

التعريف بمراقبة الاتصالات الإلكترونية
كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية
*Definition of electronic communications monitoring
As a procedure for collecting evidence in cybercrime*



بن يحيى إسماعيل أستاذ مساعد (أ)،¹
المركز الجامعي علي كافي، تندوف، الجزائر



تاريخ النشر: 2022/06/16

تاريخ القبول: 2020/12/31

تاريخ الإرسال: 2020/06/25

ملخص:

شكلت الطبيعة الخاصة للجريمة الإلكترونية تحدياً بالنسبة للتشريعات الجنائية، وامتد أثر ذلك إلى جهات التحقيق الساعية إلى جمع الأدلة التي تتيح التعرف على الجناة وكشف الحقيقة. وفي هذا الصدد اعتمدت سلطات التحقيق على إجراءات مستحدثة لمسيرة سرعة المجرم الإلكتروني في التنفيذ والاختفاء. وتعد "مراقبة الاتصالات الإلكترونية" من بين إجراءات التحقيق الحديثة والتي لجأت إليها جهات التحقيق في سعيها لجمع الأدلة الإلكترونية، وذلك من خلال تقنيات حديثة تتماشى مع طبيعة وخاصية الجريمة الإلكترونية. إن الهدف من هذا البحث يتمثل في التعريف بمراقبة الاتصالات الإلكترونية كإجراء من الإجراءات الحديثة التي لجأت إليها جهات التحقيق من أجل مواجهة الجريمة الإلكترونية من خلال سعيها إلى الحصول على تلك الأدلة الإلكترونية التي تقود إلى الجناة في عالم الجريمة الإلكترونية.

الكلمات المفتاحية:

مراقبة، اعتراض، الاتصالات الإلكترونية، الجريمة الإلكترونية، الدليل الإلكتروني.

Abstract:

The peculiarity of cybercrime constitutes a major challenge for criminal law worldwide, so it was clear that this challenge extended to investigative bodies which gathered evidence capable of identifying the

perpetrators and helped to reveal the truth. Among the modern investigative procedures adopted by investigative authorities to search for and collect electronic evidence, there is what is called "surveillance of electronic communications".

The purpose of this article is to present a concept to the surveillance of electronic communications as one of the modern procedures that investigating authorities use to combat cybercrime.

Keywords:

Electronic surveillance, cybercrime, intercept, monitoring, digital evidence.

1- بن يحيى إسماعيل، benyahiaismail@yahoo.fr

مقدمة

إن محاربة الجريمة بصفة عامة تقتضي الحصول على الأدلة التي تدين الجناة وتفقد جهات التحقيق إلى كشف الحقيقة، وفي ظل تنامي الجريمة الإلكترونية وجدت الجهات المكلفة بالتحقيق في الجرائم نفسها أمام تحديات جمة فرضتها الطبيعة الخاصة للجريمة الإلكترونية والبيئة اللامادية للعالم الافتراضي الذي ترتكب بداخله، لذلك كان لابد من إيجاد حل لهذه المعضلة.

فحرصا منه على مواكبة التشريعات الجنائية المقارنة ودعمه منه لجهات التحقيق في مواجهة الجريمة الإلكترونية، عمد المشرع الجزائري إلى سن قوانين أقر من خلالها عدة إجراءات حديثة لجمع الدليل الإلكتروني من بينها "مراقبة الاتصالات الإلكترونية". فما هو مفهوم مراقبة الاتصالات الإلكترونية؟ وكيف ومتى يمكن اللجوء إليه؟ وما هي الضوابط التي تحكمه؟

للإجابة عن هذه الإشكالية اعتمدنا على المنهجين الوصفي والتحليلي لوصف هذا الإجراء وتناوله بشيء من التحليل، وكذا المنهج المقارن من خلال الاستعانة بموقف بعض التشريعات المقارنة والفقهاء المقارن من مراقبة الاتصالات الإلكترونية. ولقد قسمنا بحثنا هذا إلى محورين رئيسيين كالآتي:

المحور الأول: مفهوم مراقبة الاتصالات الإلكترونية.

المحور الثاني: الضوابط المتعلقة بمراقبة الاتصالات الإلكترونية.

1. مفهوم مراقبة الاتصالات الإلكترونية

لفهم المقصود بمراقبة الاتصالات الإلكترونية سنعرف الاتصالات الإلكترونية ثم نتطرق لصورها، وبعد ذلك ننظر في معنى مراقبة الاتصالات الإلكترونية.

