تدابير حماية أمن المعطيات الشخصية على شبكة الانترنت
– دراسة مقارنة–

بركات كريمة [1]

[1] أستاذة محاضرة "أ"، كلية الحقوق و العلوم السياسية، جامعة البويرة، 10000 ، الجزائر.

البريد الإلكتروني: karimabk399@gmail.com

الملخص:

تطور تكنولوجيا الاتصال و الإعلام وتشعب استخدام تطبيقات شبكة الانترنت في أوساط المجتمعات، وتوسع نطاق المشكلات الأمنية لشبكات الحاسوب، و ضخامة حجم مخاطرها (الجرائم الالكترونية) التي تزداد بازدياد مستخدمي الشبكات وبظهور ثقافة جديدة في صناعة البرامج المعلوماتية الخبيثة و انتشارها في أوساط الأفراد، أصبح من غير الممكن الإلمام بجميع التهديدات و تصور تحقيقا لأمن المعلومات للشبكات المحمية بصفة نهائية و أكيدة، مما يؤدي إلى ضرورة وضع سياسة حماية أمنية تتجاوب مع عوامل و مستجدات البيئة الالكترونية الافتراضية، مع ضمان حد مقبول من المخاطر المتوقعة.

وبما أن المخاطر و التهديدات الالكترونية تمس المصالح الحيوية للدول، فإن عملية المعالجة الآلية للمعطيات الشخصية للأشخاص الطبيعيين تتطلب إرساء تدابير تقنية لها، كما تتطلب معاملات التجارة الالكترونية الاستعانة بخدمات جهات الرقابة على الانترنت (تدابير قانونية).

الكلمات المفتاحية:

المعطيات الشخصية، الحماية الأمنية، التدابير التقنية، جهات الرقابة على الانترنت.

تاريخ إرسال المقال:2020/11/02، **تاريخ قبول المقال:**2021/08/17، **تاريخ نشر المقال:**2021/10/10.

لتهميش المقال: بركات كريمة، "تدابير حماية أمن المعطيات الشخصية عل شبكة الانترنت– دراسة مقارنة–"، المجلة الأكاديمية للبحث القانوني، المجلد 12، العدد 02، 2021، ص ص. 395–412.

المقال متوفر على الرابط التالي: https://www.asjp.cerist.dz/en/PresentationRevue/72

المؤلف المراسل: بركات كريمة karimabk399@gmail.com

Measures to protect the security of personal data on the Internet - a comparative study-

Summary:

With the tremendous development of technology, communication and media, and the divergence of the uses of Internet applications, and the expansion of the security problems of computer networks, the magnitude of their risks (cybercrimes), and the emergence of a culture in the manufacture of malicious information programs, it has become impossible to be aware of the threats and to achieving information security for the protected networks in a definitive and certain way, which leads to the need to develop a security protection policy that is responsive to the factors and developments of the virtual electronic environment, while ensuring an acceptable level of risks. The process of automatic processing of personal data of natural persons requires the establishment of technical measures for them, and e-commerce transactions require the use of the services of Internet controllers.

Keywords:

personal data, security protection, technical measures, Internet censors.

Mesures de protection de la sécurité des données personnelles sur Internet –étude comparative-

Résumé :

Avec le développement des technologies de la communication et de l'information, la complexité des usages des applications Internet dans les sociétés, l'expansion des problèmes de sécurité des réseaux informatiques, l'ampleur de leurs risques (cybercrimes) qui augmentent avec l'augmentation des utilisateurs des réseaux et l'émergence d'une nouvelle culture dans la fabrication de programmes d'information malveillants et leur diffusion, il s'avère impossible de cerner toutes les menaces et encore moins d'assurer la sécurité informatique des réseaux protégés d'une manière définitive et réelle, d'où vienne la nécessité de mettre en place une politique qui s'adapte aux facteurs et aux évolutions de l'environnement électronique virtuelle, tout en assurant un seuil minimum de risques prévisibles. Etant donné que les risques et les menaces électroniques affectent les intérêts vitaux des Etats, le processus de traitement des données personnelles des personnes physiques nécessite la mise en place de mesures techniques et les transactions du commerce électronique nécessitent également l'utilisation des services de contrôleurs Internet (mesures légales).

Mots clés:

Données personnelles, protection de la sécurité, mesures techniques, censeurs Internet.

مقدمة:

إن انتشار شبكة الانترنت وتحولها إلى وسيلة مالية مربحة في مجال الأعمال، ساهم بشكل كبير في انتشار ونمو تطبيقات التجارة الالكترونية، وتطور المعدات والبرامج المعلوماتية، وتطورت نظم وتقنيات المعالجة الآلية Big Data، التي سمحت للمتعاملين الاقتصاديين بترويج مختلف السلع والخدمات عبر مواقع الكترونية افتراضية.

وأضحت هذه المواقع الالكترونية مملوءة بمختلف المخاطر المتعلقة بالقرصنة والتجسس وتدمير المواقع الالكترونية، وإساءة أو تعطيل موارد الشبكات وانتحال الهويات...إلخ، ولعل أهم المشكلات الأمنية المطروحة حاليا على مستوى شبكات الاتصالات التجارية هي تلك المتعلقة بالخصوصية والحماية، ومصداقية و إنكار المعلومات الشخصية التي يتم تداولها وتحويلها فيما بين أطراف التعاقد الالكتروني عبر مواقع التجارة الالكترونية، ولتفادي تلك التهديدات يتعين على متخذي القرار إرساء الضمانات التقنية اللازمة لحماية المعطيات الشخصية المتداولة عبر مواقع التجارة الالكترونية من جمعها ومعالجتها لأهداف غير مشروعة، وذلك بهدف خلق مناخ من الثقة مع المتعامل، لكي يقبل بإعطاء بياناته من دون التخوف من احتمال الاستعمال السيئ لها.

