دفاتر البحوث العلمية، المجلد 9، العدد 1، السنة 2021، الصفحة 227-243

# إجراءات استخلاص الدليل في الجرائم المعلوماتية

# Procedures of proof establishment in cybercrimes

**حليم رامي***

كلية الحقوق والعلوم السياسية، جامعة البليدة 2، الجزائر، h.rami@univ-blida2.dz

**تاريخ الاستلام:** 2021/05/15، **تاريخ القبول:** 2021/05/30، **تاريخ النشر:** 2021/06/08

**ملخص:** إن استخلاص الدليل، هو المرحلة التي يتم فيها تهيئة القضية بالبحث والتحري، عن طريق أشخاص أضفى عليهم القانون صفة الضبطية القضائية، لتقديمها في مرحلة لاحقة للنيابة، التي تتصرف فيها وفقا لما تملكه من سلطة الملاءمة. لذلك توجب منح ضباط الشرطة القضائية، مزيدا من الاختصاصات تسهيلا لمهامهم من جهة، ومن جهة أخرى حماية لهم من اتخاذ إجراءات خارج تلك التي يختصون بها أو يخولها لهم القانون. من هذا المنطلق سعت دول عديدة إلى تكريس مبدأ الاختصاص النوعي لضباط الشرطة القضائية في تشريعاتها، وإضافة النصوص القانونية الإجرائية اللازمة لتنظيم عملهم، تحقيقا للتوازن بين مصلحة المجتمع في التصدي لهذا النوع من الجرائم، وعدم المساس بالحقوق والحريات.

**الكلمات المفتاح:** جريمة معلوماتية؛ دليل معلوماتي؛ بحث وتحري؛ منظومة معلوماتية؛ إثبات.

**Abstract:** The establishment of the proof is a phase focusing on the preparation of the vase by means of research and investigation by persons who have been granted, under the law, the quality of judicial police officers; the case shall be subsequently submitted to the prosecutor's office which shall deal with it following the appropriate authority that he latter enjoys. Thereupon, the judicial police officers should be granted more prerogatives as to facilitate their missions on one side, and ensure their protection against the taking of procedures that do not fall within their competence or that are not conferred upon by the law, on the other side. From this point, different countries have been working on the entrenchment of the principle of qualitative competence of the judicial police officers within legislation, as well as the inclusion of legal and procedural texts needed for the organization of their work, ensuring a balance between the concern of the nation to face this kind of crime and toi avoid undermining rights and freedoms.

**Keywords:** Cybercrime; Computer proof; research and investigation; Informational system; Prove.

*المؤلف المرسل

## 1- تمهيد:

خصوصية الجرائم المعلوماتية بالنظر إلى طبيعتها الرقمية التي تميزها عن غيرها، فرضت منطقا مختلفا في التعامل معها واستيعابها على مستوى مراحل إثباتها المختلفة، من خلال تطوير أساليب البحث والتحري بما يتلاءم والمستوى التقني المتطور والمعقد لهذه الجرائم، وهو نفس المنطق الذي جعل المشرع الجزائري يسارع إلى استحداث إجراءات تحري خاصة **(تتمثل في التسرب واعتراض المراسلات السلكية واللاسلكية المنصوص عليها في المادة 65 مكرر5 وما يليها من قانون الإجراءات الجزائية)** بموجب القانون 06-22 المؤرخ في 29 ذي القعدة 1427 الموافق لـ: 20 ديسمبر 2006 المتمم للأمر 66-156 المؤرخ في 18 صفر 1386 الموافق لـ: 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية **(يتبع المخبر المركزي للشرطة العلمية والتقنية أربع مخابر جهوية موزعة عبر التراب الوطني وهي: المخبر الجهوي بوهران، المخبر الجهوي بقسنطينة، المخبر الجهوي ببشار، المخبر الجهوي بتمنراست)** وإصدار القانون 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها. رافق تشريع هذه الترسانة من القوانين، إنشاء عدة هيئات وأجهزة للوقاية من الجريمة المعلوماتية، منها ما هو تابع لوزارة العدل ومنها ما هو تابع لمصالح الأمن كالمصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التابع للمديرية العامة للأمن الوطني والمعهد الوطني للشرطة الجنائية أو المخبر المركزي للشرطة العلمية والتقنية **(منشور في الجريدة الرسمية للجمهورية الجزائرية، العدد 48 الصادرة بتاريخ 04 ذي الحجة 1427 الموافق لـ:24 ديسمبر 2006 ص 30)** وأخرى تابعة لجهاز الدرك الوطني كالمعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، الذي تم إنشاؤه بالمرسوم الرئاسي رقم 04-183 الصادر بتاريخ 26 جوان 2004، ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني. كما تم بموجب المادة 13 من القانون 09- 04 **(بالرجوع إلى نص المادة 13 من القانون 09-04 نجد أنها تنص على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على أن تحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم، وبتاريخ 08 أكتوبر 2015 صدر المرسوم الرئاسي رقم 15-261 المتضمن تشكيل وتنظيم وكيفيات سير الهيئة، حيث نصت المادة الثانية وما يليها منه على أن الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل ويقع مقرها بالجزائر العاصمة وتتولى مهامها تحت رقابة السلطة القضائية وطبقا لأحكام التشريع الساري المفعول لاسيما منها قانون الاجراءات الجزائية والقانون 09-04)** استحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ويأتي على رأس مهام هذه الهيئة، اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها **(تتولى هذه الهيئة تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال**

**ومكافحتها، بالإضافة إلى مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة والوقاية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص، كما تتولى الهيئة تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية (راجع في هذا الشأن المادة 04 من المرسوم الرئاسي رقم 15-261 الصادر بتاريخ 08 أكتوبر 2015 المتضمن تشكيل وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).** وإذا كانت أهمية هذا البحث تنبثق أساسا من نطاق التكامل بين الإجراءات التقليدية والمستحدثة، بمعنى حرص المشرع الجزائري على أن تتوفر المنظومة التشريعية إلى جانب الوسائل الكلاسيكية أو الإجراءات التقليدية في استخلاص الدليل المعلوماتي، على إجراءات مستحدثة تتلاءم مع الطبيعة الخاصة للجريمة المعلوماتية، فإن إشكالية هذه الدراسة يمكن صياغتها على النحو التالي: **ما مدى اكتمال البنية التشريعية في جانبها الإجرائي لمكافحة الجريمة المعلوماتية؟** وهو ما سنحاول الإجابة عليه من خلال هذا البحث التي يغلب عليه المنهج التحليلي من خلال تحليل النصوص القانونية، بالإضافة إلى المنهجين الوصفي والاستقرائي لاسيما وأن الدراسة تناولت بشيء من التفصيل تطور التشريع الإجرائي، لذلك وحتى تستجيب المنهجية لمتطلبات البحث، جاءت الخطة مهيكلة في مبحثين، تطرق المبحث الأول إلى الأساليب الكلاسيكية لاستخلاص الدليل المعلوماتي، أما المبحث الثاني فتناول الأساليب المستحدثة لاستخلاص الدليل المعلوماتي.