1.1 تعريف الاتصالات الإلكترونية

عرف المشرع الجزائري الاتصالات الإلكترونية بموجب المادة 02 الفقرة (و) من القانون رقم 104-09¹ على أنها " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية". وعرفها بموجب المادة 05 من المرسوم الرئاسي رقم 261-15² بأنها " كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال". ويلاحظ بأن المشرع استبدل كلمة "مختلفة" الواردة في التعريف الأول بعبارة "أيا كانت طبيعتها" كما عوض كلمة "بواسطة" بعبارة "عن طريق"، وأضاف في نهاية المادة عبارة "بما في ذلك وسائل الهاتف الثابت والنقال" التي لم تكن موجودة في المادة السابقة. ويبدو أن المشرع استدرك ثغرة يعتقد أن المادة الأولى تضمنتها.

عرف المشرع الأمريكي الاتصالات الإلكترونية بموجب قانون المراقبة السلكية³ بأنها " أي تحويل لمؤشرات أو إشارات أو كتابة أو صور أو أصوات أو بيانات أو أي معلومات من أية نوع يتم بثها جزئيا أو كليا بواسطة نظام سلكي أو لاسلكي أو كهرومغناطيسي أو كهروضوئي أو ضوئي".

2.1 صور الاتصالات الإلكترونية

من خلال محتوى المادة 05 من المرسوم الرئاسي 15-261 يدخل في مفهوم الاتصالات الإلكترونية المراسلات السلكية واللاسلكية وكذا البريد الإلكتروني.

1.2.1 - المراسلات السلكية واللاسلكية:

يقصد بالمراسلات كافة الرسائل المكتوبة أيا كانت الطريقة التي ترسل بها سواء كانت داخل مظروف مغلق أو مفتوح أو كانت عبارة عن بطاقة مكشوفة طالما أن مرسلها أراد عدم اطلاع غير المرسلة إليه عليها⁴. أما المراسلات السلكية واللاسلكية، فعرّفها المشرع الجزائري بموجب المادة 08 الفقرة 21 من القانون 2000-503 على أنها " كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريّات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية"

مما سبق يتضح بأن المراسلات التي قصدها المشرع الجزائري عند تعريفه للاتصالات الإلكترونية هي تلك التي تتم عن طريق الاتصال السلكي واللاسلكي وبالتالي استبعد المراسلات التقليدية كالرسائل الورقية المرسلة عن طريق البريد العادي وغيرها من المراسلات التي لا تدخل في مفهوم الاتصالات الإلكترونية.

2.2.1 - البريد الإلكتروني⁶ (Electronic Mail)

لم يقدم المشرع الجزائري تعريفا للبريد الإلكتروني غير أننا نجد له تعريفا لدى المشرع الفرنسي بالفقرة الأخيرة بالبند الرابع من المادة الأولى من القانون 575/2000 " كل رسالة سواء كانت نصية أو صوتية أو مرفق بها صور أو أصوات ويتم إرسالها عبر شبكة اتصالات عامة وتخزن عند أحد خوادم تلك الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها"⁷. وللإشارة فالمشرع الفرنسي كان قد نص على اعتماد مصطلح Courriel بصفة رسمية واعتبره مرادف لمصطلح Courrier électronique وذلك بقائمة المصطلحات المعتمدة والمنشور بالجريدة الرسمية الفرنسية رقم 141 بتاريخ 2003/06/20 بالصفحة 10403.

المشرع الأمريكي وبموجب القانون المتعلق بخصوصية الاتصالات الإلكترونية لسنة 1986 عرف البريد الإلكتروني على أنه "وسيلة اتصال يتم بواسطتها نقل المراسلات الخاصة عبر شبكة خطوط تليفونية عامة أو خاصة وفي الشكل الغالب تتم كتابة الرسالة على جهاز الحاسب و يتم إرسالها إلكترونياً إلى حاسب مورد الخدمة الذي يتولى تخزينها لديه حتى يأتي المرسل إليه ليستعيدها"⁸.

ولدى الفقه من يرى بأن البريد الإلكتروني يمكن تعريفه بأنه "نظام للتراسل باستخدام شبكات الحاسب يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقمياً في صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه إلا عن طريق كلمة المرور"⁹ أو أنه "طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات"¹⁰.

3.1. المقصود بمراقبة الاتصالات الإلكترونية

المشرع الجزائري لم يقدم تعريفاً لمراقبة الاتصالات الإلكترونية، بل تناول مراقبة الاتصالات الإلكترونية كإجراء بنص المادة 03 من القانون 04-09 التي نصت على أنه "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية وفقاً 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". وبينت لنا المادة 04 من نفس القانون الحالات التي تبرر اللجوء إلى المراقبة الإلكترونية، هذه الحالات هي: "أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة..."