كما أصبحت مواقع التجارة الالكترونية الهدف الرئيسي للعديد من العصابات والمجرمين الذين يقومون بتنفيذ الهجمات الالكترونية، لغرض التجسس الصناعي أو الاستيلاء أو الاستحواذ على الأموال، أو الترويج لبرامج القرصنة وسرقة المعلومات المتداولة أو المخزنة، أو القيام بعمليات التسلل والاختراق إلى الشبكات من أجل تشويه السمعة الرقمية E-réputation... الخ، في حين أصبحت شبكة الانترنت أداة اتصال فعالة لهؤلاء، للنفوذ أو التغلغل إلى داخل الشبكات الداخلية لمواقع الشركات التجارية أو الصناعية، إذ أن معظمهم ينفذون تهديداتهم الخارجية انطلاقا من شبكة الانترنت، مستغلين في ذلك الثغرات الأمنيةالمتواجدة في أجهزة أو معدات حماية الشبكة، ومن هنا تبرز أهمية الحاجة إلى وضع سياسة أمنية ناجعة للحماية العالية للمعطيات الشخصية في الفضاء الرقمي.

إن حماية وتأمين الحياة الخاصة للفرد على شبكة الانترنت، لا تكمن فقط في إعداد وتوعية المتعامل الالكتروني عن مختلف التهديدات أو الأخطار المنبثقة، من حين لآخر من هذه الشبكة، وإنما تكمن كذلك في الاستخدام الأمثل لتقنيات الحماية الأمنية المتطلبة في مواقع التجارة الالكترونية أثناء أو قبل القيام بتصرفاته التجارية، كالتسوق الالكتروني الآمن وأيضا احترام التدابير التقنية المتطلبة في عملية المعالجة الآلية للمعطيات الشخصية، والاستعانة بخدمات جهات الرقابة على الانترنت المعتمدة من طرف الجهات الرسمية في الدولة.

وتظهر أهمية الموضوع في استجابته للمطالب القانونية والأخلاقية التي تفرض وجوب احترام سرية البيانات الخاصة بالمتعاملين على شبكة الانترنت، واحترام حقهم في الخصوصية، وذلك يستلزم عدم نشر أو بث

أي بيانات خاصة بشخصيتهم، أو كشف الغطاء عن حياتهم الشخصية أو بياناتهم المالية. كما لا يجوز الاحتفاظ بهذه البيانات إلا لفترة محددة تتعلق بالنشاط التجاري أو العملية التجارية التي يقوم بها؛ من ناحية أخرى فإنه لا يجوز لأية جهة التعامل في هذه المعطيات إلا بعد الحصول على موافقة كتابية من صاحب الشأن.

وطالما أن الحركة التشريعية في ميدان حماية المعطيات الشخصية عبر شبكة الانترنت في الجزائر، لا تزال ضيقة ومتعثرة، وقد دفعت الأهمية المتزايدة للتجارة الالكترونية إلى وجوب الوقوف أمام التدابير التشريعية لحماية أمن المعطيات الشخصية الالكترونية؛ وهذا الهدف المراد تحقيقه من هذه الدراسة.

وانطلاقا مما سبق، نطرح الإشكالية التالية:

ما هي التدابير التقنية والقانونية المكرسة لحماية وتأمين المعطيات الشخصية المتداولة على شبكة الانترنت، وما مدى فعاليتها لتحقيق ذلك على ضوء التشريعات المقارنة الناجحة؟

ونظرا لحداثة الموضوع ، وكذا خصوصيته وأهميته عموما، فقد ارتأينا لمناقشة الإشكالية ولإظهار أهمية الموضوع إتباع المنهج التحليلي المقارن من أجل تحليل ومقارنة تشريعات بعض الدول(الاتحاد الأوروبي ، فرنسا وتونس) والتي تتعلق أحكامها بتنظيم موضوع حماية المعطيات الشخصية عبر الانترنت، ومقارنتها بالتشريع الجزائري، وذلك محاولة منها لإثراء الموضوع.

وللإجابة علي الإشكالية نتناول بالدراسة وضع التدابير التقنية لحماية المعطيات الشخصية (مبحث أول) والاستعانة بخدمات جهات الرقابة على الانترنت (مبحث ثان).

المبحث الأول: وضع التدابير التقنية لحماية المعطيات الشخصية

لا يمكن معالجة المعطيات الشخصية إلا في إطار الشفافية والأمانة واحترام كرامة المواطن وفقا لمقتضيات التشريعات الأساسية (الدساتير) والقوانين الخاصة بحماية المعطيات الشخصية، حيث كرست مختلف التشريعات الأجنبية (مطلب أول) والعربية (مطلب ثان) مستوى ملائم من السلامة والأمان بغية حماية هذه المعطيات الشخصية من مختلف المخاطر.

المطلب الأول: التشريعات الأجنبية

فرضت مختلف التشريعات الأجنبية مجموعة من التدابير التقنية لحماية المعطيات الشخصية للأفراد نظرا للمخاطر التي تمثلها المعالجة وطبيعة المعطيات الشخصية الواجب حمايتها، والتي سنتطرق إليها على النحو التالي:

الفرع الأول: التنظيم الأوروبي رقم 679/2016 المتعلق بحماية المعطيات الشخصية

قام المشرع الفيدرالي للإتحاد الأوروبي بإصدار تنظيم أوروبي رقم 679/2016 مؤرخ في 27 أفريل2016 يتعلق بحماية الأشخاص الطبيعية لدى معالجة معطياتهم الشخصية مع حرية تنقلها Règlement Général de la Protection des Données[1] ، الملغي للتوجيه الأوروبي رقم 46/95 المؤرخ في 24 أكتوبر1995، الذي من خلاله عرف المعطيات الشخصية بموجب الفقرة الأولى(1) من المادة 04منه، أنها "كل معلومة تتصل بشخص طبيعي معرف أو قابل للتعرف عليه، وتعتبر هوية الشخص الطبيعي قابلة للتعريف بصفة مباشرة أو غير مباشرة، لا سيما بالرجوع إلى اسمه أو رقم تعريفه أو المعطيات التي تحدد موقعه أو ما يسمح بتعريف هويته عبر الخط أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".

