المراقبة الإلكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي*

ربيعي حسين، أستاذ مساعد "أ"
كلـيّة الـحقـوق،
جامعة قسنطينة 1، الجزائر.

REBIAI Hocine, M.A «A»
Faculté de Droit,
Université Constantine 1 – Algérie.

الملخص:

لقد أصبحت حاليا وقائع الحياة تدور في جزء هام منها في الفضاء الإلكتروني، بفعل إنتشار تكنولوجيا المعلوماتية،وهو ما خلق نوعا حديثا من الحقوق كحق الفرد في الخصوصية المعلوماتية،الذي يحمي الفرد داخل الفضاء الرقمي من مختلف الممارسات التي يمكن لها أن تنتهك خصوصيته، خصوصا تلك التي تمارسها الحكومات والمؤسسات والمتعلقة بأعمال المراقبة واعتراض الاتصالات وجمع البيانات حول نشاط الأفراد داخل الفضاء الرقمي، فالدول حالياً تمتلك من القدرات أكثر من أي وقت مضى للقيام بذلك و هو ما يتعارض بشكل مباشر مع حرية الفرد في التمتع بالخصوصية داخل الفضاء الإلكتروني.

الكلمات الدالة:

المراقبة الإلكترونية- حرية الفرد-الفضاء الرقمي-الجرائم المعلوماتية.

La cyber-surveillance et le droit de l'individu à la vie privée dans l'espace numérique

Résumé :

Dans un monde qui change pour le numérique a cause de la propagation des nouvelles technologies de communication, la liberté individuelle a pris de nouvelles formes, adaptées à cette situation, parmi ces formes, on cite le droit au respect de la vie privée sur Internet, comme un moyen pour faire face à la cybercriminalité, tel que le contrôle exercé par l'Etat en raison de la sécurité nationale, en partant du principe qu'Internet conserve sans limite de durée, nos information personnelles, nos activités et notre vie personnelle, ce qui constitue une menace réel et permanente envers le principe du respect de la vie privée sur internet .

* تمّ استلام المقال بتاريخ 2015/12/27 وتمّ تحكيمه بتاريخ 2016/01/18 وقُبل للنّشر بتاريخ 2016/05/02.

Mots clés:
Cyber-surveillance, liberté, individuelle, espace numérique, cybercriminalité.

Cyber surveillance and the right of the individual to privacy in cyberspace

Abstract:
In a changing world for digital due to the new communication technologies spread, the individual freedom has taken new forms that are adapted to that situation, among those forms we mention the right to respect for privacy on the internet as a mean to cope with the cyber monitoring often exerted by the state owing to the national security, As the internet retains our personal information, our activities and our personal lives for an unlimited period, it represents a real and continuing threat to the principle of the privacy respect on the internet.

Key Words:
Cyber surveillance, individual liberty, cybercrime, cyber terrorism.

مقدمة

تعتبر الجريمة المعلوماتية أخطر صور التعدي على الحق في الخصوصية عبر الأنظمة المعلوماتية، وهي الجريمة التي اجتهدت التشريعات وعملت على مواجهتها قانونيا، من أجل ضمان حماية فعالة لأمن وخصوصية النظم المعلوماتية من تهديدات مجرمي المعلوماتية،غير أنّها أتاحت في مقابل تحقيق ذلك للدول والحكومات حق انتهاك مبدأ الخصوصية المعلوماتية المقرر لفائدة الأفراد، بدعوى تنفيذ الإجراءات المتعلقة بالبحث والتحقيق بشأن الجرائم المعلوماتية في إطار سياسة الوقاية منها و مكافحتها.

غير أنّه وفي ظل المعطيات المتعلقة بالطبيعة الخفية للجرائم المعلوماتية، وتزايد التهديدات الناجمة عنها باستهدافها لشتى المصالح و خصوصا تلك المتعلقة بالأمن القومي الدول، من خلال ظهور جرائم الإرهاب الالكتروني، فإنّه تولّد عن ذلك زيادة في نشاط المراقبة الالكترونية للأفراد عبر الشبكات بدعوى الوقاية من ومكافحة هذا النوع من الجرائم المعلوماتية، وذلك من خلال اعتراض وتسجيل محتوى الاتصالات الالكترونية، وتجميع البيانات والمعلومات المتعلقة بالحياة الشخصية للأفراد بدون علم منهم أو إذن مسبق صادر عنهم، وهو ما يشكل انتهاكا صارخا لحقهم في الخصوصية عبر المعلوماتية، خصوصا وأنّ مسألة اللجوء إلى اتخاذ مثل هذا الإجراء أصبح يشكل عادة خطيرة تنتهجها الدول بالرغم من طابعها الاستثنائي الذي تؤكده نصوص الدساتير والقوانين الداخلية.

إنّ أهمية الموضوع ترتكز حول مفهوم أساسي وهو خطورة إجراءات المراقبة الالكترونية على حرمة الحياة الخاصة للأفراد في الفضاء الرقمي، فمستخدمو الأنظمة المعلوماتية عموما وشبكة الانترنت خصوصا، يتمتعون كأصل بالحرية والحق في الخصوصية عبر الشبكات المعلوماتية، غير أنّ هذه الفكرة تعتبر نسبية إلى حد بعيد بالرغم من الضمانات القانونية المتوفرة، فكلما تعارض هذا المبدأ والمصالح العليا للدول فإنّ هذه الأخيرة تلجأ إلى المراقبة الالكترونية لمضمون ومحتوى الاتصالات الالكترونية للأفراد بدعوى حقها في الوقاية ومكافحة الجرائم المعلوماتية التي تهدد أمنها وسلامتها.

إنّ الإشكالية المطروحة للنقاش في هذا الصدد تتناول إبراز مفهوم مبدأ الخصوصية عبر النظم المعلوماتية، ومدى صمودها في وجه إجراء المراقبة الالكترونية التي تفرضها الدول والحكومات كحتمية للوقاية ومكافحة الجرائم المعلوماتية التي تهدد أمنها وسلامتها، ويمكن تلخيص مضمون الإشكالية العامة للموضوع في التساؤل التالي: إلى أي مدى تنتهك المراقبة الالكترونية كإجراء يهدف إلى الوقاية ومكافحة الجرائم المعلوماتية الماسة بأمن وسلامة الدول، حق الخصوصية المعلوماتية المقرر لفائدة الأفراد داخل الفضاء الرقمي؟

إنّ الإجابة عن هذه الإشكاليات تقتضي منا وبالضرورة اتباع منهج وصفي تحليلي لموضوع النقاش ،بالإضافة إلى المنهج المقارن من أجل الإحاطة بكل جوانب الموضوع،و ضمانا لذلك فقد قسمنا موضوعنا إلى مبحثين أساسين هما:

– المبحث الأول: مفهوم مبدأ الخصوصية عبر النظم المعلوماتية وإجراء المراقبة الالكترونية.