نشير إلى أنه ولدى اطلاعنا على المواد التي جاء بها كل من القانون 04-09 وكذا تلك التي تضمنها المرسوم الرئاسي 261-15 خلصنا إلى نتيجة مفادها بأن المشرع الجزائري تناول عملية مراقبة الاتصالات الإلكترونية في حالتين مختلفتين. الحالة الأولى تكون فيها مراقبة الاتصالات الإلكترونية كإجراء وقائي من جريمة يحتمل وقوعها، فهي لم تقع بعد والاعتداء لم يحدث، فنحن هنا أمام المراقبة الوقائية للاتصالات الإلكترونية. أما الحالة الثانية تكون الجريمة قد وقعت وبدأت التحريات والتحقيقات بشأنها، وهذه الحالة هي التي تهمنا في موضوع مراقبة الاتصالات الإلكترونية باعتبارها إجراء من إجراءات التحقيق الابتدائي يهدف إلى جمع الأدلة من أجل الكشف عن الحقيقة.

المشرع الأمريكي وبموجب قانون المراقبة السلوكية (Intercept) بالقسم 2510 (4) عرف مراقبة الاتصالات الإلكترونية على أنها "الاكتساب السمي "الالتقاط السمي، أو أي التقاط المحتويات أي اتصال سلكي أو إلكتروني أو شفوي باستخدام أي جهاز إلكتروني أو ميكانيكي أو أي جهاز آخر"¹¹.

ويعرف الفقه المراقبة الإلكترونية على أنها " العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع بيانات والمعلومات والتقصي عن الجرائم وعن المشتبه فيهم سواء أكان الخاضع للمراقبة شخصا أو مكانا أو شيئا حسب طبيعته لتحقيق غرض أمني أو لأي غرض آخر"¹². ويقترح الدكتور سامي جلال فقي حسين تعريفا للمراقبة الإلكترونية فيرى بأنها "اعتراض الاتصالات الإلكترونية أيا كان نوعها بموجب إذن قضائي من قبل الخبير المعلوماتي المخول قانونا وباستخدام التقنيات اللازمة لهذه العملية"¹³.

هذا ويجب التمييز بين مراقبة الاتصالات الإلكترونية وضبطها، فالضبط يرد على تلك الاتصالات التي تكون في حالة سكون أي بعد أن يتم تخزينها. في حين أن المراقبة تتم أثناء بث الاتصالات فالمراقبة مصاحبة لوقت البث. فالنطاق الموضوعي للمراقبة الإلكترونية للاتصالات يرد فقط على الاتصالات الإلكترونية أثناء ، باعتبار أنه لا يرد إلا على البيانات الإلكترونية المتحركة، ومن ثم فهو لا يرد على الاتصالات الإلكترونية التي تمت وانتهت أو خزنت سواء في الكمبيوتر الشخصي للمستخدم أو في الخادم المعلوماتي لدى مزود الخدمات، لأن الاتصالات الأخيرة تعد من البيانات الإلكترونية الساكنة.¹⁴ فالاتصالات الإلكترونية تتم بالهواتف النقالة أو اللوحات الذكية أو أجهزة الكمبيوتر والتي يمكن ربطها كلها بشبكة الأنترنت سلكيا أو لا سلكيا (من خلال Wifi أو خدمات الجيل الرابع والخامس 3G و 4G أو الأقمار الاصطناعية).

4.1 أشكال مراقبة الاتصالات الإلكترونية

من صور مراقبة الاتصالات الإلكترونية نجد اعتراض المراسلات السلكية واللاسلكية واعتراض البريد الإلكتروني. فالمراقبة الإلكترونية قد تستهدف الرسائل والخطابات والأحاديث التي يتم تبادلها سواء باستخدام البريد الإلكتروني أو من خلال التخاطب عبر غرف المحادثة والردشة (Chat rooms) أو باستعمال برامج وتطبيقات تتيح نفس الخدمات (Skype أو WhatsApp... إلخ)، أو من خلال خدمات تحميل الملفات (Download) أو خدمة نقل الملفات المعبر عنها اختصارا ب Ftp (filetransferprotocol)¹⁵.

1.4.1 - اعتراض المراسلات السلكية واللاسلكية:

خول المشرع الجزائري للجهات القضائية اعتراض المراسلات السلكية واللاسلكية بنص المادة 65 مكرر 05 من قانون الإجراءات الجزائية والتي أضيفت بموجب القانون 22-06. غير أن المشرع الجزائري لم يقدم تعريفا لعملية اعتراض المراسلات السلكية واللاسلكية أو كما يسميها البعض بالتنصت.