في حين تتضمن المعالجة الآلية وفقا لنص الفقرة الثانية (2) من نفس المادة 04 من التنظيم الأوروبي رقم 679/2019، على " كل عملية أو مجموعة من العمليات المنجزة أم لا بواسطة طرق آلية لمعالجة المعطيات الشخصية، مثل الجمع أو التسجيل أوالحفظ أو التنظيم أو التغيير، أو الاستغلال أو الاستعمال أو الإرسال أو التوزيع أو النشر،أو أية عملية أخرى تهدف إلى التقريب أو التبادل أو التشفير أو المحو أو الإتلاف".

حيث ينبغي على المسؤول القائم بمعالجة المعطيات الشخصية الحصول على الموافقة الصريحة للشخص المعني بمعالجة معطياته، وذلك بعد إعلامه وقبوله وفقا لإرادته الذي يملك حرية في الرجوع عن الموافقة في أي وقت، ففي حالة ما إذا كان الشخص المعني أقل من 16 سنة فيشترط الحصول على موافقة وليه الشرعي، حيث منح مشرع الاتحاد الأوروبي لكل دولة عضوة في الإتحاد، حرية تحديد السن القانوني اللازمللحصول على موافقة الولي الشرعي، على أن لا يكون سن الطفل دون 13 سنة[2].

وعليه، ألزم التنظيم الأوروبي رقم 679/2016 بموجب المادة 25 منه المسؤول عن المعالجة الآلية للمعطيات الشخصية، بضرورة اتخاذ التدابير التقنية والتنظيمية الملائمة لحماية المعطيات الشخصية المتحصل عليها ضد كل عمل غير مشروع، عندما تجرى المعالجة لحساب المسؤول عن المعالجة يجب على المعالج من

---

[1]-Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l' égard du traitement des données à caractère personnel et à la libre circulation des données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), J O U E, L 119/1 du 04/05/2016.

[2]-Art.08/01 du Règlement (UE) 2016/679.

الباطن (Sous traitant) أن يحترم الإجراءات الأمنية المتعلقة بأمن وسلامة وسرية المعطيات الشخصية، وأن لا يتصرف إلا في حدود تعليمات المسؤول على معالجة المعطيات الشخصية، إلى جانب المتطلبات المحددة بموجب المادة 28 من نفس التنظيم الأوروبي[1].

الفرع الثاني: القانون الفرنسي

قام الرئيس الفرنسي EMMANUEL Macron بإصدار الأمر رقم 1125/2018 المؤرخ في 12 ديسمبر 2018، المتعلق بتطبيق أحكام المادة 32 من القانون رقم 493/2018 المؤرخ في 20 جوان 2018، المتعلق بحماية المعطيات الشخصية[2]، المعدل للقانون رقم 17/78 المؤرخ في 06 جانفي 1978، المتعلق بالإعلام والملفات والحريات، الذي من خلاله طبق أحكام التنظيم الأوروبي رقم 679/2016، المتعلق بحماية الأشخاص الطبيعية لدى معالجة معطياتهم الشخصية، مع حرية تنقلها.

ووفقا لأحكام المواد 04 و05 و57 من الأمر المذكور أعلاه، يجب على المسؤول عن المعالجة أو المعالج من الباطن، أن لا يقوم بمعالجة المعطيات الشخصية إلا بعد الحصول على الموافقة الصريحة للشخص المعني (وفقا للشروط المحددة بموجب المادة 11/04 والمادة 07 من التنظيم الأوروبي رقم 679/2018)، وأن تتم عملية معالجتها بطريقة مشروعة ونزيهة، وفقا للغايات التي من أجلها تم جمعها ومعالجتها وأن لا تعالج لاحقا بطريقة تتنافى مع هذه الغايات، مع حفظها بشكل يسمح بالتعرف على الأشخاص المعنيين خلال المدة اللازمة لإنجاز الأغراض التي من أجلها تم جمعها ومعالجتها، وذلك باستثناء حالات حفظها في الأرشيف للمصلحة العامة أو لغايات إجراء الدراسات العلمية أو حماية المعطيات الشخصية من الضياع أو الإتلاف أو الولوج غير المرخص به أو أي عملية معالجة غير مشروعة لهذه المعطيات[3].

في حالة لجوء المسؤول عن المعالجة إلى المناولة لمعالجة المعطيات الشخصية لحسابه(المسؤول عن المعالجة)، يجب على المعالج من الباطن أن يقدم في إطار عقد المناولة الضمانات الكافية المتعلقة بإجراءات السلامة التقنية للمعالجات الواجب القيام بها مع السهر على احترامها، مع الالتزام بعدم التصرف إلا في حدود

---

[1]– مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت، بين القانون الدولي الإتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع،مصر،2017، ص ص 402–404.

[2]- Loi n° 2018/493 du 20 juin 2018 relative à la protection des données personnelles, J O R F, n° 0141 du 21 juin 2018.

[3]- Ordonnance n° 2018/1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018/493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78/17 du 06 janvier 1978 relative à l'information, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, J O R F, n° 0288 du 13 décembre 2018.

تعليمات المسؤول على معالجة المعطيات الشخصية، فعندما تتعرض هذه الأخيرة إلى انتهاكات يجب على المسؤول عن المعالجة أو ممثله، القيام بإخطار الهيئة الوطنية للإعلام الآلي والحريات (CNIL)، مع تدوين كافة هذه الانتهاكات والإجراءات المتخذة بشأنها في جرد خاص بمعالجة المعطيات الشخصية وفق الشروط المحددة بموجب المادة 30 من التنظيم الأوروبي رقم 679/2016 المذكور سابقا.

المطلب الثاني: التشريعات العربية

تحظى المعطيات الشخصية بأهمية لدى تشريعات الدول العربية على غرار كل من تونس (فرع أول)والجزائر(فرع ثان)، التي نصتمن خلالها على مجموعة من التدابيرالتقنية لحمايتها من مخاطر المعالجة الآلية.