– المبحث الثاني: آليات و وسائل تنفيذ المراقبة الالكترونية.

المبحث الأول/مفهوم مبدأ الخصوصية عبر النظم المعلوماتية وإجراء المراقبة الالكترونية

إنّ الحق في الحياة الشخصية أحد حقوق الإنسان الأساسية الذي أثار جدلا واسعا على المدى التاريخي، ولعله أبرز حق يتم التركيز عليه على نحو متعاظم في الوقت

الحاضر في ظل توظيف تقنية المعلوماتية، فلكل فرد الحق في المحافظة على سرية حياته الشخصية وعدم جعلها عرضة لأن تكون موضوعا للنشر، فالإنسان له الحق في أن يترك وشأنه ليعيش حياة بعيدة عن العلنية، ونطاق الحياة الخاصة للفرد يمتد ليشمل كل ما يتعلق بحياته من معتقداته إلى مظاهره العلنية وهي في مجموعها تدخل ضمن إطار الحقوق الشخصية[1].

وفي سبيل تكريس مبدأ الخصوصية تكلفت النصوص القانونية بما فيها الدساتير، بحماية هذا المبدأ من خلال نصها بشكل متوافق على حماية هذا الحق من خلال منع وحظر الغير من الاطلاع على مضمون الحياة الخاصة للأفراد، بقصد توفير نوع من الاستقرار والأمن للأفراد، وعملت في سبيل تحقيق ذلك على إحداث التوازن بين مفهوم الحرية الشخصية وشرعية العدالة الجزائية، من خلال منح الإجراءات المتخذة في مواجهة الحقوق الأساسية للأفراد المصداقية والشرعية، في ظل دولة القانون التي تعمل فيها السلطات على احترام سيادة القانون بهدف مراعاة ضمانات حماية الحرية الشخصية بجميع صورها[2].

المطلب الأول/مفهوم الحق في الخصوصية المعلوماتية

يتميز الحق في الخصوصية في مجال المعلوماتية بمفهوم حديث ،نتيجة تقاطع هذا الحق في ظل المفهوم التقليدي الذي يقصد به حق الفرد في حماية سرية و خصوصية اسمه وشرفه واعتباره ومراسلاته واتصالاته و تفاصيل حياته الشخصية، مع مفهوم المعلوماتية والتي يقصد بها أنظمة المعالجة الآلية للمعطيات، والتي تتكون أساسا من أجهزة الحاسوب المتصلة ببعضها البعض بواسطة شبكة اتصالات سلكية أو لاسلكية، وهو ما يولّد فكرة ضرورة حماية كل المعطيات والمعلومات الشخصية المتداولة أو المخزّنة عبر هذه الأنظمة من كل اعتداء يجعل منها متاحة للغير علنا وبدون إذن صاحبها.

الفرع الأول/نشأة فكرة الحق في الخصوصية المعلوماتية

تعتبر فكرة منح الفرد الحق في الخصوصية فكرة قديمة يعود أصلها إلى أول وثيقة ومدونة دستورية لحقوق الإنسان تعرف "بالعهد الأعظم"، والتي تنازل بموجبها ملك بريطانيا عام 1215 عن جزء من سلطاته المطلقة، فمنح عهدا بعدم القبض على أي

شخص أو حبسه أو نفيه أو مصادرة أمواله ،إلا بحكم صادر عن سلطة قانونية، وهو ما تبنته بعض التشريعات القديمة كقانون the justice of the peace act الصادر عام 1361 ببريطانيا والذي تم بموجبه تجريم اختلاس النظر واستراق السمع[3].

وقد نشأت فكرة الخصوصية المعلوماتية سنة 1967 نتيجةً لجهود الباحثين الأمريكيين في هذا المجال وهما "آلن ويستون" و "ميلير" و اللذان نشرا أعمالهما في هذا المجال تحت عنوان " الخصوصية والحرية " و " الاعتداء على الخصوصية " وهي أولى الجهود الفكرية الهادفة لتأسيس مبدأ الخصوصية المعلوماتية[4].

الفرع الثاني/تعريف الخصوصية المعلوماتية

يقصد بالخصوصية في هذا المقام خصوصية المعلومات ،وهو حق الأفراد أو المجموعات أو المؤسسات أن يحددوا لأنفسهم متى وكيف و إلى أي مدى يمكن للمعلومات الخاصة بهم أن تصل للآخرين، وعرفت كذلك بأنّها حق الفرد في أن يضبط عملية جمع المعلومات الشخصية عنه وعملية معالجتها آليا وحفظها وتوزيعها واستخدامها في صنع القرار الخاص به أو المؤثر فيه[5].

وقد عرفها الفقيه" ميلير " بـأنّها" قدرة الأفـراد على الـتحكم بـدورة المعلومات التي تتعلق بهم ويعتبر الفرد في حالة من الخصوصية إذ كان في حالة من العزلة والألفة والتستر "[6].

وترجع ضرورة منح الفرد خصوصية داخل الفضاء الرقمي بالنظر إلى الاستعمالات اللامحدودة لشبكة الأنترنت في الوقت الحاضر، وما نتج عنها من إشكاليات وتعقيدات لأمن الحياة الخاصة، فهي شبكة تتيح عمليات جمع وتخرين المعلومات المتعلقة بالأشخاص بأساليب وتقنيات لم تكن معروفة مسبقا، بالإضافة إلى أنّ :

– الانترنت كشبكة دولية يسهل جمع المعلومات بالإضافة إلى قابلية تحديد مصدرها بدقة من خلال الاستعانة بعناوين (IP) [7] التي تميز كل حاسوب عن الآخر.

– تنامي قدرات وأساليب الهيئات المكلفة بالمراقبة الالكترونية في مجال جمع المعلومات الخاصة بالأفراد، بفعل قدراتها التقنية الفائقة في هذا المجال، في إطار عملها على

تغذية بنوك المعلومات التي أنشأتها أغلب دول العالم بمعلومات شخصية تخص نشاط الأفراد عبر الشبكات[8].