بالرجوع إلى الفقه يمكن تعريف اعتراض المراسلات بأنه "إجراء تحقيقي يباشر خلصة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانوناً بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث، وهي تعتبر أيضاً وسيلة هامة من الوسائل الحديثة للبحث والتحري تستخدمها الضبطية القضائية لمواجهة الإجرام الخطير وتتم عبر وسائل الاتصال السلكية واللاسلكية"¹⁶.

2.4.1 - اعتراض البريد الإلكتروني:

يعتبر اعتراض البريد الإلكتروني من صور المراقبة للاتصالات الإلكترونية، ونظراً لكونه يعتمد على شبكة الأنترنت كوسيلة للتواصل فإن الطرق التقليدية لا تصلح لمراقبة البريد الإلكتروني، لهذا ظهرت برامج متطورة قادرة على مراقبة البريد الإلكتروني نذكر من بينها نظام كارنيفور CARNIVORE¹⁷ والذي تستخدمه وكالة المباحث الفيدرالية الأمريكية للتجسس.

5.1. الطبيعة القانونية لمراقبة الاتصالات الإلكترونية

اختلف الفقه حول الطبيعة القانونية لمراقبة الاتصالات الإلكترونية من كونها تأخذ حكم الاطلاع على الرسائل أم أنها نوع من أنواع التفتيش أم أن الأمر يتعلق بإجراء آخر من نوع خاص.

مراقبة الاتصالات الإلكترونية لا يمكنها أخذ حكم الاطلاع على الرسائل، فالرسالة لها وجود مادي عكس الاتصالات الإلكترونية، حتى وإن كان هناك تشابه يجمعهما في كونهما يحتويان على أسرار الحياة الخاصة للمرسل والمرسل إليه. كما أنه لا يمكن اعتبار مراقبة الاتصالات الإلكترونية نوعاً من أنواع التفتيش ذلك أن التفتيش يفضي إلى الضبط المادي، في حين أن الاتصالات الإلكترونية لا يمكن ضبطها كونها عبارة عن نبضات إلكترونية.

ونحن نميل للرأي الأخير الذي يعتقد بأن مراقبة الاتصالات الإلكترونية هي إجراء من نوع خاص، فهو لا يأخذ حكم الاطلاع على الرسائل كما لا يمكن

اعتباره من قبيل التفتيش، رغم أوجه التشابه بينهم لكون هذه الإجراءات مجتمعة تشترك في سعيها للوصول إلى الدليل، كما أنها تمس بالحياة الخاصة للأفراد.

2. الضوابط المتعلقة بمراقبة الاتصالات الإلكترونية

الاتصالات الإلكترونية تشمل ذلك النوع من المكالمات التي يهدأ فيها المتحدث إلى محدثه حيث تتبادل الأسرار ويتم بسط الأفكار الشخصية دون حرج أو خوف من تنصت الغير، وفي مأمن من فضول استراق السمع ويعد هذا صورة من صور ممارسة الأفراد لحياتهم الخاصة¹⁸ لذلك كان من الضروري وضع مجموعة من الضوابط كضمانات تصون حرمة الحياة الخاصة للأفراد لدى استغلالهم لوسائل الاتصالات الإلكترونية. هذه الضوابط هي:

1.2. وجود سبب ضروري يبرر اللجوء لمراقبة الاتصالات الإلكترونية

وهذا ما تضمنته المادة 65 مكرر 5 من قانون الإجراءات الجزائية¹⁹ فيجوز اللجوء إلى اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ذلك.

وفي السياق ذاته، نصت المادة 03 من القانون رقم 04-09 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". إن مراقبة الاتصالات الإلكترونية ليس إجراء آلي نستعين به كلما كنا أمام تحقيقات قضائية وإنما يجب تقييده وحصره بأسباب محددة. فالمادة 04 من القانون 04-09 الفقرة (ج) اشترطت أن يتم اللجوء إلى مراقبة الاتصالات الإلكترونية متى كان ذلك ضروريا أي حينما تواجه التحقيقات القضائية صعوبة للوصول إلى نتيجة، لكن كيف يمكن التأكد من أن جهات التحقيق في حاجة ماسة

فعلا إلى مراقبة الاتصالات الإلكترونية؟ بحسب المادة 08 بفقرتها 02 من المرسوم الرئاسي 15-261 فإن اللجنة المديرية، والتي تعتبر جهاز من ضمن الأجهزة التي تتشكل منها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، هي من تتولى النظر في مدى توافر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية. لكن هنا الأمر يتعلق بالمراقبة "الوقائية"، نرى بأن تقدير ضرورة اللجوء لمراقبة الاتصالات الإلكترونية إما يخضع لتقدير قاض التحقيق المختص وهذا في حالة فتح تحقيق قضائي، أو لتقدير وكيل الجمهورية المختص وذلك في حالة التلبس طبقا للمادة 65 مكرر 5 من قانون الإجراءات الجزائية في فقرتها الأخيرة.