الفرع الأول: القانون التونسي

قام المشرع التونسي بإصدار القانون الأساسي عدد 63-2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية[1]، الذي اعتبر المعطيات الشخصية بموجب الفصل الأول منه ضمن الحقوق الأساسية المتعلقة بالحياة الخاصة للأشخاص والمضمونة بموجب الدستور، حيث لا يجوز معالجتها إلا في إطار الشفافية والأمانة واحترام كرامتهم وفقا لمقتضيات هذا القانون[2].

في حين نص الفصل السابع والعشرون من نفس القانون على عدم إمكانية معالجة المعطيات الشخصية، إلا بعد الحصول على الموافقة الصريحة والكتابية للمعني بالأمر أو وليه في حالة ما إذا كان قاصرا أو محجورا عليه أو غير قادر على الإمضاء، إذ يمكن للمعني بالأمر أو وليه الرجوع عن الموافقة في أي وقت، وعليه يجب أن تتم عملية جمع المعطيات لغرض تحقيق الغاية التي جمعت من أجلها، وذلك باستثناء الحالات المذكورة في المادة 12 من نفس القانون الأساسي، والتي نصت على ما يلي:" لا تجوز معالجة المعطيات الشخصية في غير الأغراض التي جمعت من أجلها إلا في الحالات التالية:- إذا وافق المعني بالأمر على ذلك، -إذا كان في ذلك تحقيق لمصلحة حيوية للمعني بالأمر، - إذاكانت لأغراض علمية ثابتة".

---

[1]- القانون الأساسي عدد 63-2004 المؤرخ في 27 جويلية 2004، يتعلق بحماية المعطيات الشخصية، الرائد الرسمي للجمهورية التونسية العدد 61 الصادر في 30 جويلية 2004.

[2] - ينص الفصل العاشر (10) من القانون الأساسي عدد 63-2004، (المرجع السابق) على ما يلي:" **لا يجوز جمع المعطيات الشخصية إلا لأغراض مشروعة ومحددة وواضحة**".كما ينص الفصل الحادي عشر (11) من نفس القانون الأساسي على ما يلي:" يجب أن تتم معالجة المعطيات الشخصية بكامل الأمانة وفي حدود ما كان منها ضروريا للغرض الذي جمعت من أجله. كما يجب على المسؤول عن المعالجة الحرص على أن تكون المعطيات صحيحة ودقيقة ومحينة."

الفرع الثاني: القانون الجزائري

نص المشرع الجزائري بموجب المادة 02 من القانون رقم 18-07 المؤرخ في 10 جويلية 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1]، على أن تتم عملية المعالجة الآلية للمعطيات الشخصية مهما كان مصدرها أو شكلها في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم.

فالمعطيات الشخصية وفقا لنص المادة 03 من القانون رقم 18-07 تشتمل على كلمعلومة مهما كانت دعامتها، تتعلق بشخص معرف الهوية أو قابل للتعرف عليها بصفةمباشرة أو غير مباشرة، عن طريق الرجوع إلى رقم التعريف أو عنصر أو عدة عناصرخاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أوالثقافية أو الاجتماعية، حيث لا يمكن القيام بعملية المعالجة الآلية لهذه المعطيات إلا بعد الحصول على الموافقة الصريحة للشخص المعني، الذي يملك الحرية الكاملة في التراجع عن موافقته في أية لحظة، فإذا كان ذلك الشخص عديم أو ناقص الأهلية فإن الموافقة تخضع للإجراءات المنصوص عليها في القانون المدني[2].

وفي جميع الظروف ينبغي أن تتم عملية جمع المعطيات الشخصية لغرض تحقيق الغاية التي جمعت من أجلها وبعد الحصول على الموافقة المسبقة والصريحة للشخص المعني، وذلك باستثناء الحالات الواردة بموجب نص الفقرة الأخيرة من المادة 07 من القانون رقم 18-07، والتي لا تكون فيها موافقة الشخص المعني واجبة، إذا كانت المعالجة ضرورية:

- لاحترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة.
- لحماية حياة الشخص المعني.
- لتنفيذعقد يكون الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه.
- للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه.

---

[1] – قانون رقم 18-07 مؤرخ في 10 جويلية 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر العدد 34، الصادر في 10 جويلية 2018.

[2] – طبقا لنص الفقرتين 02 و03 من المادة 07 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، مرجع سابق. كما أنه طبقا لنص المادة 08 من نفس القانون، لا يمكن القيام بمعالجة المعطيات الشخصية المتعلقة بطفل إلا بعد الحصول على موافقة ممثله الشرعي أو عند الاقتضاء، بترخيص من القاضي المختص.

- لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة أو الغير الذي يتم إطلاعه على المعطيات.
- لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه مع مراعاة مصلحة الشخص المعني و/ أو حقوقه وحرياته الأساسية.

وانطلاقا من ذلك ألزم المشرع الجزائري المسؤول عن المعالجة إرساء واحترام إجراءات السلامة التقنية والتنظيمية لحماية المعطيات الشخصية بما يتلاءم مع المخاطر المحيطة بها، فعندما تجرى المعالجة لحساب المسؤول عن المعالجة، يجب عليه اختيار "معالج من الباطن" يقدم الضمانات الكافية بإجراء السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها مع السهر على احترامها، حيث ينبغي على المعالج من الباطن أن لا يتصرف إلا بناء على تعليمات من المسؤول على المعالجة والتقيد بالتزاماته العقدية والقانونية، كما يجب على كل شخص يعمل تحت سلطة المسؤول عن المعالجة أو سلطة المعالج من الباطن، ويقوم بمعالجة المعطيات الشخصية أن يحترم تعليمات المسؤول عن المعالجة وذلك باستثناء حالة اطلعوا أثناء ممارسة مهامهم على المعطيات الشخصية، الالتزام بالسر المهني حتى بعد انتهاء مهامهم وذلك تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول[1].

