مراقبة الاتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري

أ/ ثابت دنيازاد
جامعة تبسة

ملخص البحث:

أباح القانون 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها اللجوء إلى استعمال تقنية مراقبة الاتصالات بشأن الكشف عن الحقيقة في الجرائم الماسة بتكنولوجيات الإعلام و الاتصال عن طريق إجراءات وقواعد خاصة نظمها هذا القانون بالرغم من مساسها بحقوق وحريات الأفراد .

ومن خلال هذا البحث سيتم التعرض إلى الضمانات الموضوعية والشكلية المترتبة على ذلك من حجز للمعطيات المعلوماتية وفقا لما نص عليه القانون ومدى مساسها بالحق في حرمة الحياة الخاصة للأفراد.

La loi n : 09-04 du 5 aout 2009 relative à la prévention et à la lutte contre les infractions liées aux technologies des médias et de la communication a permis le recourir à l’utilisation de la technique de surveillance des communications électroniques en ce qui concerne la recherche de la vérité dans les infractions contre les médias et les technologies de communication à travers des procédures et des règles spécifiques contenues dans cette loi en dépit du fait qu’elles touchent aux droits et libertés des personnes.

Et à travers cette recherche nous allons aborder les garanties de fond et de forme résultant de ce qui a précédé, et ce, selon dispositions contenues dans texte de la loi et du préjudice qu’elles peuvent avoir sur le droit à la vie privée des individus.

نص المشرع الجزائري على مجموعة من القواعد الإجرائية المكملة لنصوص قانون الإجراءات الجزائية تتعلق بالقواعد التي تضمنها **القانون09-04** المؤرخ في **5أوت2009** والمتضمن القواعد المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث تضمن مجموعة من القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها ومعرفة مرتكبيها.

وبموجب هذا القانون فقد أباح المشرع الجزائري اللجوء إلى استعمال تقنية مراقبة الاتصالات الالكترونية بشأن الجرائم الماسة بتكنولوجيات الإعلام والاتصال وذلك بعد الثورة التي عرفها العالم في السنوات الأخيرة في مجال المعلوماتية وتطور وسائل الاتصال وظهور الانترنت وتطور صور الإجرام المعلوماتي، الأمر الذي تطلب ضرورة وضع نصوص قانونية تلائم خصوصيتها. كما تم من خلال هذا القانون النص على قواعد إجرائية خاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع مراعاة القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية.

والملاحظ أن هذه الإجراءات من شأنها أن تطرح لنا إشكالية مدى مساسها بالحياة الخاصة للأفراد، لذلك فقد لقيت بعض المعارضة والتخوف الكبيرين لدى النواب أثناء مناقشة القانون، وفي شرحه لمشروع القانون فقد أبرز وزير العدل أن المشرع الجزائري وهو بصدد وضع هذه النصوص القانونية والتي دامت سنتين من التحضير والدراسة والتحليل والمقارنة مع أحدث القوانين قام بموازنة بين حق الدولة في الوصول إلى الكشف عن الحقيقة وحق الدولة في مكافحة الإجرام الخطير وبين حق الأفراد في كفالة حرياتهم الشخصية لا سيما الحق في الحياة الخاصة.

وحرصا من المشرع الجزائري على عدم المساس بالحق في حرمة الحياة الخاصة للأفراد، فقد خص هذه الإجراءات ببعض القواعد والضمانات التي تضمنتها نصوص هذا القانون وقواعد الإجراءات الجزائية.

وفيما يلي سوف نتعرض إلى الضمانات الموضوعية والشكلية التي تنظم عملية مراقبة الاتصالات الالكترونية وإجراءات التفتيش داخل منظومة معلوماتية والآثار المترتبة على ذلك من حجز للمعطيات المعلوماتية ومدى مساسها بالحق في حرمة الحياة الخاصة وذلك وفقا للعناصر التالية:

- **المبحث الأول:** ماهية مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية،
- **المبحث الثاني:** الضمانات والشروط القانونية لمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية،
- **المبحث الثالث:** الآثار المترتبة على مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية.

المبحث الأول:

ماهية مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية

يجب أن نميز في هذا الصدد بين مفهوم مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية ذلك أن **القانون09-04** نص على إجراءين أساسيين يمكن اللجوء إليهما، يتمثل الإجراء الأول في مراقبة الاتصالات الالكترونية، بينما يتمثل الإجراء الثاني في تفتيش المنظومات المعلوماتية.

وقد أغفل المشرع الجزائري في هذا القانون تعريف هذه التقنيات الحديثة كما هو الحال في غالبية التشريعات المقارنة، الأمر الذي يدفعنا للوقوف على تعريفها وتحديد أساسها القانوني وذلك تبعا لما يلي:

المطلب الأول- مفهوم مراقبة الاتصالات الالكترونية:

ينصب إجراء المراقبة على الاتصالات الالكترونية وفقا لما نص عليه **القانون 09-04** ويقصد بالاتصالات الالكترونية في مفهوم هذا القانون ووفقا لما ذهبت إليه **المادة 2** بند(و): "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية".

وتعرف الاتصالات الالكترونية في الفقه المقارن بأنها الاتصالات التي تتم عن طريق جهاز الحاسب الآلي، والتي تتخذ شكل البريد الالكتروني (E.Mail) أو شكل محادثة فورية (Instant message) والتي تتم عن طريق شبكة الانترنت [1].

وتبعا لذلك تأخذ الاتصالات الالكترونية شكل مراسلات مكتوبة أو محادثات شفوية أو صور ملتقطة وهي تشكل بذلك أهم العناصر الأساسية التي يقوم عليها الحق في حرمة الحياة الخاصة[2]. ولهذا يعد هذا الإجراء من أخطر الإجراءات الحديثة التي تمس الإنسان في حقه في الخصوصية.

بينما يقصد بالمراقبة تجميع وتسجيل محتوى الاتصالات الالكترونية ومن ثم الإطلاع عليها والكشف عنها وفي ذلك أيضا تهديد للحق في حرمة الحياة الخاصة، ففي كثير من الأحيان تحوي هذه الاتصالات الالكترونية على ما يمس حياة الشخص الخاصة بوصفها مستودع سر لصاحبها.

والملاحظ أن المشرع الجزائري لم يحدد وسائل المراقبة الالكترونية ما عدا ما ذكره أنه يتوجب وضع الترتيبات التقنية الخاصة بالمراقبة، وبالرجوع إلى الفقه المقارن فقد ذهب البعض إلى تحديد أشكال المراقبة الالكترونية[3] في:

1- استخدام وسائل فنية من خلال ما يسمى بقلم التسجيل أو ما يسمى بالفخ والمتابعة، في هذه الحالة يتم تسجيل أسماء المتراسلين مع متهم معين أي مع بريده الالكتروني أو مع من يقوم بالمحادثة الفورية معه.

2- استخدام وسائل التصنت على محتوى الرسالة الالكترونية أو المحادثة الفورية الالكترونية بوسائل للاعتراض والتصنت.

المطلب الثاني- تفتيش المنظومات المعلوماتية:

نص القانون 09-04 أيضا على إجراءات أخطر من مراقبة الاتصالات الالكترونية تمس بالحق في حرمة الحياة الخاصة للأفراد تتعلق بتفتيش منظومتهم المعلوماتية والتي تحوي في الغالب على معطيات شخصية.

وتعرف المنظومة المعلوماتية بأنها أي نظام منفصل أو مجموعة من الأنظمة المتصلة بعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين[4]، كما تعرف المعطيات المعلوماتية بأنها عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية تؤدي وظيفتها[5].

والعديد من التشريعات الحديثة تجيز اللجوء إلى تفتيش الأجهزة الالكترونية لضبط المعلومات المتواجدة فيها والتي تفيد في كشف حقيقة العديد من الجرائم التي تتم عن طريق تقنية المعلومات كالتشريع الفرنسي بموجب المادة 1-57 من قانون الإجراءات الجزائية.

وتجدر الملاحظة إلى ضرورة التفرقة بين تفتيش نظام معلوماتي وقيام ضابط الشرطة القضائية دخول أندية الانترنت وتفتيش الأجهزة. فبالرجوع إلى القواعد العامة لصحة إجراء التفتيش فإنه يجوز دخول الأماكن العامة دون الحصول على إذن مسبق لكن لا يجوز لهم فتح الأشياء المغلقة الموجودة فيها، وبتطبيق ذلك في المجال الالكتروني فإنه يجوز لهم دخول نادي الانترنت والنظر إلى الأجهزة المفتوحة دون أن يقوموا بفتح جهاز الحاسب الآلي المغلق أو البحث في جهاز حاسب آلي مفتوح إلا في الحدود التي يقرها القانون.

المبحث الثاني:

الضمانات والشروط القانونية لمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية

يقصد بضمانات وقواعد اللجوء إلى الاتصالات الالكترونية تلك الضوابط والقيود التي يجب على السلطة المختصة أثناء مباشرتها لإجراء تسجيل وتجميع محتوى الاتصالات والبحث في منظومة معلوماتية احترامها. وبقدر ما تكون هذه الضوابط كافية ومحددة وواضحة تتحقق كفالة الحريات الفردية وأهمها الحق في حرمة الحياة الخاصة، وعلى العكس من ذلك فإن عدم وضع ضوابط وضمانات يفسح المجال للسلطة التقديرية للسلطة القضائية المختصة في اللجوء إلى هذه الإجراءات دون رقابة مما يشكل خطرا كبيرا على حقوق وحريات الأفراد وأهمها الحق في حرمة الحياة الخاصة.

لذلك فإن علة تقرير ضوابط اللجوء إلى هذه الإجراءات الحديثة هو إقامة توازن بين الحق في حرمة الحياة الخاصة وبين حق المجتمع في العقاب، فلا يقع

هنـاك اعتـداء علـى الحرمـات أو الحريـات، وفـي نفس الوقـت يـتم تعقـب الجـرائم والكشـف عـن مرتكبيهـا ممـا يمكـن مـن توقيـع العقـاب علـى الجـاني لا سـيما فـي الجرائم الخطيرة أو العابرة للحدود الدولية.

ويمكن تقسيم الضمانات والضوابط التـي يجـب احترامهـا أثنـاء اللجـوء إلـى مراقبـة الاتصـالات الالكترونيـة وتفتـيش المنظومـات المعلوماتيـة إلـى ضـوابط وضمانات موضوعية تتعلق بنشوء الحق في اللجـوء إلـى هـذه الأسـاليب والتقنيـات وضمانات شكلية تتعلق بصحة هذه الإجراءات.

وسوف نتعرض في هذا الشأن إلـى هـذه الضـمانات التـي جـاء بهـا المشـرع الجزائـري مقارنــة مــع التشــريع الفرنســي فــي غيــاب موقــف صــريح للتشــريع المصري وفقا لما يلي:

المطلب الأول- الضمانات الموضوعية لمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية:

يمكن إجمال الضوابط الموضوعية التي أقرها القانون لمراقبـة الاتصـالات الالكترونية في مجموعة من الضـمانات أهمهـا: تحقـق الغـرض مـن عمليـة اللجـوء إلـى المراقبـة، أن تتخـذ المراقبـة فـي حـالات معينـة حصـرها القـانون، أن تنصـب المراقبة على محل معين، أن يصدر الأمر بالمراقبة عن السلطة المختصة بذلك.

أولا- تحقق الغرض من عملية اللجوء إلى مراقبة الاتصالات الالكترونية والتفتيش:

أقر المشرع الجزائري إجـراء اللجـوء إلـى مراقبـة الاتصـالات الالكترونيـة وتفتيش المنظومة المعلوماتية في حالات استثنائية فقط لما لها من اعتداء على حق الإنســان فــي ســرية حياتــه الخاصــة واتصــالاته الشخصــية لغــرض معــين وهــو الوصــول إلـــى حقيقـــة الجريمـــة والكشـــف عـــن مرتكبيهـــا خـــلال مرحلتـــي جمـــع الاستدلالات والتحقيق الابتدائي ولم يتم التوصل إلـى ذلـك عن طريـق اللجـوء إلـى الإجـراءات التقليديـة. وهـو مـا قـال بـه المشـرع الجزائـري فـي نـص **المـادة 3** مـن **القانون 09-04** بأن يتم اللجوء إلى هذا الإجراء متى تطلبت مستلزمات التحريـات أو التحقيقات القضائية الجارية.

والملاحظ أن المشرع الجزائري لم ينص على إمكانية اللجوء إلى المراقبة بعد ارتكاب الجريمة والبحث عن حقيقة الوصول إلى مرتكبيها فقط، بل أقر أيضـا اللجوء إلى استعمال هذه التدابير كوسيلة وقائيـة للحمايـة مـن وقـوع جـرائم معينـة هي الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسـة بـأمن الدولـة أو الاعتداء على منظومة معلوماتية على نحو يهدد النظام العـام أو الـدفاع الـوطني أو مؤسسـات الدولـة أو الاقتصـاد الـوطني وفقـا لمـا نصـت عليـه **المـادة 4 فقـرة(أ) و(ب)**.

ومن جهة ثالثة تهدف هذه الإجراءات إلى تعزيز التعاون الدولي في مجـال مكافحـة الإجـرام المـنظم فـي مجـال المعلوماتيـة، ذلـك أن هـذه الجـرائم تعـد مـن

الجرائم العابرة للحدود الوطنية ولا ترتبط في كثير من الأحيان بمكان معين. ويكون ذلك في إطار المساعدة الدولية المتبادلة وفقا لما نص عليه القانون والاتفاقيات الدولية في هذا الشأن.

في حين نجد أن المشرع الفرنسي اشترط في نص المادة 100-1 من قانون الإجراءات الجزائية الفرنسي بأن يكون اللجوء إلى المراقبة ضروري لمصلحة التحقيق وتتحقق حالة الضرورة حين يكون من الصعب معرفة الجناة وضبط أدلة الجريمة بوسائل البحث والتحري العادية.

ثانيا- الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الالكترونية:

نص **القانون 09-04** على الحالات التي تسمح باللجوء إلى المراقبة الالكترونية أو دخول منظومة معلوماتية أو منظومة تخزين معلوماتية بغرض التفتيش وهي حالات التي جاءت على سبيل الحصر متمثلة في ما يلي:

1- **الوقاية من ارتكاب الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة:** الملاحظ هنا أن المشرع الجزائري أباح اللجوء إلى مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية في مرحلة سابقة على ارتكاب هذا النوع من الجرائم أي بمجرد وصول العلم إلى السلطة القضائية المختصة باحتمال ارتكاب جريمة من جرائم الإرهاب أو التخريب أو جريمة من الجرائم الماسة بأمن الدولة[6]. فنرى أن السبب في ذلك هو صعوبة التوصل إلى معرفة مرتكبي مثل هذه الجرائم وخطورة هذه الأفعال على الدولة وعلى حياة الأفراد وممتلكاتهم، ذلك أن هذه الأفعال في كثير من الأحيان تؤدي إلى نتائج جرمية وخيمة يصعب تلافيها. ضف إلى ذلك أن هذه الجرائم تتم في كثير من الأحيان عن طريق أجهزة اتصالات أو تحكم عن بعد.

2- **حالة توفر معلومات عن احتمال وجود اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني:** وتتعلق هذه الحالة أيضا باللجوء إلى إجراءات المراقبة أو التفتيش قبل وقوع جريمة الاعتداء المعلوماتي على منظومة معلوماتية-وفقا لما سيأتي شرحه- وذلك بمجرد وصول معلومات إلى السلطة القضائية بشرط أن تكون هذه المعلومات تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني. وتلعب أيضا هذه الإجراءات في هذه الحالة دورا وقائيا من شأنها الحيلولة دون وقوع مثل هذه الجرائم الخطيرة و التي تستهدف على وجه الخصوص أمن الدولة.

3- **مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية:** والملاحظ هنا أن اللجوء إلى المراقبة أو التفتيش يكون بعد ارتكاب الجريمة وأثناء مرحلة جمع الاستدلالات أو التحقيق القضائي. ويكون الغرض من ذلك هو التوصل إلى معرفة مرتكبي الجريمة وذلك في حالة عدم جدوى

الإجراءات التقليدية في الوصول إلى الحقيقة. ويجب الإشارة هنا على أنه بقراءة أولية للبند(ج) من الفقرة الأولى لنص المادة 4 يتبين أنها لم تحدد ما هي الجرائم المقصودة، وهل ينطبق ذلك على جميع الجرائم؟ نحن نرى أن هذه الفقرة طالما لم تحدد نوع معين من الجرائم على النحو الذي أشارت إليه البنود السابقة من نفس الفقرة، فإن المراقبة يلجأ إليها بمناسبة جميع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال طالما أن هذا القانون يهدف فقط إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ويتعلق الأمر خاصة بالجريمة المنظمة أو العابرة للحدود الوطنية.

4- **في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة:** ويتعلق الأمر هنا بالجرائم التي ترتكب خارج الإقليم الوطني، ومن شأن عملية مراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية في الإقليم الجزائري أن تفيد الدولة المعنية بنتائج تتعلق بمعاينة هذه الجرائم الماسة بتكنولوجيات الإعلام و الاتصال وكشف مرتكبيها، بشرط أن يتم ذلك في إطار تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة أي أن يكون ذلك في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل.

ثالثا- محل مراقبة الاتصالات الالكترونية:

تنصب عملية المراقبة على الاتصالات الالكترونية، في حين ينصب إجراء التفتيش على المنظومات المعلوماتية. وسبق التعرض لتعريف الاتصالات الالكترونية والمنظومات المعلوماتية في المطلب السابق ولا داعي لإعادة ذكرها.

رابعا- صفة الشخص الخاضع لمراقبة اتصالاته الالكترونية:

مما لا شك فيه أن اتهام شخص بارتكاب جريمة من الجرائم المذكورة في نص **المادة4** من **القانون 09-04** والتي جاءت على سبيل الحصر يكون مبررا للاعتداء على حياته الخاصة والكشف عن علاقته بالجريمة وجمع الأدلة ضده. أما غير المتهم فيطرح السؤال والذي سبق طرحه بمناسبة الحديث عن جواز إخضاعه للأساليب التقنية، هل يشترط توافر صفة المتهم في الشخص الخاضع لمراقبة اتصالاته الالكترونية وتفتيش منظومته المعلوماتية؟ أو أن هذا الإجراء يمكن اتخاذه في مواجهة غير المتهم؟

نحن نرى أنه إذا تعلق الأمر بمراقبة الاتصالات الالكترونية في الحالات المنصوص عليها قانونا والمذكورة أعلاه فإنه يجوز اتخاذها ضد المتهم الذي قامت الدلائل و القرائن حول ارتكابه أحد هذه الجرائم، وكذلك غير المتهم الذي يمكن أن تفيد عملية مراقبته التحريات والتحقيقات القضائية القائمة. وحجتنا في ذلك أن القانون خول اللجوء إلى هذه الإجراءات لمجرد الشك حتى ولو لم تقم الأدلة والقرائن على ارتكاب الجريمة وقبل وقوعها، وبالتالي يجوز مراقبة الاتصالات الالكترونية لأي شخص يمكن أن يكشف عن الحقيقة ويحتمل أن تكون

المعطيات التي يمكن جمعها لها علاقة بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

والملاحظ هنا أن المشرع الجزائري قد وسع من نطاق عملية المراقبة لتشمل أفعالا مازالت لم تقع ولم يتهم بشأنها أي شخص بعد وذلك نظرا لخطورة هذه الأفعال لخطورة هذه الأفعال على النظام العام والدولة[7]، وحسنا فعل المشرع عندما نص على وجوب عدم المساس بالحياة الخاصة للأفراد تحت طائلة تطبيق نصوص قانون العقوبات في هذا الشأن ويتعلق الأمر هنا بتطبيق أحكام المواد 303مكرر3 وما يليها من قانون العقوبات.

ونرى أن ذلك يطبق أيضا إذا تعلق الأمر بتفتيش منظومة معلوماتية لأن العبرة ليست بالشخص بل بالمنظومة في حد ذاتها إذا توفرت معلومات أن المعطيات المبحوث عنها والتي تفيد في الكشف عن الحقيقة مخزنة فيها بغض النظر عن صفة الشخص الحائز لهذه المنظومة، ولو تعلق الأمر بمنظومة تقع خارج الإقليم الوطني طالما أن التفتيش يمكن أن يتم عن بعد وبمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل. وهذا ما يؤكد الطابع الدولي لهذه الجرائم.

خامسا- السلطة القضائية المختصة بمراقبة الاتصالات الالكترونية:

تأخذ مراقبة الاتصالات الالكترونية نفس خطورة التدابير التقنية الثلاثة المنصوص عليها في **المادة 65 مكرر5** من قانون الإجراءات الجزائية والمتعلقة باعتراض المراسلات، التقاط الصور وتسجيل الأصوات لكونها تمس أيضا بالحياة الخاصة للأفراد، ومن أجل ذلك ينبغي إحاطة إجراء المراقبة بضمانات تكفل استعماله في نطاق الهدف الذي وجدت من أجله. ومن أهم الضمانات أن يعهد اتخاذ هذا الإجراء للسلطة القضائية لتضمن حيادها وكفاءتها واستقلالها، ومن ثم فالسؤال يطرح حول الجهة المختصة بإصدار الأمر أو الإذن بمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية؟

1- بالنسبة لمراقبة الاتصالات الالكترونية:

نص القانون **09-04** في الفقرة**2** من **المادة4** على أنه لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب صادر عن السلطة القضائية المختصة دون أن تحدد هذه المادة السلطة القضائية المختصة بمنح الإذن هل يرجع ذلك إلى قاضي التحقيق أو وكيل الجمهورية؟

نحن نرى أن هذه الإجراءات يمكن الاستعانة بها من طرف كل من وكيل الجمهورية وقاضي التحقيق اللذين لهما حق إصدار الإذن بمراقبة الاتصالات الالكترونية، وحجتنا في ذلك ما ذكرته **المادة 3** من نفس القانون والتي ذكرت في نصها: **"**مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات... ووفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية**"**.

وبالتالي فهناك إحالة صريحة لما ورد في القواعد العامة في قانوني العقوبات والإجراءات الجزائية في حماية الحق في حرمة الحياة الخاصة.

وتبعا لذلك وطالما أن إجراءات اتخاذ التدابير التقنية المنصوص عليها في **المادة 65 مكرر5** المتمثلة في اعتراض المراسلات، التقاط الصور، تسجيل الأصوات تتم بإذن من قاضي التحقيق متى تم فتح تحقيق قضائي أو من طرف وكيل الجمهورية قبل فتحه.

وما يؤكد ذلك أيضا أن اللجوء إلى عمليات المراقبة تدعو إليه في بعض الحالات المنصوص عليها في **المادة4** الوقاية من وقوع بعض الجرائم ولمقتضيات التحريات وهذا يكون أثناء مباشرة التحقيق الأولي أي بمناسبة مرحلة جمع الاستدلالات، وهذه المرحلة لا يتصل بها قاضي التحقيق ولا يمكن القيام بأي إجراء ما لم يطلب منه فتح التحقيق بواسطة طلب افتتاحي من طرف وكيل الجمهورية أو شكوى مصحوبة بادعاء مدني.

وفي الحالتين يوجه الإذن إلى ضابط الشرطة القضائية المختص محليا سواء بصفته مأذون له من طرف وكيل الجمهورية أو منابا من قاضي التحقيق بوضع الترتيبات التقنية لمراقبة الاتصالات الالكترونية وتسجيل محتواها. هذا الضابط بإمكانه أن يستعين بمقدمي الخدمات(8) الذين ألزمهم **القانون 09-04** بموجب نص **المادة 10** منه على وجوب تقديم المساعدات للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات التي يتعين عليهم حفظها(9).

لكن الملاحظ أن المشرع الجزائري نص على حالة خاصة في **القانون09-04** بموجب **المادة4** فقرة3 أنه إذا تعلق الأمر بمنح الإذن بمراقبة الاتصالات الالكترونية في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، فإن النائب العام لدى مجلس قضاء الجزائر هو الذي يختص بمنح إذن لمدة 6أشهر لضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في **المادة 13** من هذا القانون(10).

في حين أجاز القانون الفرنسي صراحة اتخاذ إجراء المراقبة بناء على أمر مسبب صادر عن قاضي التحقيق فقط وفقا لما تنص عليه المادة 100 من القانون رقم 91-.641

2- بالنسبة لتفتيش المنظومات المعلوماتية:

يخول إجراء تفتيش المنظومات المعلوماتية لكل من قاضي التحقيق ووكيل الجمهورية حسب الأحوال إذا ما تم فتح تحقيق أو لا، كما يخول أيضا لضابط الشرطة القضائية القيام بعمليات تفتيش المنظومات المعلوماتية وفقا لما تنص عليه **المادة 5** من **القانون09-04** والتي تنص على أنه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 من هذا القانون الدخول بغرض التفتيش ولو عن بعد....". وفي هذا الإطار نص القانون على وجوب

مراعاة القواعد الإجرائية المنصوص عليها قانونا دون أن يحدد المقصود من هذه القواعد.

نرى أن المشرع الجزائري قصد مراعاة القواعد الإجرائية المنصوص عليها قانونا والمتعلقة بدخول المنازل وفقا **للمواد44، 45، 47** من قانون الإجراءات الجزائية وذلك إذا كان التفتيش يتعلق بمنظومة معلوماتية لحاسب آلي موجود في منزل أو محل خاص ويجب الدخول إليه. لكن إذا كان التفتيش عن بعد فلا يخضع لشرط الميعاد أو حضور المعني بالأمر على النحو الذي اشترطته المادتين 45 و**47** من قانون الإجراءات الجزائية، والسبب في ذلك يعود إلى طبيعة الإجراءات المتخذة والتي يكون الغرض منها في أغلب الحالات الوقاية من وقوع الجرائم المعينة بموجب نص **المادة4** من **القانون 09-04** الأمر الذي يقتضي ضرورة مباشرة هذه الإجراءات بصفة سرية و ليست علنية في مواجهة المتهم[11].

وفي هذا الخصوص فنجد أن المشرع الفرنسي نص على إجراءات تفتيش منظومة معلوماتية من طرف ضابط الشرطة القضائية أو تكليفه عون الشرطة القضائية تحت مسوؤليته المباشرة بشرط توافر الشروط القانونية المتعلقة بتفتيش المساكن المنصوص عليها في قانون الإجراءات الجزائية الفرنسي كان ذلك في حدود الإقليم الفرنسي، فإذا تجاوز حدوده يتم ذلك مع مراعاة الاتفاقيات الدولية المبرمة في هذا الخصوص وفقا لما نصت عليه المادة 57 من نفس القانون. ولم يكتف المشرع الفرنسي بهذا النص بل نص على سلطة وكيل الجمهورية أو ضابط الشرطة القضائية عن طريق أي وسيلة في الإطلاع عند أي شخص أو مؤسسة أو تنظيم خاص أو عام أو إدارة عمومية على وثائق تفيد التحقيق ولو كانت هذه الوثائق الكترونية موجودة في نظام معلوماتي أو معطيات شخصية معالجة أليا وفقا لما ذهبت إليه المادة 60-1 من قانون الإجراءات الجزائية الفرنسي[12]، كما يمكن لقاضي التحقيق القيام بهذا الإجراء وفقا لما ذهبت له المادة 97 من قانون الإجراءات الجزائية هذا القانون.

المطلب الثاني- الضمانات الشكلية لمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية:

يعد إجراء مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية من أخطر الإجراءات مساسا بالحق في حرمة الحياة الخاصة لهذا يجب إحاطته بضمانات تكفل حماية هذا الحق، وهذا لن يتأتى إلا بمباشرته وفقا لأشكال معينة بحيث إذا ما تركت هذه الشكليات كلها أو بعضها كان اللجوء إلى هذه الإجراءات باطلا. وبالرجوع إلى **القانون 09-04** فالملاحظ أن المشرع الجزائري لم يوضح بدقة الإجراءات الشكلية الواجبة الإتباع وأخضعها للقواعد العامة المنصوص عليها في قانون الإجراءات الجزائية دون أن يحددها بدقة ونحن نرى طالما أن هذه الإجراءات ترتبط بالتدابير التقنية المنصوص عليها في قانون الإجراءات

الجزائية لاتصالها جميعا بالحق في حرمة الحياة الخاصة فإنها تخضع لنفس القواعد المنصوص عليها مع مراعاة ما تضمنه **القانون 09-04**.

ومن القواعد الشكلية التي جاء بها المشرع الجزائري أن يكون هناك إذن باللجوء إلى مباشرة هذه الإجراءات صادر من السلطة المختصة، هذا الإذن يجب أن تتوافر فيه شروط معينة فيجب أن يشمل بيانات خاصة وأن يرتبط بمدة معينة.

أولا- ضرورة صدور أمر من السلطة القضائية المختصة باللجوء إلى مراقبة الاتصالات الالكترونية والتفتيش:

يعتبر الحصول على إذن من السلطة القضائية المختصة لمراقبة الاتصالات الالكترونية من أهم الضمانات التي وضعها المشرع الجزائري أو غيره من التشريعات المقارنة للأفراد ويتعلق الأمر كما سبق الشرح بقاضي التحقيق أو وكيل الجمهورية حسب الأحوال أو النائب العام لدى مجلس قضاء الجزائر وفقا لما نصت عليه صراحة نص **المادة 4 فقرة2 و3** من **قانون09-04**، ويجب على القضاء قبل أن يصدر الإذن أن يقدر توافر حالة من الحالات الواردة على سبيل الحصر في الفقرة**1** من نص هذه المادة والسابق التعرض لها منعا للتعسف من أي جهة أخرى. ومن ثم فإذا قام ضابط الشرطة القضائية من تلقاء نفسه بهذا الإجراء، عد هذا الإجراء باطلا وبالتالي يبطل الدليل المستمد من المراقبة ومتى وقع باطلا بطلت معه جميع الإجراءات التي بنيت عليه.

أما بالنسبة لمباشرة إجراء تفتيش المنظومات المعلوماتية وفقا لما نصت عليه **المادة5** من **القانون 09-04** والذي ذكر فيها أن هذا الإجراء مخول للسلطة القضائية وضابط الشرطة القضائية. ولا يطرح الإشكال بالنسبة للسلطة القضائية التي يجوز لها القيام بالإجراء بنفسها أو تنيب عنها ضابط الشرطة القضائية للقيام بهذا الإجراء، لكن يطرح الإشكال بالنسبة لضابط الشرطة القضائية هل يخول له القانون إجراء تفتيش المنظومات المعلوماتية من تلقاء نفسه دون صدور إذن له من السلطة القضائية المختصة؟

بالرجوع إلى نص **المادة5** نجد أن المشرع الجزائري سكت ولم ينص على وجوب صدور إذن من السلطة القضائية المختصة مثلما اشترط ذلك بالنسبة لإجراء مراقبة الاتصالات الالكترونية صراحة، ومن ثم وفقا للتفسير الضيق لنص هذه المادة فإنه لا يشترط صدور إذن من السلطة القضائية المختصة لمباشرة ضابط الشرطة القضائية التفتيش. لكن بالرجوع إلى الأعمال التحضيرية لمناقشة مشروع هذا القانون فقد ذكر وزير العدل صراحة أن جميع الإجراءات المنصوص عليها في القانون **09-04** سواء المتعلقة بمراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية يجب أن تتم بعد الإذن المسبق للقضاء أي قبل اللجوء إلى هذه الإجراءات ويتم ذلك خلال مباشرة الإجراءات وبعد انتهائها أيضا[(13)]، واعتبرها من أهم الضمانات التي نص عليها القانون.

ونحن نتجه نفس الاتجاه إذ يجب أن يتم تفتيش المنظومات المعلوماتية بناء على إذن مكتوب وصريح من السلطة القضائية المختصة تماشيا مع التفسير الواسع لنص **المادة 5** والتي نصت على وجوب احترام قانون الإجراءات الجزائية، وبالرجوع إلى القواعد العامة لمباشرة إجراء التفتيش لا يملك ضباط الشرطة القضائية هذا الاختصاص إلا بناء على إذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق، وبالتالي لا يملك ضباط الشرطة القضائية اللجوء إلى تفتيش المنظومات المعلوماتية دون إذن.

وقد أشارت الفقرة2 من **المادة 5** السالف الإشارة إليها أنه في حالة ما إذا وجدت أسباب تؤدي إلى الاعتقاد 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.

والملاحظ أن المشرع الجزائري بمناسبة تمديد التفتيش لم يشترط وجوب صدور إذن من السلطة القضائية المختصة بل يكفي مجرد إخطار هذه السلطة أنه سيتم تمديده إلى منظومة معلوماتية أخرى بشرط أن يتم الدخول إليها بواسطة المنظومة المعلوماتية الأولى الصادر بشأنها الإذن بالتفتيش، ويجب أن تدعو الضرورة لذلك أي توافر حالة الاستعجال أي الخوف من محو المعطيات المخزنة أو حذفها أو تعديلها. ونحن نرى أن هذا التمديد يجب أن يكون بموافقة السلطة القضائية وتحت إشرافها المباشر ومسؤوليتها حتى لا يتعسف ضابط الشرطة القضائية في قيامه بإجراء التفتيش وفي ذلك خطر كبير على الحق في الحياة الخاصة للأفراد.

وفي هذا الصدد يتعين على المشرع الجزائري في تعديلاته اللاحقة لهذا القانون ضرورة أن يؤكد صراحة على وجوب توافر الإذن من السلطة القضائية صراحة وأن تتم عملية المراقبة أو التفتيش تحت الإشراف المباشر للسلطة القضائية المختصة.

ثانيا- بيانات الإذن بمراقبة الاتصالات الالكترونية و التفتيش:

لم يتكلم القانون 09-04 على بيانات الإذن بمراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية، لكن بالرجوع إلى القواعد العامة في قانون الإجراءات الجزائية التي أحالت إليها نصوص هذا القانون فينطبق عليه ما ينطبق على غيره من الأوامر التي تصدرها الجهات القضائية، وهذه البيانات تتعدد وتتفاوت من حيث الأهمية بين البيانات الجوهرية التي يترتب على عدم وجودها بطلان الإذن، والبيانات غير الجوهرية.

وسنتناول فيما يلي البيانات التي يجب أن تتوافر في الإذن بمراقبة الاتصالات الالكترونية أو التفتيش حسب القواعد العامة الواردة في التشريع الجزائري والمقارن على النحو التالي:

1- أن يكون الإذن بمراقبة الاتصالات الالكترونية أو التفتيش مكتوبا وصريحا:

من الشروط العامة التي يجب توافرها في الإذن بالمراقبة أو التفتيش أن يكون مكتوبا طبقا لما نصت عليه صراحة **المادة** 4 فقرة **2** من **القانون 09-04**. وهذا ما قال به المشرع الجزائري بمناسبة جميع إجراءات التحقيق تطبيقا للقاعدة العامة المعمول بها في جل التشريعات الإجرائية المقارنة أن إجراءات التحقيق يجب أن تثبت دائما بالكتابة لكي تكون أساسا صالحا لما يبنى عليها من النتائج.

إضافة إلى شرط الكتابة يجب أن يكون الإذن صريحا يستفاد منه مباشرة نية السلطة القضائية المختصة في اللجوء إلى هذا الإجراء دون غيره، ولا يكفي أن يستنتج منه ضمنا نية السلطة القضائية في أن هذا الإجراء هو المقصود و ليس غيره. وبالتالي يجب أن يذكر في الإذن صراحة أن الإذن يتعلق بمراقبة الاتصالات الالكترونية أو يرد في الإذن عبارة الأمر بتفتيش منظومة معلوماتية معينة فهنا يقع الإذن صحيحا.

وكلما تم مراعاة هذه الضمانات التي قالت بها العديد من التشريعات المقارنة وعلى وجه الخصوص التشريع الفرنسي تم التأكيد على احترام الحريات الفردية للأشخاص وخاصة الحق في حرمة الحياة الخاصة.

2- أن يكون الإذن بمراقبة الاتصالات الالكترونية أو التفتيش مؤرخا وموقعا:

لم ينص قانون الإجراءات الجزائية على هذا الشرط صراحة، لكن يفترض ذلك في أي أمر مكتوب يصدره قاضي التحقيق في جميع التشريعات المقارنة، ويشمل التاريخ اليوم والشهر والسنة والساعة.

وترجع الفائدة في تحديد تاريخ الإذن إلى معرفة ما إذا كان مصدر الإذن السلطة المختصة به محليا وقت إصداره فعلا أو كانت غير مختصة بذلك، كما يفيد أيضا في حساب المدة التي يجب خلالها تنفيذ عملية المراقبة طالما أن الإذن بالمراقبة يصدر لمدة زمنية معينة لارتباطه بالحياة الخاصة للأفراد التي يجب عدم انتهاكها إلا بالقدر اليسير الذي يجيز الكشف عن حقيقة الجريمة والتوصل إلى مرتكبيها. كما يفيد تاريخ الإذن في حساب مدة تقادم الدعوى العمومية إذا كان أخر الإجراءات التي تم اتخاذها بمناسبة الدعوى العمومية و لم تتبعه إجراءات أخرى، كم أنه يقطع تقادم الدعوى الجنائية.

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

وإذا تعددت صفحات الإذن فالأصل هو توقيع مصدره على كل صفحة من صفحاته تحرزا من احتمالات استبدال بعض صفحاته أو الإضافة إليها وذلك وفقا لما جرى عليه العمل ميدانيا، دون أن يؤدي ذلك إلى بطلان الإذن طالما تم التوقيع على الصفحة الأخيرة منه.

كما يجب أيضا أن يتضمن الإذن باللجوء إلى مراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية بطبيعة الحال اسم مصدره و صفته أي كونه قاضي تحقيق أو وكيل الجمهورية حتى يمكن التحقق من أن هذا الإذن قد صدر عن السلطة المختصة بإصداره.

3- تحديد الشخص المراد مراقبة اتصالاته الالكترونية أو تفتيش منظومته المعلوماتية:

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

ويتم تحديد الشخص المراد مراقبة اتصالاته الالكترونية ببيان اسمه ولقبه ومحل إقامته وكل ما يفيد في تعيينه ونفي الجهالة عنه.

كما يقع إجراء التفتيش صحيحا بتحديد المنظومة المعلوماتية المراد تفتيشها بدقة ومكان وجودها سواء كان مكانا عاما أو خاصا دون حاجة لذكر صاحبها إذا لم يتم التعرف عليه ذلك أنه حسب رأينا فالعبرة بالمنظومة المعلوماتية محل التفتيش التي يجب أن يتضمنها الإذن بالتفتيش.

4- بيان طبيعة الاتصالات الالكترونية المطلوب مراقبتها:

ينصب الإذن بإجراء مراقبة الاتصالات الالكترونية على محل معين يتمثل في اتصالات الشخص الالكترونية. وتبعا لذلك فيجب أن يحدد الإذن كل العناصر التي تسمح بالتعرف على الاتصالات الالكترونية المطلوب تجميعها وتسجيلها والذي يجب أن يحدد بدقة طبيعة هذه الاتصالات هل هي مراسلات الكترونية تتعلق برسائل تصل بريده الالكتروني أو أحاديث خاصة تتم عن طريق شبكة الانترنت. وعلة ذلك أن نطاق الإذن من حيث تنفيذه يتحدد بمحله فإذا صدر الإذن بمراقبة اتصالاته الالكترونية لم يتعداها إلى تفتيش منظومته المعلوماتية إلا ما تعلق منها ببريده الالكتروني والذي يرتبط باتصالات الشخص الالكترونية.

ويشترط أيضا أن تبقى الإجراءات المتخذة سواء المتعلقة بمراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية في إطار المعلومات المبحوث عنها[14]، وهو الشرط الذي نص عليه المشرع الإجرائي صراحة في نص **المادة 4** فقرة أخيرة من **القانون09-04** والتي أوجبت على أن تكون الترتيبات التقنية الموضوعة للأغراض الموجهة للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة موجهة حصريا لتجميع

وتسجيل معطيات ذات صلة بالوقاية منها وعدم الالتزام بذلك يترتب عليه توقيع العقوبات المتعلقة بالمساس بالحق في حرمة الحياة الخاصة، ويكون المشرع قد قصد تطبيق نص **المادة303 مكرر3** وما يليها من قانون العقوبات الجزائري [15].

وإذا تضمن الإذن مراقبة الاتصالات الالكترونية لشخص في مكان خاص معين فقط، فإن هذا الإذن يستدعي اتخاذ التدابير التقنية اللازمة لذلك في هذا المكان دون غيره. و تبعا لذلك فيجب أن يتضمن الإذن هذه الأماكن سواء كانت سكنية أو عامة و تحديد عنوانها تحديدا دقيقا نافيا للجهالة.

وفي هذا الصدد فيسمح الإذن المسلم بغرض وضع الترتيبات التقنية لمراقبة الاتصالات الالكترونية بالدخول إلى المحلات السكنية أو غيرها و لو خارج المواعيد المحددة في **المادة 47** من قانون الإجراءات الجزائية وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن وفقا لما للقواعد العامة المعمول بها في قانون الإجراءات الجزائية بشأن وضع التدابير التقنية لاعتراض المراسلات، التقاط الصور أو تسجيل الأحاديث طالما أن **القانون 09-04** ينص على ضرورة مراعاة الأحكام المنصوص عليها في قانون الإجراءات الجزائية.

كذلك إذا حدد الإذن إجراء تفتيش منظومة معلوماتية لا يجوز تفتيش غيرها إلا إذا ارتبطت بها وكان بالإمكان تفتيشها من المنظومة المعلوماتية الأولى وبعد إعلام الجهة القضائية المختصة، كما لا يجوز بناء على نفس الإذن مراقبة اتصالات الشخص الالكترونية. وإن كان إجراء التفتيش لا يطرح العديد من المشاكل المتعلقة بصفة الأشخاص لأنه يتعلق بدرجة خاصة بمنظومات معلوماتية، ولا يتعلق بالدخول للاماكن لأنه يمكن إجراؤه عن بعد.

5- تحرير محضر بالعمليات التقنية التي تم القيام بها:

لما كان اللجوء إلى مراقبة الاتصالات الالكترونية والتفتيش عملا من أعمال التحقيق فإنه يجب تحرير محضر بها يثبت فيه ما تم من إجراءات بشأنها، وما أسفرت عنه من أدلة حتى لو لم يشترط ذلك صراحة في نصوص **القانون 09-04**. ومن ثم فيجب على ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عمليات وضع التدابير التقنية لمراقبة للاتصالات الالكترونية وما أسفرت عنه، كذلك عمليات التفتيش التي تم القيام بها وما أسفر عنها من أدلة.

ويجب أن يذكر في المحضر أيضا تاريخ وساعة بداية هذه العمليات والانتهاء منها، وجميع الشروط الشكلية العامة في جميع المحاضر كما يجب أن يكون محررا باللغة العربية.

ثالثا- تسبيب الإذن باللجوء إلى مراقبة الاتصالات الالكترونية أو التفتيش المنظومات المعلوماتية:

سبق تعريف تسبيب الإذن بالمراقبة بأنه بيان الأسانيد الواقعية والقانونية التي أدت إلى إصداره. ومن ثم يجب على السلطة القضائية المختصة ذكر

الأسباب التي دفعت بها إلى إصدار الإذن بمراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية حتى ولو لم ينص القانون صراحة على ذلك وهو الأصل المعمول به بمناسبة معظم الأوامر التي تصدر عن السلطة القضائية، ومن ثم يجب أن يؤسس الإذن على إحدى الحالات التي نصت عليها المادة **4** من **القانون 90-04** أي أن يكون سببه الوقاية من وقوع جرائم إرهابية أو جرائم ماسة بأمن الدولة أو احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو تكون ضرورات التحري أو التحقيق الابتدائي هي التي دفعت إلى اللجوء إلى هذه الإجراءات. أو كان الإجراء في إطار تنفيذ طلبات مساعدة دولية متبادلة.

وفي هذا الصدد فقد ذهب المشرع الجزائري إلى ضرورة أن يرافق الإذن بمراقبة الاتصالات الالكترونية للوقاية من الأفعال الإرهابية والتخريبية والماسة بأمن الدولة تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها وفقا لما نصت ليه **المادة 4** فقرة**3**، ومن شأن هذا التقرير أن يوضح الأسباب والدوافع التي دفعت بالسلطة القضائية اتخاذ الأمر بمراقبة الاتصالات الالكترونية وما هو الغرض الذي يريد الوصول إليه وهذا هو المقصود بعنصر التسبيب. ويجب التأكيد على أن هذا التقرير يجب أن يصحب جميع حالات مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية[16].

وقد أكدت **المادة 5** فقرة**2** من هذا القانون على ضرورة توافر أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأنه يمكن الدخول إليها من المنظومة المعلوماتية الأولى لتمديد التفتيش إلى منظومة معلوماتية أخرى. الأمر الذي يستشف منه ضرورة توافر الأسباب لإصدار الإذن منذ البداية.

ويجب أن تكون أسباب اللجوء إلى إجراءات المراقبة والتفتيش جدية وكافية، وفي هذا الصدد يكفي الإشارة إلى الدلائل و القرائن التي تسوغ إصدار الإذن.

واشتراط أن يكون الإذن الصادر من القضاء باللجوء إلى مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية مسببا يرجع إلى أنها تعد من أخطر الإجراءات الماسة بحريات الأفراد وانتهاك حقهم الطبيعي في السرية. ولكونه إجراء استثنائي يرد على الأصل العام المنصوص عليه في الدستور والمتمثل في حرمة الحياة الخاصة للمواطنين وحقهم في سرية اتصالاتهم وهذا الاستثناء تبرره المصلحة العامة في الوقاية من الجرائم المذكورة أعلاه قبل وقوعها أو بقصد التوصل إلى كشف الحقيقة والقبض على الجناة.

كما يظهر أهمية التسبيب وفقا لما سبق وأن أشرنا إليه في أنها تعتبر الوسيلة المثلى لتقييد سلطة الجهة القضائية المختصة الذي يجب عليه أن يتثبت من المبررات التي يستند إليها عند لجوئه إلى مثل هذه الإجراءات الماسة بحريات الأفراد وانتهاك حقهم في الحياة الخاصة. زيادة على ذلك تمكين محكمة الموضوع

من بسط رقابتها على المبررات التي استند إليها السلطة المختصة في إصدارها الأمر.

رابعا ـ مدة الإذن بمراقبة الاتصالات الالكترونية:

حرصت معظم التشريعات الحديثة على تحديد مدة معينة لمباشرة أي من الإجراءات أو التقنيات الحديثة منعا من تعسف وإساءة استعمال السلطة وحماية الحق في حرمة الحياة الخاصة للأفراد، ومن ثم فإنه من الضمانات الأكيدة لحماية هذا الحق أن يرتبط اتخاذ إجراء مراقبة الاتصالات الالكترونية مدة معينة.

بالرجوع إلى **القانون 09-04**، نجد أن **المادة4** منه فقرة3 حددت مدة الإذن الذي يمنحه النائب العام لدى مجلس قضاء الجزائر لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته بشأن وضع الترتيبات التقنية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة لمدة ستة أشهر قابلة للتجديد.

والملاحظ أن المشرع الجزائري قد أطال مدة المراقبة نوعا ما في هذا النوع من الجرائم وجعلها قابلة للتجديد دون أن يحدد عدد مرات التجديد، ويمكن أن نرجع سبب ذلك إلى خطورة هذا النوع من الإجرام الذي يمس بأمن الدولة بالدرجة الأولى، ولكون هذا النوع من الإجرام هو إجرام منظم وعابر للحدود الوطنية في كثير من الأحيان حيث لا يتم الكشف عنه بسهولة إلا إذا استغرقت التحريات مدة زمنية معينة تمكن من الكشف عن حقيقته والتوصل إلى عناصر هذه التنظيمات المنتشرة عبر العديد من المواقع والأقاليم.

لكن كان من الأفضل لو نص المشرع الجزائري على عدد المرات التي يسمح فيها بالتجديد والتي لا يمكن أن تستمر لسنوات، فإذا لم تجد هذه الإجراءات نفعا في الوصول إلى الحقيقة يتعين الابتعاد عنها. ومن ثم يتعين ضرورة ربط التجديد بوجود أسباب جدية تتمثل في الوصول إلى أدلة وقرائن على وجود مثل هذه الجرائم تستدعي الضرورة وجوب استكمال التحريات بشأنها للوصول إلى الحقيقة. وفي هذا الإطار وحماية للحق في حرمة الحياة الخاصة يجب أن تكون الترتيبات التقنية الموضوعة موجهة لمعلومات تتعلق بالجريمة المقصودة دون غيرها فقط.

وتطرح مشكلة بالنسبة لباقي الحالات المنصوص عليها في **المادة4** من القانون **09-04**، حيث خص المشرع الحالة الأولى فقط بتحديد المدة دون باقي الحالات الأخرى، هل معنى ذلك أن المشرع الجزائري لم يربطها بمدة زمنية معينة؟

لا نستطيع التسليم بذلك لأن في ذلك اعتداء كبير على الحق في حرمة الحياة الخاصة للأفراد، فكلما كانت مدة المراقبة قصيرة قل الاعتداء على الحق في حرمة الحياة الخاصة وكلما طالت المدة كان الأثر واضحا في الاعتداء عليها.

وتبعا لذلك يجب أن تكون هذه الإجراءات الاستثنائية مؤقتة احتراما للحريات الفردية، وطالما لم ينص القانون**09-04** على ذلك نرجع إلى القواعد العامة في قانون الإجراءات الجزائية ومن ثم فإن هذه التدابير تتخذ لمدة لا تتجاوز 4 أشهر يمكن تجديدها إذا دعت لذلك مقتضيات البحث والتحري والتحقيق وفقا لما نصت عليه **المادة65 مكرر7.** وبزوال حالة الضرورة يجب أن ينتهي الإذن باللجوء إلى هذه المراقبة لأن الحاجة إلى وجوده لم تعد قائمة، وبالتالي فيمكن أن يستمر باستمرار التحقيق بشرط أن يكون اللجوء إلى هذه الإجراءات نافعا ومجديا.

أما التشريع الفرنسي فقد حدد طبقا للقانون 91-646 الحد الأقصى لمثل هذه الإجراءات بمدة 4 أشهر أيضا قابلة للتجديد بنفس الشروط التي صدر بناء عليها أمر المراقبة الأول وفقا لما قضت به المادة 100-2 من قانون الإجراءات الجنائية.

المبحث الثالث:

آثار مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية:

يهدف المشرع الجزائري من خلال نصه على إجراءات مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية إلى الوصول إلى أدلة الغرض منها الوقاية من وقوع جرائم خطيرة تمس أمن الدولة أو معرفة الجناة بشأن جريمة وقعت من الجرائم المرتكبة عن طريق تكنولوجيا الاتصال والإعلام، والتي لا يمكن للوسائل التقليدية الوصول إليها. ويترتب على إجراء مراقبة الاتصالات الالكترونية تجميع وتسجيل محتوى هذه الاتصالات الالكترونية، هذا التسجيل الذي يجب إفراغه في محضر معد لذلك. بينما يترتب على إجراء تفتيش المنظومات المعلوماتية حجز المعطيات المعلوماتية[17] التي تفيد في كشف حقيقة الجريمة، ومن ثم يعد حجز المعطيات هو غاية التفتيش وهو الأثر المباشر الذي يسفر عنه إجراء التفتيش ويرتبط به ارتباطا وثيقا.

وتبعا لذلك يخضع كل من إجراء مراقبة الاتصالات الالكترونية وكذا تفتيش المنظومات المعلوماتية لتنظيم قانوني محكم على النحو الذي سبق شرحه حماية لحريات الأفراد وحقهم في الحياة الخاصة، ومن ثم يعد الإجراء صحيحا إذا تخلفت أحد هذه الضمانات والشروط التي أوجبها القانون ويترتب بطلان الإجراء متى وقع مخالفة لأحد الشروط والضمانات القانونية المنصوص عليها.

وسوف نتعرض من خلال العنصرين المواليين إلى الآثار الناتجة عن كل من الإجراءين على حدى وفقا لما يلي:

المطلب الأول- الآثار المترتبة على مراقبة الاتصالات الالكترونية:

أولا- تفريغ و تحريز التسجيلات:

سبق الذكر أنه ينتج عن عملية مراقبة الاتصالات الالكترونية تجميع وتسجيل محتوى هذه الاتصالات سواء تمثلت في محادثات شفوية أو رسائل

الكترونية متبادلة عن طريق البريد الالكتروني أو التقاط صور وذلك باستعمال الترتيبات التقنية المناسبة، والملاحظ أن **القانون 09-04** لم يذكر كيف يتم ذلك وما هي الإجراءات اللاحقة لعملية التسجيل. ومن الضمانات الهامة في تنفيذ عملية المراقبة التي نص عليها قانون الإجراءات الجزائية وجوب تفريغ أشرطة التسجيل في محضر وتحريزها عقب ذلك للمحافظة على سلامتها وعدم العبث بها. ويجب أن يوضع المحضر في ملف القضية مع الأحراز المختومة التي يجب أن تبقى في يد القضاء.

هذا الإجراء الذي نصت عليه **المادة 65 مكرر 10** من قانون الإجراءات الجزائية وبتطبيق هذا النص بشأن الاتصالات الالكترونية فإنه يجب على ضابط الشرطة القضائية المأذون له أو المناب أن يقوم بنسخ أو وصف الاتصالات الالكترونية المختلفة سواء تمثلت في مراسلات الكترونية أو محادثات مسجلة وإيداعها في محضر. وإذا تصادف أن كانت هذه الاتصالات قد تمت بإحدى اللغات الأجنبية، فيجب أن تنسخ وتترجم عند الاقتضاء بمساعدة مترجم يسخر لهذا الغرض.

ونحن نرى في هذا الصدد أن تتم هذه العملية تحت إشراف السلطة القضائية دائما لأن في ذلك إحدى الضمانات الأكيدة لحماية الحريات الفردية وأهمها الحق في حرمة الحياة الخاصة، لأن مراقبة الاتصالات الالكترونية تتضمن المساس بحق الإنسان في سرية أحاديثه و مراسلاته الخاصة واللجوء إليها استثناء من القاعدة العامة والتي لا يجوز التوسع فيها بل إحاطتها بكافة الضمانات التي تكفل ذلك.

وهو الإجراء الذي نص عليه المشرع الفرنسي والذي يطبق بشأن جميع أنواع الاتصالات سواء تمت عن طريق سلكي أو لاسلكي أو الكتروني وذلك بموجب نص المادة 100-5 من قانون الإجراءات الجزائية الفرنسي والتي أوجبت على قاضي التحقيق أو مأمور الضبط القضائي القيام بتفريغ محتوى التسجيلات في محضر معد لذلك. ويجب أن يشتمل على المعلومات اللازمة لإظهار الحقيقة ويودع بالملف.

وتجدر الملاحظة في هذا الصدد وتأكيدا على الحرص على حماية حقوق وحريات الأفراد على النحو الذي سبق ذكره بشأن اعتراض المراسلات، تسجيل الأصوات والتقاط الصور فإنه يجب إبلاغ المتهم بمراقبة اتصالاته الالكترونية بعد انتهاء عملية المراقبة وتمكينه من الإطلاع على محتوى الرسائل والتسجيلات المضبوطة ويتم ذلك غالبا عن طريق إطلاع المحامي عليها في ملف القضية، والغرض ذلك تمكين الأفراد من ترتيب دفاعهم وفقا للأدلة المقدمة ضدهم. ومن ثم فمن حق المتهم أن يطعن في صحة التسجيلات وله أن يطلب من قاضي التحقيق أو المحكمة انتداب خبير لفحص التسجيلات ومطابقة الصوت المسجل على صوته الحقيقي والتأكد من البريد الالكتروني الذي يملكه الشخص.

ونحن نؤكد أيضا بمناسبة هذا الإجراء وضمانا لحقوق الدفاع لو نص المشرع الجزائري صراحة على نص خاص يوجب على سلطة التحقيق إبلاغ المتهم بأي تدبير من تدابير مراقبة الاتصالات الالكترونية المتخذة ضده وما نتج عنها من أدلة مباشرة بعد الانتهاء من هذه العمليات. ويجب أن يمنح له الوقت الكافي للرد على هذه الأدلة ومناقشتها ودحضها، لأن في ذاك ضمان أكيد لصحة الإجراءات وعدم خرق حقوق الدفاع وغياب هذا التبليغ ينجر عنه بطلان الإجراءات وما نتج عنها من أدلة يتعين استبعادها من التحقيق كأدلة إدانة.

المطلب الثاني- الآثار المترتبة على تفتيش المنظومات المعلوماتية:

يعد حجز المعطيات المعلوماتية هو النتيجة الطبيعية لإجراء تفتيش يتعلق بأي منظومة معلوماتية والتي تفيد في الوصول إلى أدلة تكشف عن الحقيقة، وتبعا لذلك فقد أخضعه المشرع الجزائري كغيره من التشريعات المقارنة إلى قواعد و ضمانات يتعين توافرها في هذا الإجراء للقول بصحته. وفي حالة استحالة إجراء حجز المعطيات يمكن للسلطة المختصة أن تقوم بالحجز عن طريق منع الوصول إلى المعطيات وذلك على النحو التالي:

أولا- حجز المعطيات المعلوماتية:

يختلف التفتيش العادي عن تفتيش المنظومات المعلوماتية من حيث طبيعة الأشياء المحجوزة. فيترتب على التفتيش العادي في الغالب أدلة مادية كالوسائل والأدوات التي ارتكبت بها الجريمة أو الناتجة عنها كالمسروقات أو الوثائق المزورة وغيرها، في حين أن تفتيش المنظومات المعلوماتية يرد على أشياء ذات طبيعة معنوية وهي المعطيات ومن ثم يترتب على هذا الإجراء حجز لمعطيات معلوماتية.

فعندما تكشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة. فإنه يتم حجز هذه المعطيات عن طريق نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز[18] وفقا للقواعد المعمول بها في قانون الإجراءات الجزائية وهذا وفقا لما نصت عليه **المادة 6** فقرة1 من **القانون 09-04**.

وقد ذهب الفقه المقارن إلى وجود العديد من المشكلات العملية المتعلقة بضبط المعلومات التي تحدث أحيانا تغييرات في البيانات عند أخذ نسخة منها أي عند صعوبة ضبط النسخة الأصلية كما لو كانت هذه النسخة الأخيرة مسجلة في النظام أو متصلة بالشبكة التي تربط بين عدة أنظمة[19].

وقد أدى ذلك بمحكمة النقض الفرنسية إلى عدم اعتبار أخذ نسخة من البيانات المسجلة في الكومبيوتر وعدم ضبط الجهاز نفسه بما فيه من ذاكرة تحتوي تلك المعلومات من قبيل الحجز في مفهوم المادة76 و97 من قانون الإجراءات الجزائية الفرنسي[20].

وفي إطار نفس قواعد هذا القانون فقد ألزم السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجرى بها العملية. لكن نحن نرى أنه إذا قام ضابط الشرطة القضائية بالتفتيش فيجب أن تتم هذه العملية تحت إشراف السلطة القضائية التي أمرت بالتفتيش حتى لا يتعسف ضباط الشرطة القضائية أثناء تأدية مهامهم أو يعبثوا بمحتوى هذه الدعامة الالكترونية أو يطلعوا على أسرار تمس الحياة الخاصة أثناء إطلاعهم على المعطيات، ويجب أن ينوه المشرع الجزائري عن ذلك صراحة في تعديلاته اللاحقة لهذا القانون وهذا لتأكيد الضمانات القانونية لحماية حريات الأفراد وحقهم في الحياة الخاصة.

وفي إطار حجز المعطيات المعلوماتية يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها، ذلك أن هذه العمليات تحتاج في كثير من الأحيان لأصحاب الاختصاص والخبرة الفنية لكن يلزمون بكتمان العمليات التي يقومون بها تحت طائلة تطبيق العقوبات المنصوص عليها في قانون العقوبات.

وفي سبيل الوصول إلى الحقيقة تملك السلطة المكلفة بالتفتيش وفقا لما نصت عليه المادة 6 فقرة أخيرة استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات ويكون ذلك بغرض جعلها قابلة للاستغلال لأغراض التحقيق. ويجب أن تلتزم هذه السلطة بعدم المساس بمحتوى المعطيات ذلك أن المساس بها يؤدي إلى تحريف الوقائع ويمكن أن يؤدي إلى تغليط المحكمة أو تضليل العدالة عند البحث عن الحقيقة، ولهذا يجب أن تتم هذه العملية تحت إشراف ورقابة السلطة القضائية المختصة.

ولم يكتف المشرع الجزائري بشروط التفتيش بل نص على ضمانات وقواعد شكلية خاصة بإجراءات الحجز والتي أحال فيها **القانون09-04** لقانون الإجراءات الجزائية تتمثل فيما يلي:

1- الإطلاع على دعامة التخزين الالكترونية حق منحه القانون للسلطة المكلفة بالتفتيش سواء كان ضابط شرطة قضائية أو قاضي التحقيق حسب الأحوال، وكذلك الأشخاص المذكورين في نص **المادة 45** و**المادة 48** الذين حضروا عملية التفتيش وهم الشخص المراد تفتيش منزله أو صاحب المنزل أو ممثله أو الشاهدين إذا تم تفتيش المنظومة المعلوماتية في مسكن ولم يقع التفتيش عن بعد.والجدير بالذكر أن **المادة 45** من قانون الإجراءات الجزائية ألزمت ضابط الشرطة القضائية أنه في حالة ما إذا كان يباشر إجراء التفتيش في أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني أن يتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر.

2- يجب وضع دعامة التخزين الالكترونية التي تم نسخ المعطيات عليها في حرز يتم غلقه وختمه إذا أمكن ذلك، فإذا تعذرت الكتابة عليها توضع في وعاء أو كيس يغلق بإحكام ويوضع عليه شريط من الورق ويختمه. وهو ما قضت به **المادة 45** فقرة **3** قانون الإجراءات الجزائية.

3- لا يجوز فض الأحراز إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا أو من ضبطت لديه هذه الأشياء طبقا لما ذهبت إليه المادة **48** فقرة **3** و ذلك تفاديا للادعاء بتغيير الأحراز. و هو الشرط الذي قالت به معظم التشريعات الحديثة كالتشريع المصري بموجب نص المادة 57 من قانون الإجراءات الجنائية المصري و المادة 56 من قانون الإجراءات الجزائية الفرنسي.

4- يمنع إذاعة أو إفشاء مضمون المعطيات التي تم نسخها وتسجيلها والناتجة عن تفتيش منظومة معلوماتية تحت طائلة توقيع العقوبات المنصوص عليها قانونا.

5- يجب على ضابط الشرطة القضائية أو قاض التحقيق عن طريق كاتبه تحرير محضر بجرد المحجوزات، ويحتوي في الغالب هذا المحضر على البيانات التالية:

- أن يتضمن كافة العمليات التي تم إجراؤها والمعطيات المحجوزة وإثبات أماكن وجودها وظروف حجزها،
- بيان أسماء القائمين على التفتيش وأسماء الحاضرين،
- ذكر تاريخ وساعة التفتيش،
- توقيع القائم بالتفتيش على كل صفحة من صفحات المحضر وتوقيع الشهود والمتهم إن حضروا عملية التفتيش.

والغرض أو الحكمة من إلزامية تحرير محضر التفتيش ليكون شاهدا على ما تم القيام به الإجراءات، والخوف من العبث بالمستندات ومحاولة استبدالها.

ثانيا- الحجز عن طريق منع الوصول إلى المعطيات:

نص المشرع الجزائري بموجب نص **المادة7** على أنه في حالة استحالة إجراء حجز للمعطيات المعلوماتية ونسخها على دعامة تخزين الكترونية لأسباب تقنية حالت دون ذلك، في هذه الحالة يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحويها المنظومة المعلوماتية أو إلى نسخها والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة. وذلك بغرض عدم إتلاف أو العبث بهذه المعطيات. ومما لا شك فيه انه يجب الاستعانة بذوي الاختصاص للقيام بمثل هذه الإجراءات على أن يتم ذلك تحت إشراف السلطة القضائية. والملاحظ أن مثل هذه الإجراءات هي إجراءات تقنية و ليست قانونية الأمر الذي يتطلب توظيف ضباط شرطة قضائية مختصون في الجانب المعلوماتي لكن يتم توظيفهم على مستوى مصالح الأمن

والدرك الوطني. ضف إلى ذلك ضرورة تكوين قضاة التحقيق ووكلاء الجمهورية في الجرائم المعلوماتية[21].

الخاتمة:

تعرضنا من خلال هذه الدراسة إلى مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية كإجراءات جديدة استحدثها المشرع الجزائري بموجب **القانون09-04** والذي يعد من القوانين العربية الرائدة في هذا المجال حيث نص عليه بعد تفاقم الإجرام المعلوماتي وعدم القدرة على السيطرة عليه عن طريق الإجراءات التقليدية المنصوص عليها بموجب قانون الإجراءات الجزائية. وتعد هذه الإجراءات من أخطر الإجراءات الماسة بحق الإنسان بحرمة حياته الخاصة لارتباطه باتصالاته الخاصة، لذلك فقد عمل المشرع الجزائري على إحاطتها بكافة الضمانات لحماية الحق في حرمة الحياة الخاصة.

ومن خلال هذه الدراسة توصلنا إلى ما يلي:

من حيث النتائج:

لقد حرص المشرع الجزائري على احترام الحق في حرمة الحياة الخاصة من خلال نصه على مجموعة من الضمانات الإجرائية سواء كانت شكلية أو موضوعية والتي يجب مراعاتها أثناء إجراء المراقبة الالكترونية وتفتيش المنظومات المعلوماتية كإجراءات جديدة للوصول إلى الأدلة استحدثها المشرع الإجرائي بموجب **القانون 09-04** تتمثل على وجه الخصوص فيما يلي:

- نص المشرع الجزائري على إمكانية اللجوء إلى مراقبة الاتصالات الالكترونية وتفتيش المنظومة المعلوماتية في حالات استثنائية لأنها تمثل اعتداء على حق الإنسان في سرية حياته الخاصة واتصالاته الشخصية حددتها **المادة 4** من **القانون 09-04** السالف الذكر.
- أقر المشرع الجزائري اللجوء إلى استعمال المراقبة الالكترونية أو تفتيش المنظومات المعلوماتية كوسيلة وقائية للحماية من وقوع جرائم معينة هي الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة أو الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني وفقا لما نصت عليه **المادة 4** فقرة(أ) و(ب). وبذلك خرج المشرع عن القاعدة التي تقتضي اللجوء إلى مثل هذه الإجراءات بعد وقوع الجريمة وليس قبلها. كما يلجأ إليها إذا دعت مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية، أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.
- لا يتخذ أمر اللجوء إلى المراقبة الالكترونية أو تفتيش المنظومات المعلوماتية إلا بموجب إذن من السلطة القضائية المختصة. وإذا تعلق الأمر بمنح الإذن بمراقبة الاتصالات الالكترونية في حالة الوقاية من الأفعال الموصوفة بجرائم

الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، فإن النائب العام لدى مجلس قضاء الجزائر هو الذي يختص بمنح إذن لمدة **6**أشهر لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

- ولم يكتف المشرع الجزائري بشروط تفتيش المنظومات المعلوماتية بل نص على ضمانات وقواعد شكلية خاصة بإجراءات الحجز نصت عليها **المادة 7** من **القانون09-04**، وحسنا فعل المشرع الجزائري ذلك للمحافظة على الأدلة الناتجة عن التفتيش.

ومع ذلك فقد كشفت هذه الدراسة عن **نقص بعض الضمانات** التي يوفرها التشريع الجزائري تتمثل في يلي:

- لم يحدد المشرع الجزائري وسائل المراقبة الالكترونية بموجب **القانون 09-04**، إنما اكتفى بما ذكره من ضرورة وضع الترتيبات التقنية الخاصة بالمراقبة، وفي هذا قصور يجب التنبه إليه.
- اكتفى المشرع الجزائري في **القانون 09-04** بالنص على أن الإجراءات تتخذ بموجب إذن من السلطة القضائية المختصة، في حين لم يحدد ما هي السلطة القضائية المختصة.
- عدم تحديد المشرع الجزائري صراحة للمدة التي يتم خلالها إجراء المراقبة الالكترونية ماعدا الحالة المتعلقة بحالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- خلو التشريع الجزائري من تنظيم عملية تنفيذ المراقبة الالكترونية وما يحيط بذلك من ضمانات.
- لم يشترط وجوب صدور إذن من السلطة القضائية المختصة بمناسبة إجراء تمديد تفتيش منظومة معلوماتية بل اكتفى بمجرد إخطار هذه السلطة أنه سيتم تمديده إلى منظومة معلوماتية أخرى مرتبطة، وفي هذا خطر من تعسف ضابط الشرطة القضائية أثناء قيامه بمهامه في تحديده للمنظومة المرتبطة.
- لم يبين المشرع الجزائري كيفية تحريز التسجيلات الناتجة عن المراقبة الالكترونية أو وكيفية إبقائها سليمة على نحو يمنع العبث بمحتوياتها. كما استنتجنا خلو التشريع الجزائري أيضا من بيان مصير التسجيلات والمستندات بعد انتفاء الغرض منها.
- عدم تحديد المشرع الجزائري للقواعد التي من شأنها أن تراعي حقوق الدفاع والمتعلقة على وجه الخصوص بوضع التسجيلات المتعلقة بالمراقبة الالكترونية ومحاضر تفريغها في ملف الدعوى وإبلاغ المتهم بحقه في الإطلاع عليها وتحضير دفاعه بشأنها.
- عدم تحديد الجزاء الإجرائي المترتب على عدم مراعاة الضمانات الإجرائية المنصوص عليها في **القانون09-04** ما إذا كان بطلان مطلق أو نسبي.

من حيث الاقتراحات:

وتبعا لذلك فإنه يتعين ضرورة وجوب إحاطة إجراء اللجوء إلى مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية بالضمانات التالية:

1- إعادة صياغة نص المادة 3 من القانون 09-04 والتي أحالت إلى تطبيق قواعد قانون الإجراءات الجزائية وذلك بذكر النصوص القانونية المحال إليها على وجه التحديد، وعدم الاكتفاء بعمومية النص لأن من شأن ذلك أن يوسع من نطاقه ويؤدي إلى الخروج عن نية وقصد المشرع.

2- يتعين على المشرع الجزائري في تعديلاته اللاحقة لهذا القانون أثناء تأكيده على وجوب توافر الإذن من السلطة القضائية أن يحدد هذه السلطة القضائية بدقة، على أن يشترط أيضا أن تتم عملية المراقبة أو التفتيش تحت الإشراف المباشر للسلطة القضائية المختصة.

2- وللارتباط بين تسجيل الأحاديث الخاصة والتقاط الصور فيجب أن تحظى المراقبة الالكترونية بنفس الضمانات الإجرائية من وجوب أن يتضمن الإذن بالمراقبة الالكترونية على بيانات معينة إلزامية كتحديد اسم الشخص المراد اتخاذ التدابير التقنية ضده، وطبيعة الاتصالات التي سيتم مراقبتها.

3- يجب على المشرع الجزائري أن ينص على مدة الإذن بمراقبة الاتصالات الالكترونية في الحالات التي لم يحدد فيها القانون ذلك بموجب نص المادة 4 من القانون 09-04، أو الإحالة إلى المواد 65 مكرر5 إلى 65 مكرر10 صراحة لتطبيق نفس الأحكام القانونية إذا كانت نية المشرع الإجرائي تتجه لذلك. مع وجوب تحديد عدد المرات التي يمكن فيها تجديد الإذن باللجوء إلى المراقبة الالكترونية على أن يكون الأمر مسببا، حتى لا تتعسف الجهة القضائية المختصة. وفي ذلك ضمان أكيد لحماية الحق في حرمة الحياة الخاصة.

4- يجب على المشرع الجزائري تعديل نص المادة 5 من القانون 09-04 وذلك بالنص على وجوب صدور إذن من السلطة القضائية المختصة بمناسبة إجراء تمديد تفتيش منظومة معلوماتية وعدم الاكتفاء بمجرد إخطار هذه السلطة بأنه سيتم تمديده إلى منظومة معلوماتية أخرى مرتبطة،لأن في هذا خطر من تعسف ضابط الشرطة القضائية أثناء قيامه بمهامه في تحديده للمنظومة المرتبطة.

5- يجب على المشرع الجزائري تضييق نطاق الأشخاص القائمين على تنفيذ إجراءات المراقبة الالكترونية، مع تبيان نوع ومكان الأجهزة الفنية التي يتم عن طريقها التصنت على الاتصالات أو تسجيلها.

6- ومن الضمانات الهامة التي يجب أن ينص عليها المشرع الجزائري في تنفيذ عملية مراقبة الاتصالات الالكترونية الإحالة إلى الإجراءات التي نص عليها قانون الإجراءات الجزائية من وجوب تفريغ أشرطة المراقبة في محضر وتحريزها عقب ذلك للمحافظة على سلامتها وعدم العبث بها، ويجب أن يوضع المحضر في ملف القضية مع الأحراز المختومة التي يجب أن تبقى في يد

القضاء. ويجب أن تتم هذه العملية كذلك تحت إشراف السلطة القضائية دائما لأن في ذلك إحدى الضمانات الأكيدة لحماية الحريات الفردية وأهمها الحق في حرمة الحياة الخاصة.

7- يجب أن ينص المشرع الجزائري على نص خاص يوجب على سلطة التحقيق إبلاغ المتهم باتخاذ إجراء مراقبة اتصالاته الالكترونية أو تفتيش منظومته المعلوماتية وما نتج عنها من أدلة مباشرة بعد الانتهاء من هذه العمليات. ويجب أن يمنح له الوقت الكافي للرد على هذه الأدلة ومناقشتها ودحضها، لأن في ذلك ضمان أكيد لصحة الإجراءات وعدم خرق حقوق الدفاع.

8- يجب أن ينص المشرع الجزائري على ضرورة محو أو إتلاف التسجيلات أو الصور أو المستندات المتحصل عليها من إجراء مراقبة الاتصالات الالكترونية أو تفتيش منظومة المعلوماتية بعد صدور حكم نهائي في الدعوى كما هو معمول به في التشريعات المقارنة.

9- وجوب النص على بطلان إجراء اللجوء إلى إجراء مراقبة الاتصالات الالكترونية أو تفتيش منظومة المعلوماتية صراحة إذا لم تراعى الضمانات المنصوص عليها قانونا، وتبعا لذلك عدم قبول النتائج المستمدة من هذه الأدلة.

الهوامش:

(1) د/ شيماء عبد الغني محمد عطا لله:" الحماية الجنائية للتعاملات الالكترونية، دراسة مقارنة بين النظامين اللاتيني والأنجلو أمريكي"، رسالة دكتوراه، جامعة المنصورة، 2005، ص286.

(2) جرم المشرع الجزائري من خلال نص المادة 303 مكرر3 من قانون العقوبات الجزائري الاعتداء على حرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

1 – بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

2 - التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه. بالتالي فالحديث الخاص أو السري للشخص أو صورته الملتقطة في مكان خاص تعد أهم عناصر الحق في حرمة الحياة الخاصة.

وتبعا لذلك فإن الحق في حرمة الحياة الخاصة وفقا لنص هذه المادة يتكون من عنصرين أساسين: الأحاديث الخاصة والسرية للأفراد والصورة.

(3) للمزيد من التفصيل في الموضوع راجع في هذه الأساليب التقنية والمشاكل التي تعترضها، د/ شيماء عبد الغني محمد عطاء الله: المرجع السابق، ص302.

(4) انظر في ذلك المادة2 فقرة (ب) من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

(5) انظر في ذلك المادة2 فقرة (ج) من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

(6) نص الفصل الأول من الباب الأول: الجنايات والجنح ضد الشيء العمومي، على الجنايات والجنح ضد أمن الدولة في المواد 61 إلى 96 مكرر والتي تشمل: جرائم الخيانة والتجسس، جرائم التعدي الأخرى على الدفاع الوطني أو الاقتصاد الوطني، الاعتداءات والمؤامرات والجرائم الأخرى ضد سلطة الدولة وسلامة أرض الوطن، جنايات التقتيل والتخريب المخلة بالدولة، الجرائم الموصوفة بأفعال إرهابية أو تخريبية وجنايات المساهمة في حركات التمرد.

(7) أنظر في ذلك المادة4 فقرة أخيرة من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

(8) يقصد بمقدمي الخدمات في مفهوم القانون 09-04 وفقا لما نصت عليه المادة 2 بند(د) هم:

- كل كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات.

- أي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

(9) انظر في المعطيات التي يتعين على مقدمي الخدمات حفظها نص المادة 11 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

(10) في إطار القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تقرر إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على أن تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم الذي لم يصدر بعد، لكن وفقا لما ذكره المشرع الجزائري في نص المادة 4 فقرة3 من هذا القانون فإنه سوف يكون ضمن تشكيلتها ضباط للشرطة القضائية.

(11) يجب في هذا الصدد مراعاة الشروط الخاصة بالتفتيش والتي سبق التعرض لها أهمها ضرورة أن يتم التفتيش بطريق مشروع وعدم التعسف في التفتيش.

(12) يستثنى من تطبيق هذه المادة المحامي والموثق والمحضر القضائي الذين يشترط موافقتهم للحصول على الوثائق والمعلومات الالكترونية الموجودة في نظام معلوماتي متعلق بهم.

(13) انظر الجريدة الرسمية للمناقشات الصادرة عن المجلس الشعبي الوطني بتاريخ 6جويلية2009، السنة الثالثة رقم122، ص22.

(14) انظر في هذه الضمانة الجريدة الرسمية للمناقشات الصادرة عن المجلس الشعبي الوطني بتاريخ 6جويلية2009، السنة الثالثة رقم122، ص22.

(15) تثور مشكلة التمييز بين الاتصالات التي تتناول موضوع الجريمة وتلك التي تمس بالحياة الخاصة. وبالتالي يتوجب على ضابط الشرطة القضائية الاحتياط أثناء الاحتياط أثناء المراقبة والقيام بتسجيل ما يفيد في الوقاية من الأفعال المذكورة دون غيرها.

(16) ذهب وزير العدل في شرحه للقانون 09-04 أمام البرلمان للمصادقة عليه إلى التأكيد على أن جميع الإجراءات المتخذة بشأن مراقبة الاتصالات الالكترونية أو تفتيش المنظومات المعلوماتية يجب أن تتخذ تحت ضمانة أن تتم هذه الإجراءات بعد تقديم تقرير يبين طبيعة الترتيبات والمعلومات المبحوث عنها. انظر الجريدة الرسمية للمناقشات الصادرة عن المجلس الشعبي الوطني بتاريخ 6 جويلية2009، السنة الثالثة رقم122، ص22.

(17) تعرف المعطيات المعلوماتية بأنها عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شانها جعل منظومة معلوماتية تؤدي وظيفتها. وهذا وفقا لما ذهبت إليه المادة2 فقرة (ج).

(18) من الطبيعي أن تختلف طريقة ضبط البيانات المعالجة أليا عن ما هو متبع عند ضبط الأشياء المادية كالمخدرات والأشياء المسوقة والسلاح المستخدم في الجريمة، وهو ما ذهبت إليه أيضا الاتفاقية الأوروبية لجرائم السيبر لسنة 2001 و التي أجازت أن يتم الضبط عن طريق اخذ نسخة من البيانات المخزنة على أي وسيط من وسائط التخزين الخاصة بالحاسب الآلي.

(19) شيماء عبد الغني محمد عطاء الله: المرجع السابق، ص 429.

(20)Cass.crim, 13oct1998: D2000; Rev.sc.crim2004, p69.

(21) وهو ما سعت إليه وزارة العدل التي تقوم بصفة دورية بتكوين قضاة متخصصين في الأشكال الجديدة من الإجرام وإرسالهم فترات تكوينية إلى الخارج وذلك للاستفادة من الخبرات الأجنبية في هذا الشأن.