2.2. صدور إذن مكتوب من السلطة القضائية المختصة

اشتترطت المادة 04 من قانون 09-04 بفقرتها الأخيرة وجوب صدور رخصة عن الجهة القضائية المختصة والتي حددتها المادة 65 مكرر 5 من قانون الإجراءات الجزائية، ففي حالة التلبس يصدر الإذن عن وكيل الجمهورية، أما في حالة فتح تحقيق قضائي فالإذن يصدر عن قاض التحقيق.

طبقا للمادة 65 مكرر 7 يكون الإذن مكتوبا ومتضمنا للعناصر التالية²⁰:

- الاتصالات المراد التقاطها.

- الأماكن المقصودة لهذا الغرض، سواء تعلق الأمر بالمساكن أو غيرها.

- ذكر الجريمة التي تبرر اللجوء إلى هذه التدابير.

- تحديد المدة بأربعة أشهر كحد أقصى قابلة للتجديد.

3.2. الجهة المناط بها تنفيذ مراقبة الاتصالات الإلكترونية

المراقبة الإلكترونية عمل تقني، لذلك أجاز المشرع الجزائري لوكيل الجمهورية أو لضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه، تسخير جهات مختصة للتكفل بالجوانب التقنية. نصت المادة 65 مكرر 8 بأنه "يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر

كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 5 أعلاه". والجهة المختصة يقصد بها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وهذا ما جاء بالمادة 04 في فقرتها 04 من المرسوم الرئاسي 15-261 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.

لا يعني ذلك بأن المشرع غفل عن هذا الأمر، بل 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 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". يتضح بأن المشرع خول مراقبة الاتصالات الإلكترونية لجهة وأشخاص محددين وهم:

1.3.2. الجهة:

يتم إنشاء "وحدة مراقبة" من طرف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، يتم تزويدها بالوسائل التقنية الضرورية.

2.3.2. الأشخاص:

حددتهم الفقرة 02 من المادة 22 من المرسوم الرئاسي 15-261 وهم:

– المستخدمون التقنيون: وهم من ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني. وهذا ما جاء بالمادة 18 الفقرة الأخيرة

من المرسوم الرئاسي 15- 261²¹... وتزود أيضا بمستخدمي الدعم التقني والإداري، ويجلب هؤلاء المستخدمون من ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني".

- **قاضي:** يتولى إدارة وحدة المراقبة ومراقبة عمل المستخدمين التقنيين. وهو من بين القضاة المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال التي يتم تزويدها بقضاة طبقا لنص المادة 18 الفقرة 01 من المرسوم الرئاسي 15-261 التي جاء بها " تزود الهيئة بقضاة وفقا للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول".

- **ضابط أو أكثر من ضباط الشرطة القضائية:** مهمتهم مساعدة القاضي الذي يتولى إدارة ومراقبة عمل وحدة المراقبة. ويتم اختيار هذا الضابط من بين أولئك الضباط الذين تم تزويد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بهم، والذين تم جلبهم من بين ضباط المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني، ويتم تحديد عددهم بموجب قرارات مشتركة ما بين الوزراء المكلفين بالعدل، والدفاع الوطني، والداخلية. وهذا ما نصت عليه الفقرة الثانية للمادة 18 من المرسوم الرئاسي 15-261 "... كما تزود بضباط وأعاون للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني، يحدد عددهم بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل، والدفاع الوطني، والداخلية..."

4.2. إحاطة العملية بالسرية

يجب ضمان سرية إجراء مراقبة الاتصالات الإلكترونية ووجوب حماية المعلومات المتحصل عليها طبقا للفقرة 02 للمادة 23 من المرسوم الرئاسي 15-261 التي نصت على " يتخذ مسؤول الوحدة أثناء سير العملية كل التدابير اللازمة، بالاتصال مع المسؤولين المعنيين في الهيئة، من أجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة".

وإذا استهدفت عملية مراقبة الاتصالات الإلكترونية أشخاصا ملزمون قانونا بكتتمان السر المهني وجب عدم المساس بهذا السر، وذلك طبقا للمادة 65 مكرر 6 من قانون الإجراءات الجزائية، والتي جاء بها " تتم العمليات المحددة في المادة 65 مكرر 5 أعلاه، دون المساس بالسر المهني المنصوص عليه في المادة 45 من هذا القانون...". وكما يلاحظ فإن ذات المادة تحيلنا إلى المادة 45 من قانون الإجراءات الجزائية التي نصت بفقرتها 04 على أنه "...غير أنه يجب عند تفشيش أماكن يشغلها شخص ملزم قانوناً بكتتمان السر المهني أن تتخذ مقبماً جميع التدابير اللازمة لضمان احترام ذلك السر...".