فإذا تعرضت المعطيات الشخصية عبر شبكات الاتصالات المفتوحة للجمهور إلى الإتلاف أو الضياع أو إفشائها أو الولوج غير المرخص إليها، يجب على مقدم الخدمات Fournisseur، أن يقوم وفقا لنص المادة 43 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. بإخطار السلطة والشخص المعني في حالة المساس بحياته الخاصة، وذلك ما لم تقرر السلطة الوطنية أن الضمانات الضرورية لحماية المعطيات الشخصية لصاحبها قد تم اتخاذها من قبل مقدم الخدمات، حيث يجب على هذا الأخير أن يكون لديه جردا محينا(Un inventaire à jour) حول الانتهاكات المتعلقة بالمعطيات الشخصية والإجراءات التي اتخذها بشأنها.

كما تخضع عملية معالجة المعطيات الشخصية لتصريح مسبق لدى السلطة الوطنية أو لترخيص منها، وذلك ما لم يوجد نص قانوني يقضي بخلاف ذلك، حيث يمكن للمسؤول عن المعالجة أن يباشر تحت مسؤوليته عملية معالجة المعطيات الشخصية بمجرد استلامه وصل الإيداع (يسلم أو يرسل إليه إلكترونيا في أجل أقصاه 48 ساعة)، فعندما يتبين للسلطة الوطنية أثناء دراسة طلب التصريح أن المعالجة المعتزم القيام بها تتضمن

[1]- راجع أحكام المواد من 38 إلى 41 من القانون رقم 18-07 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المرجع السابق.

أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص، فإنها تقرر إخضاع المعالجة المعنية لنظام الترخيص المسبق حيث يجب أن يكون القرار مسببا مع تبليغه للمسؤول عن المعالجة في أجل العشرة (10) أيام التي تلي تاريخ إيداع طلب التصريح[1].

المبحث الثاني: الاستعانة بخدمات جهات الرقابة على الانترنت

يعتبرميدان التجارة الالكترونية أكثر عرضة وتهديدا من طرف القراصنة، الذين يتقنون استخدام تقنيات التجسس والنصب والاحتيال ونهب أو سرقة الأموال، وقرصنة البيانات الشخصية والسرية لأصحاب البطاقات المصرفية الذكية، والتصنت على الاتصالات...إلخ، الأمر الذي أدى بأصحاب مواقع التجارة الالكترونية إلى الاستعانة بخدمات شركات الأمن المعلوماتي التي تستعين بكفاءات بشرية متميزة، يتمتعون بخبرات واسعة في مجال تكنولوجيا الاتصال والإعلام، وتستخدم أحدث التقنيات التكنولوجية في كشف الفيروسات والبرمجيات الخبيثة المعقدة بشتى أنواعها، وكذلك تقوم بإخطار عملائها بمستجدات التهديدات المكتشفة مع اتخاذ التوصيات أو الاحتياطات اللازمة لتفاديها.

وعليه، تسمح التقنيات المعتمدة من طرف شركات الأمن المعلوماتي بالتفتيش العميق في صفحات المواقع وأنظمة الشبكات، بغية البحث عن عمليات الاختراق أو رصد والكشف عن الثغرات الأمنية المتواجدة على مستوى أنظمة الحماية الأمنية للشبكات المتسببة من طرف أنواع معينة من الديدان أو الفيروسات وأحصنة طروادة[2]، حيث تقوم هذه الشركات بإتاحة برمجيات الوقاية من مختلف الفيروسات والبرمجيات الضارة وفقا لمستويات عالية من الأمان المتطلبة، فمن بين أهم شركات الأمن المعلوماتي التي يعول عليها في كشف وترصد ومكافحة مختلف الجرائم والتهديدات الالكترونية نجد كل من: KasperSky, F-Secure, ESET, Symantec, Virus Blok Ada, E-trust, MacAFee,...etc.

---

[1]- راجع أحكام المواد من 12 إلى 21 من القانون رقم 18-07 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية، المرجع السابق.

[2]- "حصان طروادة " Cheval de Troie هي شفرة صغيرة، يتم تحميلها مع برنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالبا ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه و سرقة بياناته، وهي تمكن المنشئ من تنفيذ أي يريده على الحاسوب المصاب، بما في ذلك إرسال الملفات واستلامها وتشغيلها وحذفها وعرض البيانات وإعادة تشغيل الحاسوب. وغالبا ما تستخدم أحصنة طروادة المتسللة لتوحيد مجموعة من الحواسيب الضحية لتشكل شبكة بوت نت أو زومبي التي يمكن استخدامها لأغراض إجرامية.

وباتت مخاطر أمن المعلومات ترقى إلى مستوى تهديد الأمن الوطني للدول، الأمر الذي دفع بهذه الأخيرة إلى إحداث وكالات أمن وطنية تشرف على عمليات رقابة وأمن مختلف شبكات الاتصالات، والتنبؤ من مختلف التهديدات الخارجية والداخلية التي من شأنها أن تمس بأمنها واقتصادها الوطنيين واستقرار مؤسساتها ومصالحها الحيوية، حيث سنتطرق إلى بعض التشريعات الأجنبية (مطلب أول)، والوطنية (مطلب ثان)، المنشئة لهذه الوكالات على النحو التالي:

المطلب الأول: التشريعات الأجنبية

قامت معظم الدول الأجنبية بإرساء منظومة أمنية موثوقة شاملة تشرف على وكالات أمنية وطنية، بغية التنبؤ من مختلف التهديدات عبر شبكات الاتصالات، ونذكر من بين هذه التشريعات الأجنبية ما يلي:

الفرع الأول:التنظيم الأوروبي رقم 460/2004 المتعلق بإنشاء وكالة AESRI

قام المشرع الفدرالي للإتحاد الأوروبي، بموجب المادة 01 فقرة أولى (1/01) من التنظيم الأوروبي رقم 460/2004 المؤرخ في 10 مارس 2004، المتعلق بإنشاء **وكالة أوروبية مكلفة بأمن الشبكات والمعلومات**[1]، باستحداث وكالة أوروبية تشرف على سلامة أمن الشبكات والمعلومات Agence Européenne chargée de la Sécurité des Réseaux et de l'Information (**AESRI**).