## 2- الأساليب الكلاسيكية لاستخلاص الدليل المعلوماتي:

غالبا ما يكون مسرح ارتكاب الجريمة المعلوماتية مركبا من بيئتين، إحداهما تقليدية والثانية افتراضية، تحتوي كلاهما على مجموعة من العناصر والمعطيات التي تساعد في الكشف عن الجريمة وظروف ارتكابها، لذلك يتم اللجوء إلى الاعتماد على أساليب منظمة إجرائيا لاستخلاص الدليل الذي يبنى عليه اسناد المسؤولية الجزائية وإثبات الجريمة، وهي كما هو منصوص عليها قانونا: المعاينة، التفتيش، شهادة الشهود، الخبرة.

### 1.2- المعاينة:

المقصود بالمعاينة في الجريمة المعلوماتية هو الوقوف على الآثار التي يخلفها مستخدم النظام المعلوماتي، حيث يعتبر الانتقال إلى عين المكان أولى الخطوات التي يقوم بها رجال الضبطية القضائية في تعاملهم مع مسرح الجريمة لمعاينة وإثبات الأثار والمخلفات المادية والمحافظة عليها، وإثبات حالة الأماكن والأشخاص عن طريق الكتابة والتخطيط والصور ويمنع إحداث اي تغيير في معالم مسرح الجريمة، كما يراعى تسجيل وقت وتاريخ التقاط الصور

والفيديو، والسرعة في اتخاذ الإجراءات الكفيلة بإثبات هوية بعض الحضور وسماعهم، وفي بعض الحالات منعهم من مغادرة الأمكنة، وإخطار نيابة الجمهورية بذلك فورا. كما يجب التأكيد على ضرورة التقيد بالنصوص القانونية التي تنظم إجراءات المعاينة، من أجل إضفاء طابع الشرعية على الإجراءات، وعدم المساس بالحقوق والحريات الفردية أو التعرض لها إلا في حدود ما يسمح به القانون احتراما لمبدأ قرينة البراءة، وفي الأخير يجب تدوين المعاينة بكافة تفاصيلها في محضر لتمكين القاضي من الاطلاع عليها. وبالرجوع إلى نص المادة 47 الفقرة 03 من قانون الإجراءات الجزائية، فإن المشرع الجزائري أجاز المعاينة عندما يتعلق الأمر بجرائم المساس بأنظمة المعالجة الآلية للمعطيات في كل محل سكني أو غير سكني وفي أي ساعة من ساعات النهار أو الليل وذلك بناء على إذن من وكيل الجمهورية المختص، أما في ما يتعلق بالجرائم الماسة بالمعطيات ذات الطابع الشخصي، فقد منح المشرع الجزائري للسلطة الوطنية **(حيث تتمتع هذه السلطة بالشخصية المعنوية والاستقلال المادي والإداري، وتقيد ميزانيتها في ميزانية الدولة وتخضع للمراقبة طبقا للتشريع المعمول به، وتتشكل السلطة الوطنية من ثلاث شخصيات من بينهم الرئيس، ويختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال السلطة الوطنية، إضافة إلى 3 قضاة يقترحهم المجلس الأعلى للقضاة من بين قضاة المحكمة العليا ومجلس الدولة، وأيضا عضو من كل غرفة من البرلمان، يتم اختياره من قبل رئيس كل غرفة بعد التشاور مع رؤساء المجموعات).** أما في حالة وقوع جريمة من الجرائم المنصوص عليها في القانون 18-07 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، فإنه بالإمكان القيام بالتحريات المطلوبة ومعاينة المحلات والأماكن التي تتم فيها معالجة المعطيات الشخصية، باستثناء محلات السكن التي لا يجوز معاينتها **(المادة 49 من القانون 18-07 المؤرخ في 25 رمضان 1439 الموافق لـ 10 يونيو 2018 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، منشور في الجريدة الرسمية عدد 34)**،كما يجوز للضبطية اثناء قيامها بالتحري عن الجرائم المرتكبة من مخالفة أحكام القانون 18-07، الولوج إلى كافة المعطيات الشخصية المعالجة وإلى كافة المعلومات والوثائق مهما كانت دعامتها، ولا يعتد بالسر المهني للمعطيات الشخصية المعالجة أمام السلطة الوطنية **(المادة 49 من القانون 18-07 المؤرخ في 25 رمضان 1439 الموافق لـ 10 يونيو 2018 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، منشور في الجريدة الرسمية عدد 34).** تجدر الإشارة في هذا الإطار أنه بالإضافة إلى ضباط وأعوان الشرطة القضائية، أوكل المشرع الجزائري مهمة البحث ومعاينة الجرائم المنصوص عليها في القانون 18-07 إلى أعوان الرقابة الذين تلجأ إليهم السلطة الوطنية تحت إشراف وكيل الجمهورية **(المادة 50 من القانون 18-07 المؤرخ في 25 رمضان 1439 الموافق لـ 10 يونيو 2018 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، منشور في الجريدة الرسمية عدد 34)** على أن تتم المعاينة بواسطة محاضر يتعين توجيهها فورا إلى وكيل الجمهورية

المختص إقليميا **(المادة 51 من القانون 18-07 المؤرخ في 25 رمضان 1439 الموافق لـ 10 يونيو 2018 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، منشور في الجريدة الرسمية عدد 34).**