الفرع الثالث/الضمانات القانونية لحق الخصوصية المعلوماتية

تقدّس أغلب الاتفاقيات الدولية والمواثيق والعهود الدولية والدساتير الوطنية و القوانين الداخلية الحق في الحياة الخاصة، وتوفر نصوصا قانونية هامة بهدف ضمان حماية قصوى له ونجدها موزعة على مستويين الأول دولي والثاني وطني داخلي.

الفقرة الأولى/الحق في الخصوصية المعلوماتية في ظل النصوص الدولية

يجد الحق في الخصوصية معناه بوجه عام دون تخصيص في أغلب نصوص الدولية المتعلقة بحقوق الإنسان، بحيث تنص المادة 12 من الإعلان العالمي لحقوق الإنسان على أنّه " لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"[9].

كما تنص المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية الذي أُعتمد من قبل الجمعية العامة للأمم في 16 ديسمبر 1966 بأنّه" لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته، من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس"، و هو ما تتفق بشأنه و توضحه نصوص المواد 08 من الاتفاقية الأوروبية لحقوق الإنسان لسنة 1950، و المادة 11 من الاتفاقية الأمريكية لحقوق الإنسان لسنة 1969، و كذلك المادة 21 من الميثاق العربي لحقوق الإنسان[10].

و يعتبر القرار 167/68 المعتمد من قبل الجمعية العامة للأمم المتخذة بتاريخ 2013/11/18 تحت عنوان "الحق في الخصوصية في العصر الرقمي" أحدث الجهود الدولية التي تهدف إلى تعزيز الحق في الخصوصية المعلوماتية، بالنظر إلى قلة حصانة تكنولوجيا المعلومات أمام إجراء المراقبة الالكترونية، فقد أظهرت الدراسات الحديثة أنّ هناك استراتيجيات تكنولوجية حديثة تعزز ممارسات المراقبة الالكترونية، وهو ما يشكّل تعديا بالغا على حريات الأفراد وعلى مقومات بناء مجتمع مدني، وقد تضمن

القرار 167/68 مجموعة من ستة (06) توصيات تهدف إلى الحد من الأثر السلبي الذي يمكن أن تخلّفه مراقبة الاتصالات واعتراضها على حقوق الإنسان، فحقوق الإنسان المحمية خارج الفضاء الالكتروني يجب أن تكون محمية داخل الفضاء الالكتروني، كما أنّه يجب على الدول الأعضاء أن تعيد النظر في ممارساتها وتشريعاتها المتعلقة بالمراقبة الالكترونية تنفيذا لالتزاماتها بموجب القانون الدولي الإنساني[11].

الفقرة الثانية/الحق في الخصوصية المعلوماتية في نطاق التشريع الجزائري

يتجسد هذا المبدأ على المستوى الوطني من خلال جملة الضمانات القانونية المقررة بموجب أحكام الدستور، بنصه على ضمان حرمة الحياة الخاصة للمواطن و ضمان سرية المراسلات و الاتصالات الخاصة بكل أشكالها، بحيث تنص المادة 39 من دستور الجمهورية الديمقراطية الشعبية لسنة 1996 على أنّه : " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون، سرّية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"، وقد قرر المشرع حسب ما تقضي به المادة 137- ق 22-06 من قانون العقوبات الجزائري عقوبة مقدارها الحبس من (03) ثلاث أشهر إلى (05) خمس سنوات وبغرامة من 30.000 إلى 50.000 دج ضد كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد في حال قام أي منهم بإتلاف رسائل بريدية أو تسهيل فضها أو اختلاسها أو إتلافها، وهو ما تؤكده المادة 127 الفقرة 01 و 02 و 03 من الفصل الثاني تحت عنوان الأحكام الجزائية الخاصة من القانون 03-2000 المؤرخ في 05 أوت 2000 المحدد للقواعد المتعلقة بالبريد و المواصلات السلكية و اللاسلكية بالقول:"تطبق العقوبات المنصوص عليها في المادة 137- ق 22-06 من قانون العقوبات على كل شخص مرخص له بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه و الذي في إطار ممارسة مهامه، يفتح أو يحوّل أو يخرّب البريد أو ينتهك سرية المراسلات أو يساعد في ارتكاب هذه الأفعال، و تسري نفس العقوبات على كل شخص مرخص له بتقديم خدمة مواصلات سلكية و لا سلكية و على كل عامل لدى متعاملي الشبكات العمومية للمواصلات السلكية و اللاسلكية و الذي في إطار أداء مهامه ينتهك بأي طريقة كانت سرية المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق المواصلات السلكية و اللاسلكية، أو الذي أمر أو ساعد في ارتكاب هذه الأفعال".

بالإضافة إلى جملة الجزاءات العقابية التي تقررها نصوص المواد من 303 إلى 303 مكرر 3 ق 06-23 من قانون العقوبات الجزائري بالنسبة للأشخاص العاديين سواء الطبيعيين أو المعنويين، و التي تنص على أنّه كل من يفض أو يتلف رسائل أو مراسلات موجهة للغير و ذلك بسوء نية و ذلك في غير الحالات المنصوص عليها في المادة 137 يعاقب بالحبس من شهر واحد إلى سنة و بغرامة من 25000 دج إلى 100,000 دج أو بإحدى هاتين العقوبتين[12].

أما إذا ما تعمّد أيا كان المساس بحرمه الحياة الشخصية للأشخاص باستعمال أساليب تقنية كالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، أو صور لشخص في مكان خاص، بغير إذن صاحبها أو شرع في ذلك فإنّ العقوبة تكون من 06 ستة أشهر إلى 03 ثلاث سنوات حبسا و بغرامة من 50,000دج إلى 300,000دج، و تطبق نفس العقوبة على كل من احتفظ أو وضع أو سمح بوضع في متناول الجمهور او الغير و بأي وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة الأفعال السابقة[13].

من خلال استقراء النصوص القانونية السابقة و التي يقرها التشريع الجزائري فإنّنا نلحظ و بجلاء تقديس مفهوم الحق في الخصوصية بما فيها المعلوماتية من قبل المشرع الجزائري ضمانا و التزاما منه بحماية و ترقية حقوق الأفراد.

المطلب الثاني/مفهوم المراقبة الالكترونية كإجراء للوقاية ومكافحة الجرائم المعلوماتية

تعتبر المراقبة الالكترونية استثناءا على قاعدة الحق في الخصوصية المعلوماتية، فهي إجراء ينتهك حرمة وسرية المعلومات الشخصية المعالجة آليا،والأصل أنّ هذا الإجراء استثنائي ولا يلجأ إليه إلا في حالات تنفيذ إجراءات وقائية من الجرائم المعلوماتية الماسة بأمن وسلامة الدول ،أو في حال تنفيذ الإجراءات القضائية المتعلقة بملاحقة مرتكبي الجرائم المعلوماتية، ولا يكون ذلك إلا بناءا على رخصة قانونية تسمح صراحة وحصريا باللجوء إلى هذه التقنية[14]، غير أنّ واقع الحال يدل على عدم التزام الدول باحترام هذه المعطيات التشريعية والضمانات، فتلجأ إلى المراقبة الالكترونية

بشكل سري عادة من أجل الوقاية من الجرائم المعلوماتية بالنظر إلى الطابع الخفي لهذه الجرائم وصعوبة تحديد هوية مرتكبيها.

الفرع الأول/تعريف المراقبة الالكترونية للاتصالات

تعتبر المراقبة (La Surveillance)من أهم مصادر التحري والتي يُستعان بها غالبا في البحث والتقصي عن الجرائم سواء التامة أو الخائبة، التقليدية أو المستحدثة فهي إجراء لا يستغنى عنه إذ تعتبر أسرع درب لكشف الجرائم.

وتعــرف المراقبة في مجال المعلوماتية بالمراقبة الإلكترونية(la cyber-surveillance) ويقصد بها : مــراقبة شبكة الاتصالات، أو ذلك العمل الذي يقوم به المُرَاقِب باستخدام التقنية الالكترونية لجمع البيانات والمعلومات حول المشتبه فيه ،سواء كان شخصا أو مكانا أو شيئا حسب طبيعته، وذلك مرتبط بالزمن لتحقيق غرض أمني ولأي غرض آخر.

إذن فالمراقبة الالكترونية كأصل وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه يقوم بها الشخص " المُرَاقِبُ الالكتروني " وهو في العادة من ضباط الشرطة القضائية، يتميز بالكفاءة التقنية العالية في مجال المعلوماتية التي تتماشى مع نوع الجريمة، يستخدم في ذلك التقنية الالكترونية، كأن يراقب نشاط أحد القراصنة المعلوماتيين، أو يقوم بنسخ البريد الالكتروني لمراقبة اتصالات المشتبه فيه عند ارساله او استقباله للبريد الالكتروني[15].

ويعتبر المشتبه فيه في إطار تنفيذ إجراء المراقبة الالكترونية عادة، هو شبكة الأنترنت وحاسوب الشخص الذي أساء استعمالها، فتتم مراقبة اتصالاته الإلكترونية المشتبه فيها والتي تتم عن طريق الأنترنت[16].

الفرع الثاني/واقع المراقبة الإلكترونية بين ضمانات النص و التطبيق الفعلي

إذا كان من الظاهر بأنّ إجراء المراقبة الإلكترونية للإتصالات عبر شبكات الإتصال و مختلف الأنظمة المعلوماتية هو إجراء شرعي قانوني، بما أنّه يستند إلى مبررات أساسها الوقاية و مكافحة الجرائم المعلوماتية و خصوصا الإرهابية منها، و بأنّه إجراء لا يتم تنفيذه إلا بناء على أمر من السلطات القضائية المختصة، و بجملة من الضمانات القانونية التي تحمي حق الفرد في الخصوصية المعلوماتية، إلا أنّ واقع الحال لا يشير

إلى ذلك في كل الأحوال، فقد أشارت المستشارة العليا للأمم المتحدة المكلفة بترقية حقوق الإنسان السيدة "نافي بلاي" في تقرير لها حول نشاطات المراقبة الإلكترونية و مدى تعارضها مع المبادئ الأساسية المتعلقة بحقوق الإنسان، إلى ارتفاع عدد الهيئات المكلفة بتنفيذ هذا الإجراء حول العالم، وهو ما يفسر ازدياد عدد حالات المراقبة الإلكترونية للحياة الخاصة للأفراد، وتعارضها مع المبادئ الأساسية لحقوق الإنسان، كما أشار السيد" فرانك لاراي" في تقريره A/HRC/23/ 40 باعتباره المكلف الخاص من قبل هيئة الأمم المتحدة بترقية وحماية حرية التعبير ،إلى ضرورة احترام الإجراءات الشرعية في مجال ممارسة المراقبة الإلكترونية للاتصالات من أجل ضمان هذه الحقوق الأساسية، بعد ما لاحظه من خروقات عديدة في مجال التعسف في اللجوء إلى إجراءات المـــراقبة الإلكترونية إما دون مبرر حقيقي أو دون استيفاء الضمانات القانونية اللازمة[17].

إنّ هذا الطرح المتعلق بتعسف الدول في اللجوء إلى إجراء المراقبة الإلكترونية للاتصالات عبر الشبكات مرده زيادة وتنامي عدد الهيئات الحكومية والخاصة والتي تمارس إجراءات المراقبة الإلكترونية، فقد أحصت منظمة" صحفيون بلا حدود" في تقريرها الصادر سنة 2014 تحت عنوان" أعداء الأنترنت" بمناسبة إحيائها فعاليات اليوم العالمي لمحاربة الرقابة على شبكة الأنترنت،إثنان و ثلاثون (32) هيئة خاصة وحكومية تقوم بممارسة المراقبة الإلكترونية على الأنشطة المعلوماتية للمستخدمين عبر شبكة الأنترنت،و يرتكز نشاطها إما على حذف بعض المعلومات أو حجزها أو تغييرها، وقد صنف هذا التقرير ثلاث هيئات تشكل أكبر تهديد على الحق في الخصوصية وتنتهك حرمة الحياة الخاصة عبر الشبكات وهي في الأصل تنتمي إلى دول تتغنى بشعارات حماية الحقوق والحريات الفردية وهي:

1-National Security Agency التابع للولايات المتحدة.

2-Le centre de développement des thématiques التابع للهند.

3-Gouvernement communication Headquaters التابع لبريطانيا.

بالإضافة إلى مؤسسات خاصة في هذا المجال أبرزها مؤسسة Issworld و Milipol، و التي تمارس هذا الإجراء بعيدا عن أي ضمانة قانونية، تضع خبراتها وخدماتها تحت

تصرف الدول الراغبة في مراقبة الأنشطة المعلوماتية لأفرادها بشكل سري، وعلى رأسها إيران والبحرين والصين[18].

وكمثال عن الأساليب الحكومية المنتهجة في مجال اللجوء السري للمراقبة الإلكترونية، ما قامت به الصين سنة 2006 حينما صرح الوزير المكلف بالأمن العام لديها عن إطلاق مشروع تحت اسم " الدرع الذهبي" من خلال تفعيل نظام شامل للمراقبة الإلكترونية، أو ما حدث سنة 2009 أين حاولت الحكومة الصينية فرض تثبيت برنامج تجسس يعرف " بالسد الأخضر " على كل الحواسيب التي تسوق داخل الصين وهو ما يمكنها من بسط سيطرتها على كل أنشطة مستخدمي النظام المعلوماتي في الصين غير أنّ هذا الطلب قوبل بالرفض من قبل منظمة التجارة العالمي[19].

المبحث الثاني/آليات و وسائل تنفيذ المراقبة الالكترونية

تعتبر المراقبة الالكترونية إجراء يتعارض مع الحق في الخصوصية المعلوماتية، غير أنّها كإجراء يتوافق مع المصالح العليا للدول باعتبارها وسيلة فعالة في مراقبة نشاط الأفراد المشتبه فيهم في إطار التحريات والتحقيقات القضائية عن الجرائم المعلوماتية، كما أنّها إجراء يسمح بالوقاية من الجرائم المعلوماتية التي من شأنها المساس بمجالات الأمن والنظام العام والدفاع الوطني والتي تصنف عادة في خانة الجرائم الإرهابية.

إنّ اللجوء إلى هذا الأسلوب يستدعي من القائمين على تنفيذه الإلمام بالمعرفة الدقيقة بمجال النظم المعلوماتية، والحيل والأساليب الإجرامية لارتكاب الجرائم المعلوماتية،بالإضافة إلى معرفة الآليات القانونية لضمان شرعية هذا الإجراء الذي يكتسي طابعا خاصا في العالم الرقمي، وهو ما يدفعنا إلى التساؤل حول طبيعة هذا الإجراء و الوسائل والأساليب المستعملة لأجل تنفيذه.

المطلب الأول/آليات تنفيذ المراقبة الإلكترونية

يتم تنفيذ المراقبة الالكترونية من خلال استهداف الاتصالات الالكترونية التي يجريها المشتبه فيه من خلال استعماله لأي وسيلة إلكترونية، إما في شكل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها تمت عن طريق وسيلة الكترونية[20].

تنصب إجراءات المراقبة الإلكترونية على جملة المعلومات والبيانات المتداولة عبر النظم المعلوماتية، والتي تعرف بالمعطيات المتعلقة بحركة السير Données relative au trafic وقد تكون هذه المعطيات والبيانات إما ساكنة أو متحركة، ويمكن تعريفها بأنّها " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات، توضح مصدر الاتصال والوجهة المرسل إليها والطريق الذي تسلكه والوقت وتاريخ وحجم ومدة الاتصال"[21].

الفرع الأول/المراقبة الإلكترونية الواردة على البيانات الساكنة

يتولى عادة ضباط الشرطة القضائية المنتمون إلى وحدات مختصة في الوقاية ومكافحة الجرائم المعلوماتية مهام تنفيذ إجراء المراقبة الإلكترونية بناء على إذن من وكيل الجمهورية أو قاضي التحقيق، غير أنّ هذا الإجراء لا يمكن له أن يتم إلا من خلال جهود مزودي الخدمة بالأنترنت أو مقدمي الخدمات الذين يمكن تعريفهم بأنّهم: أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام اتصالات، أو أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال[22].

ويحــق للقائمين بتنفيذ إجراء المراقبة الالكترونية أن يطلبوا من مقدمي الخدمات تزويدهم بالمعلومات المتعلقة بالاتصالات الالكترونية التي يجريها المشتبه فيه إما من خلال:

الفقرة الأولى/الأمر بالتحفظ المعجل على البيانات

يقصد به الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزة أو تحت سيطرة مزودي الخدمات، في انتظار اتخاذ إجراءات قانونية أخرى بشأنها، كالتفتيش، ويتضح أنّ الهدف من هذا الإجراء هو الاحتفاظ بالبيانات المعلوماتية المخزّنة لدى مزودي الخدمة بالإنترنت قبل حذفها من قبلهم بعد انقضاء مدة الحفظ والتي حددها المشرع الجزائري بسنة واحدة حسب نص المادة 11من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها[23].

يعتبر هذا الإجراء بالنسبة لغالبية الدول سلطة قانونية جديدة مستحدثة كليا، فهو أداة للتنقيب على أثار الجرائم المعلوماتية في إطار مكافحتها أو الوقاية منها نظرا للأسباب التالية:

1-قابلية البيانات المعلوماتية للتلاشي فمن السهل التلاعب بها وتغيير محتواها وبالتالي فقدان عناصر اثبات الجريمة.

2-ارتكاب غالبية الجرائم المعلوماتية بواسطة النظم المعلوماتية أو بواسطة نظم الاتصالات وبالتالي تحديد هوية المرسل والمرسل إليه يساعد في الكشف عن مرتكب الجريمة.

3-استعمال مضمون هذه الاتصالات كدليل للإثبات[24].

الفقرة الثانية /تقديم بيانات معلوماتية متعلقة بهوية المشترك

الأصل أنّ البيانات الشخصية المتعلقة بمستخدمي الشبكة تدخل في إطار الحق في الخصوصية الذي تحميه كل النصوص الدولية والإقليمية والوطنية لحقوق الإنسان، غير أنّه وفي ظل تنامي الإجرام المعلوماتي أصبحت غالبية التشريعات تجيز للجهات المختصة في إطار أداء مهامها المتعقلة بالوقاية ومكافحة الجرائم المعلوماتية، حق الاطلاع على البيانات الشخصية للمشترك، من خلال تقديم طلب لمزودي الخدمات بالأنترنت من أجل مدّهم بها، كما هو عليه في القانون الجزائري بموجب- المادة 10 و 11 و 12 من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعـــلام و الإتصال و مكافحتها، أو كما هو عليه الحال في التشريع الفـرنسي حسب نص المادة 43-9 من القانون 719-2000 الخاص بحرية الإتصالات[25].

ويشير مصطلح المشترك l'abonné إلى عديد الطوائف منهم الشخص الذي يدفع مقابل الخدمة ،و العميل الذي يدفع مسبقا نظير الخدمات، و الشخص المستفيد من الخدمة مجانا، و الشخص المخول له استخدام حساب المشترك، وتعتبر من قبيل بيانات المشترك، هويته، عنوانه البريدي، رقم هاتفه، بيانات فاتورته أو بياناته الشخصية المدرجة في العقد[26].

الفرع الثاني/المراقبة الإلكترونية الواردة على البيانات المتحركة

يعرف هذا الإجراء تحت وصف اعتراض المراسلات الإلكترونية، أو الاعتراض وتجميع المراسلات في الوقت الفعلي لمرور البيانات، وهو إجراء يتم عن طريق سلطة مختصة، أو عن طريق مزودي الخدمات[27].

إنّ المراقبة الالكترونية على البيانات المتحركة يقصد بها "اعتراض وتجميع البيانات أثناء بثها وليس الحصول عليها في شكل بيانات الكترونية مخزنة"[28].

وتعتبر البيانات المستهدفة هي تلك المتعلقة بالاتصالات في فترة الإنتاج ولحظة نقلها عبر الاتصال، وهو ما يفسر مصطلح "الوقت الفعلي"، وتكون البيانات هنا في شكل غير مادي يتم نقلها في شكل ذبذبات صوتية أو إلكترونية، والجدير بالذكر أنّ هذه العملية لا تشوش على تدفق البيانات بحيث تصل الشخص المرسل إليه، وبدلا من ضبطها ماديا فإنّه يتم تسجيلها ونسخها أثناء فترة نقلها والبيانات التي يتم اعتراضها وتجميعها نوعان:

1-بيانات متعلقة بالمرور Données relative au trafic

2-بيانات متعلقة بالمحتوى Données relative au contenu[29].

الفرع الثالث/مظاهر التعسف في اللجوء إلى المراقبة الإلكترونية

بالرغم من جملة الضمانات القانونية الممنوحة لحق الخصوصية المعلوماتية، وحصر أساليب المراقبة الإلكترونية قانونا إلا أنّ التقارير الدولية الصادرة عن مختلف الهيئات المكلفة بالدفاع عن حقوق الإنسان تشير إلى لجوء الدول و الحكومات إلى أساليب سرية وغير مباشرة لممارسة المراقبة الالكترونية على نشاطات الأفراد عبر شبكات الاتصال، ويمكن تلخيص هذه الممارسات في الأساليب التالية:

الفقرة الأولى/أساليب قانونية وتشريعية

تلجأ بعض الدول إلى استصدار قوانين خاصة تبيح لها إجراء المراقبة الإلكترونية خارج نطاق الضمانات القانونية التي توفرها القوانين وعلى رأسها الدستور، ففي سنة 2013 صدر في فرنسا قانون تحت اسم La Loi de la Programmation Militaire بحيث تجيز نص المادة 20 منه إمكانية مراقبة الاتصالات الهاتفية وعبر شبكة الأنترنت في الوقت الفعلي لمرور البيانات، دون إذن أو إشراك لأي قاضي، وذلك بهدف البحث عن

معلومات استخبارية تتصل بالأمن القومي، بهدف حماية الاقتصاد الوطني،و الوقاية من الأعمال الإرهابية[30].

الفقرة الثانية/تعزيز عمل مزودي الخدمات في مجال المراقبة الالكترونية

نذكر في هذا المجال القانون الصادر في 2014/02/05 بتركيا تحت رقم 5651،الذي عزز عمل مزودي الخدمات في مجال الاحتفاظ بالمعطيات الشخصية للمشتركين، وذلك بتمديد مدة حفظ البيانات و المعطيات المتعلقة بنشاط المشترك عبر شبكة الأنترنت إلى سنتين(02)، وضرورة تزويد السلطات المختصة بها بناء على طلب بسيط صادر عنها دون مبرر، تتضمن تاريخ الزيارات عبر شبكة الأنترنت التي قام بها المشترك/المواقع التي زارها المستخدم/عناوين IP التي استخدمها وحتى رسائل ومضمون رسائل بريده الالكتروني[31].

الفقرة الثالثة / شرط الحصول على رخصة النشر على شبكة الأنترنت

تم في سنغافورة سنة 2009 وضع نظام خاص من قبل السلطات في شكل حاجز مالي يقضي بضرورة دفع مقابل يقدر بـ 29000 أورو من قبل كل مؤسس موقع على شبكة الأنترنت، ينشر أخباراً عن أوضاع البلاد، ولكل موقع إلكتروني يبث من سنغافورة و يزوره أكثر من 50.000 ألف متصفح وذلك لأجل الحصول على رخصة النشر عبر شبكة الأنترنت[32].

إذن مما سبق فإنّه يتضح لنا أنّ المراقبة الإلكترونية ليست ذلك الإجراء القانوني الذي يراعى عند تنفيذه مبادئ إحترام الحق في الخصوصية المعلوماتية على الدوام، فأغلب الدول و الحكومات أصبحت تلجأ إلى ممارسة هذا الإجراء بذريعة الوقاية و مكافحة الجرائم المعلوماتية الماسة بأمنها و سلامتها، حتى و إن تعارض مع كل الضمانات القانونية الموضوعة و الحقوق المعترف بها للأفراد داخل الفضاء الرقمي.

المطلب الثاني/واقع المراقبة الإلكترونية للإتصالات على المستوى الوطني

يعتبر التشريع الجزائري تشريعا حديث العهد في مجال تنظيم الفضاء الرقمي، و ذلك نتيجة حداثة عهد المجتمع الجزائري مع تقنية المعلوماتية، التي تعتبر في حالة انتشار واسع النطاق في الآونة الأخيرة، و لعل أنّ الدليل على ذلك هو المعدلات المنخفضة للجرائم المعلوماتية على المستوى الوطني مقارنة بما هو عليه الحال في الدول

المتقدمة ففي هذا الصدد سجلت الوحدات المتخصصة لمركز الوقاية من الجرائم المعلوماتية للدرك الوطني سنة 2009 ثمانية عشرا (18) قضية معالجة بينما سجلت في العشر أشهر الأخيرة من سنة 2015 مائتين و أربعين(240) قضية معالجة [33].