وتشرف الوكالة الأوروبية لأمن الشبكات والمعلومات وفقا لنص المادة 03 من نفس التنظيم المذكور أعلاه على المهام المتعلقة بجمع واستغلال المعلومات المفيدة، التي تسمح بالتنبؤ والكشف عن مختلف التهديدات أو الجرائم الالكترونية التي تمس بأمن الاتحاد الأوروبي والإحاطة بجميع المخاطر بغية توحيد استراتيجيات السياسة الأمنية، مع تنظيم عمليات التوعية لمستخدمي الشبكات والمعلومات وتزويدهم بالمستجدات الطارئة حول مخاطر استعمال التقنيات التكنولوجية الحديثة، وكذا توحيد المعايير في المعدات والبرمجيات المستخدمة في مجال أمن الشبكات والمعلومات، مع تكثيف وتنسيق التعاون فيما بين دول الإتحادالأوروبي أو مع الدول الأجنبية بشأن أمن الشبكات والمخاطر المتعلقة بها.

الفرع الثاني: القانون الفرنسي

قام المشرع الفرنسي بإحداث الوكالة الوطنية لأمن أنظمة المعلومات(ANSSI) لدىالوزير الأول والملحقة بالأمين العام للدفاع والأمن الوطنيين، بموجب المادة الأولى(01) من المرسوم رقم 834/2009 المؤرخ في 07

[1]- Règlement (CE) n° 2004/460 du parlement européen et du conseil du 10 mars 2004 instituant l'agence européenne chargée de la sécurité des réseaux et de l'information, J O U E, n° L77/1 du 13/03/2004.

جويلية 2009 المتعلق بإنشاء مصلحة ذات اختصاص وطني تدعى" الوكالة الوطنية لأمن أنظمة المعلومات"[1].

وتشرف الوكالة وفقا لنص المادة 03 من نفس المرسوم على مجموعة من المهام: كالمساهمة في اقتراح القواعد القانونية المتعلقة بحماية أنظمة المعلومات والتحقق من مدى تطبيق إجراءاتها، وضمان المراقبة الوقائية للاتصالات الالكترونية لغرض الكشف عن الجرائم الالكترونية التي تمس بأمن الدولة ومؤسساتها والاقتصاد الوطني، مع القيام بعمليات التنسيق والتوعية للوقاية من الجرائم الالكترونية ومكافحتها والسهر على إعداد استراتيجيات الوقاية منها، وكذا تنفيذ مخططات الطوارئ من خلال تنبيه وإخطار كافة المستخدمين من مختلف التهديدات الالكترونية، والتعاون مع نظيراتها الأجنبية في المجالات المتعلقة بأمن الشبكات والمعلومات، والإشراف على مخططات التصديق والاعتماد على المراكز والوسائل والمعدات المستخدمة في أمن أنظمة المعلومات والشبكات[2].

المطلب الثاني: التشريعات العربية

أصبحت مخاطر شبكة الانترنت تمس جميع الدول التي رفعت شعار التحول إلى مجتمع المعلومات، وبالخصوص الدول العربية التي قامت بإحداث وكالات أمن وطنية للرقابة والتنبؤ من مختلف التهديدات عبر شبكات الاتصالات، نذكر من بينها:

الفرع الأول: القانون التونسي

قام المشرع التونسي بموجب الفصل الثاني (02) من القانون عدد 05-2004 المؤرخ في 03 فيفري 2004 المتعلق بالسلامة المعلوماتية[3]، بإحداث **الوكالة الوطنيةللسلامة المعلوماتية** كمؤسسة عمومية لا تكتسي الصبغة الإدارية،وتتمتع بالشخصية المعنوية والذمة المالية المستقلة وتخضع إلى التشريع التجاري في علاقاتها مع الغير.

وتشرف الوكالة، وفقا للفصل الثالث(03) من نفس القانون، على جميع المهام المتعلقة بمراقبة النظم المعلوماتية وشبكات مختلف الهياكل العمومية والخاصة، مع ضمان اليقظة التكنولوجية في مجال السلامة المعلوماتية، والسهر على تنفيذ الترتيبات المتعلقة بإجبارية التدقيق الدوري للسلامة المعلوماتية والشبكات ومدى

---

[1]-Décret n° 2009/834 du 07 juillet 2009 portant création d'un service à compétence nationale dénommé » Agence nationale de la sécurité des systèmes d' information », J O R F, n° 0156 du 08 juillet 2009.

[2]- Anne SOUVIRA, Myriam QUEMENER, « Cyber-sécurité et entreprises : se protège juridiquement et se forme »,Revue sécurité et stratégie, 4, (11), 2012, pp. 90, 91.

16- قانون عدد 05-2004 مؤرخ في 03 فيفري 2004 يتعلق بالسلامة المعلوماتية، الرائد الرسمي للجمهورية التونسية، العدد 10، الصادر في 03 فيفري 2004.

تنفيذ التوجهات الوطنية، والإستراتيجية العامة لسلامة النظم المعلوماتية والشبكات وكذا الخطط والبرامج المتعلقة بالسلامة المعلوماتية في القطاع العمومي باستثناء التطبيقات الخاصة بالدفاع والأمن الوطنيين، والتنسيق بين المتدخلين في هذا المجال، ووضع وإعداد ونشر مقاييس وأدلة فنية خاصة بالسلامة المعلوماتية والعمل على تشجيع تطوير حلول وطنية في مجال السلامة المعلوماتية.

الفرع الثاني: القانون الجزائري

أنشأ المشرع الجزائري بموجب المادة 13 من القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، "**هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها**"، كمؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة وزارة الدفاع الوطني، بعدما كانت تابعة لوزارة العدل سابقا طبقا للمرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير هذه الهيئة الملغى[2].

