيقة، وهذا الشرط نصّت عليه المادّة 2/8 من الإتفاقية الأوربية لحقوق الإنسان[39]. وفي فرنسا يُشترط مبدأ الضرورة بالنسبة لاعتراض الاتصالات صراحةً بنص المادّة 706-95 فقرة1 من ق إج ج، حيث يتعيّن على قاضي الحريات والحبس أن يقوم بتقديره والتأكد منه في طلب وكيل

الجمهورية. ومسألة تقدير الضرورة لاتخاذ اجراء اعتراض الإتصالات السلكية واللاسلكية ترجع إلى قاضي الحريات والحبس، حيث يجب أن يتضمّن الإذن جميع العناصر التي تسمح بالتعرّف على الإتصال، والجريمة التي تُبرّر الإجراء، والمدّة التي يجري فيها المادّة(100-1)[40].

- **في الجزائر** نصّت عليه المادّة 65 مُكرّر 5 من ق إ ج فقرّرت أنّه لا يتمّ اللجوء إلى هذه المراقبة إلا إذا دعت إلى ذلك ضرورات التحري والتحقيق الإبتدائي في جرائم مُحدّدة على سبيل الحصر ومن بينها أفعال الجريمة المعلوماتية. وكذلك نصّت المادّة3 من القانون 09-04، بأنّه لا يتم اللجوء إلى مراقبة الإتصالات الإلكترونية إلا إذا استدعت ذلك مقتضيات ومستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون. كما حصرت المادّة 4 من نفس القانون مراقبة الإتصالات الإلكترونية بحالات مُحدّدة من بينها في الفقرة (ج) حالة مُقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

وتُعتبر مسألة تقدير ضرورة اللجوء إلى هذه العمليات من عدمه حسب المادّة 65 مكرر5 من ق إج متروكةً دائمًا لتقدير القاضي الذي أصدر الإذن سواء قاضي التحقيق أو وكيل الجمهورية. غير أنّ القانون لا يُلزم القاضي بتسبيب إذن المراقبة، لذا فإنّه يصعب التأكّد من توفر هذا الشرط.

ثانيًا: صفة الشخص محل المراقبة:

أ) ضرورة ارتباط الشخص بالجريمة: في التشريع المصري نظرًا لعموم نص المادّتين 95 و206 من قانون الإجراءات الجنائية فمن الفقه من يعتبر سلطة القاضي واسعة بعموم النص إذ يملك أن يمُدّ المراقبة لغير المُتهم متى كان في تلك المراقبة فائدة في إظهار الحقيقة[41]. وهناك رأي فقهي آخر يستلزم أن يكون المتّهم طرفًا في الحديث الذي تجري مُراقبته، وأنّه لا يُمكن إهدار الحماية الدستورية والقانونية لحرمة وسرّية الحياة الخاصّة لشخص لم يُتهم بجريمة، وليس له شأن بملف متابعتها. لأنّ هذا الإجراء استثنائي، والإتهام المبني على الدلائل الجدّية القوية هو الذي يُبرّر اللجوء إلى هذا الإستثناء والتسلل إلى الحياة الخاصة للفرد، من أجل الكشف عن حقيقة الجريمة.

كما أنّ الإستثناء لا يجوز التوسع في تفسيره[42]. فكل شخص له علاقة بالجريمة محل التحقيق سواء كان شاهدًا أو مشتبهًا فيه يمكن أن يخضع لاعتراض مراسلاته السلكية واللاسلكية، حتى ولو لم يكن يوجد ضدّه أي اشتباه لمشاركته في الجريمة، فالمبرّر الوحيد لاتخاذ الإجراء هو مبدأ الضرورة، وهو يخضع لتقدير القاضي أمام غرفة التحقيق، أو قاضي الحكم[43].

ب) إستثناء بعض الأشخاص من إجراء المراقبة الإلكترونية: .كرّس القانون الفرنسي حماية إجرائية لبعض الوظائف، بأن يقع إجراء اعتراض المراسلات تحت طائلة البطلان إذا خالف أحكام هذه الحماية.

مثل حماية المحامين وحقوق الدفاع في الفقرة الثانية من المادّة 100-7 من ق إ ج ف التي ألزمت قاضي التحقيق قبل اتخاذ إجراء اعتراض مراسلات المحامي في مكتبه أو بيته بإعلام النقيب. والمادّة 100-5 قرّرت أنّه لا يجوز وصف المكالمات التي يقوم بها المحامي ويصب موضوعها في مُمَارسة حقوق الدفاع، مع استثناء وحيد هو وجود قرائن على مساهمة المحامي نفسه في الجريمة. وكذلك حمايةً لأعضاء البرلمان نصّت المادّة 100-7 ق إ ج على أنّه لا يُمكن إجراء اعتراض الاتصالات الهاتفية لعضو البرلمان في مكتبه أو بيته إلا بعد إخطار رئيس الهيأة من طرف قاضي التحقيق.

في الجزائر لم يأت المُشرّع بمثل هذه الإستثناءات الصريحة بل اكتفى في المادّة 65 مكرر1/6 بالنّص على ضرورة عدم المساس بالسرّ المهني إذا تعلّق الأمر بتنفيذ هذه العمليات في أيّة أماكن يوجد بها أشخاص مُلزمون بالسرّ المهني، مثل السرّ المهني للمحامي والطبيب والموثق[44].

كما نصّت المادّة3 من القانون 09-04 على ضرورة مراعاة مراقبة الإتصالات الإلكترونية للأحكام القانونية التي تضمن سرّية المراسلات والاتصالات. وألزمت المادّة 27 من المرسوم 15-261، مُستخدمي هذه الهيئة بالسرّ المهني وواجب التحفّظ. كما يتضمّن اليمين الذي يؤدّونه القسم على كتمان الأسرار والمعلومات التي يطّلعون عليها أثناء قيامهم بمهامهم والتي من بينها مراقبة الإتصالات الإلكترونية.

الفرع الثاني: الشروط الإجرائية لترخيص المُراقبة الإلكترونية(الإذن القضائي بالمراقبة):

تتعلّق الشروط الإجرائية لترخيص المراقبة الإلكترونية في اعتراض المراسلات السلكية واللاسلكية والإلكترونية، بالإذن القضائي الذي يُرخص استخدامها. نصّت عليه كافة التشريعات المقارنة ومنها التشريع الجزائري في المادّة 65مُكرّر5 من ق إ ج وذلك في فقرتها الأولى «يجوز لوكيل الجمهورية المُختص أن **يأذن** بما يأتي...»، وفي فقرتها الأخيرة « في حالة فتح تحقيق قضائي تتم العمليات المذكورة بناءً على **إذن** من قاضي التحقيق وتحت رقابته المُباشرة ».كما نصّت المادّة الرابعة من القانون 09-04، أنّه لا يتمّ اللجوء إلى مراقبة الإتصالات الإلكترونية إلاّ بإذن الجهات القضائية المُختصّة، وتُحيل المادّة 3 إحالة عامّة على قانون الإجراءات الجزائية.

أوّلاً: السلطات المختصّة بإصدار الإذن بالمراقبة:

أ) في التشريع الفرنسي: في ظل قانون 10 جويلية1991 كانت المادّة 100 من ق إ ج ف، وما بعدها من ق إ ج ف لا تسمح باعتراض المراسلات إلا أثناء التحقيق الإبتدائي، ثمّ جاء قانون 9 مارس 2004 يسمح بتطبيقه أثناء التحريات الأولية في أفعال الإجرام المنظم عندما تقتضي ذلك ضرورات الحقيق في التلبس أو التحقيق الأوّلي(المادّة 706-95 ق إ ج ف)[45] وهي المذكورة على سبيل الحصر في المادّة 706-73 ق إ ج ويجوز لقاضي التحقيق بموجب أمر مُسبّب وبعد إخطار وكيل الجمهورية أن يأذن بالإلتقاط عن بُعد

لمُعطيات معلوماتية وتسجيلها وحفظها ونقلها، مثلما هي ظاهرة على شاشة الحاسوب أو مثلما تمّ كتابتها بأحرف الجهاز(الم706-102 ق إ ج)[46].

وترجع سلطة اتخاذ إجراء اعتراض المراسلات السلكية واللاسلكية والالكترونية، في الجريمة المنظمة لقاضي الحرّيات والحبس بالمحكمة ذات الإختصاص الشامل(*TGI*)بطلب من وكيل الجمهورية المُختص. أمّا بالنسبة للمجالات الأخرى في الجنايات أو الجنح التي تُساوي أو تزيد عقوبتها عن سنتين حبس، فقاضي التحقيق هو الذي له سلطة اتخاذ الإجراء(المادّة 100 ق إ ج) أو في إطار التحقيق التكميلي لقضاة غرفة التحقيق أو محكمة الجنح أو محكمة الجنايات (المادّتان 205،283)[47].

ب) **في التشريع الجزائري** يُمكن اللجوء إلى المُراقبة الإلكترونية بجميع أنواعها في كلتا مرحلتي التحريات الأولية والتحقيق القضائي الإبتدائي، ومن ثمّ يصدُر الإذن من قاضي التحقيق في إطار التحقيق الابتدائي. ومن وكيل الجمهورية في إطار التحقيق الأوّلي وتحقيقات التلبّس، وهنا يجدُر التنبيه أنّ النسخة العربية لنص الفقرة الأولى من المادّة 65 مكرّر5 من ق إ ج سقطت منها عبارة « التحقيقات الأوّلية» التي وردت في النسخة الفرنسية لنفس المادّة حيث تنص أنّه تُطبق هذه الإجراءات في مرحلة التحرّيات سواء في التحقيقات الأولية أو تحقيقات التلبّس.

وما لم يُخطر قاض التحقيق بملف الدعوى لا يحق له إصدار إذن بإجراء عمليات اعتراض المراسلات عندما يتعلق الأمر بوجود دلائل على الجرائم المنصوص عليها في المادة 65 مكرر5 ق إ ج ج بأنّها ستُرتكبُ مُستقبلاً[48]. وإذا تعلّق موضوع المراقبة بجرائم الإرهاب والتخريب وأمن الدولة يصدر الإذن عن النائب العام لمجلس قضاء الجزائر إلى الهيأة الوطنية للوقاية من الجريمة الإلكترونية المذكورة في المادّة 13 من القانون 09-04، بناءً على تقرير يُبيّن طبيعة الترتيبات التقنية المُستعملة والأغراض المُوجّهة لها. وتدخل جرائم المعلوماتية والجرائم الأخرى التي يُسمح فيها بمراقبة الاتصالات الالكترونية داخلة في اختصاص الأقطاب القضائية الجزائرية بموجب المواد 37،40،329 ق إ ج الجزائري، وكذلك الإختصاص الإقليمي الموسّع لضباط الشرطة القضائية في المراقبة بالمادّة 16مُكرّر إ ج.

ثانيًا: مضمون الإذن:

يجب أن يكون الإذن باعتراض الاتصالات الإلكترونية مكتوبًا يتضمّن جميع العناصر التي تبيّن حقيقة الإتصال المُعترض، بحيث ينبغي التحديد الدقيق لنوع الجريمة التي تُبرّر الإجراء، والتحديد الواضح والمُفصّل لجهاز الكمبيوتر الخاضع للمراقبة وطبيعة المُعطيات المُراد التقاطها أو اعتراضها والمُدّة (المادة 65 مُكرّر7).

ويزيد القانون الفرنسي عن القانون الجزائري بضرورة تسبيب الإذن. فالقانون الفرنسي وفّر إمكانية المُراقبة الحقيقية لاحترام مبدأ الضرورة والملاءمة في اتخاذ هذا الإجراء عن طريق اشتراط أن يكون الأمر

أو الإذن المُرخص للإجراء مُسبّبًا. وهو الشرط الذي تنصّ عليه المادّة 706-97/1 من ق إ ج ف[49]. لأنّ الملاءمة لا تنتج فقط عن توافر الشروط القانونية لتطبيق الإجراء، بل تخضع للسلطة التقديرية للقاضي حالةً بحالة. والمشرّع أخضع هذه الملاءمة للرقابة القضائية عن طريق فرض تسبيب الإذن[50]. فعندما يكون الإذن بالإعتراض غير مُسبب يصعب مراقبة مدى توافر هذا الشرط. وتجاهل هذا الشرط ينبغي أن يُرتّب البطلان.

ينبغي على المُشرّع الجزائري أن يُظيف شرط التسبيب بالنسبة للمراقبة التي تتمّ بواسطة التقاط أو اعتراض الاتصلال الإلكتروني لأنّ الدستور[51] أرسى بموجب الفقرة الثالثة من المادّة 39 ضمانة تسبيب الأمر القضائي في الإجراءات التي تتضمّن المساس بحرمة الحياة الخاصّة وقرّر الجزاء الجنائي على انتهاكها. وهذا احترامًا لما نصّت عليه الفقرة الثانية من نفس المادّة 39 وهو ضمان سرّية المراسلات والإتصالات الخاصّة للأفراد بكلّ أشكالها. لكن إذا تمّت مُراقبة الإتصالات الإلكترونية عن طريق أسلوب التسرّب الرقمي فإنّه يُشترط تسبيب الإذن لأنّ المُشرّع اشترطه تحت طائلة البطلان بالنسبة لأحكام التسرّب في المادّة 65 مُكرّر15 ق إ ج.

ثالثًا: مُدّة مراقبة الإتصالات الإلكترونية:

أ) في فرنسا تُحدّد المادّة 95.706 من ق إ ج مُدّة المراقبة بـ (15) يومًا قابلة للتجديد مرّة واحدة وفق نفس الشروط الشكلية والزمنية، على أن تتمّ عملية الإعتراض تحت إشراف الأمانة العامة لوزارة العدل التي تتكفل بالتنسيق بين مُختلف الإدارات المُختصّة في مجال اعتراض المراسلات[52].

ب) في الجزائر حدّدتها القواعد الخاصّة للمراقبة الإلكترونية في المادّة 65 مُكرّر7 قانون الإجراءات الجزائية بمدّة(4) أشهر قابلة للتجديد. أمّا القانون09-04 فلم يشترط المُدّة في غير حالة الجرائم الإرهابية والتخريبية والماسّة بأمن الدولة، بالتالي تخضع لنفس المدّة التي نصّت عليها المادّة 65 مُكرّر7 ق إ ج، لكن إذا تعلّق موضوع المراقبة بجرائم الإرهاب والتخريب وأمن الدولة فقد حدّدت المادّة 4 فقرة 5 من القانون09-04 مُدّة الإذن الذي يمنحه النائب العام لمجلس قضاء العاصمة للهيئة الوطنية للوقاية من الجريمة الإلكترونية هي(6)أشهر قابلة للتجديد وذلك على أساس تقرير يبيّن طبيعة الترتيبات التقنية المُستعملة والأغراض المُوجهة لها.

المطلب الثاني: شروط تنفيذ مُراقبة الإتصالات الإلكترونية:

الفرع الأوّل: الجهات المُكلّفة بتنفيذ مُراقبة الإتصالات الإلكترونية:

بمُقتضى المادّة 65 مكرّر8 ق إ ج ج يتمّ تنفيذ إذن المُراقبة من طرف ضابط الشرطة القضائية سواء في إطار مهامه الأصلية أثناء التحقيقات الأولية أو في إطار الإنابة القضائية أثناء التحقيق الابتدائي، كما يمكن للقاضي الذي أصدر إذن المراقبة أن يُسخّر كل عون مُؤهّل لدى مصلحة أو وحدة أو هيئة عمومية

أو خاصّة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذآورة في المادة 65 مكرر 5 أعلاه.

أوّلاً: الهيئة الوطنية للوقاية من الجرائم المُتصلة بتكنولوجيا المعلومات والإتصال:

طبقًا للمادة 13 من القانون 09-04 المتعلّق بالوقاية من جرائم تكنولوجيا اللإعلام والاتصال، أُنشئت الهيئة الوطنية للوقاية من الجرائم المُتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، وحدّدت مهامها المادّة 14 ومن بين مهامها أنّها تُكلّف بمُساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تُجريها بشأن الجرائم ذات الصلة بتكنولوجيا اللإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات.

وتجسّد نظام الهيئة بالمرسوم الرئاسي رقم 15-261 المُتعلّق بتشكيل وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المُتصلة بتكنولوجيا الإعلام والإتصال، حيث نصّت المادّة الرابعة منه أنّ هذه الهيئة تمارس مهامها تحت رقابة السلطة القضائية وطبقًا للتشريع الساري المفعول لاسيما قانون الإجراءات الجزائية.

وطبقًا للمادّة11 من نفس المرسوم تُكلّف هذه الهيئة حصريًا عن طريق مُديرية المُراقبة والوقاية واليقظة الإلكترونية بتنفيذ عمليات المُراقبة الوقائية للإتصالات الإلكترونية " من أجل الكشف عن الجرائم المُتصلة بتكنولوجيا الإعلام والاتصال بناءً على رُخصة مكتوبة من السلطة القضائية وتحت رقابتها طبقًا للتشريع الساري المفعول"، هو يتمثل خاصّة في المواد 65 مُكرّر5 إلى 65 مُكرّر10 من قانون الإجراءات الجزائية.

ونصّت المادّة 21 من نفس المرسوم « قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة تُكلّف الهيئة حصريًا بمراقبة الإتصالات الإلكترونية وتسجيل مُحتواها في حينها والقيام بإجراءات حجز وتفتيش داخل منظومة معلوماتية تحت سُلطة قاض مُختصّ، ووفقًا للأحكام المنصوص عليها في المادّة 4 من القانون 09-04، المُتعلّق بالوقاية من الجرائم المُتصلة بتكنولوجيا الإعلام والاتصال».

يعمل في هذه الهيئة مُستخدمون تقنيون، وتُزوّد الهيئة بضباط وأعوان للشرطة القضائية من المصالح العسكرية للإستعلام والأمن الوطني والدرك الوطني، ويمكن أن تستعين الهيئة بخبراء وموظفين مُختصّين من الوزارات المعنية بتكنولوجيا الإعلام والإتصال. وتتكوّن الهيئة من عدّة مصالح مُبيّنة في المادّة 6 من المرسوم، من بينها مُديرية المُراقبة والوقاية واليقظة الإلكترونية، وهي المصلحة المُكلّفة بتنفيذ عمليات مراقبة الإتصالات الإلكترونية، تتوفر على مركز العمليات التقنية ومُلحقات جهوية ووحدات تتبعها، تقوم بتنفيذ عمليات المراقبة على مُستواها.

ثانيًا: مُقدّموا خدمة الإتصالات الإلكترونية:

أ) في الجزائر يخضع تنفيذ المراقبة عن طريق اعتراض الإتصالات الإلكترونية في الجزائر لنفس أحكام التصنّت والتقاط الأصوات والصور في قانون الإجراءات الجزائية، ويُضيف قانون مكافحة جرائم تكنولوجيا الإعلام والإتصال في مجال مراقبة أو اعتراض الإتصالات الإلكترونية بعض الأحكام الإجرائية التي تُمثل صورًا للمراقبة الإلكترونية في مجال الإنترنيت أو إجراءات تنفيذية مُكمّلة لاعتراض المراسلات الإلكترونية، تمثلت في تقديم المساعدة للسلطات القضائية للتحرّي والتحقيق من طرف مُقدمي خدمات الإتصال الإلكتروني، وذلك بحفظ مُعطيات حركة السير الإلكتروني، وحجز واستعمال مُعطيات الإعلام الآلي.

حيثُ تُلزم المادّة 10 من قانون مكافحة جرائم تكنولوجيا الإعلام والإتصال مُقدمي خدمات الإتصال الإلكتروني بتقديم المُساعدة للسلطات المُكلفة بالتحريات والتحقيقات القضائية لتجميع وتسجيل المُعطيات المُتعلقة بمُحتوى الإتصالات في حينها، وذلك بوضع المُعطيات التي يتعيّن عليهم حفظها وفق المادّة 11 من نفس القانون تحت تصرّف السلطات المذكورة، مع التزامهم بواجب كتمان السر تحت طائلة عقوبات إفشاء أسرار التحرّي والتحقيق.

وتُعرّف الفقرة (د) من المادّة2 من هذا القانون « مقدّم الخدمات » بأنه: أيُ كيان عام أو خاص يُقدم لمُستخدمي خدماته، القدرة على الإتصال بواسطة منظومة معلوماتية أو نظام للإتصالات. وأيُّ كيان آخر يقوم بمُعالجة أوتخزين مُعطيات معلوماتية لفائدة خدمة الإتصال المذكورة أولمُستعمليها.

ب) في فرنسا تتم المساعدة التي يُقدّمها مُزودو خدمات الإتصال الإلكتروني، في إطار التسخيرة المعلوماتية، فبغرض تجميع عناصر الأدلّة الرقمية، يمكن للقضاة أو ضبّاط الشرطة القضائية اتخاذ العديد من إجراءات التحري في شكل تسخيرة، من خلال فرض الإلتزام على أي شخص بتقديم خدمة نظرًا لما يملكه هذا الشخص من وسائل تقنية أو خبرات غير متوفرة لدى السلطات القضائية. مثل التسخيرة التي تنصّ عليها المواد 60-1 و77-1-1 و99-3 و99-4 من قانون الإجراءات الجزائية، والتي تسمح بتسخير الأشخاص المُختصّين والإدارات والمصالح أثناء تحقيقات التلبس أو التحقيق الأولي، من أجل الإطلاع على ملفات يحوزونها تتضمّن معطيات رقمية أو في منظومات المعالجة الآلية، عن طريق الإنترنيت أو وسائل الإتصال الإلكترونية.

وتسمح المادّة 20-1لضابط الشرطة القضائية أن يدخل عن طريق شبكات الإعلام الآلي أو الإنترنت إلى بعض الهيآت العمومية والأشخاص المعنوية الخاصة، ويضع تحت تصرّفه المعلومات التي تفيد في كشف الحقيقة، والتي يُمكن نقلها أو تحويلها في شكل رقمي.

وتنُصّ المادّة 77-21 من ق إ ج ف على أنّه بإمكان ضابط الشرطة القضائية بإذن من وكيل الجمهورية والإذن المُسبق لقاضي الحريات والحبس، أن يُسخر بعض المؤسسات والأشخاص من أجل أن يضعوا تحت تصرّفهم المعلومات المُتحصل عليها عن طريق شبكات الإتصال المعلوماتية والإنترنيت في أقرب الآجال. وهذا تحت طائلة العقوبات المُقرّرة بالمادّة 121-2 من قانون العقوبات[53]. وقانون مكافحة الإرهاب ومراقبة الحدود 2006-64 وسّع نطاق مراقبة الإتصالات الإلكترونية في جرائم الإرهاب، إلى الأشخاص الذين يقدمون بصفة مهنية خدمة عمومية للإتصال عبر شبكة الإنترنيت كمقاهي الإنترنيت وموزّدي خدمة (*WIFI*)[54].

الفرع الثاني: التدابير المُتخذة أثناء وبعد عملية المراقبة:

أوّلاً: التقيّد بمضمون الإذن ومنع تحويل الإجراءات:

إذا كان موضوع الإجراء هو المراقبة الصوتية والبصرية للأشخاص، فلا يُمكن أن تكون له أهداف أخرى من غير المنصوص عليها في مادّة المراقبة الصوتية والبصرية. أي أنّه في الترخيص بوضع الترتيبات التقنية من أجل التقاط أو بث أو تثبيت أو تسجيل الكلام والصور، لا يُمكن استغلال فرصة الدخول إلى مكان خاص بمُناسبة وضع ترتيبات التنصّت، والقيام بعمليات تفتيش وحجز، وهو ما يُسمّى بمبدأ منع تحويل الإجراءات(*détournement de procédure*) فلإجراء عملية تفتيش لا مانع من إصدار إذن بإجراء التفتيش بشكل مُستقل، وفق شروطه الخاصّة. وفي الحالة العكسية فيمكن وضع الترتيبات التقنية للتنصّت بمناسبة تنفيذ إذن بالتفتيش، شريطة أن يتمّ التفتيش فعلاً[55].

وفي الجزائر بيّنت المادّة 9 من قانون مكافحة جرائم تكنولوجيا الإعلام والاتصال 09-04 حدود استعمال المعطيات المتحصل عليها أثناء المُراقبة أو التفتيش المعلوماتي مُقرّرةً أنّه تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به لا يجوز استعمال المعلومات المُتحصل عليها عن طريق عمليات المُراقبة المنصوص عليها في هذا القانون إلاّ في الحدود الضرورية للتحريات أو التحقيقات القضائية وفي الحالة العكسية حالة اكتشاف جرائم أخرى غير مذكورة في إذن المراقبة، نصّت المادّة 65 مُكرّر2/6 على عدم ترتُّب البطلان للإجراءات العارضة.

ثانيًا: تحرير محاضر المراقبة:

من أهمّ ضمانات المتّهم في عملية المراقبة الإلكترونية أن يتمّ تنفيذها تحت السلطة والرقابة المستمرة للقاضي من خلال وجوب تحرير محاضر العمليات والنسخ والوصف والتدابير الاحتياطية بعد انتهاء عملية المراقبة.

أ) محضر العمليات: عن هذه العملية من طرف ضابط الشرطة القضائية المُكلّف بها، يدرج في ملف الإجراءات، ويكون لمحامي المتهم الخاضع للمراقبة الإطلاع عليه من أجل مُناقشته أو إنكار مضمونه والمطالبة بإجراء خبرة على الصوت المُسجل أو الصور الملتقطة. حيث يُدوّن في هذا المحضر جميع مُجريات سير عملية وضع الترتيبات التقنية، وكل مرحلة من مراحل عمليات الإلتقاط والتثبيت والتسجيل الصوتي أو المرئي، وفيه تاريخ وساعات بداية ونهاية الإجراء (المادة 65 مُكرّر9).

في عمليات الاعتراض والتسجيل والالتقاط، لا يتم انتظار بلوغ مرحلتها النهائية لتحرير محضر بشأنها، فعلى قاضي التحقيق أو وكيل الجمهورية بحكم مراقبته المباشرة للعمليات وضابط الشرطة القضائية المنتدب لإجراء العمليات تحرير محاضر عن كل مرحلة على حدة، إذ يُحرّر بشكل منفصل محضر الترتيبات التقنية ومحضر الدخول إلى المساكن ومحضر الالتقاط ومحضر التثبيت ومحضر التسجيل الصوتي أو محضر التسجيل السمعي البصري، ومحضر عملية الاعتراض ومحضر تسجيل المراسلات. وإذا كانت المكالمات التي تم اعتراضها أو التسجيلات الصوتية أو السمعية البصرية بلغة أجنبية تتم ترجمتها بمساعدة مترجم يتم تسخيره لهذا الغرض.

ويجب أن تُبنى عملية حفظ الدليل الرقمي على أسس علمية، وتحديث أسلوب تحرير المحاضر في هذا الشأن، بحيث يجب ألاّ ينحصر المحضر في ظهره التقليدي بل يجب التذكير بضرورة الارتباط بالخبرة وتحديدها في محضر ضبط الدليل العلمي[56].

ويثير هذا الإجراء بعض الصعوبات فيما لو كان ضابط الشرطة القضائية أثناء تنفيذ المراقبة تحصّل على عناصر مُهمّة تفيد في الكشف عن الحقيقة فبادر بإرسالها إلى قاضي التحقيق. فلو وجد قاضي التحقيق نفسه مُضطرًا لإجراء استجواب مع المُتهم فهل يلتزم بإطلاع المحامي على ملف التحقيق ومن ثمّ إفساد تحقيقه؟ فبعض قضاة التحقيق يقومون بسحب محضر الوصف من ملف الإجراءات، أو سحب الإنابة القضائية كاملة نسختها الثانية[57].

وتقضي المادّة 25 من المرسوم المُتعلّق بالهيئة الوطنية للوقاية من الجرائم المُتصلة بتكنولوجيا الإعلام والإتصال بأنّه تُسجل الإتصالات الإلكترونية التي تكون موضوع مراقبة وتُحرّر وفقًا للشروط والأشكال المنصوص عليها في ق إ ج. وتُسلّم التسجيلات والمُحرّرات إلى مصالح الشرطة والسلطات القضائية المُختصّة التي تحتفظ دون سواها بهذه المُعطيات أثناء المُدّة القانونية.

ب) محضر النسخ والوصف: تأكيدًا على ضمانات صحّة التسجيلات المأخوذة للمكالمات، قرّر المشرّع الفرنسي بموجب المادّة 100-4 فقرة 1 بأنّ كل عملية اعتراض أو تسجيل يجب أن تكون موضوع محضر للوصف، يقع على عاتق قاضي التحقيق أو ضابط الشرطة القضائية المُنتدب أو وكيل الجمهورية بحسب الإطار الإجرائي. حيث يُدوّن فيه تاريخ وساعة البداية والنهاية لكل عملية، ثم وصف المكالمات التي تفيد في

إظهار الحقيقة. ويجب إدراج هذا المحضر ووثيقة الإنابة القضائية في ملف التحقيق بعد تنفيذ الإعتراض، من أجل تمكين الدفاع من الإطلاع عليها. وتكون لضابط الشرطة القضائية السلطة التقديرية، بأن يصف فقط المحادثات المفيدة في إظهار الحقيقة[58].

وفي الجزائر وطبقًا للمادّة 65 مُكرّر1/10 من ق إ ج ينتقي ضابط الشرطة القضائية من هذه التسجيلات ما يكون مُفيدًا في إظهار الحقيقة وينسخه ويصفه، أي يُفرغه بنقله إلى معطيات كتابية، ويحرّر محضرًا مُستقلاً عن هذا النقل ولو بالتلخيص والإختصار لمضمون التسجيلات، ويودع المحضر بدوره في ملف الإجراءات. وإذا كانت الإتصالات قد تمّت بلُغة أجنبية، تُرتجم وجوبًا إلى اللغة العربية، بمساعدة ترجمان مسجل بجدول المترجمين المقبولين لدى المحاكم. كما يجوز الإستعانة بخبراء وذوي الإختصاص في حالة اشتمال المراسلة على رموز أو ألغاز.

ج) اتخاذ تدابير احتياطية بعد انتهاء عملية المراقبة:

1- وضع التسجيلات في أحراز مُقفلة: يعتبر هذا الإجراء من الضمانات الأساسية في تنفيذ عمليات المُراقبة الإلكترونية، قبل تقديم الدليل المتحصل عليه من تسجيل المُكالمات إلى المحكمة، والغرض منه هو التأكد من سلامة الأشرطة والدعامات الإلكترونية ومنع تغييرها أو التلاعب فيها بالحذف أو الإضافة، غير أنّه لم يرد النصّ عليه في القانون الجزائري، ويُمكن إخضاعه للأحكام العامّة المُتعلّقة بالمضبوطات الناتجة عن التفتيش.

لكن في فرنسا نصّت عليه المادّة 2/100-706 من ق إ ج الفرنسي بالنسبة لالتقاط الصور والأصوات. وحسب التعليمة التطبيقية (*CRIM 04–13 G1 du 2 Septembre 2004*) يجب الإحتفاظ بالأشرطة الأصلية للتسجيل في أحراز مختومة. بخلاف الأمر بالنسبة للتنصّت الهاتفي، وتفاديًا لاضطرار اللجوء إلى كسر الأختام عن الحرز بحضور المتهم المراقب يقوم قاضي التحقيق باستنساخ نسخة ثانية من الشريط، من أجل الرجوع إليها كُلما اقتضى الأمر، والسماح بالإطلاع عليها وفحصها من طرف محامي المتهم المراقب إذا كان يريد مناقشتها، أو فحص مدى شرعيتها وصحتها،[59]. ويجب تحريز الأشرطة المغناطيسية التي تحتوى تسجيلات جميع المكالمات التي تمّ اعتراضها، حفاظًا على صحتها ومطابقتها للحقيقة وهذا الضبط والتحريز لا يمنع استعمال نسخة من التسجيلات في إجراءات أخرى[60].

2- إتلاف التسجيلات: حمايةً للأسرار والحياة الخاصة، ألقت القوانين على عاتق كل من يشارك في عملية المراقبة واجب التحفظ بشأن نتائجها بعد الانتهاء من الإجراء، وتحقيق الغرض المقصود من المراقبة باستخدامها كدليل في الملف الإجرائي. بضرورة إتلاف جميع أشرطة التسجيل الأصلية ونُسختها. نصّت على هذا الإجراء المادّة 102-706 ق إ ج الفرنسي. بتقريرها أنّ التسجيلات السمعية أو السمعية البصرية يجب أن يتم إتلافها وتحطيمُها تحت إشراف وعناية وكيل الجمهورية أو النائب العام عند

انقضاء أجل تقادم الدعوى العمومية. مع تحرير محضر الإتلاف. والحكم نفسه ينطبق على التسجيلات الهاتفية بموجب المادّة 706-95 ق إ ج ف، بالإحالة إلى المادّة 100-6 من نفس القانون. فبمجرّد الإنتهاء من استخدام التسجيلات المستمدّة من اعتراض المراسلات السلكية واللاسلكية يجب إتلافها[61]. ويكون الإحتفاظ بالتسجيلات محدودًا بفترة زمنية معينة وهي ميعاد تقادم الدعوى العمومية إذا لم يتم استخدامها، ثمّ إتلافها وتحرير محضر بهذا الإتلاف من طرف وكيل الجمهورية أو النائب العام(المادّة100-6 ق إ ج ف)[62]. ونفس الإجراء ألزمت به المادّة 113من المسطرة الجنائية المغربي قاضي التحقيق وقضاة النيابة[63]، وغاب في التشريع الجزائري.

خاتمة:

في مجال الإجرام المعلوماتي الذي يستخدم المنظومة المعلوماتية وشبكات الاتصال والانترنت كوسيلة أو يتخذها هدفًا إجراميًا، ظهرت أهمية المُراقبة الإلكترونية للمُراسلات والاتصالات الإلكترونية كأسلوب إجرائي للتحقيقات الجنائية واستنباط الدليل الرقمي الذي تأكّدت مشروعيته في الإثبات الجنائي رغم قداسة الحياة الخاصّة وحرية سرية المراسلات والاتصالات، وهذا تغليبًا لمصلحة المجتمع في حمايته من الإجرام الإلكتروني والسبراني الخطير، ممّا جعل مُعظم تشريعات الدول تُكرّس المُراقبة الإلكترونية باعتبارها من أكفأ الأساليب الإجرائية، ومن بينها التشريع الجزائري الذي نظمها في قانون الإجراءات الجزائية وقوانين أخرى، بتحديد شروط ترخيصها وتنفيذها التي تضمن نجاعتها وفعاليتها. ويكفل الضمانات الإجرائية الأساسية لحماية خصوصية المراسلات والاتصالات الالكترونية من المراقبة غير المشروعة أثناء التحرّي والتحقيق. وأفضى البحث إلى التوصيات الآتية:

1- إظافة شرط التسبيب بالنسبة لإذن مُراقبة الاتصلال الإلكتروني.

2- سلطة اتخاذ الإجراء في قاضي التحقيق فقط، وفي جرائم محدودة.

3- النصّ على إجراء إتلاف تسجيلات المُراقبة ومحضر الإتلاف بعد استخدامها.

4- النصّ على السماح لضباط الشرطة القضائية المؤهلين خصيصًا لاستخدام التسرّب الرقمي.

الهوامش والمراجع:

[1] محمود مُحمّد جابر، الجرائم الناشئة عن استخدام الهواتف النقالة – جرائم نظم الاتصال والمعلومات، دراسة مقارنة، دار الكتب والوثائق القومية، المكتب الجامعي الحديث، الإسكندرية 2018، ص107.

[2] محمود أحمد طه، التعدّي على حق الإنسان في سرّيّة اتصالاته الشخصية بين التجريم والمشروعية، دار النهضة العربية، القاهرة، الطبعة الثانية، 1999، ص166.

[3] عادل عبد الجواد مُحمّد الكردوسي، التعاون الأمني العربي ومُكافحة الإجرام المُنظم عبر الوطني، مكتبة الآداب، القاهرة، الطبعة الأولى 2005، ص190.

[4] عبد العزيز نويري، الحماية الجزائية للحياة الخاصّة- دراسة مُقارنة بين القانون الجزائري والقانون الفرنسي، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2015، ص 119.

[5] فضيلة عاقلي، "الحماية القانونية للحق في حُرمة الحياة الخاصّة دراسة مُقارنة" ، رسالة دكتوراه في القانون الخاص، جامعة الإخوة منتوري . قسنطينة، 2012، ص 77،78.

[6] *Nathalie CAZE-GAILLARDE, " Atteintes à la Vie privée ", Répertoire de droit pénal et de procédure pénale, mai 2005, éd Dalloz, tome VII, sous la direction d'Yves MAYAUDE, mise à jour, Avril 2006, p4.*

[7] عبد العزيز نويري ، المرجع السابق، ص 55.

[8] حسن حُسين البراوي، "مدى حماية الحق في الخصوصية في القانون المدني القطري"، المجلة القانونية والقضائية لوزارة العدل القطرية،العدد الأوّل، 2010، ص101.

[9] نصر الدين مروك، " الحق في الخصوصية "، مجلّة موسوعة الفكر القانوني التابعة لمركز الدراسات القانونية والقضائية بالجزائر، دار الهلال للخدمات الإعلامية، حيدرة، العدد الثاني بدون تاريخ، ص 86.

[10] سوزان عدنان، "إنتهاك حُرمة الحياة الخاصّة عبر الإنترنت دراسة مُقارنة"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29 العدد الثالث، 2013، ص 433.

[11] ممدوح خليل بحر، حماية الحياة الخاصّة في القانون الجنائي دراسة مُقارنة، دار النهضة العربية، القاهرة، 2014، ص67.

[12] دستور 28 نوفمبر1996 الصادر بموجب المرسوم الرئاسي رقم 438.96 بتاريخ 7ديسمبر 1996 المتعلّق بإصدار نص تعديل الدستور المُصادق عليه في استفتاء 28ديسمبر 1996. وتمّ تعديله القانون رقم 16-01 مؤرّخ في 26 جمادى الأولى 1437 هجري المُوافق 6 مارس 2016ميلادي يتضمن التعديل الدستوري، الجريدة الرسمية عدد 14 لسنة 2016.

[13] الصادر بموجب القانون رقم 16-01 مؤرّخ في 26 جمادى الأولى 1437 هجري المُوافق 6 مارس 2016 ميلادي يتضمن التعديل الدستوري، الجريدة الرسمية عدد 14 بتاريخ 07 مارس 2016.

[14] *Sous La coordination de Marie VERONICA et Pablo PALAZZI, Défis du droit à la protéction de la vie privée – Yves POULLET, Pour une troisiéme génération de réglementation de protection de donée,3e éd, Bruylant, Bruxelle, BELGIQUE. 2008, p 30.*

[15] *Frédéric DESPORTES, Laurence LAZERGES-COUSQUER, Traité de procédure Pénale,3e éd, ECONOMICA, Paris,2009, p 1367.*

[16] *Code Pénal, Annotation par Yves MAYAUD, Code Pénal, éd DALLOZ, n° 108, Annotation de jurisprudence et bibliographie par Yves MAYAUD. Paris Cedex 2011, p 820.*

[17] *Christian De VALKENEER, KAMINSKI Dan, " Au croisement de la recherche proactive et des écoutes téléphoniques: construction et danger du mutualisme légistique ", Revu de droit pénal et de criminologie, année 83 Mars 2003 Bruxelles,, p 311 - 312.*

[18] القانون رقم 18-04 المُؤرّخ في 10 مايو 2018 الجريدة الرسمية، 27 في 13ماي 2018.

[19] القانون رقم 2000-03 المؤرّخ في 5 غشت 2000، الجريدة الرسمية 48 بتاريخ 6 غشت 2000.

[20] الجريدة الرسمية، عدد 34 بتاريخ 10 يونيو 2018.

[21] الجريدة الرسمية، عدد 47 بتاريخ في 16 غشت 2009.

[22] الجريدة الرسميةعدد 53 بتاريخ 8 أكتوبر 2015.

[23] *Jean PRADEL, Michel DANTI-JUAN, Manuel de droit pénal spécial, éditions Cujas, n° 03, Paris, 2004, p 209.*

[24] أضيفت المواد 87 مُكرّر11 و87 مُكرّر12 و394 مُكرّر8 بالقانون 16-02 في 19 يونيو 2016،الجريدة الرسمية، عدد 37 لسنة 2016.

[25] القانون 09-04 المؤرّخ في 05 غشت 2009،الجريدة الرسمية، عدد 47 مؤرّخة في 16 غشت 2009.

[26] *Myriam QUEMENER, Yves CHARPNEL, Op cit, p169,245* .

[27] أنظر عمر مُحمّد بن يونس، الإتفاقية الأوربية حول الجريمة الإفتراضية (المذكرة التفسيرية)، منشورات الإتحاد الأوربي، الطبعة الأولى المُعرّبة 2005، ص166،163،161

[28] عمر مُحمّد بن يونس، " الدليل الرقمي "، المؤتمر الدولي الثاني لقانون الانترنت، مالطا من 27 إلي 31 نوفمبر 2006، منشورات المنظمة العربية للتنمية الإدارية بجامعة الدول العربية، 2006، ص8.

[29] *Myriam QUEMENER, Yves CHARPNEL, Op cit, p 176.*

[30] عمر مُحمّد بن يونس، الجريمة الافتراضية، المرجع السابق، ص57،55. 124، 128، 130.

[31] *Myriam QUEMENER, Yves CHARPNEL, Cybercriminalité - Droit pénale appliqué, éd ECONOMICA, 2010, p180. 181*

[32] *Myriam QUEMENER, Yves CHARPNEL, Op cit, p 182.*

[33] *Ibid, p175-176.*

[34] *Bertrand RENARD; Caroline VANDRESSE, La Belgique ou l'incrimination de l'organisation criminelle comme soutien des techniques d'enquête. Sous la direction de Maria LUISA CESONI, Criminalité organisée - des représentations sociales aux définitions juridiques, L.G.D.J paris, George éditeur Genève, Bruylant Bruxelles, 2004, p 479.*

[35] *SOPHIE Sontag Koenig, Technologies de l'information et de la communication et défense pénale, éd mare et martin, Paris, 2015, p 181-183*

[36] *Myriam QUEMENER, Yves CHARPNEL, Op cit, p 169.*

[37] القانون رقم 06-01 المؤرّخ في 20 فيفري 2006، الجريدة الرسمية عدد 14 في08 مارس 2006. المتمم بالأمر 10- 05 المؤرّخ في 26 غشت 2010، الجريدة الرسمية عدد 14 في01 سبتمبر 2010.

[38] القانون رقم 09-04 المؤرّخ في 05 غشت 2009، الجريدة الرسمية، عدد 47 مؤرّخة في 16 غشت 2009، ص6

[39] *Serge GUINCHARD; Jaque BUISSON, procédure pénale, éd Litec n°6, Paris, 2010, p 1121.*

[40] *Frédéric DESPORTES, Laurence LAZERGES-COUSQUER, Op cit, p 1367.*

[41] محمود أحمد طه، المرجع السابق، ص196

[42] ياسر الأمير فاروق محمّد، "مراقبة الأحاديث الخاصّة في الإجراءات الجنائية"، رسالة دكتوراه، جامعة القاهرة، 2008، ص543.

[43] *Serge GUINCHARD; Jaque BUISSON, Op Cit, p 1120.*

[44] جمال نجيمي، إثبات الجريمة على ضوء الإجتهاد القضائي - دراسة مُقارنة - دار هومة للطباعة والنشر والتوزيع، الجزائر، 2011، ص 446.

[45] *Jean PRADEL , " Le crime organisé après la loi française du 09 Mars 2004 dite loi de Perben II ", Rrevue de droit pénal et de criminologie, éd la charte, Bruxelles, n° 02, 2005. p151.*

[46] *Frédéric DESPORTES, Laurence LAZERGES-COUSQUER, Op Cit, p 1367.*

[47] *Serge GUINCHARD; Jaque BUISSON, Op Cit, p 1121.*

[48] فوزي عمارة " اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية" مجلّة العلوم الإنسانية، جامعة منتوري قسنطينة، عدد 33، جوان، 2010، ص242.

[49] *Joceline LEBLOIS-HAPPE, Autorisation et contrôle des écoutes téléphoniques, rôle du JLD " Actualité Juridique Pénal, n° 6/2008, juin 2008,p 284-285.*

[50] *Frédéric DESPORTES, Laurence LAZERGES-COUSQUER, Idem, p 1378 - 1379.*

[51] دستور28 نوفمبر1996 الصادر بموجب المرسوم الرئاسي رقم 96-438 بتاريخ 7ديسمبر 1996 المُصادق عليه في استفتاء 28ديسمبر 1996. المُعدّل بالقانون رقم 16-01 المؤرّخ في 6 مارس 2016 م، الجريدة الرسمية عدد 14 في 07 مارس 2016.

[52] *Myriam QUEMENER, Yves CHARPNEL, Op cit, p 169.*

[53] *Myriam QUEMENER, Yves CHARPNEL, Op cit, p 173-174.*

[54] *Marie-Hélène GALMARD, Op cit, p 14-15.*

[55] *Frédéric DESPORTES, Laurence LAZERGES-COUSQUER, Op Cit, p 1379.*

[56] عمر مُحمّد بن يونس، " الدليل الرقمي "، المرجع السابق، ص 11.

[57] *Jean PRADEL, " Un exemple de restauration de la légalité criminelle - le régime des interceptions de correspondances émises par la voie des télécommunications (commentaire de la loi n° 91-646 du 10 juillet 1991), Recueil Dalloz 1992, Chroniques, p 49.*

[58] *Jean PRADEL, " Un exemple de restauration de la légalité criminelle: le régime des interceptions de correspondances émises par la voie des télécommunications ", Op cit, p49.*

[59] *Code De Procédure Pénale, Annotation de jurisprudence et bibliographie par Jean François RENUCCI, éd DALLOZ, n° 50, Paris Cedex 2009, p 1219.*

[60] *Serge GUINCHARD; Jaque BUISSON, Op Cit, p1123-1125.*

[61] *Jean PRADEL, " Un exemple de restauration de la légalité criminelle - le régime des interceptions de correspondances émises par la voie des télécommunications ", Op cit, p49.*

[62] *Serge GUINCHARD; Jaque BUISSON, Op Cit, p1124.*

[63] قانون المسطرة الجنائية وفق آخر التعديلات، إعداد وتقديم، امحمّد لفروجي، مطبعة النجاح الجديدة، الدار البيضاء، ط(2) 2012، ص69.