5.2. تحرير محضر

تقوم وحدة المراقبة بإعداد محضر يتضمن الإجراءات التي قامت بها طبقا للمادة 22 الفقرة الأخيرة من المرسوم 15-261 التي نصت " ...وتحرر أشغالها في محضر يعد طبقا لأحكام قانون الإجراءات الجزائية". يحرر هذا المحضر وفقا لأحكام المادة 65 مكرر 9 من القانون 06-22 المعدل لقانون الإجراءات الجزائية التي نصت بأنه "يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري. يذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاؤها منها".

الخاتمة:

من خلال عرضنا لمفهوم مراقبة الاتصالات الإلكترونية يتضح جليا مدى أهمية هذا الإجراء إذ يشكل سندا لجهات التحقيق في مواجهة الجريمة الإلكترونية، إذ أنها تتعامل مع كم هائل وضخم من البيانات التي لا نهاية لها والمتدفقة بوتيرة لا يمكن مجاراتها إلا من خلال الاعتماد على إجراءات جديدة لجمع الأدلة الإلكترونية التي من شأنها إيصال جهات التحقيق إلى الجناة وبالتالي الكشف عن

الحقيقة. هذه الإجراءات كان ولا بد من أن تتضمن تقنيات متطورة وأساليب حديثة تجاري تلك التقنيات والأساليب التي يستخدمها المجرم الإلكتروني في تنفيذ جرائمه الإلكترونية.

تخضع مراقبة الاتصالات الإلكترونية لضوابط أوجب القانون احترامها بالنظر لما تشكله مراقبة الاتصالات من خطورة ومساس بالحياة الخاصة للأفراد. بحيث حصر مهمة القيام بهذا الإجراء في جهة محددة هي "وحدة المراقبة" وفي أشخاص محددين وذلك بعد الحصول على إذن مكتوب وبعد التأكد فعلا من وجود ضرورة ملحة تستدعي اللجوء إلى مراقبة الاتصالات الإلكترونية، والتي بدونها لا يمكن التوصل إلى نتائج والحصول على الأدلة.

كما أسند القانون مهمة الرقابة على الجهة المباشرة للمراقبة الإلكترونية إلى جهة قضائية محددة، واشترط تحرير محاضر تتضمن كل التفاصيل المتعلقة بعملية المراقبة الإلكترونية.

الاقتراحات:

رغم أهمية مراقبة الاتصالات الإلكترونية كإجراء يساهم في جمع الأدلة الإلكترونية، إلا أنه يصطدم بمسألة في غاية الحساسية ألا وهي الخصوصية وما يثار بشأنها من جدل وردود أفعال تتعلق بالانتهاكات التي تطل حرماتها وسريتها. ففسرية الاتصالات تعد من صميم الحياة الخاصة للأفراد، وإخضاعها للمراقبة هو انتهاك صريح لمستودع أسرار الناس، لذلك وجب مراعاتها أكثر بالعمل على حصر تلك الحالات التي يتم فيها اللجوء إلى مراقبة الاتصالات الإلكترونية.

وفي الحقيقة فإن هذا الأمر يعتبر معضلة يصعب تجسيدها على أرض الواقع، وهي ليست وليدة أو نتاج الجريمة الإلكترونية بل أن هذا الوضع كان قائما حتى قبل ظهور الإجرام الإلكتروني، مادام أن الجدل حول إشكالية التوفيق بين مصلحة المجتمع من جهة والحريات الشخصية من جهة أخرى ساد في ظل الجريمة التقليدية ولا يزال مستمرا إلى غاية يومنا هذا.

كما أن موضوع التعاون الدولي يثير معضلة أخرى تكمن في مدى تقبل هذه الدولة أو تلك للتعاون مع باقي الدول على مراقبة الاتصالات الإلكترونية، خاصة إذا كان المستهدف من عملية المراقبة أحد مواطني هذه الدولة. لذلك على الدول السعي لإيجاد صيغة حقيقية ومجدية للتعاون فيما بينها عندما يكون اللجوء إلى مراقبة الاتصالات الإلكترونية إجراء لا بد منه من أجل استيفاء الأدلة المتعلقة بالجريمة الإلكترونية، فالدول غالباً لا تتعاون إلا إذا كان التهديد مشترك والمصالح مشتركة أما إذا تعارضت مصالحها فتأبى التعاون أو تلجأ للمعاملة بالمثل، ولو أن الدول القوية إما تمارس ضغوطاً لإجبار الدول الضعيفة على التعاون أو أنها تستغل تطورها التكنولوجي وتباشر بمراقبة الاتصالات الإلكترونية سواء برضا أو دون رضا الدول الأخرى مما يشكل انتهاكاً لسيادة الدول ويقوض ويهدم كل الجهود الرامية إلى التعاون.

الهوامش

¹ القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 47 الصادرة في 25 شعبان 1430 الموافق 16 غشت 2009.

² المرسوم الرئاسي رقم 15-261 المؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53 الصادرة في ذي الحجة عام 1436 الموافق 8 أكتوبر 2015.

³ أشار إليه ومحمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، دار الجامعة الجديدة، الإسكندرية، 2018، ص 326. "The Wiretap Statute" (Title III), 18 U.S.C. 2510-2522 (2)

⁴ أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة السابعة، 1993م ص 578..

⁵ القانون رقم 03-2000 المؤرخ في 5 جمادى الأول عام 1421 الموافق 5 غشت سنة 2000 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الجريدة الرسمية للجمهورية الجزائرية العدد 48 الصادرة في 6 جمادى الأول عام 1421 الموافق 6 غشت سنة 2000.

⁶ يعد العالم الأمريكي رايموند صامويل توملينسون Raymond Samuel Tomlinson مخترع البريد الإلكتروني، إذ صمم على شبكة الإنترنت برنامجا لكتابة الرسائل يسمى (send message) وذلك بهدف تمكين العاملين بالشبكة تبادل من الرسائل فيما بينهم، ومن ثم ابتكر برنامجا يسمى (Cygnat) ويسمح بنقل الملفات من جهاز حاسوب إلى آخر ومن ثم قام بدمج البرنامجين في برنامج واحد ونتج عنه البريد الإلكتروني. للمزيد أنظر كل من جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 20. وسامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية، 2011، ص 253. وخالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008. وكذلك محتوى الرابط:

<https://www.aljazeera.net/encyclopedia/icons/2016/3/7/-البريد-توملينسون-مخترع>
الإلكتروني

⁷ Article 1/ IV, alinéa 5 (LOI n° 2004-575 du 21 juin 2004, JORF n°0143 du 22 juin 2004- pour la confiance dans l'économie numérique)

"...On entend par courrier électronique tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère".

⁸ "Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines.

In its most common form, messages are typed in to a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company, If The intended addressee subscribes to the service, the message is stored... such as systems operated by private companies for internal correspondence". Electronic Communications Privacy Act of 1986 (ECPA).

أنظر: عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة، 2005، ص12.

⁹ مناني فراح، أدلة الإثبات الحديثة في القانون، دار الهدى، عين مليلة، 2008، ص 59.

¹⁰ عبد الهادي فوزي العوضي، المرجع السابق، ص12.

¹¹ "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

للمزيد حول هذا التعريف أنظر سامي جلال فقي حسين، المرجع السابق، ص 283. ومحمد كمال شاهين، المرجع السابق، ص 328.

¹² مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، الطبعة الأولى، مطابع الشرطة، القاهرة، 2003، ص 192.

¹³ سامي جلال فقي حسين، المرجع السابق، ص 284.

¹⁴ شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 305-306 أشار إليها رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، 2013، ص 179.

¹⁵ أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، الطبعة الأولى، دار الوفاء لدنيا الطباعة والنشر، الإسكندرية، 2016، ص 443.

¹⁶ ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، 2009، ص 150.

¹⁷ وتعني تسمية كارنيفور "أكل اللحم" في إشارة إلى كون هذا البرنامج يقوم بالتهام كافة البيانات المتدفقة عبر الشبكة. أنظر في هذا المعنى فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016، ص 76.

وكانيفور CARNIVORE هو برنامج تم تطويره من طرف مكتب التحقيقات الفيدرالي FBI وهو مصمم ليسمح بجمع معلومات محددة حول رسائل البريد الإلكتروني أو أية اتصالات إلكترونية أخرى. وتجدر الإشارة إلى أنه وبعد أحداث 2001/09/11 تم تغيير تسمية البرنامج من كانيفور إلى دي سي أس 1000 (DCS1000).

وإذا كان كانيفور هو البرنامج الأشهر إلا أن هناك برامج أخرى منافسة له ففي بريطانيا أصدر مجلس العموم قانونا يحمل اسم RIP وبموجبه يفرض على كافة الشركات المزودة

لخدمات إنترنت أن تقوم بالتعاون مع السلطات في التحقيقات الأمنية بتثبيت جهاز (صندوق أسود) مشابه لكارنيفور بجانب أجهزتها المزودة. وكذلك الوضع في روسيا، حيث هناك صدر قانون يحمل اسم SORM ويفرض على الشركات المزودة لخدمات الإنترنت إلزامية تحويل كافة البيانات المتداولة إلى جهاز وكالة الاستخبارات الروسية FSB للاطلاع عليها واستخدامها دون أمر من المحكمة. لمزيد من المعلومات على الرابطين التاليين:

<https://www.epic.org/privacy/carnivore/default.html>

<https://ar.wikipedia.org/wiki/كارنيفور>

¹⁸ محمد كمال شاهين، المرجع السابق، ص 325.

¹⁹ القانون رقم 22-06 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 الصادر بالجريدة الرسمية العدد 84 المؤرخة في 24 ديسمبر 2006 يعدل ويتم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، تنص المادة 65 مكرر 5:

"إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

-اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

-وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبحث وتسجيل الكلام المنفوخ به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن. تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص.

في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة".

20 المادة 65 مكرر 7 " يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 أعلاه، 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".

21 المادة 18 من المرسوم الرئاسي 15- 261 "تزود الهيئة بقضاة وفقا للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول. كما تزود بضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني، يحدد عددهم بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل، والدفاع الوطني، والداخلية. وتزود أيضا بمستخدمي الدعم التقني والإداري، ويجلب هؤلاء المستخدمون من ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني".

قائمة المراجع:

أولا: المؤلفات

- سرور، أحمد فتحي، (1993)، الوسيط في قانون الإجراءات الجنائية، مصر، القاهرة، دار النهضة العربية.
- الصغير، جميل عبد الباقي، (2002)، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مصر، القاهرة، دار النهضة العربية.
- إبراهيم، خالد ممدوح، (2008)، حجية البريد الإلكتروني في الإثبات، مصر، الإسكندرية، دار الفكر الجامعي.
- حسين، سامي جلال فقي، (2011)، التفتيش في الجرائم المعلوماتية، مصر، دار الكتب القانونية.
- العوضي، عبد الهادي فوزي، (2005)، الجوانب القانونية للبريد الإلكتروني، مصر، القاهرة، دار النهضة العربية.
- العازمي، فهد عبد الله العبيد، (2016)، الإجراءات الجنائية المعلوماتية، مصر، دار الجامعة الجديدة.
- شاهين، محمد كمال، (2018)، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، مصر، الإسكندرية، دار الجامعة الجديدة.

- موسى، مصطفى محمد، (2003)، المراقبة الإلكترونية عبر شبكة الإنترنت، مصر، القاهرة، مطابع الشرطة.
- مناني، فراح، (2008)، أدلة الإثبات الحديثة في القانون، الجزائر، عين مليلة، دار الهدى.
- فاروق، ياسر الأمير، (2009)، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، مصر، الإسكندرية، دار المطبوعات الجامعية.
- يوسف، أمير فرج، (2016)، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، الإسكندرية، دار الوفاء لدنيا الطباعة والنشر.
- عبد الغني محمد عطا الله، شيماء، (2007)، الحماية الجنائية للتعاملات الإلكترونية، الإسكندرية، دار الجامعة الجديدة.
- خالد عمر، رشاد، (2013)، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، الإسكندرية، المكتب الجامعي الحديث.

ثانياً: القوانين

- القوانين باللغة العربية

- القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 47 الصادرة في 25 شعبان 1430 الموافق 16 غشت 2009.
- القانون رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 الصادر بالجريدة الرسمية العدد 84 المؤرخة في 24 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.
- القانون رقم 03-2000 المؤرخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الجريدة الرسمية للجمهورية الجزائرية العدد 48 الصادرة في 6 جمادى الأولى عام 1421 الموافق 6 غشت سنة 2000.
- المرسوم الرئاسي رقم 15-261 المؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53 الصادرة في ذي الحجة عام 1436 الموافق 8 أكتوبر 2015.

-القوانين باللغة الأجنبية

Loi n° 2004-575 du 21 juin 2004, JORF n°0143 du 22 juin 2004- pour la confiance dans l'économie numérique.

ثالثاً: مواقع الإنترنت

- الجزيرة (2016)، توملينسون.. مخترع البريد الإلكتروني يترجل
<https://www.aljazeera.net/encyclopedia/icons/2016/3/7/-البريد-توملينسون-مخترع-البريد-الإلكتروني>
(consulté le 14/04/2020)
- ويكيبيديا (2019)، كارنيفور
 - <https://ar.wikipedia.org/wiki/كارنيفور> (consulté le 25/12/2019)
 - Epic,(2005),Significant New FBI Carnivore Documents Obtained by EPIC, <https://www.epic.org/privacy/carnivore/default.html> (consulté le 25/12/2019)