وتتحدد تشكيلة الهيئة الوطنية وتنظيمها وكيفيات سيرها طبقا للمرسوم الرئاسي رقم 19-172 المؤرخ في 6 يونيو 2019[3] الملغي للمرسوم الرئاسي رقم 15-261 السابق الذكر، حيث تضم الهيئة، **مديرية عامة** (التي تضم **المديرية التقنيةومديرية الإدارة والوسائل**)، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وكذا تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم[4].

وإلى جانب المديرية العامة تضم الهيئة، **مجلس توجيه** يرأسه وزير الدفاع الوطني أو ممثله ويتشكل من وزارات الداخلية، العدل والمواصلات السلكية واللاسلكية يكلف بالتداول حول الإستراتيجية الوطنية للوقاية من الجرائم المحددة في المرسوم وكذا التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية

---

[1]- قانون رقم 09-04 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر العدد 47، صادر في 16 أوت 2009.

[2]- مرسوم رئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر العدد53، صادر في 08 أكتوبر 2015 (ملغى).

[3]-مرسوم رئاسي رقم 19-172 مؤرخ في 06 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها وتنظيمها وكيفيات ذلك، ح ر العدد 37، الصادر في 09 يونيو 2019، يلغي المرسوم الرئاسي رقم 15-261.

[4] - طبقا لنص المادة 9 من المرسوم الرئاسي رقمن 19-172، المرجع السابق.

المعنية، والقيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة (المادة 6 من المرسوم رقم 19-172).

ويعين المدير العام للهيئة الوطنية ومستخدموها طبقا للتنظيم المعمول به في وزارة الدفاع الوطني طبقا لنص المادة 19 من نفس المرسوم السابق الذكر.

وتقوم **المديرية التقنية** لدى الهيئة، بمهمة مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات بشأن الجرائم المعلوماتية، بما فيها جمع وتسجيلوحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية[1]. وانجاز الخبرات القضائية أو جمع وتسجيل وحفظ كل المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية[2].

كما تتولى**المديرية التقنية** كذلك طبقا لنص المادة 11 من المرسوم الرئاسي رقم 19-172،القيام بمهمة المراقبة الوقائية للاتصالات الالكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة.

إلا أننا إذا رجعنا إلى نص المادة 04 من القانون رقم 09-04،نجد أن المشرع قد حدد الحالات التي تسمح باللجوء إلى المراقبة الالكترونية على الاتصالات، بأربعة حالات فقط – ذكرت منها حالة واحدة بنص المادة 11 من المرسوم رقم 19-172- وهي المتعلقة بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أوالجرائم الماسة بأمن الدولة، أما الحالات الثلاثة الأخرى فهي: توافر معلوماتعن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، ولمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية، وفي إطار طلبات المساعدة القضائية الدولية المتبادلة.

إلا أنه في حالة اللجوء للمراقبة الالكترونية لمقتضيات التحريات والتحقيقات في كل قضية مستعصية صغيرة كانت أم كبيرة، في رأينا يؤدي إلى تعميم استخدام هذه التقنية دون حد أو حصر.

[1]- طبقا لنص المادة 1/12 من المرسوم الرئاسي رقم 19-172، المرجع السابق.

[2]- طبقا لنص المادة2/12 من نفس المرسوم الرئاسي السابق الذكر.

ويلتزم المتعاملون ومقدمو الخدمات بتقديم المساعدة الضرورية **للمديرية التقنية** من أجل تنفيذ مهامها، حيث يجب في هذه الحالة على مقدمي الخدمات[1]، مراعاة أحكام المادتين 10 و11 من القانون رقم 09-04، التي على إثرها يلتزمون تحت طائلة العقوبات بتقديم المساعدة للسلطات القضائية في حالة إجراء التحريات القضائية، حول محتوى الاتصالات، مع وضعها تحت تصرفها في سرية تامة وحفظ المعطيات المتعلقة بحركة السير لمدة سنة (01) واحدة ابتداء من تاريخ التسجيل، كالمعطيات التي تسمح بالتعرف على مستعملي الخدمة حيث ينبغي في هذه الحالة على متعامل الهاتف النقال وكذا الانترنت، الالتزام بحفظ المعطيات التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه، وكذا المعطيات المتعلقة بالتجهيزات الظرفية المستعملة في الاتصال أو الخصائص التقنية وتاريخ ووقت ومدة كل اتصال، أو المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، أو التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم في الاتصال وكذا عناوين المواقع الالكترونية المطلع عليها.

كما يجب على مزود خدمات الانترنت وفقا لنص المادة 12 من القانون رقم 09-04 التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، وكذا وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بتواجدهم.

وتمارس الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مهامها أصلا تحت رقابة وزارة الدفاع الوطني وتخضع لمجموع الأحكام التشريعية والتنظيمية المطبقة في وزارة الدفاع الوطني، كمـــا تمارس مهامها المرتبطة بالشرطة القضائية وفقا لأحكام التشريع المعمول به، لاسيما قـــانـــون

---

[1]- تنص المادة 01/د-هـ من القانون رقم09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على ما يلي: د-**مقدمو الخدمات:**

1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام الاتصالات،

2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها".

هـ- **المعطيات المتعلقة بحركة السير:** " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة".

الإجراءات الجزائية[1]والقانون رقم 09-04 المذكور أعلاه[2] مع مراعاة بالخصوص الأحكام القانونية التي تضمن "سرية" المراسلات والاتصالات[3].

غير أنه بالرجوع إلى نص المادة 12 من المرسوم رقم 19-172 السالف الذكر، نجد أن من بين مهام **المديرية التقنية** التابعة للهيئة، أنها تزود السلطات القضائيةومصالح الشرطة القضائية بناء على طلبها، بالمعلومات والمعطياتالمتعلقة بالجرائم الالكترونية في سرية تامة، حيث تشرف على جميع "الملحقات الجهوية" التابعة لها وعلى مركز العمليات التقنية الذي تزوده بمختلف المنشآت والتجهيزات والوسائل المادية، والمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات الالكترونية.