الفرع الأول/الجهود التشريعية في مجال إقرار إجراء المراقبة الإلكترونية

بالرغم من المعدلات المنخفضة للجرائم المعلوماتية في الجزائر إلا أنّ ذلك لم يمنع المشرع الجزائري من إقرار نصوص قانونية تتضمن أحكاما خاصة للوقاية و مكافحة الجرائم المعلوماتية إدراكا منه لخطورة هذا النوع من الجرائم و سهولة انتشاره بفعل إنتشار تقنية المعلوماتية ،و قد نص التشريع الإجرائي الجنائي الجزائري بدءا على إمكانية الوضع تحت المراقبة الالكترونية في مجال مكافحة الجرائم المعلوماتية حسب نصوص المواد 65 مكرر 5 إلى مكرر 10 قانون 06-22، وذلك تحت الفصل الرابع الموسوم باعتراض المراسلات و تسجيل الأصوات والتقاط الصور، بحيث يجوز لوكيل الجمهورية و كذلك لقاضي التحقيق في حال فتح تحقيق قضائي، منح إذن لضابط الشرطة القضائية المكلفين بالبحث و التحري عن الجرائم المعلوماتية، يتضمن اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية دون موافقة المعنيين بها، وذلك لمدة أقصاها 04 أشهر قابلة للتجديد، و قد تعزز اللجوء إلى هذا الأسلوب سنة 2009 بموجب نص كل من المادتين 03 و 04 الواردتين ضمن فصول القانون 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها اللتان عبرتا صراحة عن إجازة مباشرة إجراء الرقابة الإلكترونية فيما تعلق بالجرائم المعلوماتية، و لكن دون ذكر الهيئة المكلفة بتولي ذلك، و قد استمر الوضع كذلك إلى غاية صدور المرسوم الرئاسي 15-261 الذي حدد تشكلية و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال بتاريخ 08 أكتوبر 2015، و التي أصبحت تتولى إجراءات المراقبة الإلكترونية للإتصالات بصفة حصرية دون غيرها من الجهات.

الفرع الثاني/دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال في تنفيذ المراقبة الإلكترونية

تعود فكرة إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال إلى سنة 2009 و بالضبط منذ تاريخ 05 أوت 2009 تاريخ صدور القانون 09-04 المتعلق بتحديد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، بحيث جاء في نص المادة 13 منه على أنّه تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحته، تحدد تشكيلة الهيئة و تنظيمها و كيفية سيرها عن طريق التنظيم، و قد استلزم الأمر لصدور التنظيم الإنتظار لمدة 06 سنوات كاملة، أين صدر المرسوم الرئاسي رقم 15-268 بتاريخ 08 أكتوبر 2015 ضمن العدد الثالث و الخمسين 53 للجريدة الرسمية، و الذي تضمن في فصوله تحديد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

الفقرة الأولى/اختصاصات الهيئة في مجال المراقبة الإلكترونية

بيّنت الفقرة الثانية 02 من المادة 04 من المرسوم الرئاسي 15-261 أبرز مهام هذه الهيئة في مجال المراقبة ا إلكترونية و هي :

1-ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية و التخريبية و الماسة بأمن الدولة و ذلك تحت سلطة قاضي مختص و و ذلك كإختصاص حصري .

2-تجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مسارها من أجل إستعمالها في الإجراءات القضائية.

3-المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا المعلومات

الفقرة الثانية/طبيعة عمل الهيئة في مجال المراقبة الإلكترونية

تتولى مديرية المراقبة الوقائية و اليقظة الإلكترونية التابعة للهيئة تنفيذ عمليات المراقبة الوقائية للإتصالات الإلكترونية و القيام بإجراءات التفتيش والحجز داخل الأنظمة المعلوماتية إذا ما تعلق الأمر جرائم الإرهاب او التخريب و الجرائم الماسة بأمن

الدولة بناء على رخصة مكتوبة من السلطة القضائية و تحت رقابة القاضي المختص، ويعتبر هذا الإجراء تكليفا حصريا للهيئة بموجب نص المادتين 21 و 42 من المرسوم الرئاسي 15-261، و بالتالي لا يجوز إتخاذ أي إجراء في مواجهة الجرائم المعلوماتية الإرهابية أو ذات الطابع التخريبي أو الماسة بأمن الدولة من قبل أي جهة أخرى سواء أمنية كانت أو قضائية، و تحول كل عمليات المراقبة الإلكترونية التي كانت تمارسها في السابق هيئات وطنية أخرى إلى إختصاص الهيئة.

إذن و بالنظر إلى التشكيلة و المهام الملحقة بهذه المديرية فإنّه يمكن وصفها بأنّها المركز العملياتي للهيئة بما أنّها تتولى الجانب التقني الخاص بإنجاز الأعمال المتعلقة بالبحث و التحقيق في الجرائم المعلوماتية، و لعل أنّ ما يزيد من دورها الفعال هو تنصيبها على رأس مركز العمليات التقنية و كذلك الملحقات مما يبرز دورها الفعال في تسيير و تأطير الأعمال المتعلقة بالوقاية أو بمكافحة الجرائم المعلوماتية[34].

خاتمة

من خلال عرضنا لما سبق يمكننا أن نخلص إلى أنّ إجراء المراقبة الإلكترونية لنشاط الأفراد عبر شبكات الأنظمة المعلوماتية، هو إجراء كباقي الإجراءات المتخذة في سبيل الوقاية و مكافحة الجرائم التقليدية، فهو إجراء لا يمكن الإستغناء عنه في مجال الوقاية و مكافحة الجرائم المعلوماتية بالنظر إلى الطبيعة الخاصة لهذه الجرائم و التي تعتبر خفية في غالبها، و خصوصا تلك التي تتسم بالخطورة البالغة على أمن و سلامة الدول و مواطنيها، و التي أصبحت توصف بجرائم الإرهاب الإلكتروني، و ذلك بالرغم من صور التعدي البالغة التي يشكلها في مواجهة حق الفرد في الخصوصية المعلوماتية، فمن الصعب تغليب مصلحة الفرد على مصلحة الجماعة إذا ما تعلق الأمر بجرائم الإرهاب طالما أنّ هذه الأخيرة تستهدف مصالح الدول و الجماعات مجتمعة دون تمييز، غير أنّه ليس من الضروري تأصيل مبدأ إنتهاك الخصوصية المعلوماتية للأفراد خصوصا في ظل إعتمادهم شبه المطلق على تقنية المعلوماتية، بدعوى الوقاية و مكافحة جرائم الإرهاب الإلكتروني من خلال تعميم اللجوء إلى المراقبة الإلكترونية السرية خارج نطاق الضمانات القانونية و التشريعية المقررة.

في الأخير فإنّنا نتوقع و في ظل الإنتشار اللامحدود لتقنية المعلوماتية و شبكة الأنترنت، و في ظل إستغلالها في النشاطات الإرهابية التي أصبحت تهدد الأمن الدولي عموما ، ازديادا لمظاهر المراقبة الإلكترونية و سقوطا لعديد من الأحكام التي كانت تنادي بضرورة الحفاظ على حق الفرد في الخصوصية داخل الفضاء الرقمي.

الهوامش:

(1). بولين أنطونيوس أيوب – الحماية القانونية للحياة الشخصية في مجال المعلوماتية – دراسة مقارنة – الطبعة الأولى- منشورات الحلبي الحقوقية- بيروت – لبنان– 2009-ص 08.

(2). علي حسن أحمد الطوالبة - التفتيش الجنائي على نظم الحاسوب و الانترنت- دراسة مقارنة- عالم الكتب الحديث – اربط- الأردن – 2004- ص 205.

(3). بولين أنطونيوس أيوب-مرجع سابق-ص 44.

(4). بولين أنطونيوس أيوب-مرجع سابق-ص 56.

(5). سوزان عدنان الأستاذ-" إنتهاك حرمة الحياة الخاصة عبر الأنترنت- دراسة مقارنة" - مقالة منشورة بمجلة جامعة دمشق للعلوم الإقتصادية و القانونية – المجلد 29- العدد 03- دمشق- سوريا- 2013-ص 433.

(6). بولين أنطونيوس أيوب-مرجع سابق-ص 56.

(7). عنوان بروتوكول الأنترنت- (Adresse IP) Adresse internet Protocol و يعرف أيضا بالعنوان الرباعي المنقط، و هو عنوان رقمي خاص بكل حاسوب يضمن التعريف به على شبكة الانترنت و تحديد موقعه، يتكون من أربعة مجموعات من الأرقام تفصل بينها النقاط.

(8). Toby Mendel et Natalia Torres- Etude mondial sur le respect de la vie privé sur l'internet et la liberté d'expression – collection de L'Unesco sur la liberté de l'internet-secteur de la communication et de l'information – l'organisation des nations unies pour l'éducation la science et la culture- Paris – France- 2013-p 7

(9). أُعتمد الإعلان العالمي لحقوق الإنسان ونشر على الملأ بموجب قرار الجمعية العامة للأمم المتحدة 217 ألف (د-3) المؤرخ في 10ديسمبر 1948.

(10). أُعتمد الميثاق العربي لحقوق الإنسان في نسخته الحديثة من قبل الأعضاء المشاركين في القمة العربية السادسة عشرة التي استضافتها تونس في 23ماي 2004.

(11). الحق في الخصوصية في العصر الرقمي- تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان- مجلس حقوق الإنسان الدورة السابعة والعشرون- ديسمبر 2013- الجمعية العامة للأمم المتحدة – ص 01 - متوفر على شبكة الأنترنت- تاريخ التصفح : 2015/12/12. الرابط الإلكتروني :
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_ar.doc

(12). المادة 303 ق 06-23 قانون العقوبات الجزائري.

(13). المادة 303 مكرر و المادة 303 مكرر 1 ق 06-22 قانون العقوبات الجزائري.

(14). لمزيد من التفصيل راجع نص المادة 04 فقرة 04-05 من المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيات الإعلام و الإتصال.

(15) نبيلة هبة هروال- الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات – دار الفكر الجامعي- الإسكندرية- مصر – 2007-ص 198،197.

(16) نبيلة هبة هروال- مرجع سابق- ص 199.

(17) Macdonald Raegen- liberté sur internet et droit a la vie privée protection des données a caractère personnel et respect des formes l égales – Rapport présenté pour la Conférence des ministres du conseil de l'Europe responsable des medias et de la sécurité de l'information – Belgrade-Serbie- le 7 – 8 Novembre 2013-p 08 disponible sur internet – date de consultation 01 /11/2015. lien directe: http://www.coe.int/t/dghl/standardsetting/media/belgrade2013/MCM(2013)008_Rapport_MacDonald_fr.pdf

(18) Les Ennemis d'internet 2014- rapport publier par l'organisation Reporters Sans Frontières a l'occasion de la journée mondiale contre la cyber-censure-12 Mars 2014- p 03 ,04. disponible sur internet- date de consultation : le 01 /11/2015.
lien directe : www .12Mars .rsf .org

(19) Toby Mendel et Natalia Torres- op cit – p : 21.

(20) المادة 05 فقرة 01 - المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال.

(21) المادة 2-الفقرة-ه القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

(22) المادة 2-الفقرة-د القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

(23) عائشة بن قارة- حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن- دار الجامعة الجديدة – الإسكندرية – مصر – 2010-ص 154.

(24) هلالي عبد اللاه أحمد – إتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقا عليها – الطبعة الأولى– دار النهضة العربية – مصر – 2008- ص 198،197.

(25) عائشة بن قارة-مرجع سابق – ص 161.

(26) هلالي عبد اللاه أحمد-مرجع سابق- ص 231،230.

(27) نص المادة 20 و 21 من إتفاقية بودابست لمكافحة الجرائم المعلوماتية - المنبثقة عن اجتماع المجلس الأوربي ببودابست - المجر تحت رقم 185- بتاريخ 21 نوفمبر 2001.

(28) بوعناد فاطمة الزهرة-" مكافحة الجريمة الإلكترونية في التشريع الجزائري"-مقالة علمية منشورة بمجلة الندوة للدراسات القانونية- العدد الأول – مركز الدراسات القانونية – الجزائر- سنة 2013-ص 72 .

(29) هلالي عبد اللاه أحمد- مرجع سابق- ص 275،274.

(30) Les Ennemis d'internet 2014 -Op cit – P 05.

(31) Les Ennemis d'internet 2014 -Op cit – P07

(32) Les Ennemis d'internet 2014 -Op cit – P08

(33) المقدم عزالدين عزالدين من مركز الوقاية من جرائم المعلوماتية ومكافحتها القيادة العامة للدرك الوطني - الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها- ورقة بحثية مقدمة لأشغال الملتقى الوطني للوقاية من الجرائم المعلوماتية و مكافحتها- كلية الحقوق- جامعة بسكرة – الجزائر – 16و17 نوفمبر 2015- ص 30

(34) المواد11-13-14- 18-21 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.