## 2.2- التفتيش:

التفتيش هو إجراء من إجراءات التحقيق يهدف للبحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وفقا للضمانات والقيود المقررة قانونا والتفتيش في الجرائم المعلوماتية يحتاج إلى تقنيات خاصة، لسهولة إخفاء المعطيات وصعوبة تحديد مكانها و الذي من الممكن أن يكون خارج مسرح الجريمة تماما او خارج حدود الدولة كليا، لذلك يجب أن نميز بين التفتيش الذي يقع على المكونات المادية والتفتيش الذي يقع على المكونات المنطقية أو كما تسمى المعنوية. ففي الحالة الأولى التي يقع فيها التفتيش على المكونات المادية لأنظمة المعالجة الآلية للمعطيات فإن الإشكال لا يطرح، لأنه يخضع للقواعد العامة للتفتيش، إلا أنه يجب مراعاة مكان تواجد هذه المعدات، فإذا كانت في مكان خاص فإن صحة الإجراء تقتضي الالتزام بالشروط المنصوص عليها في المادتين 46 و47 من قانون الإجراءات الجزائية، وهي الحصول على الموافقة الكتابية لصاحب المسكن، فضلا عن حضوره هو أو من يمثله مع مراعاة المواعيد الخاصة بالتفتيش، في حين يخضع التفتيش إذا كان محله في مكان عام للقواعد الإجرائية الخاصة بتفتيش الأشخاص، وعليه فإنه لا يوجد أي مانع قانوني لفحص وتفتيش المكونات المادية لأنظمة المعالجة الآلية للمعطيات باعتبارها أشياء استنادا لنص المادة 44 من قانون الإجراءات الجزائية. أما الحالة الثانية والتي تتعلق بتفتيش المكونات المنطقية لنظام المعالجة الآلية، فقد ثار خلاف حول مدى صلاحيتها لأن تكون موضوعا للتفتيش، فيرى جانب من الفقه بأن التفتيش يقع على المكونات ذات الطبيعة المادية وليس على البيانات التي ليس لها مظهر مادي محسوس **(خالد، 2009، ص 195)**. في حين يرى جانب آخر أن أحكام الاجراءات الجزائية الخاصة بالتفتيش يمكن أن تتناسب مع المكونات المعنوية، باعتبارها قابلة للضبط والتخزين في وسائط مادية أو طبعها على دعائم ورقية **(خالد، 2009، ص 198)**. وهو نفس اتجاه المشرع الجزائر ي الذي أجاز صراحة بموجب نص المادة الخامسة من القانون 09-04 للسلطات القضائية المختصة وكذا ضبّ اط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 منه، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، كما أجاز التفتيش عندما يتعلق الأمر بمنظومة تخزين معلوماتية. ونظرا لخطورة التفتيش باعتباره إجراء يمس بالدرجة الأولى بحقوق الأفراد وحرياتهم، وجب على المشرع إحاطته بضوابط تشكل في حقيقتها ضمانات لتكريس التوازن بين حماية المجتمع من جهة وعدم المساس بحقوق الافراد وحرياتهم من جهة أخرى، من بينها ضرورة الحصول على إذن مكتوب بالتفتيش استنادا لنصوص المواد 44، 64 و68 من قانون

الإجراءات الجزائية، وضرورة حضور صاحب المسكن عملية التفتيش، وإلزامية حصول التفتيش في التوقيت المحدد قانونا. إلا أن خصوصية الجريمة المعلوماتية فرضت على المشرع أن يورد استثناءات على هذه الضوابط، من بينها التعديل الذي ألحقه على قانون الاجراءات الجزائية بالقانون 06-22 والذي استثنى بموجبه حضور المشتبه فيه أو الشاهدين عملية التفتيش، بالإضافة إلى الاستثناء الوارد بالفقرة الثالثة من المادة 47 من قانون الاجراءات الجزائية والمتعلق بجواز إجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل إذا تعلق الأمر بنوع معين من الجرائم من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

### 3.2- شهادة الشهود:

تعرف الشهادة بأنها تقرير الشخص لما يكون قد رآه أو سمعه بنفسه أو أدركه بإحدى حواسه الأخرى، فهي التعبير الصادق عن مضمونها والإدراك الحي للشاهد بالنسبة للواقعة التي شاهدها أو سمعها أو أدركها بحاسة من حواسه بطريقة مباشرة والمطابقة لحقيقة الواقعة التي يشهد عليها في مجلس القضاء ممن تقبل شهادتهم بعد أداء اليمين **(القدسي، 2010، ص 130)** لذلك فهي وسيلة من وسائل الإثبات، التي تكتسي أهمية بالغة في الدعوى الجزائية، باعتبارها إجراء من إجراءات التحقيق عبر مختلف مراحله، من خلالها يتم الحصول على المعلومات التي يدلي بها من تواجد في مسرح الجريمة أو كل من توفرت لديه معلومات تفيد في كشف ملابسات الجريمة للإدلاء بها أمام السلطة المختصة. وإذا كانت الشهادة في الجريمة المعلوماتية لا تختلف من حيث ماهيتها عن الشهادة في الجريمة التقليدية، فإن الشاهد في الجريمة المعلوماتية يختلف من حيث مفهومه عن الشاهد في الجريمة التقليدية، لأن الشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للمعطيات متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات داخله.

### 4.2- الخبرة:

للخبرة دور بالغ الأهمية في الإثبات المعلوماتي، على اعتبار أن استخلاص الأدلة الرقمية غالبا ما يكون منوطا بفئة متخصصة في هذا المجال، يكون دورها هو وضع معطيات ذات طابع تقني أمام جهة التحقيق والحكم، وأتاح المشرع الجزائري للنيابة اللجوء للخبير في مرحلة التحقيق الابتدائي بموجب نص المادة 35 مكرر من قانون الاجراءات الجزائية، إلا أن أهمية الخبرة في مجال التحقيق في الجريمة المعلوماتية جعلت المشرع الجزائري لا يكتفي بالنصوص التقليدية التي تنظم الخبرة وأدرجها في الفقرة الأخيرة من المادة الخامسة من القانون 09-04 بالنص على أنه يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة

المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

**3 - الوسائل المستحدثة لاستخلاص الدليل المعلوماتي:**

أدى ظهور الجريمة المعلوماتية كنمط جديد من الإجرام له خصوصيته التقنية والمعقدة إلى إسراع المشرعين في مختلف الدول إلى مواكبة لهذا التطور من خلال سن قواعد قانونية جديدة أو تعديل تلك التي لم تعد تستجيب من الناحية الموضوعية أو الإجرائية لمكافحة الظاهرة الإجرامية. وهو ما حذا بالمشرع الجزائري إلى استحداث إجراءات تحري خاصة بموجب المادة 65 مكرر 05 من قانون الإجراءات الجزائية، تتمثل أساسا في التسرب، اعتراض المراسلات السلكية واللاسلكية، تسجيل الأصوات والتقاط الصور، وإجراءات أخرى تضمنها القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والمتمثلة في مراقبة الاتصالات الالكترونية و تفتيش المنظومات المعلوماتية.