وتتمتع **المديرية التقنية**بصلاحيات واسعة في مراقبة جميع الاتصالات الإلكترونية، حيث يمكنها مباشرة مهامها الرقابية حتى ولو كان ذلك خارج إطار الرقابة القضائية أو القانونية، وفي رأينا أن مصدر هذه الصلاحيات الواسعة التي تتمتع بها **الهيئة الوطنيةللوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها**، في القيام بإجراء تقني مهم كالرقابة الالكترونية هو أنها موضوعة تحت سلطة وزارة الدفاع الوطني، (وتخضع للتنظيم القانوني المعمول به في ذات الوزارة)، التي لا تقيدها أية قيود أثناء ممارستها مهامها، خاصة إن كانت مبررة بغرض تحقيق هدف إيجابي معمول به لدى دول العالم ألا وهو **التنبؤ بمختلف التهديدات الإلكترونية** (الإرهاب الإلكتروني، الجرائم المنظمة...) التي تشكل خطرا على النظام العام والأمن والاقتصاد الوطنيين، أو حتى القيام بعمليات التجسس على الاتصالات الداخلية أو الجوسسة المضادة Contre (espionnage) على الاتصالات الأجنبية لمقتضيات الأمن والاقتصاد الوطنيين ومؤسسات الدولة.

لكن بالمقابل نجد أن ممارسة تلك المهام خارج إطار الرقابة القضائية أو القانونية يشكل تعديا أو مساسا بسرية المراسلات والاتصالات والمعطيات الشخصية المحمية بموجب القوانين الخاصة، ونحن نعلم أن المادة 09 من القانون رقم 09-04 المذكور أعلاه، منعت تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به،

---

[1]- أمر رقم 66-155 مؤرخ في 08 يونيو 1966، يتضمن قانون الإجراءات الجزائية، معدل ومتمم.

[2]-تنص المادة 04 من القانون رقم 09-04 على ما يلي: " يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه.....، لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا **بإذن مكتوب من السلطة القضائية المختصة**...."

[3]- طبقا لنص المادة 03 من القانون رقم 09-04 الذي جاء فيه :" مع مراعاة الأحكام القانونية التي تضمن **سريةالمرسلات والاتصالات**، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة على الاتصالات الالكترونية خارج الحدود الضرورية للتحريات أو التحقيقات القضائية.

الخاتمة

إن حماية أمن المعطيات ذات الطابع الشخصي على شبكة الانترنت، تحتل مكانا بارزا لدى دراسة أسرار العلاقات التجارية وخطورة مراقبة النظم وملاحقة المعلومات على حق الخصوصية؛ إذ ينعدم الأمن بتاتا في البيئة الإلكترونية الافتراضية، نتيجة كثرة الأخطار والتهديدات الالكترونية التي غالبا ما يصعب التنبؤ بها، و بسبب شيوع وسائل تقنية استلزمتها التجارة الالكترونية، تتيح تعقب الاتصالات ومعرفة معلومات تفصيلية عن مستخدم الشبكة. وإن كان التناقض قائما بين موجبات الحماية الأمنية والقانونية للمعطيات وبين موجبات حماية الخصوصية، فإن التوفيق بينها جاء عبر القواعد التشريعية التي وضعت المعايير، وأجازت أنشطة لا تخرق الخصوصية، وفي الوقت ذاته تحمي نشاط التجارة الالكترونية.

والجزائر قامت بعد تأخر واضح، بإقرار أرضية تشريعية ملائمة تضمن من خلالها حماية المعطيات الشخصية للأفراد، من خلال إصدار القانون رقم 18-07، وإن كان هذه الحماية تستمد إطارها القانوني من قوانين أخرى كقانون العقوبات، وقانون الإجراءات الجزائية وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. وقد جاء هذا القانون ليكرس حماية المعطيات الشخصية للأفراد، الذي نص عليه الدستور في المادة 47 منه، وحدد التدابير التقنية الضرورية الواجب احترامها في مجال معالجة المعطيات وهذا للحد من الآثار السلبية لشبكة الانترنت والتي باتت اليوم منصة لتبادل المعطيات بلا قيد ولا شرط، مما يهدد الحياة الخاصة.

كما أنشأ المشرع الجزائري هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والتي تلعب دورا كبيرا في حماية مستخدمي الانترنت، بالنظر إلى الصلاحيات الممنوحة لها في مجال الإشراف على عمليات رقابة وأمن مختلف شبكات الاتصالات، والتنبؤ من مختلف التهديدات الخارجية والداخلية التي من شأنها أن تمس بأمنها واقتصادها الوطنيين واستقرار مؤسساتها.

وبهدف تحيين المنظومة القانونية الجزائرية ذات الصلة بالموضوع، ارتأينا تقديم التوصيات الآتية:

- نشر الوعي الرقمي بين المستخدمين، وكيفيةتفاديالتعدي على معطياتهم الشخصية.
- إعداد سياسة أمنية محكمة مدروسة بدقة من طرف اختصاصيين في مجال أمن المعلومات، والعمل على توثيق إجراءات الحماية وتحديثها بصفة دورية، مع السعي إلى استقطاب كوادر مؤهلة من ذوي الخبرة في مجال الحماية الأمنية.

– ضرورة تكييف وتحيين قانون حماية المعطيات الشخصية للأشخاص الطبيعيين مع المستجدات لا سيما التكنولوجية والعلمية، والتي تعرف تطورا يوما بعد آخر.

– تنسيق الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها مع باقي الأجهزة الأخرى على المستوى الداخلي، كما أن التعاون الدولي يبقى أمرا لا غنى عنه في محاربة ومكافحة الجرائم الالكترونية التي هي في كثير من الأحيان دولية عابرة للإقليم، كما أن مرتكبيها يسعون إلى اخفاء ممارستهم بكل احترافية مما يصعب من مهمة الهيئة وباقي الجهات المعنية بذلك.

– ضمان تأمين المعطيات الخاصة بالأفراد والشركات والمؤسسات محليا ودوليا، بهدف استقدام المستثمرين الأجانب.

– المصادقة على اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي.