مراقبة الاتصالات الالكترونية وحق الفرد في الخصوصية المعلوماتية

Electronic communications control and the right of informational privacy

تاريخ الإرسال: 2019/11/01	تاريخ القبول: 2020/09/14	تاريخ النشر: 2021/01/31

*ط.د. مرزوقي كريمة
جامعة مولود معمري- تيزي وزو
merzoukikarima0@gmail.com

ملخص :

أصبحت اليوم ثورة تكنولوجيات المعلومات والاتصالات تشكل عاملا مهما في انتهاك حياة الفرد من خلال التعدي على خصوصية معلوماته، حيث ساهم هذا التطور في تقييد الحقوق والحريات الأساسية للأفراد عن طريق جمع وحفظ ومعالجة البيانات الخاصة بهم. كما سهلت هذه الثورة من ناحية أخرى ارتكاب عدة أنواع من الجرائم الخطيرة الأكثر تعقيدا وتنظيما يصعب اكتشافها ونسبتها لمرتكبيها.

كل هذا حتم علينا إيجاد وسيلة تتلاءم مع هذا النوع من الإجرام. وهو ما ذهب إليه المشرع الجزائري من خلال استحداث إجراء مراقبة الاتصالات الالكترونية كإجراء جديد تمليه الضرورة لمواجهة الإجرام المستحدث. إلا أن هذه الوسيلة بدورها تؤدي إلى انتهاك الخصوصية المعلوماتية، لهذا قام المشرع بتقييدها بمجموعة من الضوابط والحدود حماية لحقوق وحريات الأفراد.

الكلمات المفتاحية : الاتصالات الالكترونية، المراقبة، الخصوصية المعلوماتية، الإجرام المستحدث .

Abstract:

Today, the information and communication technologies (ICT) revolution has become an important factor in violating one s life, by infringing on the privacy of information. This development has restricted the fundamental rights and freedoms of individuals by collecting, preserving and processing their data.

*المؤلف المرسل: مرزوقي كريمة

On the other hand, this revolution has facilitated the commission of several types of serious and more complex and organized crimes that are difficult to detect and attribute to the perpetrators.

Consequently. it is indespensible to find a way to deal with this type of crimes.This is what the Algerian legislator went through the introduction of electronic communications control as a new measure dictated by the necessity to face the new crime. However, this method in turn leads to a violation of information privacy , so the legislator restricted it with a set of controls and borders to protect the rights and freedoms of individuals.

***Keywords**: Electronic Communications; Surveillance ; information Privacy ; crime.*

مقدمة:

تعاني المجتمعات في الآونة الأخيرة من انتهاك الخصوصية بما فيها الخصوصية المعلوماتية، وذلك في ظل انتشار ثورة تكنولوجيات المعلومات والاتصالات التي نتج عنها تدفق المعلومات عن طريق استعمال أجهزة الكمبيوتر وشبكة الانترنت[1].

وقد صاحب هذا التطور تزايد ملحوظ في الاعتماد على النظم المعلوماتية التي تلعب دورا بارزا في تقدم المجتمع الحديث، الذي أصبح يعتمد على المعلوماتية باعتبارها عصب الحياة الاقتصادية والسياسية والاجتماعية، إلا أن هذه النظم شكلت خطرا على حق الفرد في خصوصية معلوماته، حيث ساهمت في تقييد الحقوق والحريات الأساسية للأفراد عن طريق جمع وحفظ ومعالجة البيانات الخاصة بهم، الأمر الذي دفع بالدول إلى العمل للوصول إلى إقرار حماية للحق في الخصوصية المعلوماتية، لذا حرص الإعلان العالمي لحقوق الإنسان ومختلف الاتفاقيات الدولية والإقليمية على التأكيد على حماية حق الإنسان في الخصوصية وفي سرية مراسلاته ومحادثاته، كما أحاط معظم دساتير وقوانين الدول بما فيها الجزائر هذا الحق بحماية دستورية وجنائية وذلك بنصها على معاقبة كل من يعتدي عليه.

ومع ذلك فإن مستوى حماية الخصوصية التي توفرها معظم التشريعات أصبحت اليوم غير كافية، خاصة أمام انسكاب البيانات يوما بعد يوم، فالانترنت تخلق مناطق

جديدة ومساحة واسعة للتحايل على الحدود التشريعية[2]، وبذلك يبقى الحق في الخصوصية المعلوماتية محل انتهاك لاسيما أمام تعزيز القدرة المتنامية لأجهزة الدولة على إجراء المراقبة الإلكترونية من خلال اعتراض وتسجيل محتوي الاتصالات والمراسلات الالكترونية سرا دون علم المعني بالأمر، وقد خلق هذا النوع من الانتهاك قلقا لدى المواطنين في معظم الدول، بسبب التطور المتزايد لوسائل التكنولوجيا الحديثة.

كما تسبب أيضا هذا التطور في تسهيل تطوير الجرائم كالجريمة المنظمة والجرائم المعلوماتية ....، فهي كلها جرائم خطيرة بالنظر للأضرار التي تلحقها بمصالح الدولة من جهة، ومن جهة أخرى صعوبة اكتشافها ونسبتها لمرتكبها بالاعتماد على الوسائل التقليدية التي أصبحت عاجزة وغير كافية، فلم يكن أمام المشرع الجزائري إلا استحداث المراقبة الإلكترونية كإجراء جديد لمواجهة الإجرام المستحدث.

وعلية فالمراقبة الإلكترونية إجراء استثنائي تمليه الضرورة، وباعتباره انتهاك لحق الخصوصية المعلوماتية، كان لزاما على المشرع الجزائري لأجل تحقيق التوازن بين حق الفرد في الخصوصية وحق المجتمع في مكافحة الجريمة، أن يقيد هذا الإجراء بمجموعة من الضمانات حماية من التعسف في استخدامه من طرف الجهة المختصة به.

تتمحور على هذا النحو إشكالية هذه الدراسة في معرفة **مدى توفير حماية للحق في الخصوصية المعلوماتية، ومدى تعرضه للانتهاك أثناء مراقبة الاتصالات الالكترونية؟**

وللإجابة عن هذه الإشكالية ارتأينا تقسيم موضوع هذه الدراسة إلى مبحثين:

المبحث الأول: الحق في الخصوصية المعلوماتية بين الحماية والانتهاك.

المبحث الثاني: مراقبة الاتصالات الالكترونية إجراء جديد لمواجهة الإجرام المستحدث.

المبحث الأول : الحق في الخصوصية المعلوماتية: بين الحماية والانتهاك

شهد العالم تطورا ملحوظا في تكنولوجيات المعلومات والاتصالات، وبذلك ظهر ما يعرف بالفضاء الرقمي[3] أين تتفاعل المجتمعات البشرية بأسرها في مختلف جوانب الحياة، وهكذا توسع نطاق الخصوصية من المادي إلى الافتراضي وبذلك ظهر ما يعرف بالحق في الخصوصية المعلوماتية.

يعتبر الحق في الخصوصية المعلوماتية من الحقوق الشخصية اللصيقة بالإنسان، وحفاظا عليه من كل مساس وانتهاك تمت حمايته من خلال تكريسه دوليا وداخليا (المطلب الأول)، غير أن التزايد المستمر لتطور تقنية المعلوماتية، وانتشار ظاهرة جمع البيانات والمعلومات الخاصة وتخزينها ومعالجتها على الحاسوب الآلي، وتسهيل المعاملات والتواصل بين المجتمعات باستعمال شبكة الانترنت نتج عنه تعدد صور انتهاك الخصوصية المعلوماتية لاسيما باستحداث المراقبة الالكترونية (المطالب الثاني).

المطلب الأول : حماية حق الخصوصية المعلوماتية

حظي الحق في الخصوصية بما فيه الخصوصية المعلوماتية بالاهتمام اللازم من طرف معظم الدول، وقد تبلور هذا الاهتمام بصدور الإعلان العالمي لحقوق الإنسان عن الأمم المتحدة، كما اهتمت به الاتفاقيات الدولية والإقليمية (الفرع الأول)، واهتم المشرع الجزائري هو الآخر بالحق في الخصوصية المعلوماتية وكرس له حماية دستورية وقانونية

الفرع الأول : الجهود الدولية المكرسة لحماية الحق في الخصوصية المعلوماتية

دفع التطور الهائل لتكنولوجيات الإعلام والاتصال وظهور ما يعرف بالثورة المعلوماتية، إلى تضافر الجهود الدولية والإقليمية لحماية حق الخصوصية من كل اعتداء من طرف الغير، بحيث اهتمت العديد من المنظمات الدولية وعلى رأسها منظمة الأمم المتحدة بموضوع حماية الخصوصية المعلوماتية، تجسد ذلك في الإعلان العالمي لحقوق الإنسان[4]، الذي أكد حماية الحق في الخصوصية بما فيه الخصوصية المعلوماتية وأولاه أهمية خاصة، ويتضح ذلك من خلال نص المادة 12 منه التي تهدف إلى إضفاء الحماية اللازمة لحق الإنسان في خصوصيته.

إلا أنه يبقي الإعلان العالمي لحقوق الإنسان غير ملزم على الدول الأعضاء، لذلك فإن تطبيق مبادئه اختلف من دولة لأخرى من الدول الأعضاء، حسب الظروف السياسية والاقتصادية والاجتماعية، وطبيعة سكانها ونوع الحكم فيها، وبالرغم من عدم الزاميته إلا

أنه ضمن حماية حقوق وكرامة الإنسان[5]، بما فيها الخصوصية المعلوماتية من خلال منع تعرض الفرد لأي تعسف من طرف الغير.

كما تضمن العهد الدولي للحقوق المدنية والسياسية مجموعة من المبادئ المتعلقة بحقوق الإنسان، ومن أهمها الحق في الخصوصية وهو ما تضمنته المادة 17 منها، والتي يتضح من محتواها أن العهد الدولي أكد على كفالة كل من الحريات العامة وحماية الحق في الخصوصية بما فيها الخصوصية المعلوماتية من خلال منع الاعتداء على المراسلات الشخصية، سواء من طرف الأفراد أو من قبل الدولة، وقد جاء ملزما لجميع الدول الأعضاء الموقعة عليه، بخلاف الإعلان العالمي الذي لا يعتبر ملزما لاقتصاره على فرض التزامات أدبية باحترام ما تناوله من قواعد تتعلق بحقوق الإنسان[6].

ورغم الجهود المبذولة لحماية الحق في الخصوصية المعلوماتية فإنها تبقي غير كافية في مواجهة الانتهاكات التي يتعرض لها هذا الحق، كما أن الحماية المكرسة سواء في الإعلان العالمي لحقوق الإنسان أو العهد الدولي للحقوق المدنية والسياسية جاءت بصفة غير مباشرة وغير صريحة، بدون أن تبين المعلومات التي تتمتع بحماية خاصة، والطريقة التي يتعرض لها هذا الحق للاعتداء من طرف الغير.

وعليه بدأ الاهتمام أكثر بالحق في الخصوصية المعلوماتية بعد انعقاد مؤتمر طهران في الفترة مابين 22 أفريل و13 ماي 1968، حيث اعتبر محركا أساسيا حول مدى تأثير التطور التكنولوجي على مجال حقوق الإنسان وحرياته، وبالخصوص على حماية الحياة الخاصة والبيانات الشخصية. وانطلاقا من هذا المؤتمر بدأت العديد من الهيئات والمؤسسات تساهم في إرساء الخصوصية المعلوماتية، بحيث وضعت منظمة التعاون الاقتصادي والتنمية إبتداءً من عام 1978 قواعد إرشادية من أجل حماية الخصوصية ونقل البيانات[7].

كما لعب مجلس أوروبا دورا كبيرا في إخراج ووضع اتفاقية عالمية بشأن حماية الخصوصية، حيث تبنت لجنة وزراء أوروبا في 28 جانفي 1981 اتفاقية "حماية الأفراد في نطاق المعالجة الآلية للبيانات الشخصية" المعروفة باسم الاتفاقية رقم 108[8].

واهتم الاتحاد الأوربي هو الآخر بموضوع حماية المعطيات والبيانات الخاصة في نفس اللحظة التي طرحت فيها مسألة الاهتمام بحقوق الإنسان على المستوى العالمي منذ منتصف سبعينات القرن المنصرم، حيث أولت الهيئة جهودا بشأن توحيد القواعد المقررة

في قوانين حماية الخصوصية ابتداء من 1976 فصدرت عنه تعليمات عديدة منها ما يتعلق بحماية الأفراد من أنشطة التقييم الآلي للبيانات، وحماية الأفراد في مواجهة التطوير التقني في معالجة البيانات[9].

وقد حددت الأمم المتحدة وفقا للقرار 45/195 مجموعة من المبادئ التوجيهية لتنظيم الملفات الشخصية المحسوبة و10 مبادئ رئيسية منها تتعلق بحماية البيانات، وتطبيق هذه المبادئ في المقام الأول على التشريعات الوطنية ولكنها ملزمة أيضا للمنظمات الحكومية الدولية[10]، وإلى جانب هذا قدم الاتحاد الأوربي سنة 1995 حزمة أدلة توجيهية متكاملة حول حماية الأشخاص الطبيعيين فيما يتعلق بتجهيز البيانات الشخصية وحرية تنقل هذه البيانات، والتي تكملها توجيهات 2002 و2006، وكذلك توجيه 2009[11].

جاءت هذه النصوص لحماية حق الخصوصية المعلوماتية، إلا أنها لم تتحدث بشكل مباشر عن عملية المراقبة الالكترونية الناتجة عن التطورات التكنولوجيا الهائلة التي زادت من قدرة الدول على المراقبة وجمع البيانات، وهو ما قد يؤدي إلى انتهاك حق الأفراد في خصوصيتهم، لذلك ظهرت العديد من التوجهات الدولية بهذا الشأن أهمها قرار الجمعية العامة للأمم المتحدة رقم (176/68) الذي جاء تحت عنوان "الحق في الخصوصية في العصر الرقمي"[12] والذي يعتبر أحدث الجهود الدولية التي تهدف إلى حماية الحق في الخصوصية المعلوماتية، حيث عبرت عن قلقها بشأن القدرة المتنامية للمؤسسات الحكومية على الوصول إلى خصوصية الأفراد من خلال المراقبة عبر الوسائل التكنولوجية سواء كان الأشخاص المراقبين داخل الدولة أو خارجها.

وقد تضمن هذا القرار مجموعة من ستة (06) توصيات تهدف إلى الحد من الأثر السلبي الذي يمكن أن تخلفه مراقبة الاتصالات واعتراضها وجمع البيانات على حقوق الإنسان، وأكدت أن الحق في الخصوصية هو حق من حقوق الإنسان، ومشددة على أن حقوق الإنسان المحمية خارج الفضاء الإلكتروني يجب أن تكون محمية داخل الفضاء الإلكتروني[13]، كما يجب على الدول الأعضاء أن تعيد النظر في إجراءاتها وممارستها وتشريعاتها المتعلقة بالمراقبة الالكترونية، وذلك بهدف تأكيد الحق في الخصوصية تنفيذا لالتزاماتها بموجب القانون الدولي لحقوق الإنسان[14].

ويتضح من استقراءنا لهذه النصوص المكرسة لحق الخصوصية بما فيها الخصوصية المعلوماتية أنها أكدت الحفاظ على الحق في الخصوصية، ومنعت تعرضه لأي اعتداء من طرف الغير سواء الأفراد أو الدولة.

الفرع الثاني : الجهود الداخلية المكرسة لحماية حق الخصوصية المعلوماتية في التشريع الجزائري

يتجسد مبدأ حق الخصوصية المعلوماتية على المستوى الوطني من خلال مجموعة الضمانات القانونية المقررة بموجب أحكام الدستور، وذلك بنصه على ضمان حرمة الحياة الخاصة للمواطن وضمان سرية المراسلات والاتصالات الخاصة بكل أشكالها، إضافة إلى الحماية الجزائية التي كرسها المشرع الجزائري في قانون العقوبات وبعض القوانين الخاصة، وذلك من خلال توقيع العقاب على كل من يعتدي على الحق في الخصوصية المعلوماتية.

أولا : الضمانات الدستورية لحماية حق الخصوصية المعلوماتية

يعتبر الحق في الخصوصية المعلوماتية مبدأ دستوري أقرته معظم الدساتير، ومنها الدستور الجزائري الذي كرس حماية حق الإنسان في حياته الخاصة من خلال دستور 1996[15] في المادة 39 التي تنص على: **"لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه، ويحميها القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".**

يتبين من محتوى هذا النص أن الدستور الجزائري أولى الحق في الخصوصية المعلوماتية اهتماما، من خلال تكريس حماية لسرية المراسلات والاتصالات الخاصة من كل انتهاك تتعرض لها، إلا أنه لم يحدد الوسيلة المستعملة لانتهاك هذا الحق، كما أنه لم يحدد طبيعة المراسلات والاتصالات المحمية، وهذا دليل على أن كل أنواع المراسلات والاتصالات محمية، ويظهر ذلك من خلال قوله "بكل أشكالها مضمونة".

وقد تم تعزيز حماية الحق في الخصوصية من خلال التعديل الدستوري 2016[16]، حيث تم تعويض المادة 39 السابقة الذكر بالمادة 46 التي أضيف لها فقرتان إلى جانب محتوى المادة 39، فكرس حماية الحق في الخصوصية المعلوماتية صراحة وفقا للفقرة 04 من المادة 46[17] من خلال نصه على حماية الأشخاص الطبيعيين في مجال معالجة

المعطيات ذات الطابع الشخصي، واعتبره حقا أساسيا يضمنه القانون ويعاقب على انتهاكه.

يتضح أن الدستور الجزائري أولى أهمية كبيرة لحق الخصوصية المعلوماتية، خاصة من خلال التعديل الدستوري 2016 الذي كرس صراحة حماية كل أشكال المراسلات والاتصالات الخاصة واعتبره حقا أساسيا مضمونا قانونا، ويعاقب كل من يحاول الاعتداء عليه سواء من طرف الأفراد أو الدولة، ولم يكتف التشريع الجزائري بوضع حماية دستورية للحق في الخصوصية المعلوماتية بل سعى أيضا لوضع حماية جزائية من خلال عدة نصوص قانونية.

ثانيا : الحماية الجزائية لحق الخصوصية المعلوماتية

كرس المشرع الجزائري الحماية الجزائية للحق في الخصوصية المعلوماتية، من خلال استحداث نصوص تجريمية خاصة لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم 04-15[18] بإضافة القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" وفقا للمواد 394 مكرر إلى 394 مكرر 7.

وقد كان تدخل المشرع الجزائري في مجال الخصوصية المعلوماتية فعالا بالرغم من تأخره، بحيث جرم من خلاله مجموعة من الأفعال التي يقترفها الأشخاص بواسطة الحاسب الآلي لغرض انتهاك خصوصية الغير[19].

وحاول المشرع الجزائري من خلال تجريم الاعتداء على المعلوماتية تكريس حماية لحق خصوصية الأفراد داخل الفضاء الرقمي، ومعاقبة كل من تسول له نفسه انتهاك خصوصية غيره من خلال التعدي على المنظومة المعلوماتية سواء بالدخول أو البقاء عن طريق الغش، وغيرها من صور الاعتداء.

و تم تكريس أيضا حماية جزائية للحق في الخصوصية في مختلف القوانين الخاصة من بينها القانون رقم 2000-03 المؤرخ في 2000/08/05 والذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية[20]، حيث سارع هذا القانون إلى مواكبة التطور الذي شهدته التشريعات العالمية بهدف مسايرة التطور التكنولوجي، من خلال إحاطة سرية المراسلات بحماية خاصة من أي انتهاك[21] ورتب عقوبة على كل من يقوم بفتح أو تحويل أو تخزين البريد، أو القيام بانتهاك سرية المراسلات وفقا للمادة 137 من قانون العقوبات الجزائري، وهو ما تؤكده المادة 127 من القانون رقم 2000-03 أعلاه.

ولم يكتف المشرع الجزائري بهذه الحماية فقط، بل تبنى نصوصا جديدة خلال تحديث المنظومة التشريعية بموجب القانون رقم 06-23 السابق الذكر، وذلك بتوقيع العقاب على كل من حاول المساس بحرمة الحياة الخاصة للأشخاص عن طريق التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة، أو التقاط أو تسجيل أو نقل صورة بغير موافقة صاحبها أو رضاه[22]، أو فض و إتلاف رسائل أو مراسلات موجهة إلى الغير بسوء نية وهو ما نصت عليه المادة 303 .

ويتبين من خلال هذه النصوص القانونية أن المشرع الجزائري أقر حماية جزائية للحق في الخصوصية بما فيها المعلوماتية من خلال حماية صور الأفراد ومكالماتهم أو أحاديثهم الخاصة، وحماية الرسائل والمراسلات الموجهة للغير، ومنع انتهاكها من طرف الغير، وهذا يعتبر ضمانة والتزاما منه بحماية حقوق الأفراد.

وقد تم تعزيز هذه الحماية أيضا من خلال سن القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 04 منه التي تضمن حماية هذا الحق في حالة المساس به من طرف الغير.

ومن تحليلنا للنصوص السابقة يتضح أن المشرع الجزائري كرس حماية دستورية وقانونية للحق في الخصوصية المعلوماتية، إلا أنها تبقى غير كافية لاسيما أمام توفر الوسائل الدقيقة التي أنتجها التطور التكنولوجي وسهولة الحصول عليها، وهو ما سهل استعمالها من طرف الأشخاص حيث تساعدهم في الحصول على معلومات تمس خصوصية الغير، وبذلك تعددت صور انتهاك الخصوصية المعلوماتية.

المطلب الثاني : صور انتهاك الخصوصية المعلوماتية

أصبح العالم الإفتراضي يهيمن من خلال وسائله وأدواته على حقوق الإنسان في مختلف المجالات، مما أدى إلى ظهور أنماط جديدة لانتهاك الحقوق بما فيها حق الخصوصية المعلوماتية، وهذا نتيجة لتطور التكنولوجية المعلوماتية بشكل كبير، الأمر الذي أدى إلى صعوبة حصر صور هذا الانتهاك. سنحاول من خلال دراسة هذا المطلب الإشارة إلى أبرز الانتهاكات التي تمس حق الخصوصية نتيجة استخدام النظم المعلوماتية التي يتم من خلالها إدخال وإخراج مختلف البيانات والمعلومات هذا من جهة(الفرع الأول) و من جهة أخرى استخدام شبكة الانترنت التي فتحت مجالات عديدة للاستفادة منها، ولكن في نفس الوقت أدت إلى سهولة انتهاك الخصوصية لاسيما من خلال استعمال البريد

الإلكتروني الذي يتم من خلاله تبادل البيانات والمعلومات والصور وغيرها من الأمور(الفرع الثاني).

الفرع الأول : انتهاك الخصوصية من خلال النظم المعلوماتية

تعتبر النظم المعلوماتية في العصر الحديث مستودعا خطيرا للكثير من أسرار الناس التي يمكن الوصول إليها بسهولة وسرعة دون بذل أي جهد، فأصبحت محل لانتهاك الخصوصية المعلوماتية.

ويتحقق انتهاك الخصوصية داخل النظم المعلوماتية، بالإفشاء غير المشروع للبيانات والمعلومات الاسمية، عن طريق نقل البيانات الاسمية من قبل المسيطرة عليها بمناسبة معالجتها، أو حفظها، أو نقلها إلى شخص أو وجهة غير مختصة بتلقي هذه البيانات، فعليه لا يعتبر تخزين البيانات حتى ولو كان برضي المعنى بالأمر أنها قابلة للتداول، ولا يعني كذلك أنها انتقلت من حالة الخصوصية إلى حالة العلانية عن طريق الاطلاع عليها من قبل عدد كبير من الأشخاص العاملين في مجال المعلوماتية، ومن ثم تنتهك سريتها وقد تصل في أحيان كثيرة إلى ابتزاز الشخص الذي تتعلق به هذه المعلومات[23].

كما يحدث انتهاك الخصوصية المعلوماتية من خلال التلاعب غير المصرح به بالمعلومات في صورة إدخال معلومات صحيحة غير مصرح بإدخالها، أو عن طريق تغذية النظام المعلوماتي بمعلومات مغلوطة أو غير صحيحة، كما يحدث أيضا التلاعب بتغيير المعلومات داخل النظام واستبدالها بمعلومات أخرى[24] ، أو عن طريق المحو بإزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام، أو نقل وتخزين جزء منها في المنطقة الخاصة بالذاكرة[25].

كل هذه الصور تؤدي إلى انتهاك صارخ لخصوصية الأفراد، خاصة أمام الانتشار الواسع للنظم المعلوماتية، التي يسعى الجميع للتعامل معها، واعتبارها وسيلة لممارسة كافة نشاطاتهم الحياتية. والتي تتم من خلال أجهزة اتصال لاسيما "شبكة الانترنت"[26] التي تنعكس هي الأخرى سلبا على خصوصية الأفراد.

الفرع الثاني : انتهاك الخصوصية المعلوماتية باستعمال الانترنت

تعتبر شبكة الانترنت أحد تطبيقات الثورة التكنولوجية المعلوماتية في شتي مجلات الحياة، وإلى جانب الايجابيات التي أنتجتها، انعكست في المقابل سلبيا على خصوصية الأفراد بسبب تزايد استخدام النظم المعلوماتية المتصلة بشبكة الانترنت من جانب

الشركات والسلطات العامة، حيث أن الكثير من المعاملات التي يقوم بها الأفراد في مختلف البلدان تظهر الآن على شبكة الانترنت، وبالتالي سيكون من الممكن توزيع البيانات الخاصة عن بعد[27]، وعليه فالخصوصية المعلوماتية محل انتهاك بسبب هذه التغيرات لاسيما من خلال اعتراض مراسلات البريد الالكتروني، حيث يعتبر الحق في سرية المراسلات عبر البريد الالكتروني من الحقوق الشخصية المكفولة دستوريا وقانونيا، وكل انتهاك لسرية المراسلات يعتبر صورة من صور انتهاك الخصوصية المعلوماتية.

وفي الوقت الحالي أصبح من السهل تعرض مستخدم البريد الإلكتروني إلى انتهاك خصوصيته والتوصل إلى معلوماته السرية أو الشخصية من طرف الأفراد أو الدولة، ويعود ذلك إلى تطور التقنيات المستخدمة في اختراق أجهزة الحاسب الآلي الذي ينتج عنه تسريب البيانات الرئيسية والمعلومات الخاصة بمستخدم البريد الإلكتروني[28].

فقد يتحقق انتهاك الخصوصية المعلوماتية باستعمال البريد الالكتروني عن طريق اعتراض المراسلات والاتصالات الالكترونية لغرض معرفة محتواها، إضافة إلى التنصت بالإطلاع على المحادثات الخاصة التي تجري عبر شبكة الانترنت سرا دون موافقة أطراف المراسلة، وكما يعتبر أيضا التقاط الصور أو نقلها من الانتهاكات التي تمس الخصوصية، باعتبار الصورة حق من حقوق الخصوصية يحضر على الغير التقاطها أو نقلها عبر شبكة الانترنت دون موافقة صاحبها.

كما أدى الانتشار الواسع لشبكة الانترنت إلى ظهور الفيروسات التي تعتبر صورة من صور انتهاك الخصوصية المعلوماتية، إذ يعتبر المتخصصون هذا الفيروس بأنه مرض يصيب الحاسوب وهو عبارة عن برنامج صغير يزرع بالأقراص والأسطوانات الخاصة بالحاسب لأهداف تخريبية، مثل تدمير البيانات والمعلومات المخزنة داخل الحاسوب أو تعديلها، أو استخدام المعلومات بصورة غير مشروعة[29].

بالرغم من خطورة هذه الانتهاكات على الخصوصية المعلوماتية لاسيما مراقبة الاتصالات الإلكترونية واعتراض المراسلات والتقاط وتسجيل الصور والأحاديث الخاصة، إلا أن المشرع الجزائري أقر مشروعيتها كاستثناء للحق في الخصوصية المعلوماتية بهدف مواجهة الإجرام المستحدث.

المبحث الثاني : مراقبة الاتصالات الالكترونية إجراء جديد لمواجهة الإجرام المستحدث

يرد على القاعدة العامة التي تعتبر المراقبة الالكترونية انتهاك للحق في الخصوصية استثناء يجيز هذا الإجراء وذلك دفعا لضرر أكبر، وهو حق المجتمع في الكشف عن الجريمة ومواجهتها، وهذا لاعتبار أن حق أفراد المجتمع في الأمن وفي الحفاظ على حقوقهم يعلو على حق المجرمين أو المشتبه فيهم في الحفاظ على حقهم في السرية، والخصوصية بما فيها الخصوصية المعلوماتية.

وعليه فالضرورة تقتضي اتخاذ بعض الإجراءات الماسة بالخصوصية من أجل الكشف عن الحقيقة، مما يؤدي إلى وجوب تقرير مشروعية هذه الإجراءات. وهذا ما ذهب إليه المشرع الجزائري من خلال إقرار مشروعية المراقبة الالكترونية كإجراء استثنائي وتقييده بمجموعة من الضمانات القانونية (المطلب الأول)، إضافة إلى إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال تتولى تنفيذ إجراء المراقبة الالكترونية (المطلب الثاني).

المطلب الأول : مراقبة الاتصالات الالكترونية في التشريع الجزائري

تعتبر المراقبة الإلكترونية استثناءا لمبدأ الحق في الخصوصية المعلوماتية، تتم عن طريق مراقبة المراسلات الالكترونية وتسجيل الأصوات والتقاط الصور بوسائل جد متطورة، وهذا نتيجة للثورة التكنولوجية الحديثة التي لعبت دورا هاما في ظهورها.

وعمل المشرع الجزائر على إقرار المراقبة الالكترونية كإجراء استثنائي من خلال استحداث القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (الفرع الأول)، وسعيا من المشرع الجزائري لتخفيف التأثيرات السلبية لهذا الإجراء على حماية الحق في الخصوصية المعلوماتية، ومحاولة منه إيجاد نوع من التوازن بين المصلحة الفردية والمصلحة العامة، عمل على وضع مجموعة من الضمانات القانونية التي تقيد اللجوء لإجراء المراقبة الالكترونية (الفرع الثاني).

الفرع الأول : إقرار مشروعية مراقبة الاتصالات الالكترونية كإجراء استثنائي

تم إقرار مشروعية مراقبة الاتصالات الإلكترونية كإجراء استثنائي لمواجهة الإجرام المستحدث، تجسيدا لمضمون الاتفاقيات الدولية[30] التي نادت بضرورة استخدام مثل هذا الإجراء في ظل التطورات التي يشهدها الإجرام المنظم، وعملا بمبدأ سمو المعاهدات

الدولية على القوانين الداخلية بادرت الجزائر على تكريس هذا الإجراء صراحة بموجب القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك وفقا لنص كل من المادتين 03 و04 اللتان عبرتا صراحة عن إجازة اللجوء لإجراء المراقبة الإلكترونية في مواجهة الجرائم المعلوماتية.

وعلى هذا النحو خرج المشرع الجزائري عن القاعدة العامة التي تقتضي تنفيذ إجراءات التحقيق عند ارتكاب الجريمة لجمع الأدلة والقرائن، وجعل مراقبة الاتصالات الالكترونية مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة، من خلال القيام بعمليات المراقبة المسبقة، وهو ما نصت عليه المادة 3 من القانون أعلاه التي حددت دواعي اللجوء إلى مراقبة الاتصالات الالكترونية، المتمثلة في مقتضيات حماية النظام العام، ومستلزمات التحريات أو التحقيقات القضائية الجارية[31].

وقد أدرج المشرع الجزائري هذه الآلية ضمن التدابير الوقائية من الجرائم التي ترتكب بواسطة المعلوماتية، إلى جانب منح إمكانية القيام بإجراء مراقبة الاتصالات الالكترونية في إطار التحريات والتحقيقات القضائية بهدف الوصول إلى أدلة لا يمكن الوصول إليها دون اللجوء إلى هذه الآلية، يمكن كذلك تطويع هذه الآلية لكي تعمل في بيئة الرقابة لغرض الوقاية من احتمال وقوع جرائم خطيرة من شأنها تهديد كيان الدولة و هو ما قررته المادة 4 من القانون رقم 09-04 السابق ذكرها التي منحت إمكانية القيام بعمليات المراقبة الالكترونية للاتصالات للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة وكذا في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني.

وتهدف هذه الآلية كذلك إلى تعزيز التعاون الدولي في مكافحة الإجرام المستحدث في مجال المعلوماتية، ذلك أن هذا الإجرام أصبح عابرا للحدود الوطنية ولا يرتبط في كثير من الأحيان بمكان معين. ويكون ذلك في إطار المساعدة الدولية المتبادلة وفقا لما نص عليه القانون والاتفاقيات الدولية في هذا الشأن[32].

وعليه لا يجوز اللجوء إلى إجراء المراقبة الالكترونية[33]، إلا في الحالات المذكورة في المادة 04 من القانون رقم 09-04 كما يلي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في 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 الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

يتضح من خلال استقراء هذه الحالات أن المشرع الجزائري قلص من الحالات التي يمكن اللجوء فيها إلى إجراء المراقبة الإلكترونية وحصرها في الجرائم التي تمس الأمن الوطني، وحالات تنفيذ المساعدة القضائية ومقتضيات التحريات والتحقيقات القضائية[34]، إلا أنه لم يحدد على سبيل الحصر الجرائم المعنية بهذه المراقبة مما يتضح أنه يمكن تطبيقها على جميع الجرائم في حالة توفر ضرورة التحريات ومستلزمات التحقيقات القضائية.

وتتضمن المراقبة الالكترونية اعتراض الاتصالات[35] والبيانات الهاتفية واستخدام أجهزة التنصت المختلفة، والدارة التلفزيونية المغلقة، ونظم التعرف على لوحات أرقام السيارات وغيرها من الأجهزة[36]، بهدف المنع والكشف عن الجرائم الخطيرة التي تهدد حياة الأفراد والجماعات، هذا ما جعل من الضروري التنازل عن حماية الحق في الخصوصية في مواجهة النشاطات الإجرامية الخطيرة، فمع تطور الجريمة والأساليب المستعملة في اقترافها استوجب اللجوء لهذا الإجراء استثناءا في الحالات المذكورة على سبيل الحصر لتمكين الجهات القضائية من وضع حد لمثل هذه الجرائم، إلا أن المشرع الجزائري لم يترك هذا الإجراء دون رعاية قانونية بل قيده بمجموعة من الضمانات.

الفرع الثاني : تقييد إجراء المراقبة الالكترونية بمجموعة من الضمانات القانونية

حرص المشرع الجزائري على تحديد الضمانات التي تسمح باللجوء لإجراء المراقبة الالكترونية للحد من التعسف في استخدامه من طرف السلطة المختصة به، وحفاظا على الحق في الخصوصية المعلوماتية من كل اعتداء عليه، فقد اشترط للجوء إلى مراقبة الاتصالات الالكترونية الحصول على إذن من طرف السلطة القضائية (أولا)، إضافة إلى

الاحتفاظ بالسرية (ثانيا) واستعمال المعطيات المتحصل عليها عن طريق المراقبة في حدود ضيقة (ثالثا)

أولا : ضرورة الحصول على إذن من طرف السلطة القضائية المختصة

يعد الإذن من بين الضمانات التي وضعها المشرع الجزائري لمراقبة الاتصالات الالكترونية، حفاظا على خصوصية الأفراد بما فيها الخصوصية المعلوماتية، وبذلك نصت الفقرة 2 من المادة 14 من القانون رقم 09-04 السابق الذكر علي أنه لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب صادر عن السلطات القضائية المختصة دون تحديد فيما تتمثل هذه السلطة، إلا أنه بالرجوع إلى المادة 3 من نفس القانون نجد أنها نصت على: **" ...مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات ... ووفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية".**

ويتبين أن المشرع الجزائري أحال بصفة صريحة إلى قانون الإجراءات الجزائية بخصوص ما يتعق بمحتوى المادتين 3، 4 من قانون 09-04، وعليه تتمثل إذن السلطة القضائية المختصة في منح الإذن بمراقبة الاتصالات الالكترونية في وكيل الجمهورية قبل فتح التحقيق أو قاضي التحقيق في حالة فتح تحقيق قضائي هذا كقاعدة عامة.

كما يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضابط الشرطة القضائية المنتمية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، إذن لمدة 06 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها، وهذا عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة[37].

وعليه لا يتم القيام بمراقبة الاتصالات الالكترونية إلا بإذن مكتوب من السلطات القضائية المختصة، غير أن ما يلاحظ هو سكوت المشرع الجزائري عن تحديد مدة الإذن للقيام بعملية المراقبة، مكتفيا فقط بتحديد مدة الإذن الممنوح من طرف النائب العام لدى مجلس قضاء العاصمة ب 6 أشهر قابلة للتجديد في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أما بالنسبة للإذن الممنوح في الحالات الأخرى المنصوص عليها في المادة 4 من القانون 09-04 فتخضع لأحكام

قانون الإجراءات الجزائية وتحديدا المادة 65 مكرر 5 وما يليها وهذا طبقا لنص المادة 3 من القانون 09-04.

ويجب على القضاء قبل إصدار الإذن تقدير مدى توفر حالة من الحالات الواردة على سبيل الحصر في الفقرة الأولى من المادة 4 السابقة الذكر، وذلك منعا للتعسف من أي جهة أخرى، ويبطل أي إجراء يتم دون الحصول على الإذن، ما يؤدي إلى بطلان الدليل المستمد منه وبالتالي جميع الإجراءات التي بنيت عليه[38].

وعليه يعتبر الإذن من أهم الضمانات المقررة لإجراء مراقبة الاتصالات الالكترونية، من أجل تحقيق التوازن بين المصلحة العامة من خلال مواجهة الإجرام المستحدث، والمصلحة الخاصة من خلال حماية حقوق وحريات المتهم.

ثانيا : الالتزام بالسرية أثناء مراقبة الاتصالات الالكترونية

اشترطت المادة 10 من قانون رقم 09-04 على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وكذا المعلومات المحصلة منها، لذا يعاقب كل من يتجه نحو استغلال هذا الإجراء لأغراض شخصية، أو كل تجاوز لحدود المراقبة الالكترونية نحو انتهاك حرمة الحياة الخاصة للأفراد، وهذا ما أقرته المادة 4 من القانون أعلاه، وإلى جانب الالتزام بالسرية أثناء إجراء المراقبة الإلكترونية، تلتزم الجهة المختصة بهذا الإجراء أيضا بتحرير محضر كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، وأن يذكر في المحضر تاريخ و ساعة بداية هذه العمليات والانتهاء منها[39].

ثالثا : حدود استعمال المعطيات المتحصل عليها
عن طريق مراقبة الاتصالات الالكترونية

ينتج عن مراقبة الاتصالات الالكترونية تجميع وتسجيل محتوى هذه الاتصالات سواء تمثلت في محادثات شفوية أو رسائل الكترونية متبادلة عن طريق البريد الالكتروني أو التقاط الصور وذلك باستعمال الترتيبات التقنية المناسبة، وحفاظا على مثل هذه المعطيات المتحصل عليها عن طريق المراقبة قيد المشرع استعمالها في الحدود الضرورية للتحريات والتحقيقات القضائية تحت طائلة العقوبات المنصوص عليها في قانون العقوبات وهو ما أكدت عليه المادة 9 من القانون 04/09.

ويهدف المشرع الجزائري من خلال تقييد إجراء المراقبة الالكترونية بمجموعة من الضمانات القانونية إلى الموازنة بين احترام الخصوصية بما فيها الخصوصية المعلوماتية، ومواجهة الإجرام المستحدث، حتى لا يتم الإخلال بالأحكام القانونية التي تضمن سرية المراسلات والاتصالات في حالة ما إذا تركت الحرية لرجال الضبطية في مراقبة الاتصالات الالكترونية.

ولتحقيق هذا الهدف تم إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كآلية لتنفيذ المراقبة الالكترونية.

المطلب الثاني : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها آلية لتنفيذ مراقبة الاتصالات الالكترونية

تعتبر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من بين الآليات الجديدة التي كرسها التشريع الجزائري، حيث مهد القانون رقم 09-04 السابق الذكر بموجب المادة 13 منه إلى إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وإلى غاية 2015 صدر المرسوم الرئاسي رقم 15-261[40] يحدد اختصاصات الهيئة وطبيعة العمل بها، إلا أنه تم إلغاءه وتم استحداث المرسوم الرئاسي رقم 19- 172 المؤرخ في06 يونيو سنة 2019 الذي يحدد تشكيلة هذه الهيئة وتنظيمها وكيفية سيرها[41] ، تسعى بذلك هذه الهيئة إلى الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بإتباع مجموعة من الإجراءات بما فيها مراقبة الاتصالات الالكترونية، الأمر الذي يستدعي التعريف بها (الفرع الأول)، وتحديد الدور الذي تلعبه من خلال الصلاحيات الممنوحة لها ولكل الأقسام المشكلة لها (الفرع الثاني).

الفرع الأول : تعريف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

تعتبر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جهازا استحدث بموجب القانون رقم 09-04 السابق الذكر والمرسوم الرئاسي رقم 19-172. حيث عرف المشرع الجزائري هذه الهيئة بموجب المادة 2 من المرسوم الرئاسي رقم 19-172 **" الهيئة مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني".**

يتضح من خلال نص هذه المادة أن الهيئة تتمتع بمجموعة من الخصائص، والتي تتمثل أساسا في كونها هيئة إدارية مستقلة، بمعنى أنها لا تخضع لأي رقابة، كما أنها تتمتع بالشخصية المعنوية، حيث أضفى عليها المشرع الجزائري هذه الخاصية ليضمن استقلاليتها، ضف إلى ذلك تتمتع بالاستقلالية المالية، حيث تتولى مديرية الإدارة والوسائل إعداد احتياجات الهيئة في إطار تحضير تقديرات الميزانية التي تشتمل على باب الإيرادات الذي يحتوي على الإعانات التي تمنحها الدولة، وعائدات كل النشاطات المرتبطة بموضوعها، وباب النفقات يحتوي على نفقات التسيير ونفقات التجهيز[42]. وكما يتولى كذلك مجلس التوجيه دراسة مشروع ميزانية الهيئة والموافقة عليه و هو ما أكدت عليه المادة 6 من المرسوم الرئاسي رقم 19-172 السابق الذكر.

الفرع الثاني: دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في تنفيذ مراقبة الاتصالات الالكترونية

منح المشرع الجزائري تنفيذ إجراء مراقبة الاتصالات الالكترونية في حالة الوقاية من الأفعال الموصوفة بالجرائم الإرهابية والتخريبية أو الجرائم الماسة بأمن الدولة للهيئة الوطنية دون سواها، وبذلك تلعب الهيئة دورا بارزا أثناء تنفيذها لهذا الإجراء، ويتضح ذلك من خلال مختلف المهام الموكلة لها. مما جعل دورها يتخذ طابعا توجيهيا وآخر رقابيا.

أولا : الطابع التوجيهي لدور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

يتجسد الطابع التوجيهي لدور الهيئة في مجموعة من الصلاحيات المتمثلة في:

- التداول حول الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- التداول حول مساءل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- القيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بالدقة.

- اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجراءم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[43].

يكلف بهذه المهام مجلس التوجيه[44] التابع للهيئة الوطنية، حيث يعمل على الموافقة على برنامج عمل الهيئة، كما يقوم بإعداد نظامه الداخلي والمصادقة عليه أثناء أول اجتماع له، ويتولى دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه، وإبداء رأيه في كل مسألة تتصل بمهام الهيئة، وتقديم كل اقتراح يتصل بمجال اختصاصها، وكما يساهم في ضبط المعايير القانونية في مجال اختصاصه، ودراسة مشروع ميزانية الهيئة والموافقة عليه[45].

ثانيا : الطابع الرقابي لدور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

تمارس الهيئة الوطنية اختصاص ذو طابع رقابي، وذلك بهدف تنفيذ الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وباعتماد العديد من التدابير الرقابية التي تتجسد في:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية
- تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم [46].

تتولى بذلك المديرية العامة مراقبة أعمال الهيئة الوطنية من خلال ما يلي:

- السهر على حسن سير الهيئة
- إعداد مشروع ميزانية الهيئة
- وإعداد وتنفيذ برنامج عمل الهيئة
- تنشيط وتنسيق ومتابعة ومراقبة أنشطة هياكل الهيئة

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها
- تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعلومات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم
- إعداد التقرير السنوي لنشاطات الهيئة. وهو ما جاء في نص المادة 9 من المرسوم الرئاسي رقم 19-172 السابق الذكر.

وعليه يتم تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من طرف المديرية التقنية التابعة للمديرية العامة، والتي تتولى بدورها مساعدة السلطات القضائية ومصالح الشرطة القضائية بناء على طلبها، بما في ذلك مجال الخبرات القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التي تتطلب اللجوء إلى أساليب التحري الخاصة للهيئة، وهذا ما أقرته المادتان 11و12من المرسوم الرئاسي رقم 19-172 السابق الذكر، و المادة 14 من ق رقم09-04. كما تتولى جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية.

زيادة عن ذلك تتولى جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية[47].

ويتضح من خلال ما سبق، أن تدعيم الهيئة الوطنية بالمديرية العامة قد جاء من أجل مساعدتها على أداء المهام الموكلة لها بشكل أكثر دقة وتنظيما، وعلى توزيع هذه المهام حتى لا تكون عبئا على الهيئة ومن ثم تفعيل دورها في الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ويظهر أن المشرع الجزائري قد منح صلاحيات عديدة للهيئة الوطنية من أجل ممارسة نشاطها وتنفيذ مهامها في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، غير أن هذه الصلاحيات ليست مطلقة بل مقيدة، ويظهر ذلك من خلال غياب دورها في ترتيب العقوبات اللازمة التي قد تترتب عن القضايا المتعلقة بتكنولوجيات الإعلام والاتصال، فغياب صفة الردعية لدى الهيئة يجعلها هيئة إدارية. كما اكتفى المشرع الجزائري بمنح الهيئة دور الوقاية فقط، دون المتابعة الفعلية لهذه القضايا التي من شأنها زرع الثقة لدى المواطنين وتشجيعهم للإخطار والتبليغ عن كل ما يتصل بهذه الجرائم.

ويتضح من خلال المهام الموكلة لهذه الهيئة أن المشرع الجزائري يهدف إلى مكافحة ومواجهة الإجرام المستحدث بطرق حديثة تتماشي مع التطور الذي عرفته الجريمة ووسائل ارتكابها، لذلك عمل على إنشاء هذه الهيئة التي تحرص على التنفيذ السليم لإجراء المراقبة الإلكترونية، من خلال الدور الذي تلعبه في مواجهة الإجرام المستحدث.

ويبقى الدور الذي تلعبه الهيئة الوطنية في تنفيذ المراقبة الالكترونية محددا في نطاق ضيق وهو الوقاية من الأفعال الإرهابية أو التخريبية والاعتداءات على أمن الدولة، ومساعدة السلطات القضائية، ويعود هذا التضييق إلى إمكانية تعسف هذه الهيئة في مراقبة الاتصالات الالكترونية وانتهاك حريات الأفراد وحقوقهم ولاسيما حق الخصوصية المعلوماتية، لذا جعل المشرع دورها محصورا في الجرائم الخطيرة الماسة باستقرار وأمن الدولة.

الخاتمة:

وفي ختام هذه الدراسة نخلص إلى أن الحق في الخصوصية المعلوماتية ليس مضمونا بصفة مطلقة، بل هو حق نسبي وضيق لوجود اعتبارات اقتضت وضع استثناءات له، وبالرغم من الحماية المكرسة له دوليا وتشريعا إلا أن حياة الأفراد وأسرارهم في البيئة المعلوماتية، لا تزال معرضة للاعتداء، لاسيما أمام تزايد المعاملات بين مختلف المجتمعات داخل الفضاء الرقمي.

وعلى ذلك تعد المراقبة الإلكترونية للاتصالات انتهاكا صارخا لحق الخصوصية المعلوماتية كقاعدة عامة، إلا أنه إذا أجريت وفقا للضمانات القانونية المقررة لها تعتبر إجراءً مشروعاً لإنفاذ القانون. حيث جاء إقرار مشروعية المراقبة الإلكترونية كاستثناء لحق الخصوصية المعلوماتية، لوجود ضرورة حتمية تتمثل في مواجهة الإجرام المستحدث الذي يتسم بخطورة وطبيعة خاصة عابرة للحدود الوطنية، يصعب الكشف عنها بالوسائل التقليدية.

ومن أجل تنفيذ عملية مراقبة الاتصالات الالكترونية تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، رغبة في القضاء على الممارسة غير القانونية التي تعود بالسلب على المصلحة العامة للبلاد. حيث تم منحها عدة صلاحيات لممارسة مهامها، إلا أنها تتميز بالطابع الوقائية أكثر منه مكافحة، مما يجعل دورها محدودا ومقتصرا.

وعليه توصلنا من خلال دراستنا هذه إلى وضع الاقتراحات الآتية:

- استحداث قانون خاص يعالج موضوع الخصوصية داخل الفضاء الرقمي أو ما يعرف بالخصوصية المعلوماتية، بما يتناسب مع التطور الحاصل في العالم الرقمي.

- ضرورة التعاون الدولي لمواجهة مختلف أشكال الإجرام في البيئة المعلوماتية الافتراضية.

- وجوب تدخل المشرع الجزائري وإقرار ضوابط أكثر بخصوص إجراء مراقبة الاتصالات الالكترونية التي تتضمن في طياتها مساسا بالخصوصية المعلوماتية، وذلك بإعادة ضبط حالات اللجوء إلى هذا الإجراء بشكل يضمن عدم استعماله المفرط، بالإضافة إلى تحديد مرات تجديد اللجوء إليه وعدم تركه مفتوحا إلا في حالات محددة حصرا يجب النص عليها صراحة.

- فرض إجراءات رقابة صارمة على التجاوزات القانونية التي تسجلها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، خاصة فيما يتعلق بسرية العملية وحماية المعلومات المستقاة من المراقبة، تحقيقا للأمن المعلوماتي.

الهوامش:

[1]- تعتبر فترة الستينات والسبعينات، الفترة التي أثير فيها لأول مرة وبشكل متزايد مفهوم الخصوصية المعلوماتية كمفهوم مستقل عن بقية مفاهيم الخصوصية، ويعود الفضل في توجيه الانتباه لهذا المفهوم إلى المؤلفين الأمريكيين ويستن وميلر، فقد قدم ويستن تعريفا لخصوصية المعلومات في كتابه الخصوصية والحرية عام 1967 على أنها: " حق الأفراد في تحديد متي وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين "، في حين جاء تعريف ميلر أكثر عمقا إذ عرف خصوصية المعلومات في كتابه الاعتداء على الخصوصية أنها: "قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم". أنظر: مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، ط 1، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، 2016، ص ص 41-42.

كما يعرف الحق في الخصوصية المعلوماتية أنه حق الأفراد أو المجموعات أو المؤسسات أن يحددوا لأنفسهم، متى وكيف أو إلى أي مدى يمكن للمعلومات الخاصة بهم أن تصل للآخرين. وكذلك عرفت بأنها حق الفرد في أن يضبط عملية جمع المعلومات الشخصية عنه، وعملية معاملتها آليا، وحفظها، وتوزيعها، واستخدامها في صنع القرار الخاص به أو المؤثر فيه. أنظر: سوزان عدنان الأستاذ، " انتهاك حرمة الحياة الخاصة عبر الانترنت- دراسة مقارنة-"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد03، دمشق، سوريا، 2013، ص 433.

[2] - *HENRIK ZIEGELDORF Jan, Privacy in the internet of Things; Threats and challenges, pp3-4 in* https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf

[3] - الفضاء الرقمي أو ما يطلق عليه الفضاء السيبراني هو شبكة متنامية بسرعة من تكنولوجيا الحوسبة والاتصالات التي تربط العالم، فقد غيرت بعمق حياتنا، حيث أصبح أفراد المجتمع ينفذ عدد لا يحصى من المعاملات الاجتماعية، الاقتصادية، والسياسية من خلال الفضاء السيبراني، إلا أن إمكانية إجراء مراقبة واسعة النطاق لجميع هذه الأنشطة تشكل تهديدا خطيرا للخصوصية المعلوماتية، وهذا ما جعل الجمهور يتخوف بالفعل من الخصوصية. أنظر:

KANG Jerry, Information Privacy in Cyberspace Transaction, Stanford law review, vol. 50;1193,1998,p 1193, p 1195.

[4]- اعتمد الإعلان العالمي لحقوق الإنسان بموجب قرار الجمعية العامة للأمم المتحدة 217ألف (د-3) المؤرخ في 10 ديسمبر1948، وانضمت إليه الجزائر عن طريق دسترته في المادة 11 من دستور 1963، الجريدة الرسمية العدد 64، الصادرة بتاريخ 10 سبتمبر 1963.

[5] - عاقلي فضيلة، الحماية القانونية للحق في حرمة الحياة الخاصة دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة الإخوة متنوري- قسنطينة، 2012، ص 31.

[6] - عاقلي فضيلة، المرجع نفسه، ص 30.

[7] - مصطفى بن قارة عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، مجلة الفقه والقانون، العدد الثاني والأربعون، أفريل، 2016، مجلة إلكترونية متوفرة على الموقع الالكتروني:

http://kadhanews.com/index.php/2014-01-27-23-23-04/item/2671-2016-04-07-11-39-07 ص 78.

[8] - MATTATIA Fabrique, Traitement des donnes personnelles- Le guide juridique- la loi informatique et libertés de la CNIL jurisprudences, Edition Eyrolles, Paris, 2013, p.13.

[9] - مصطفى بن قارة عائشة، مرجع سابق، ص 79.

[10] -PUDDEPHATT Andrew et les autres, Etude mondiale sur le respect de la vie privée sur l'internet et la liberté d expression, L'organisation des Nation Unies pour l'éducation, France, 2013, p.72.

[11] - MATTATIA Fabrique, Op. Cit., p.16.

[12] - قرار الجمعية العامة للأمم المتحدة رقم 167/68 الصادر بتاريخ 18 ديسمبر 2013 يتعلق بالحق في الخصوصية في العصر الرقمي، رقم الوثيقة A/ RES/68/167 ، الصادرة بتاريخ 21 جانفي 2014.

[13]- الفرد لديه بالفعل وجود افتراضي في الفضاء الرقمي الذي يحل محل ما يسمى أحيانا " مساحة الجسد " وله شخصية رقمية تتألف من مجموعة البيانات الضرورية غير متصلة في مكان آخر والتي لا يمكن أن تكون مسبقا. أنظر:

KIRBY Michael, Les droit de l'homme dans le cyberspace, Edition Unesco/Economica, Paris, 2005, p. 15.

[14] - قرار الجمعية العامة للأمم المتحدة رقم 167/68.

[15] - المرسوم الرئاسي رقم 96- 438 مؤرخ في 7 ديسمبر 1996 متضمن تعديل الدستور، الجريدة الرسمية العدد 76، الصادرة في 8 ديسمبر1996.

[16] - القانون رقم 16-01، مؤرخ في 06 مارس 2016، يتضمن التعديل الدستوري، الجريدة الرسمية العدد14، الصادرة في 08 مارس 2016.

[17] - راجع المادة 46 من دستور 2016.

[18] - القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية العدد 71، الصادرة في 10 نوفمبر 2004.

[19] - بشاتن صفية، الحماية القانونية للحياة الخاصة (دراسة مقارنة)، رسالة دكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص 419.

[20] - القانون رقم 2000-03 المؤرخ في 05 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الجريدة الرسمية العدد 48، الصادرة في 06 أوت 2000.

[21] - زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، د ط، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011، ص76.

[22] - راجع المادتين 303 مكرر و303 مكرر1 المضافتين بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66-156، المتضمن قانون العقوبات.

[23] - بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا" الإعلام والاتصال"، أطروحة دكتوراه العلوم في العلوم القانونية، تخصص قانون دستوري، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2015، ص141.

[24] - حمودى ناصر، الحماية الجنائية لتظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، 2006، ص ص 79-80.

[25] - قارة آمال، الحماية الجنائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2007، ص 122.

[26] - يتبين من الناحية العملية أن العديد من سمات الانترنت تشكل إشكالية كبيرة فيما يتعلق بحق المستخدمين في التحكم في بياناتهم الشخصية، فالطبيعة العابرة للحدود الوطنية للانترنت تجعل من الصعب في بعض الأحيان التحكم في البلدان والولاة القضائية التي تنتقل فيها البيانات، كما أن التقدم في تكنولوجيات المعالجة المحسوبة يجعل من الممكن معالجة كميات متزايدة من البيانات الشخصية مما يجعل من الصعب الاحتفاظ بخصوصية هذه البيانات. أنظر:

PUDDEPHATT Andrew et les autres, Op. Cit., p. 25.

[27] - KIRBY Michael et les autres, Op. Cit., p. 14.

[28] - معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، رسالة ماجستير في العلوم القانونية، تخصص القانون الجنائي والعلوم الإجرامية، كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر، باتنة، 2012، ص 72.

[29] - سوزان عدنان الأستاذ، مرجع سابق، ص 435.

[30] - من بين الاتفاقيات التي نصت على ضرورة استخدام المراقبة الالكترونية نجد اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من قبل الجمعية العامة بموجب القرار 25/55 الصادر بتاريخ 15 نوفمبر 2000، وذلك بموجب المادة 20 منها. إضافة إلى اتفاقية الأمم المتحدة لمكافحة الفساد التي دخلت حيز النفاذ بتاريخ 29 سبتمبر2003، نصت ه ي الأخرى على استخدام المراقبة الإلكترونية بموجب المادة 50 منها تحت مصطلح الترصد الإلكتروني.

[31] - زبيحة زيدان، المرجع السابق، ص 138.

[32] - ثابت دنيازاد، مراقبة الاتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والإنسانية، العدد السادس، جامعة العربي التبسي، تبسة، 2016، ص ص 209، 210.

[33] - تنصب إجراءات المراقبة الإلكترونية على جملة من المعلومات والبيانات التي قد تكون إما ساكنة كالأمر بالتحفظ المعجل على البيانات أو تكون متحركة وهي التي يقصد بها اعتراض وتجميع البيانات أثناء بثها وليس الحصول عليها في شكل بيانات الكترونية مخزنة، و يتم تداول هذه المعلومات والبيانات في النظم المعلوماتية. أنظر: ربيعي حسين، المراقبة الإلكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد 01، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2016، ص ص 420، 422.

[34] - محمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، أعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، 29 مارس 2017، مركز جيل البحث العلمي، الجزائر، 2017، ص 74.

[35] - تتضمن الاتفاقية الأوربية للمساعدة القانونية المتبادلة المؤرخة في 29 ماي 2000 عدة أحكام ترمي إلى مواجهة حالات جديدة في مجال اعتراض الاتصالات السلكية واللاسلكية، وذلك خارج الأنماط التقليدية للمساعدة المتبادلة، وهي نوعين جاءت في التقرير التفسيري للاتفاقية: الحالة الأولى تتعلق بالاتصالات من خلال نظام الأقمار الصناعية، بحيث يحدث الاعتراض في هذه الحالة على مستوى المحطة الأرضية، أما الحالة الثانية فتتعلق بالاتصالات التي تتلقاها أو تصل مثلا إلى الدولة "أ" والتي يمكن اعتراضها من طرف الدولة "ب" دون الحاجة إلى المساعدة من الدول "أ". لمزيد أنظر:

DE VAKENEER Christian, Manuel de L enquête pénale, 3 édition, Larcier, Belgique, 2006, pp 335-336.

[36] - الممارسات الجيدة في مجال أساليب التحري الخاصة، ورقة معلومات أساسية من الأمانة، مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، تقرير الفريق العامل المعني بتهريب المهاجرين، وثائق الأمم المتحدة، الوثيقة رقم: CTOC/COP/WG7/2013/2، ص 7.

[37] - راجع المادة 04 من القانون رقم 09-04، مؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47،الصادرة بتاريخ 16 أوت 2009.

[38] - ثابت دنيازاد، المرجع السابق، ص 215.

[39]- يتم الرجوع في هذه الحالة إلى القواعد العامة لقانون الإجراءات الجزائية وتحديدا المادة 65 مكرر 9 و65 مكرر 10 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 84، الصادرة بتاريخ 24 ديسمبر2006. وهذا نظرا للارتباط الموجود بين الإجراءات المنصوص عليها في هذه المواد وإجراء مراقبة الاتصالات الالكترونية، فوفقا للمادتين يلتزم ضابط الشرطة القضائية بتحرير محضرين الأول يتضمن عملية الاعتراض من خلال المعلومات المطلوبة تسجيلها وأماكن التسجيل وبداية ونهاية التسجيل، أما المحضر الثاني يتعلق بالجوانب التقنية من خلال تحديد الأدلة المستعملة أو جهاز العون المسخر، وبالنسبة للحالة المتعلقة بالوقاية من الأفعال الإرهابية والتخريبية أو الماسة بأمن الدولة تختص الهيئة الوطنية بتحرير المحضر.

[40] - المرسوم الرئاسي رقم 15-261، مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53، الصادرة في 8 أكتوبر 2015.

[41] - المرسوم الرئاسي رقم 19-172، مؤرخ في 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، الجريدة الرسمية العدد 37، الصادرة في 9يونيو 2019.

[42] - راجع المادتين 15و16 من المرسوم الرئاسي رقم 19-172.

[43] - راجع المادة 06 من المرسوم الرئاسي رقم 19-172.

[44] - يرأس مجلس التوجيه وزير الدفاع الوطني أو ممثله، ويتشكل من ممثلي الوزارات الآتية: - وزارة الدفاع الوطني، - الوزارة المكلفة بالداخلية، - وزارة العدل، - الوزارة المكلفة بالمواصلات السلكية واللاسلكية. أنظر المادة 5 من المرسوم الرئاسي رقم 19-172 .

[45] - راجع المادة 6 من المرسوم الرئاسي رقم19-172.

[46] - راجع المادة 14 من القانون رقم09-04 .

[47] - راجع المادة12 من المرسوم الرئاسي رقم 19-172.