## 1.3- التسرب:

بالنسبة للتسرب فهو إجراء تم النص عليه في الفصل الخامس من الكتاب الأول من الباب الثاني من قانون الإجراءات الجزائية بموجب المواد من 65 مكرر 11 إلى غاية 65 مكرر 18، ويقصد به قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة، بإيهامهم بأنه فاعل معهم أو شريك. و يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض، هوية مستعارة أو أن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 **(يسمح القانون طبقا لأحكام المادة 65 مكرر 14 لضابط أو لعون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة و أن يرتكب عند الضرورة الأعمال التالية: اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها، واستعمال أو وضع تحت تصرف مرتكبي الجرائم الوسائل ذات الطابع القانوني او المالي و كذا وسائل النقل و التخزين أو الإيداع أو الحفظ أو الاتصال)**، ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على ارتكاب جرائم **(المادة 65 مكرر 12 من قانون الاجراءات الجزائية المعدل والمتمم).**

أما التسرب في إطار الجريمة المعلوماتية، فهو ما يعرف بالتسرب الرقمي الذي يتم عن طريق الدخول إلى الأنظمة المعلوماتية بصورة متخفية مستخدما أسماء وأوصاف مستعارة أو وهمية يندس عن طريقها في المجموعات لرصد الأشخاص المشتبه فيهم لارتكابهم أو شروعهم في ارتكاب جرائم، والتقاط البيانات الخاصة بهم.

ويتم اللجوء لهذا الإجراء عندما تقتضي ضرورات التحري والتحقيق في الجرائم المنصوص عليها حصرا في نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية **(المادة 65 مكرر 11 من قانون الاجراءات الجزائية المعدل والمتمم)**، والتي من ضمنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات. لذلك فإن القانون رقم 09-04 يكمل قانون الاجراءات الجزائية في حصر الأفعال المعنية بالتسرب من خلال نص المادة 02 منه التي تنص على أنه يقصد في مفهوم هذا القانون بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية. إلا أنه ونظرا لخطورة هذا الإجراء فقد أحاطه المشرع بمجموعة من الضوابط المنظمة بنصوص قانونية، فلا يمكن أن يتم إلا بموجب إذن صادر عن وكيل الجمهورية المختص إقليميا أو من طرف قاضي التحقيق بعد إخطار وكيل الجمهورية، وفي كلتا الحالتين يجب إخطار النائب العام بذلك **(المادة 65 مكرر 11 من قانون الاجراءات الجزائية المعدل والمتمم)**. ويجب أن يكون الإذن مكتوبا ومسببا تحت طائلة البطلان، كما يجب أن يتضمن الجريمة التي تبرر اللجوء لهذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته **(المادة 65 مكرر 15 الفقرة 1-2 من قانون الاجراءات الجزائية المعدل والمتمم)**، على ألا تتجاوز مدة عملية التسرب أربعة أشهر **(المادة 65 مكرر 15 الفقرة 3 من قانون الاجراءات الجزائية المعدل والمتمم)**، يمكن تجديدها حسب مقتضيات التحري والتحقيق بإذن مكتوب ومسبب، يكون بنفس المدة ونفس الشروط **(المادة 65 مكرر 15 الفقرة 4 من قانون الاجراءات الجزائية المعدل والمتمم)**، كما يجوز للقاضي الذي رخص بهذا الإجراء أن يأمر في أي وقت بوقفها قبل انقضاء الآجال القانونية للعملية **(المادة 65 مكرر 15 الفقرة 5 من قانون الاجراءات الجزائية المعدل والمتمم)**. وللأهمية البالغة التي تكتسيها الرخصة لصحة الإجراءات، اشترط المشرع أن تودع في ملف الاجراءات بعد انتهاء العملية **(المادة 65 مكرر 15 الفقرة 6 من قانون الاجراءات الجزائية المعدل والمتمم)**. يبقى أن نشير إلى أن عملية التسرب وما يرافقها من أعمال قد يقوم بها المتسرب تعد أفعالا مجرمة، لكن القيام بها في إطار عملية تسرب وفقا للشروط المنصوص عليها قانونا لا يرتب على القائم بها أية مسؤولية جزائية استنادا لنص المادة 65 مكرر 14 من قانون الاجراءات الجزائية، وكذا الفقرة الأولى من المادة 39 من قانون العقوبات التي تنص على أنه لا جريمة إذا كان الفعل قد أمر أو أذن به القانون. كما أنه لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات **(المادة 65 مكرر 16 الفقرة 1 من قانون الاجراءات الجزائية المعدل والمتمم)**، وفي حالة ما أراد القاضي سماع المتسرب فإنه لا يكشف عن هويته ويجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية **(المادة 65 مكرر 18 من قانون الاجراءات الجزائية المعدل والمتمم)**.

أما في حالة ما إذا تقرر وقف العملية أو انتهاء المهلة المحددة في رخصة التسرب أو في حالة عدم تمديدها يمكن للعون المتسرب أن يواصل النشاطات المنصوص عليها في المادة 65 مكرر 14 من قانون الاجراءات الجزائية

للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على ألا يتجاوز ذلك مدة أربعة اشهر **(المادة 65 مكرر 17 الفقرة 1 من قانون الاجراءات الجزائية المعدل والمتمم)**، و يتم إخطار القاضي الذي أصدر الرخصة في أقرب الآجال **(المادة 65 مكرر 17 الفقرة 2 من قانون الاجراءات الجزائية المعدل والمتمم)**. وفي حالة انقضاء مهلة الأربعة أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه، يمكن للقاضي أن يرخص بتمديدها لمدة أربعة أشهر على الأكثر **(المادة 65 مكرر 17 الفقرة 2 من قانون الاجراءات الجزائية المعدل والمتمم)**.

### 2.3- اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور:

استحدثت هذه الإجراءات بموجب المواد من 65 مكرر 5 إلى غاية 65 مكرر10 من قانون الإجراءات الجزائية، وهي مهام تقتضيها ضرورة التحقيق في الجرائم 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. بالنسبة لاعتراض المراسلات، فإنه يعرف على أنه عملية مراقبة سرية للمراسلات السلكية واللاسلكية، في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في ارتكاب جريمة **(عبد الرحمان، 2010، ص 72-73)**. وبالإضافة إلى أن المشرع الجزائري لم يضع تعريفا لاعتراض المراسلات، فإنه لم يحدد كذلك المقصود من وسائل الاتصالات السلكية واللاسلكية، هل هي الإتصالات الهاتفية فقط على اعتبار أن إجراءات التحري والتحقيق في العديد من الجرائم تتطلب اللجوء إلى مراقبة المحادثات الهاتفية **(أحسن، 2008، ص 113)** أم يمتد للمراسلات التي تتم عبر الشبكة بين عدة أنظمة معلوماتية، وكل أشكال النقل المعلوماتي للبيانات، وهو الطرح الذي تضمنته اتفاقية بودابيست **(تم اعتماد الاتفاقية وتقريرها التفسيري من طرف لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة في 8 نوفمبر 2001 وفتح باب التوقيع على الاتفاقية في بودابيست بتاريخ 23 نوفمبر 2001 بمناسبة المؤتمر الدولي حول الجريمة الالكترونية)**. والذي في رأينا نجده أقرب للصواب نظرا للتطور الكبير لتكنولوجيا المعلوماتية والكمية الهائلة التي تتنقل بصورة مستمرة لاسيما مع الانتشار الواسع لوسائل التواصل الاجتماعي. أما بالنسبة لتسجيل الأصوات كأسلوب من أساليب التحقيق في الجريمة المعلوماتية فقد تناولته الفقرة الثانية من المادة 65 مكرر 5من قانون الإجراءات الجزائية، و يقصد به تسجيل المحادثات الشفوية بصفة سرية أو خاصة في مكان خاص أو عام. ومعنى المحادثة في مفهوم المادة هو كل صوت له دلالة التعبير عن معنى، ولا يشترط لغة معينة أو دلالة لغوية، إذ يصدق هذا الوصف حتى لو كان الأمر يتعلق بصيحات **(جميلة، 2015، ص 178)**. أما الهدف من هذا الإجراء، فهو متابعة المحادثات أو المكالمات الهاتفية ومراقبتها والتصنت عليها، ثم تسجيل الأصوات على أجهزة خاصة أو عن طريق وضع ميكروفونات

حساسة لها القدرة على التقاط الاصوات وتسجيلها، وقد يكون كذلك عن طريق التقاط إشارات لاسلكية أو إذاعية. كما أجاز المشرع الجزائري استنادا إلى نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية، وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أوسرية في أماكن خاصة أو عامة **(المادة 65 مكرر 2 من قانون الاجراءات الجزائية المعدل والمتمم)**، وهو ما يؤكد أن المشرع الجزائري أخذ بالمعيار الموضوعي، بحيث تكون طبيعة الحديث هي أساس الحماية الجزائية بغض النظر عن المكان الذي تجرى فيه وهو نفس موقف المشرع الفرنسي **(جميلة، 2015، ص 179)** والمصري **(جميلة، 2015، ص 179)**. وفي إطار توسيع نطاق إجراءات البحث والتحري في مجال مكافحة الجريمة المعلوماتية، تم بموجب نص المادة 65 مكرر الفقرة 02 من قانون الإجراءات الجزائية النص على إجراء التقاط الصور، الذي هو عملية استخدام كاميرات تصوير أو أجهزة خاصة لالتقاط الصور والصوت لوضعية شخص أو عدة أشخاص في حالة اشتباه بغرض استخدامها كدليل في شكل مادة مرئية. وبالرغم من أن هذا الإجراء قد أقره المشرع الجزائري إلا أنه يشكل مساسا كبيرا بحرمة الحياة الخاصة للأفراد لاسيما في الأماكن الخاصة التي لا يعتقد فيه الشخص بأنه محل مراقبة أو تصوير، وربما هذا ما يفسر الإجراءات المشددة التي تفرضها اللجنة الأمنية الولائية على كل من يريد تثبيت كاميرات مراقبة خارجية، هذا إذا سلمنا بأن الانتشار الواسع لكاميرات المراقبة في الشوارع العامة الغاية منه المحافظة على النظام العام ومكافحة الجريمة بختلف أنواعها. إضافة إلى ذلك، فإن حماية الحياة الخاصة للأشخاص، حق كرسه الإعلان العالمي لحقوق الإنسان **(المادة 12 من الإعلان العالمي لحقوق الإنسان)** والعديد من الاتفاقيات الدولية **(من بين هذه الإتفاقيات: الاتفاقية الدولية للحقوق المدنية والسياسية 1966 الاتفاقية الأوروبية لحقوق الإنسان 1950 الاتفاقية الأمريكية لحقوق الإنسان، الميثاق الإفريقي لحقوق الإنسان والشعوب الميثاق العربي لحقوق الإنسان)** التي اتفقت جميعها على احترام خصوصية كل شخص، وعدم التدخل في شؤون حياته الخاصة والمساس بسرية مراسلاته، حتى وإن كان الهدف الأسمى هو حماية المجتمع والتصدي للظاهرة الإجرامية. وهي نفس الأسباب التي جعلت اتفاقية بودابست لمكافحة الجرائم المعلوماتية، تجرم الاعتراض غير القانوني المتعمد ودون وجه حق بواسطة وسائل تكنولوجية للبيانات المرسلة غير العامة من وإلى كمبيوتر **(المادة 03 من اتفاقية بوادبست لمكافحة الجريمة المعلوماتية 2001)**.

وكرس الدستور الجزائري نفس المبدأ عندما أقر بأنه لا يجوز انتهاك حرمة الحياة الخاصة للمواطن، وضمان سرية المراسلات والاتصالات الخاصة بكل أشكالها، وعدم المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. كما أكد المشرع الدستوري على حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي **(المادة 46 من الدستور الجزائري المعدل بموجب القانون رقم 16-01 المؤرخ في 06 مارس 2016. منشور بالجريدة الرسمية المؤرخة في 07 مارس 2016)**. لذلك كان من الضروري وضع ضوابط لاعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور في شكل ضمانات يتعين التقيد

والالتزام بها منعا للتجاوزات. أولى هذه الضمانات، هو التأكيد على أنه يتم اللجوء لهذا الإجراء إلا في حالات الضرورة في التحري والتحقيق في جرائم محددة على سبيل الحصر من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، و بموجب إذن صادر عن وكيل الجمهورية المختص إقليميا أو من طرف قاضي التحقيق، بعد إخطار وكيل الجمهورية، وفي كلتا الحالتين يجب إخطار النائب العام بذلك **(المادة 65 مكرر 5 من قانون الاجراءات الجزائية المعدل والمتمم)**. ويجب أن يكون الإذن مكتوبا ومسببا تحت طائلة البطلان، كما يجب أن يتضمن كل العناصر التي تسمح بالتعرف على الاتصالات، المطلوب التقاطها، والأماكن المقصودة سكنية أو غيرها، والجريمة التي تبرر اللجوء لهذا الإجراء **(المادة 65 مكرر 7 الفقرة 1 من قانون الاجراءات الجزائية المعدل والمتمم)**، على ألا تتجاوز مدة عملية التسرب أربعة أشهر يمكن تجديدها حسب مقتضيات التحري والتحقيق بإذن مكتوب ومسبب، ضمن نفس الشروط الزمنية والشكلية **(المادة 65 مكرر 7 الفقرة 2 من قانون الاجراءات الجزائية المعدل والمتمم)**. كما أنه على ضابط الشرطة القضائية المأذون له والمناب من طرف القاضي المختص، أن يحرر محضرا عن كل عملية اعتراض وتسجيل وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري ويضمن هذا المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

### 3.3- مراقبة الاتصالات الالكترونية:

تعرف على أنها مراقبة شبكة الاتصالات باستخدام التقنية الإلكترونية، لجمع بيانات أو معلومات عن المشتبه فيه، سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن، لتحقيق غرض أمني أو لأي غرض آخر **(نبيلة عبلة، 2007، 198)**. وقد استحدث المشرع الجزائري هذا الإجراء بموجب المادة 03 من القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فلم يعرف أو يحدد المقصود بمراقبة الاتصالات الالكترونية، واكتفى فقط بتحديد مفهوم الاتصالات الالكترونية في الفقرة (و) من المادة 02 من القانون 09-04 على أنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة وسيلة إلكترونية". وهو التعريف الذي لا يختلف في مضمونه عن ذلك الذي جاءت به المادة 05 الفقرة الأولى من المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وكيفات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تعرف الاتصالات الالكترونية بأنها "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق وسيلة إلكترونية بما في ذلك وسائل الهاتف الثابت والنقال".وطبقا لنص المادة 04 الفقرة السادسة من المرسوم الرئاسي 15-261، فقد أسند المشرع الجزائري ضمان المراقبة الوقائية للاتصالات الالكترونية، للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بهدف الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص.

أما الحالات التي يتم اللجوء فيها إلى مراقبة الاتصالات الإلكترونية، فقد حددتها على سبيل الحصر، المادة 04 الفقرة الأولى من القانون 09-04، وتتمثل أولا، في الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وثانيا في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أما ثالثا، فلمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الابحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، ورابعا وأخيرا، في إطار تنفيذ المساعدة القضائية المتبادلة.و أكد المشرع الجزائري على شرط الحصول على إذن مكتوب من السلطة القضائية المختصة للقيام بعمليات المراقبة الإلكترونية في الحالات السالفة الذكر، على أن يعود الاختصاص عندما يتعلق الأمر بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، للنائب العام لدى مجلس قضاء الجزائر، الذي يمنح الإذن لضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها لمدة 06 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها **(لفقرة 02 و03 من المادة 04 من القانون 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت سنة 2009)**، والمتمثلة أساسا في الحصول على معطيات من شأنها الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة. أما الحالات الأخرى فتسري عليها الأحكام الواردة في المواد من 65 مكرر 11 إلى غاية 65 مكرر 18، وهي إسناد سلطة منح الإذن إلى قاضي التحقيق أو وكيل الجمهورية كل حسب اختصاصه، على أن يكون الإذن مكتوبا ومتضمنا كافة عناصر المهمة، صالحا لمدة 04 أشهر قابلة للتجديد عند الضرورة مع إخطار النائب بذلك **(المادة 65 مكرر 7 من قانون الاجراءات الجزائية المعدل والمتمم)**. وكغيرها من الإجراءات الخطيرة التي تمس بحقوق وحريات الافراد، فقد أحاط المشرع الجزائري المراقبة الإلكترونية بمجموعة من الضمانات **(تنص المادة 107 من قانون العقوبات على أنه "يعاقب الموظف العمومي بالسجن المؤقت من خمس إلى عشر سنوات إذا أمر بعمل تحكمي أو ماس سواء بالحرية الشخصية للفرد أو بالحقوق الوطنية لمواطن أو أكثر)**، التي يأتي على رأسها ضرورة الحصول على الإذن الكتابي المسبق وخضوع المراقبة للسلطة القضائية، بالإضافة إلى السرية التامة في الإجراءات احتراما للسر المهني المقرر في المادة 45 الفقرة الرابعة من قانون الإجراءات الجزائية، لاسيما وأنه لا يمكن أن يشارك في عملية المراقبة إلا اعضاء الوحدة أو الوحدات التي أوكلت لها السلطات القضائية القيام بهذه المهمة **(المادة 23 من المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وكيفات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها)**. ولا يجوز استعمال

المعلومات المتحصل عليها عن طريق عمليات المراقبة الالكترونية، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية وهذا تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به **(المادة 04 من القانون 09-04،**

**المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت سنة 2009).** ويتم حفظ هذه المعلومات وفق القواعد المطبقة على حماية المعلومات المصنفة **(المادة 24 من المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وكيفات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).**

### 4.3- تفتيش المنظومات المعلوماتية:

تفتيش المنظومات المعلوماتية هو الإجراء الذي استحدثه المشرع الجزائري بموجب المادة 05 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أجاز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص عليه في المادة 04 من ذات القانون **(تتمثل هذه الحالات في: - الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة - حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني - لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الابحاث الجارية دون اللجوء إلى المراقبة الإلكترونية. - في إطار تنفيذ المساعدة القضائية المتبادلة).**

الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، ومنظومة تخزين معلوماتية.

وبالرغم من أن المشرع الجزائري لم يحدد المقصود بتفتيش المنظومات **(عرف المجلس الأوروبي تفتيش المنظومات المعلوماتية بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل قانوني)**، ربما للطابع التقني لهذه العمليات، إلا أنه عرف المنظومات المعلوماتية على أنها أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات، تنفيذا لبرنامج معين **(المادة 02 الفقرة (ب) من القانون 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت سنة 2009).** ولقد أصاب المشرع الجزائري بوضع هذا التعريف لإزالة اللبس والغموض الذي ورد في المادة 394 مكرر عندما استعمل المشرع الجزائري مصطلح منظومة للمعالجة الآلية للمعطيات، ثم استعمل في المادة 394 مكرر 1 مصطلح نظام معالجة آلية، وهو ما تم تفسيره على أن الجريمة لا تقوم في الحالة الأولى إلا إذا تم ارتكابها على منظومة كاملة للمعالجة الآلية للمعطيات أي مجموعة أنظمة مترابطة إذا ما تقيدنا بنص المادة التي تستعمل مصطلح نظام معالجة آلية للمعطيات. لذلك جاء نص المادة 02 في فقرتها (ب) من القانون 09-04 ليقطع الشك باليقين ويؤكد على

أن المنظومة المعلوماتية تكون في شكل نظام منفصل أو في شكل مجموعة من الأنظمة المتصلة ببعضها **(عرفت المادة 02 الفقرة الخامسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، النظام المعلوماتي، بأنه: مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات).**

كما يدخل في إطار التفتيش المعلوماتي ما يعبر عنه بتفتيش المنظومات المعلوماتية عن بعد، فهو يعتبر نتيجة طبيعية للتطور الرهيب لتكنولوجيا المعلومات لاسيما مع الإمكانيات الكبيرة التي توفرها في التواصل ونقل البيانات عبر العالم، وتخزينها في مكان داخل وخارج أقاليم الدول، في شكل شبكة معلوماتية. وهو ما حذا بالمشرع الجزائري إلى تناول موضوع تفتيش المنظومات المعلوماتية عن بعد من خلال نص المادة 05 من القانون 09-04، حيث يميز بين صورتين، الأولى: إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك، وهو ما من شأنه حل المشاكل القانونية والقضائية المتعلقة بتمديد الإختصاص في تفتيش المنظومات المعلوماتية، والمتعلقة كذلك بمشروعية الدليل المتحصل عليه أمام الجهات القضائية. أما الصورة الثانية فهي إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل. لذلك حرصت الكثير من الدول على إبرام إتفاقيات ثنائية أو متعددة الاطراف لتسهيل التعاون الإجرائي في المتابعة. وفي نفس الإطار، ووفقا لما جاء به تقرير المجلس الأوروبي، فإن الاختراق المباشر، يعد انتهاكا لسيادة دولة أخرى، ما لم توجداتفاقية دولية في هذا الشأن، و أن استرجاع البيانات التي تم تخزينها بالخارج دون علم الدولة الأخرى ورضاها، يعد انتهاكا لسيادتها وخرقا للقوانين **(خالد، 2009، ص 203).** إضافة إلى ذلك فقد مكن المشرع الجزائري السلطات المكلفة بالتفتيش، تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات التي تتضمنها، وذلك قصد مساعدة هذه السلطات في عملها وتزويدها بكافة المعلومات الضرورية لإنجاح وإنجاز المهمة **المادة 05 الفقرة 4 من القانون 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت سنة 2009).** وحرصا على تكريس الشرعية الإجرائية في حال أثمرت عملية التفتيش عن وجود معطيات مخزنة، استحدث المشرع الجزائري بموجب نص المادة 06 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،ما يسمى بحجز المعطيات، وهو إجراء من خلاله يجيز للسلطة التي تباشر التفتيش في منظومة معلوماتية، في حالة اكتشافها معطيات مخزنة مفيدة في الكشف عن الجرائم أو مرتكبيها أن تنسخ هذه المعطيات، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز، وفقا للقواعد المقررة في قانون الاجراءات الجزائية

هذا ما لم يكن من الضروري حجز كل المنظومة. أما عن القواعد المقررة في قانون الإجراءات الجزائية التي أشارت إليها المادة 06 من القانون 09-04، فهي تلك الضوابط المنصوص عليها في نص المادة 84 من قانون الإجراءات الجزائية التي تجعل لقاضي التحقيق وضابط الشرطة المنوب عنه، فقط دون غيرهما الحق الإطلاع على المستندات المبحوث عنها، مع مراعاة ما تقتضيه ضرورات التحقيق التي يأتي على رأسها كتمان السر المهني واحترام حقوق الدفاع **(المادة 83 الفقرة الثالثة من قانون الإجراءات الجزائية المعدل والمتمم)**.

وتوضع الأشياء المحجوزة بعد إحصائها بصورة فورية في أحراز مختومة لا يتم فتحها إلى بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا، كما يمكن استدعاء كل من ظبطت لديه هذه الاشياء لحضور هذا الإجراء **(المادة 84 من قانون الإجراءات الجزائية المعدل والمتمم)**. ويتم حجز المعطيات وفقا لما نص عليه المشرع الجزائري بطريقتين مختلفتين تتمثل أولاهما في نسخ المعطيات المعلوماتية، والثانية في الحجز عن طريق منع الوصول إلى المعطيات المعلوماتية. فبالنسبة لنسخ المعطيات فإنه وبالرجوع إلى نص المادة 06 من القانون 09-04، أجاز المشرع استخلاص الدليل عن طريق نسخ المعلومات المضبوطة وتخزينها في دعامات، مع الحرص على استعمال كافة الوسائل التقنية لتشكيل أو إعادة تشكيل المعطيات محل البحث وفحصها واستخلاصها، من أجل جعلها قابلة للاستغلال لأغراض التحقيق مع مراعاة عدم المساس بمحتوى المعطيات **(المادة 06 الفقرة 3 من القانون 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت سنة 2009)**.

أما الحجز عن طريق منع الوصول إلى المعطيات، فهو طريقة استثنائية، يتم اللجوء إليها في حالة عدم إمكانية إجراء الحجز عن طريق النسخ لأسباب تقنية، لذلك فإنه يتعين على السلطة التي تقوم بالتفتيش، استعمال التقنيات المناسبة، لمنع الوصول أو إلى نسخ المعطيات التي تحتويها المنظومة المعلوماتية الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة **(المادة 07 من القانون 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت سنة 2009)**. كما يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة **(المادة 08 من القانون 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت سنة 2009)**، وفي كل الأحوال فإنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة، إلا في الحدود الضرورية للتحريات والتحقيقات القضائية **(المادة 09 من القانون 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت سنة 2009)**.

## 4- الخاتمة:

تأخر المشرع الجزائري كثيرا في التعامل مع الطبيعة الخاصة للجرائم المعلوماتية سواء من حيث استحداث النصوص القانونية الموضوعية التي تجرم وتعاقب على الأفعال التي تدخل ضمن إطار الجريمة المعلوماتية، أو من حيث النصوص القانونية الإجرائية التي تسهل عمل أجهزة البحث والتحري، وإنشاء هيئات للوقاية من الجرائم المعلوماتية ومكافحتها، بالرغم من الاهتمام الدولي المبكر بهذه الظاهرة.

حيث لم يصدر تشريع خاص بالجريمة المعلوماتية في الجزائر إلى غاية سنة 2004 بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات في القسم السابع مكرر تحت اسم المساس بأنظمة المعالجة الآلية للمعطيات، والذي تضمن المواد من 394 مكرر إلى غاية 394 مكرر7. كما أنه لم يتم استحداث إجراءات تحري خاصة إلا بموجب القانون 06-22 المؤرخ في 29 ذي القعدة 1427 الموافق لـ: 20 ديسمبر 2006 المتمم للأمر 66-156 المؤرخ في 18 صفر 1386 الموافق لـ: 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، وانتظر المشرع الجزائري إلى غاية سنة 2009 لإصدار القانون 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ: 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

**ويمكن تقديم نتائج دراستنا في ما يلي:**

- أن الترسانة القانونية المتخصصة التي استحدثها المشرع الجزائري، وبالرغم من تأخرها، فإنها تعتبر تدعيما نوعيا للمنظومة التشريعية في الجزائر، ساهمت بالقدر الكبير في توفير الإطار الإجرائي لمكافحة الجريمة المعلوماتية عن طريق استخلاص الدليل باعتباره حالة قانونية بواسطتها يتم إسناد المسؤولية الجزائية للجاني، وتأطير عمل الضبطية القضائية بما أنها تتمتع باختصاص نوعي عام، يجيز لها اتخاذ أي إجراء ضمن حدود اختصاصها الإقليمي الذي يتحدد بالدائرة الإقليمية التي تمارس فيها وظائفها العادية أو كامل التراب الوطني إذا تعلق الأمر بالجرائم المنصوص عليها في المادة 16 من قانون الإجراءات الجزائية.

- من خلال تحليلنا للنصوص القانونية المتضمنة لإجراءات البحث والتحري المستحدثة نجد أن المشرع الجزائري وبالرغم من خطورة هذه الإجراءات ومساسها بالحياة الشخصية للمشتبه فيهم، فإنه كرس كافة الضمانات الكفيلة بتحقيق التوازن بين حماية المجتمع من جهة والمحافظة على حقوق وحريات الاشخاص من جهة أخرى، من خلال الإشراف القضائي، لاسيما إلزامية الحصول على الإذن المسبق من السلطة القضائية المختصة قبل أي إجراء.

- الطبيعة الخاصة للجريمة المعلوماتية فرضت على المشرع الجزائري نمطا جديدا من الأدلة وهو الأدلة الرقمية، ويبقى استحداث المشرع الجزائري لقواعد إجرائية جديدة في البحث والتحري في هذا النوع من الجرائم، اعترافا صريحا منه بأن الدليل الرقمي هو الأنسب في إثباتها.

أما التوصيات التي يمكن أن نقدمها على ضوء ما توصلنا إليه من خلال هذا البحث فيمكن إجمالها في النقاط التالية:

- ضرورة تفعيل الضمانات المقررة لحماية الحياة الخاصة للأفراد في مرحلة البحث والتحري، وتكريس ضمانات أخرى من خلال مواكبة المشرع الجزائري للتطور السريع لهذا النوع من الإجرام.

- ضرورة مراجعة قواعد الاختصاص الداخلي لإيجاد حل سريع لمشكلة الاختصاص القضائي، والسعي بشكل جدي وفعال لفتح قنوات التنسيق الدولي والتعاون القضائي لحل مشكلات تمديد إجراءات البحث والتحري.

- تكوين أفراد الضبطية القضائية تكوينا أكاديميا متخصصا في مجال تقنية المعلومات وفي المجال القانوني مع ضرورة توفر الأجهزة الأمنية على قواعد بيانات تهتم برصد وتحليل الإحصائيات المتعلقة بالجرائم المعلوماتية.

## 6- الإحالات و قائمة المراجع :


- ممدوح إبراهيم خالد،2009، فن التحقيق الجنائي، بدون طبعة، الإسكندرية، مصر، دار الفكر الجامعي.
- بارعة القدسي، 2010، أصول المحاكمات الجزائية، الجزء الثاني، دمشق، منشورات جامعة دمشق.
- خلفي عبد الرحمان، 2010، محاضرات في قانون الإجراءات الجزائية، الجزائر، دار الهدى.
- بوسقيعة أحسن، 2008، التحقيق القضائي، الجزائر، دار هومة.

- محلق جميلة، 2015، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، العدد 42.
- هروال نبيلة عبلة، 2007، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات –دراسة مقارنة- مصر، دار الكتب القانونية، دار شتات للنشر و البرمجيات.