

الحق في خصوصية المعطيات ذات الطابع الشخصي في ضوء القانون رقم 07-18

The Right to the Protection of personel Data Privacy under Law No. 18/07

أ. د / عياشي جمال

جامعة الجزائر 1، يوسف بن خدة

dr.djamelayachi@gmail.com

طالبة الدكتوراه / عبد العزيز سومية *

كلية الحقوق والعلوم السياسية، جامعة يحيى فارس بالمدينة

abdelaziz.soumia@univ-medea.dz

تاريخ إرسال المقال: 15-03-2026 تاريخ قبول المقال: 25-05-2026 تاريخ نشر المقال: 06-06-2026

الملخص:

تكتسي حماية المعطيات ذات الطابع الشخصي أهمية بالغة في العديد من الاتفاقيات الدولية المتعلقة بحقوق الإنسان وكذا التشريعات المقارنة، باعتبارها تدخل في صميم الحياة الخاصة للفرد، وأسراره التي لا ينبغي لأحد الاطلاع عليها أو انتهاكها، ولقد هذا التشريع الجزائري حذو هذه التشريعات، حيث حرص على الاعتراف بهذا الحق، وتقرير الضمانات القانونية اللازمة لحمايته، حيث أصدر المشرع الجزائري في هذا السياق القانون رقم 07-18، الذي يعد أول خطوة تشريعية لوضع إطار قانوني من أجل تنظيم حماية الأفراد عند معالجة البيانات ذات الطابع الشخصي، إذ حدد هذا القانون المبادئ العامة التي تحكم جمع هذه البيانات واستعمالها، كما نص على إنشاء هيئة وطنية مهمتها الإشراف على حماية المعطيات الشخصية ومراقبة مدى احترام الأحكام المتعلقة بها، وقد عدل هذا القانون لاحقا بموجب القانون رقم 11-25، غير أن التحديات التي فرضتها البيئة الرقمية أثبتت محدودية الآليات القانونية التي كرسها المشرع الجزائري في هذا الشأن، مما اقتضى الاستعانة بالحماية التقنية كآلية وقائية ومكملة للآليات القانونية.

الكلمات المفتاحية: المعطيات ذات الطابع الشخصي، الحياة الخاصة، التشفير، المعالجة الآلية.

Abstract:

The protection of personal data is of paramount importance in both international human rights conventions and comparative legislation, as it is considered an integral part of an individual's private life and secrets, which should not be accessed or violated by anyone. Algeria legislation has followed suit, ensuring the recognition of this right and establishing the necessary legal guarantees for its protection. In this context, the Algerian legislator enacted Law No. 18-07, which represents the first legislative step toward establishing a legal framework for the protection of individuals in the processing of personal data. This law set out the general principles governing the collection and use of such data and provided for the creation of a national authority responsible for supervising the protection of personal data and monitoring compliance with the relevant legal provisions. The law was later amended by Law No. 25-11. However, the challenges posed by the digital environment have demonstrated the limitations of the legal mechanisms established by the Algerian legislature in this regard, necessitating the use of technical protection as a preventive and complementary mechanism to legal mechanisms.

Key words: Personal data, Private life, Encryption, Automated processing.

*المؤلف المرسل

1- مقدمة

يعد الحق في الحياة الخاصة من أقدس الحقوق الدستورية الملازمة للفرد وأهمها على الإطلاق، حيث يعتبر أساساً لحماية كرامة الإنسان واستقلاله، كما أنه يشكل ضماناً للعيش بحرية وأمان. فالإنسان يميل بفطرته للرغبة في السكنى والخلوة، وعدم تعكير صفو حياته في كل ما له صلة بالجانب الخفي من ذاته، سواء أكان ذلك الجانب متعلقاً بالحق في سرية محادثاته أو الحق في المسكن الذي يأويه، أو غيرها من الحقوق الأخرى التي يرى أنها تدخل ضمن نطاق حياته الخاصة.

ولقد حظي هذا المبدأ الأخلاقي باهتمام واسع في الفكر القانوني، ويتجلى ذلك من خلال إحاطته بسياج متين من المبادئ والنصوص القانونية التي بينت مضمونه وكفلت حمايته ووجوب احترامه، غير أنه مع التطور العلمي والتكنولوجي الذي شهدته معظم دول العالم وولوجها عصر الرقمنة والأنترنت، فإن مفهوم حماية هذا الحق وآليات حمايته شهد تحولا جذريا، وهذا كردة فعل على تغير طبيعة الحق في الحياة الخاصة من العالم المادي المحسوس إلى بيئة افتراضية تتحكم فيها مجموعة من الوسائل الإلكترونية والتقنية المتطورة، التي تقوم بالمعالجة الرقمية للعناصر المكونة للحياة الخاصة لتصبح معدة على شكل بيانات شخصية قابلة للجمع والتخزين والتحليل والتداول.

ولقد برز هذا التحول من خلال توحيد الجهود التشريعية الدولية والوطنية من أجل تطويع نصوصها القانونية بما يتلاءم وتلك البيئة، ونلمس ذلك من خلال ما ورد في الاتفاقيات التي عالجت هذا الحق، عرفت الاتفاقية الأوروبية رقم 108 الصادرة عن مجلس أوروبا البيانات ذات الطابع الشخصي بأنها كل معلومة متعلقة بشخص طبيعي محدد الهوية أو يمكن التعرف عليه، كما اعتبر التوجيه الأوروبي رقم 95/46 الصادر في 24 أكتوبر 1995 أن البيانات الشخصية تشمل أي معلومات ترتبط بشخص طبيعي يمكن تحديد هويته بشكل مباشر أو غير مباشر، وذلك سواء عن طريق اسمه أو رقم تعريف خاص به، أو عبر مجموعة من العناصر المميزة لهويته، كخصائصه الجسدية أو النفسية أو الاجتماعية أو الاقتصادية أو الثقافية.

وبهذا، وفي إطار تنظيم مسألة حماية المعطيات الشخصية قد شكل هذان التعريفان مرجعا أساسيا اعتمدت عليه عديد التشريعات الأوروبية، التي سعت إلى ملائمة أحكامها القانونية مع المبادئ التي تضمنها ذلك التوجيه.

حيث هذا المشرع بدوره حذو هذه الاتفاقيات لتكون نصوصه أكثر انسجاما معها وهو ما يتجلى وهو الأمر الذي حاول المشرع الجزائري تجسيده سواء في تعديله للدستور سنة 2016⁽¹⁾ من خلال إعادة النظر في مفهوم الحياة الخاصة، حيث تم إدراج المعطيات الشخصية كمبدأ لا يمكن المساس به⁽²⁾، أو بموجب إصداره للقانون رقم 07-18 المتعلق بحماية المعطيات ذات الطابع الشخصي⁽³⁾، والذي تم تعديله لاحقا بموجب القانون رقم 11-25⁽⁴⁾، حيث مس هذا التعديل إدراج مجموعة من الأحكام والنصوص القانونية، وإلغاء نصوص أخرى، بغرض معالجة بعض النقائص التي ظهرت أثناء تطبيق القانون القديم.

لكن رغم مسيرة النصوص القانونية للتطورات التي عرفت البيئية الافتراضية وما حملته من مظاهر التقدم والسرعة وعصرنة حياة البشر، إلا أن التحديات والمخاطر العديدة التي أفرزتها الثورة الرقمية لاسيما فيما يخص حماية البيانات الشخصية والتي تدخل في صميم الحياة الخاصة للأفراد داخل البيئية الافتراضية، أثار تساؤلات حول جدوى الآليات القانونية، وكذا الحلول البديلة لحماية البيانات الشخصية، وهو ما يقودنا لطرح الإشكالية التالية:

إلى أي مدى وفق المشرع الجزائري، من خلال القانون رقم 11-25 المعدل للقانون رقم 07-18 في مواجهة التحديات المتعلقة بانتهاك حرمة البيانات الشخصية في البيئية الرقمية؟

لقد اعتمدنا في سبيل الإجابة على التساؤل المطروح على التقسيم الآتي :

حيث نتعرض للآليات القانونية المقررة لحماية المعطيات ذات الطابع الشخصي، ثم نقدم تقييما لواقع حماية البيانات الشخصية.

(1) قانون رقم 01-16 مؤرخ في 26 جمادى الأولى عام 1437 الموافق 6 مارس سنة 2016، يتضمن التعديل الدستوري. ج. ر. ع 14، الصادر في 27 جمادى الأولى عام 1437 هـ الموافق 7 مارس سنة 2016م.

(2) المادة 46 من القانون رقم 01-16، المرجع السالف الذكر.

(3) قانون رقم 07-18 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. ج. ر. ع 34، الصادر في 25 رمضان عام 1439 هـ الموافق 10 يونيو سنة 2018م، معدل ومتمم.

(4) قانون رقم 11-25 مؤرخ في 28 محرم عام 1447 الموافق 24 يوليو سنة 2024، يعدل ويتم القانون رقم 07-18 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. ج. ر. ع 48، الصادر في 28 محرم عام 1447 هـ الموافق 24 يوليو سنة 2024م.

2- الآليات القانونية المقررة لحماية المعطيات ذات الطابع الشخصي

كرس المشرع الجزائري حماية قانونية واسعة على الحق في خصوصية البيانات الشخصية، يتجلى ذلك من خلال إدراجها في الدستور كجزء لا يتجزأ من مقومات الحياة الخاصة، وكذا بموجب إصداره للقانون رقم 07-18، وهذا مسايرة منه للتطورات الحاصلة في عالم الرقمنة من جهة، وإضفاءً لحماية فعالة للمعطيات ذات الطابع الشخصي من الانتهاكات التي تتعرض لها باستمرار من جهة أخرى. تتحدد آليات الحماية عبر نطاقين رئيسيين: يمثل أولاهما الإطار الموضوعي الذي يحدد طبيعة البيانات المشمولة بالحماية ومجال تطبيقها، أما ثانيهما فيتعلق بالإطار الإجرائي الذي يبين الإجراءات والآليات المعتمدة لضمان هذه الحماية.

1.2- الإطار الموضوعي لحماية المعطيات ذات الطابع الشخصي.

أولى المشرع الجزائري مسألة حماية المعطيات ذات الطابع الشخصي أهمية بالغة، باعتبارها تتعلق بكرامة الإنسان وبكل ما له صلة بحياته الخاصة التي لا يرغب أن يطلع عليها الغير، في هذا المضمار حدد المشرع الجزائري مجموعة من الحقوق التي يستطيع الشخص أن يباشرها من أجل حماية بياناته الشخصية عبر الفضاء الرقمي، وبالمقابل فرض على المسؤول عن المعالجة مجموعة من الالتزامات.

1.1.2- حقوق الشخص المعني بحماية المعطيات ذات الطابع الشخصي

خول المشرع الجزائري الشخص المعني بحماية بياناته الشخصية عبر البيئة الرقمية مجموعة من الحقوق التي بموجبها يستطيع منع كل اعتداء أو انتهاك قد يمسها، وتتمثل هذه الحقوق فيما يلي:

أولاً: الحق في الإعلام

يعتبر الحق في الإعلام من بين الحقوق التي كفلها الدستور والتشريعات المختلفة، إذ يهدف إلى تمكين الأفراد من معرفة كيفية جمع ومعالجة بياناتهم الشخصية، ويشمل هذا الإعلام بيان هوية المسؤول عن المعالجة، والغرض من جمع البيانات، إضافة إلى معلومات أخرى ذات صلة مثل الجهات التي يمكن أن ترسل إليها هذه البيانات، وما إذا كان تقديمها إلزامياً أو اختيارياً، والآثار المترتبة على عدم تقديمها، والحقوق التي يتمتع بها الشخص المعني، وكذلك إمكانية إرسال هذه البيانات إلى دولة أخرى، كما يجب إعلام الشخص، عند استخدام شبكة مفتوحة، بإمكانية تداول البيانات عبر هذه الشبكات وما قد يترتب عن ذلك من مخاطر تتعلق بسلامتها أو احتمال استعمالها من قبل أطراف غير مخول لها بذلك، ومن هذا المنطلق ألزم القانون المتعلق بحماية المعطيات ذات الطابع الشخصي المسؤول عن المعالجة، أو من ينوب عنه، بإبلاغ الشخص المعني مسبقاً وبشكل واضح عند جمع بياناته.

وقد استثنى المشرع من واجب الإعلام المسبق بعض الحالات كتعذر إبلاغ الشخص المعني عندما تتم معالجة البيانات لأغراض إحصائية أو علمية أو تاريخية، وذلك شرط إخطار الجهة الوطنية المختصة بسبب هذا التعذر، كما يُستثنى أيضا هذا الالتزام عندما تتم المعالجة بصدد تنفيذ نص قانوني، أو عندما تخصص المعالجة حصريا لأغراض صحفية أو أدبية أو فنية⁽⁵⁾، وذلك في إطار حماية حريات وحقوق أخرى.

ثانيا: الحق في الولوج

كرس القانون للأفراد الحق في الاطلاع على بياناتهم الشخصية الخاضعة لعمليات المعالجة، ويشمل هذا الحق إمكانية الاستفسار عن طبيعة هذه البيانات وخصائصها ومصدرها، وكذا معرفة الجهات التي تم إرسالها إليها، وبموجب هذا الحق يمكن للشخص المعني طلب تأكيد من المسؤول عن المعالجة بشأن ما إذا كانت بياناته الشخصية قد خضعت للمعالجة أم لا.

كما أن هذا الحق لا يقتصر على مجرد التأكد من وجود المعالجة، بل يمتد كذلك إلى الحصول على معلومات تتعلق بالأغراض التي تتم من أجلها المعالجة، وفئات المعطيات المعنية بها، والجهات التي يمكن أن تكون قد تلقتها، كما يحق للشخص المعني الاطلاع على هذه البيانات في صيغة واضحة ومفهومة، فضلا عن الحصول على المعلومات المتوفرة حول مصدرها⁽⁶⁾.

ومن جهة أخرى، يلتزم المسؤول عن المعالجة بتمكين الشخص المعني من ممارسة هذا الحق إذا ما استوفى الطلب الشروط القانونية اللازمة، أما في الحالات التي يكون فيها الطلب غير دقيق أو مفتقرا إلى بعض المعطيات الضرورية التي تسمح بتنفيذ الإجراءات المرتبطة بحق الولوج، فيحق للمسؤول عن المعالجة مطالبة المعني بتقديم معلومات إضافية لتوضيح طلبه⁽⁷⁾. ويتم ذلك قبل انقضاء الأجل المحدد من طرف اللجنة الوطنية المختصة، والتي بدورها تحدد أجلا من أجل الرد على طلبات الولوج المشروعة، أما إذا اتسمت الطلبات بالطابع التعسفي فيمكن للمسؤول عن المعالجة الاعتراض عليها، خاصة إذا ما تكررت أو أفرط عددها، شريطة إثبات هذا الطابع التعسفي⁽⁸⁾.

(5) المادة 33 من القانون رقم 18-07، المرجع السالف الذكر.

(6) المادة 1/34-2 من القانون رقم 18-07، المرجع السالف الذكر.

(7) يحي تومي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07: دراسة تحليلية، مج4،

العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، جانفي 2020، ص 1531.

(8) المادة 3/34 من القانون رقم 18-07، المرجع السالف الذكر.

ثالثا: الحق في التصحيح

يحق للشخص المعني بالمعالجة متى تبين أن بياناته غير صحيحة أو تمت معالجتها بشكل لا يتوافق مع أحكام القانون المنظم لحماية المعطيات ذات الطابع الشخصي أو كانت محظورة قانونا، بطلب تعديل بياناته الشخصية أو تحيينها أو حذفها أو تقييد استعمالها، وذلك بتقديم طلب إلى المسؤول عن المعالجة يطالب فيه بإجراء التصحيحات اللازمة، ويلتزم هذا الأخير بالاستجابة لهذا الطلب وإجراء التعديلات المطلوبة دون فرض أي مقابل مالي على صاحب الطلب، وذلك خلال أجل محدد لا يتجاوز عشرة (10) أيام، وفي حالة الرفض أو عدم الرد يتم اللجوء إلى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي للقيام بالتحقيقات الضرورية والتصحيحات اللازمة، وإعلام المعني بمآل طلبه. كما يلاحظ أن المشرع أعطى استعمال حق التصحيح لورثة المعني⁽⁹⁾.

في هذا المقام، نؤيد ما ذهب إليه المشرع الجزائري من خلال منح الورثة حق التصحيح، وهذا يعني أنهم بعد وفاة الشخص المعني، يحق لهم ممارسة حقوقه المتعلقة ببياناته الشخصية، بما في ذلك طلب تصحيح أو محو أو تقييد معالجة هذه البيانات لضمان استمرارية حماية حقوقهم وحرمة حياتهم الخاصة، خاصة إذا كانت المعطيات تتعلق بأمور حساسة تؤثر على سمعتهم أو ميراثهم، كما أن الفقرة الأخيرة من المادة 35 من القانون رقم 07-18 تكرر مبدأ أن حقوق حماية البيانات الشخصية ليست حقوقاً مؤقتة مرتبطة بحياة الفرد فقط، بل هي حقوق تمتد لتشمل ورثته لحماية إرثه وسمعته، مما يضمن عدم ضياع هذه الحقوق بوفاة صاحبها.

رابعا: الحق في الاعتراض

قصد حماية الشخص المعني بالمعالجة من استغلال بياناته الشخصية التي قد تضر بحرمة حياته الخاصة يمكنه تقديم اعتراض على معالجة معطياته ذات الطابع الشخصي، لأسباب مشروعة. غير أن ممارسة هذا الحق قد تكون مقيدة في بعض الحالات، لاسيما عندما تكون المعالجة مفروضة بموجب التزام قانوني، أو عندما يكون تطبيق هذا الحق مستبعدا صراحة بموجب إجراء قانوني ورد في السند الذي يجيز عملية المعالجة، كما يمكنه رفض استخدام هذه المعطيات في أغراض دعائية وخاصة في مجال الإشهارات التجارية ومنها الإلكترونية.⁽¹⁰⁾

(9) المادة 35 من القانون رقم 07-18، المرجع السالف الذكر.

(10) المادة 36 من القانون رقم 07-18، المرجع السالف الذكر.

خامسا: منع الاستكشاف المباشر

تعتمد التجارة الإلكترونية على أشكال متعددة من الإشهارات التجارية الإلكترونية للوصول إلى أكبر عدد من المستهلكين ويعتبر الاستكشاف المباشر إحدى صور الإشهار الإلكتروني ووسيلة تتطلبها التجارة، غير أن ذلك من شأنه المساس بحرمة الحياة الخاصة للمستهلك الإلكتروني، والذي يظل دائما الطرف الضعيف في البيئة الافتراضية، وعلى هذا الأساس يضمن القانون 07-18 حماية الشخص الذي يجري استكشافه، وهو الزبون من خطر انتهاك المورد الإلكتروني للمعطيات الشخصية لهذا الشخص في البيئة الرقمية⁽¹¹⁾.

2.1.2-التزامات المسؤول عن المعالجة

رتب المشرع الجزائري على المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي مجموعة من الالتزامات وهي على نوعين:

أولا: الالتزامات العامة

يتعين على المسؤول عن المعالجة تنفيذ مجموعة من الالتزامات العامة، وهي التزامات ترافق كل عملية معالجة تقريبا وتفرض بصورة دائمة على جميع المسؤولين عن المعالجة، وتتمثل فيما يلي:

- **ضمان سلامة وسرية المعالجة:** يقع على عاتق المسؤول عن معالجة البيانات اتخاذ جميع التدابير التقنية والتنظيمية والفنية الضرورية لضمان حماية المعطيات التي يشرف عليها، وصيانتها من الإتلاف أو الضياع العرضي، بالإضافة إلى منع أي استخدام غير قانوني، مثل النشر غير المصرح به أو الاختراق الإلكتروني أو الوصول غير المسموح به، ويولي ذلك أهمية أكثر في الحالات التي تتطلب إرسال البيانات عبر شبكات معينة⁽¹²⁾، ويجب أيضا الحفاظ على سرية المعالجة وسلامتها بالنسبة للأشخاص الذين يطلعون على البيانات أثناء تأدية مهامهم، مع الالتزام بالعقوبات القانونية المقررة في التشريعات السارية⁽¹³⁾.

⁽¹¹⁾ يزيد بوحليط، عبد الرحمان فطناسي، الحماية الإدارية والجزائية في مجال المعطيات ذات الطابع الشخصي على ضوء القانون 07-18، مجلة أبحاث قانونية وسياسية، مج6، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحيى، جيجل، ديسمبر 2021، ص 63.

⁽¹²⁾ المختار بن قوية، المعطيات الشخصية في ظل قانون 07-18 بين حتمية الرقمنة ومخاطر الاختراق، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مج 9، العدد 1، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، جوان 2024، ص 244.

وانظر أيضا: المادة 38 من القانون رقم 07-18، المرجع السالف الذكر.

⁽¹³⁾ المادتان 38 و 40 من القانون رقم 07-18، المرجع نفسه.

وإذا ما تم تكليف طرف ثالث بالمعالجة، يتعين على المسؤول عنها اختيار معالج من الباطن يوفر الضمانات الكافية لتحقيق السلامة التقنية والتنظيمية للمعالجات، وضمان احترام التعليمات الصادرة عن المسؤول الأصلي⁽¹⁴⁾، ويتم ذلك عادة بواسطة عقد أو سند قانوني بين الطرفين، يحدد فيه التزامات الطرف الثالث والتزامه بالتصرف وفق تعليمات المسؤول عن المعالجة، كما يلزم هؤلاء الأشخاص، وفقا للقانون العام ولأحكام القانون المتعلق بحماية المعطيات الشخصية، بالحفاظ على سرية المعلومات ولو بعد انتهاء مهامهم⁽¹⁵⁾.

– **الالتزام بمسك سجل معالجة البيانات:** يعد الالتزام بمسك سجل المعالجة من بين الالتزامات العامة الواقعة على عاتق المسؤول عن المعالجة، إذ يهدف إلى توثيق مختلف عمليات المعالجة بشكل مستمر ومنهجي، بما يعزز مبدأ الشفافية ويكرس مبدأ المساءلة داخل المؤسسة، ويمكن من تتبع مسار البيانات وضمان احترام الأغراض القانونية المحددة للمعالجة.

فرض المشرع الجزائري على المسؤول عن المعالجة مسك سجل للمعالجات وتوثيق العمليات المرتبطة بالبيانات⁽¹⁶⁾، ويعتبر هذا الالتزام من أهم مظاهر المسؤولية والمساءلة في التشريعات الحديثة، إذ يجسد الانتقال من حماية تقوم على رد الفعل بعد وقوع الانتهاك إلى حماية استباقية قائمة على التوثيق المسبق والرقابة المستمرة، فمسك سجل المعالجة لا يقتصر على كونه إجراء تنظيميا داخليا، بل يعد أداة قانونية لإثبات مدى احترام المسؤول عن المعالجة لالتزاماته، وتمكين السلطة المختصة من التحقق من مشروعية العمليات المنجزة على البيانات، وهو ما ينسجم مع الطابع العام لهذا الالتزام، باعتباره جزءا ثابتا من البنية التنظيمية لأي معالجة للمعطيات الشخصية، وليس مرتبطا بحادثة عارض أو ظرف استثنائي.

– **معالجة المعطيات ذات الطابع الشخصي المرتبطة بخدمات التوقيع والتصديق الإلكتروني:** تعد هيئة التصديق جهة قانونية مخولة بجمع البيانات الشخصية المتعلقة بالأفراد، وذلك لتنفيذ التزامات قانونية تتعلق بخدمات التوقيع الإلكتروني، ولذلك، يشترط القانون على المسؤول على هيئة التصديق والتوقيع

⁽¹⁴⁾ سهام بن دعاس، فوزية بن عثمان، ضمانات حماية المعطيات الشخصية في البيئة الرقمية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، مج 15، العدد 1، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، أبريل 2022، ص ص 1691، 1692.

⁽¹⁵⁾ فيصل بوخالفة، حماية المعطيات ذات الطابع الشخصي بين النصوص التقليدية ومتطلبات التقنية، مجلة الدراسات والبحوث القانونية، مج 8، العدد 1، تصدر عن مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، جانفي 2023، ص 69.

⁽¹⁶⁾ المواد 41 مكرر 2 و 41 مكرر 3 و 45 مكرر 3 من القانون رقم 11-25، المرجع السالف الذكر.

الإلكتروني جمع البيانات الشخصية مباشرة من أصحابها، حتى لا يُعد ذلك خرقا للقانون وعدم استعمالها لأغراض أخرى إلا بعد الحصول على تصريح صريح من الشخص المعني⁽¹⁷⁾.

ثانيا: الالتزامات الخاصة

أضاف المشرع التزامات خاصة يقوم بها المسؤول عن المعالجة، وهي التزامات ترتبط بحالات أو عمليات معينة، من بين هذه الالتزامات إخطار السلطات المعنية عن وقوع اختراق في البيانات، والنقل الدولي للمعلومات.

- **الالتزام بالإخطار بحوادث خرق المعطيات الشخصية:** يلتزم المسؤول عن المعالجة بإخطار الجهة المختصة، وأحيانا الشخص المعني، عند وقوع اختراق أو تسريب أو دخول غير مشروع إلى البيانات الشخصية، وذلك داخل أجل محدد، مع تقديم مبرر في حالة تجاوز هذا الأجل. ويهدف هذا الالتزام إلى تكريس الشفافية وتمكين الجهات المختصة والأشخاص المعنيين من اتخاذ التدابير الضرورية للتقليل من آثار الانتهاك، كما يعكس هذا الالتزام تطورا في فلسفة حماية المعطيات ذات الطابع الشخصي، إذ لم تعد الحماية تقتصر على منع الاختراقات فقط، بل أصبحت تشمل أيضا سرعة التعامل مع نتائجها عند حدوثها، لذلك ألزم المشرع الجزائري المسؤول عن المعالجة بعدم إخفاء الحادثة والتصريح بها وفق الأطر القانونية المعمول بها⁽¹⁸⁾.

- **الالتزام بضوابط نقل المعطيات إلى الخارج:** كان القانون رقم 18-07 يسمح بنقل المعطيات ذات الطابع الشخصي إلى دولة أجنبية في إطار التعاون الدولي، دون أن يحدد بصورة دقيقة جميع الضوابط المتعلقة بهذه العملية، إذ اتسم بطابع حمائي للمعطيات ذات الطابع الشخصي من خلال تركيزه على حماية الخصوصية كغاية أساسية، مع اعتماد قدر من المرونة في آليات التطبيق والرقاب، أما التعديل الجديد فقد جاء لتنظيم هذا النظام القانوني بشكل أكثر تفصيلا، عبر تكريس التزام قانوني يحد من سلطة المسؤول عن المعالجة في هذا المجال، حيث لم يعد نقل المعطيات يتم تلقائيا، بل أصبح مرتبطا بمجموعة من الشروط والضمانات، من بينها ضرورة تبرير عملية النقل وتحديد أهدافها بوضوح، والتأكد من توفر مستوى كاف من الحماية في الدولة المستقبلة، بما يضمن حماية المعطيات من أي مساس أو استغلال غير مشروع⁽¹⁹⁾، كما استحدث المشرع قيودا مهما يتمثل في منع إعادة نقل البيانات إلى طرف ثالث دون الحصول على موافقة مسبقة من الجهة التي قامت بإرسالها، ويقصد بذلك عدم السماح للدولة أو المنظمة الدولية المستقبلية للبيانات بإعادة تحويلها إلى جهة أخرى، حفاظا على التحكم

(17) المختار بن قوية، المرجع السابق، ص 245.

(18) المادتان 45 مكرر 9 و 45 مكرر 10 من القانون رقم 25-11، المرجع السالف الذكر.

(19) المادة 45 مكرر 13 من القانون رقم 25-11، المرجع السالف الذكر.

في مسار البيانات وضمان عدم استعمالها خارج الغرض الذي نقلت من أجله⁽²⁰⁾، وهو ما يعكس توجه المشرع نحو تعزيز السيطرة القانونية على التدفقات العابرة للحدود للبيانات الشخصية.

غير أن المشرع أقر استثناء على هذا المنع، يتمثل في جواز إعادة نقل البيانات إذا وافقت الدولة التي أرسلتها مسبقاً، أو إذا استدعت ذلك ضرورة مرتبطة بالمصالح الأساسية للدولة أو بوجود تهديد خطير وفوري يمس الأمن العام⁽²¹⁾ ويعكس هذا الاستثناء تغليباً ظرفياً لاعتبارات الأمن العام على شرط الموافقة، في حالات استثنائية تنسم بالخطورة والاستعجال، مثل التهديدات الإرهابية أو الجرائم العابرة للحدود التي تتطلب تبادلاً سريعاً للمعلومات بين عدة جهات.

وعليه، يكتسي نقل المعطيات إلى خارج الإقليم الوطني أهمية خاصة، إذ لا يعتبر إجراء إدارياً بسيطاً، بل عملية قانونية مقيدة تخضع لشروط دقيقة تهدف إلى تحقيق توازن دقيق بين حماية المعطيات الشخصية من جهة، وضمان فعالية التعاون الأمني والقضائي الدولي من جهة أخرى، مع إبقاء إعادة النقل محكومة بضوابط صارمة تمنع أي استعمال غير مشروع للبيانات.

2.2- الإطار الإجرائي لحماية المعطيات ذات الطابع الشخصي

لم تقتصر حماية المعطيات الشخصية على الضمانات الموضوعية التي تمكن الأفراد من حماية خصوصياتهم الاجتماعية والمهنية في البيئة الرقمية، بل شملت أيضاً الحماية الإجرائية، والتي تهدف إلى وضع آليات وإجراءات عملية لضمان احترام هذه الحقوق، وفي هذا الإطار، سنتناول هذه الدراسة الأجهزة المكلفة بحماية المعطيات الشخصية، ثم طبيعة الآليات التي أقرها المشرع لتحقيق هذه الحماية.

1.1.2- آليات الرقابة على معالجة المعطيات ذات الطابع الشخصي

أوكل المشرع الجزائري مسؤولية حماية البيانات الشخصية إلى هيئات محددة، تهدف إلى ضمان احترام خصوصية الأفراد في البيئة الرقمية، ويتمثل دور هذه الأجهزة في مراقبة الالتزام بالقوانين المنظمة للمعطيات الشخصية، والتحقيق في أي تجاوزات أو انتهاكات قد تقع في العالم الافتراضي، فضلاً عن اتخاذ الإجراءات اللازمة لمعاقبة المخالفين، ومن بين هذه الأجهزة نجد السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (أولاً)، والأقطاب الجهوية (ثانياً)، مندوب حماية المعطيات (DPO) (ثالثاً)، والضبطية القضائية (رابعاً).

أولاً: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

أنشأت السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي وقد تم تأسيسها

(20) المادة 45 مكرر 13 الفقرة 1 من القانون رقم 11-25، المرجع السالف الذكر.

(21) المادة 45 مكرر 13 الفقرة 2 من القانون رقم 11-25، المرجع السالف الذكر.

عبر مرسوم رئاسي، باعتبارها هيئة إدارية مستقلة، متمتعة بالشخصية المعنوية والاستقلالية المالية والإدارية، ويقع مقرها في الجزائر العاصمة، وتدرج ميزانيتها ضمن ميزانية الدولة⁽²²⁾.

أ- تشكيل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

يتشكل هيكل السلطة من مجموعة من الأعضاء ذوي الاختصاص في المجال، حيث يتم اختيار رئيس الجمهورية لثلاثة أعضاء من بينهم الرئيس، ويقترح المجلس الأعلى للقضاء ثلاثة قضاة من بين قضاة المحكمة العليا ومجلس الدولة، كما يتم تعيين عضو عن كل غرفة من البرلمان بالتشاور بين رئيس الغرفة ورؤساء المجموعات البرلمانية، بالإضافة إلى ممثل عن المجلس الوطني لحقوق الإنسان، وممثلين عن عدة وزارات، وهي: وزارة الدفاع الوطني، ووزارة الشؤون الخارجية، والوزارة المكلفة بالداخلية، ووزارة العدل حافظ الأختام، ووزارة المواصلات والتكنولوجيات والرقمنة، ووزارة الصحة، ووزارة العمل والضمان الاجتماعي.

ولابد على أعضاء السلطة التمتع بالخبرة القانونية أو التقنية اللازمة للعمل في مجال معالجة المعطيات الشخصية، كما يجوز للسلطة الاستعانة بأي شخص مؤهل لدعم مهامها، حيث يتم تعيين الرئيس وبقية الأعضاء عبر مرسوم رئاسي لفترة تقدر بخمس سنوات قابلة للتجديد⁽²³⁾، ولابد من تأدية الأعضاء لليمين القانونية أمام مجلس قضاء الجزائر العاصمة قبل مباشرة مهامهم⁽²⁴⁾.

ب- مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تعمل السلطة الوطنية على التأكد من موافقة معالجة المعطيات الشخصية لأحكام القانون، مع حرصها على حماية حقوق الأفراد والحريات العامة والحفاظ على خصوصية الحياة الشخصية متى تم استخدام تكنولوجيات الإعلام والاتصال، وتتمثل مهامها أساسا في تلقي التصريحات المتعلقة بمعالجة هذه المعطيات ومنح التراخيص، إضافة إلى إعلام الأشخاص المعنيين بحقوقهم وواجباتهم، كما تقدم السلطة استشارات قانونية وتقنية للأفراد والجهات الراغبة في معالجة بياناتها الشخصية أو القيام بتجارب من شأنها أن تؤدي إلى مثل هذه المعالجة.

كما يندرج من مهام السلطة أيضا تلقي الشكاوى والطعون المتعلقة بمعالجة البيانات الشخصية، ومسايرة نتائجها وإبلاغ أصحابها بمآلها، ويضاف لاختصاصها منح التراخيص لنقل المعطيات الشخصية

(22) المادة 22 من القانون رقم 07-18، المرجع السالف الذكر.

(23) المادة 23 من القانون رقم 07-18، المرجع السالف الذكر.

(24) المادة 24 من القانون رقم 07-18، المرجع السالف الذكر.

إلى الخارج وفق الشروط القانونية، وإصدار الأوامر اللازمة لحماية البيانات، بما في ذلك تعديل المعطيات أو إغلاقها أو سحبها أو إتلافها إن اقتضى الأمر ذلك⁽²⁵⁾.

وتكون مسؤولية الرئيس وأعضاء السلطة في الحفاظ على سرية المعطيات والمعلومات التي يطلعون عليها أثناء أداء مهامهم، ما لم ينص القانون على خلاف ذلك⁽²⁶⁾، وفي هذا الإطار، يحق للسلطة الاستعانة بأعوان وضباط الشرطة القضائية وأعوان رقابة آخرين مؤهلين لإجراء البحث والمعاينة بشأن الجرائم المرتبطة بالمعطيات الشخصية، على أن يتم ذلك تحت إشراف وكيل الجمهورية⁽²⁷⁾، ويتم توثيق نتائج المعاينة بمحاضر رسمية، تُرفع فوراً إلى وكيل الجمهورية المختص إقليمياً.

ثانياً: الأقطاب الجهوية

يشكل إدراج الأقطاب الجهوية ضمن منظومة حماية المعطيات ذات الطابع الشخصي تطوراً مهماً في الهيكل الرقابي الذي أقره المشرع الجزائري، ويقصد بالأقطاب الجهوية الهياكل الإقليمية التابعة للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، والتي تتكفل بمهام المراقبة والتدقيق على مستوى الجهات والمؤسسات التي تعالج البيانات، سواء كانت عمومية أو خاصة، كإدارات والبنوك وشركات الاتصالات والمؤسسات الصحية والجامعات وغيرها من الجهات التي تتعامل يومياً مع المعطيات الشخصية⁽²⁸⁾.

ويهدف هذا التنظيم إلى ما يُعرف فقهيًا بـ "تقريب الرقابة من الواقع العملي للمؤسسات"، من خلال الانتقال من رقابة مركزية محضة إلى رقابة ميدانية أكثر قرباً من الواقع العملي، أي تحويل الرقابة من مستوى نظري إداري يعتمد على التقارير والمراسلات إلى رقابة ميدانية مباشرة، تقوم على الزيارات والتفتيش والتحقق الفعلي من مدى احترام قواعد حماية البيانات داخل الأنظمة المعلوماتية للمؤسسات، وهو ما يسمح بتعزيز فعالية الرقابة على مستوى المؤسسات المعالجة للبيانات. وعليه، يُعد هذا التحول استجابة عملية للتطورات الرقمية المتسارعة، حيث أصبحت معالجة البيانات تتم بشكل معقد ومتداخل، مما يستدعي رقابة تقنية وقانونية قريبة من بيئة المعالجة نفسها.

(25) المادة 25 من القانون رقم 07-18، المرجع السالف الذكر.

(26) المادة 26 من القانون رقم 07-18، المرجع السالف الذكر.

(27) المادة 50 من القانون رقم 07-18، المرجع السالف الذكر.

(28) المادة 27 مكرر من القانون رقم 11-25، المرجع السالف الذكر.

ثالثا: مندوب حماية المعطيات (DPO)

يُعتبر استحداث منصب مندوب حماية المعطيات ذات الطابع الشخصي (DPO)⁽²⁹⁾ من أبرز المستجدات التي أقرها المشرع في إطار تعزيز منظومة حماية البيانات، وهذا التعديل مستوحى بصورة واضحة من نظام اللائحة الأوروبية العامة لحماية البيانات GDPR، حيث يهدف المشرع من ورائه إلى إرساء آلية رقابة داخلية دائمة داخل المؤسسات التي تقوم بمعالجة المعطيات الشخصية. ويقوم هذا النظام على فكرة نقل جزء من مسؤولية الامتثال من السلطة الرقابية الخارجية إلى داخل المؤسسة نفسها، من خلال تعيين شخص مختص يتولى متابعة مدى احترام قواعد حماية البيانات بشكل يومي ومستمر. ولا يفرض تعيين مندوب حماية البيانات على جميع المسؤولين عن المعالجة بصورة مطلقة، وإنما يرتبط بطبيعة المعالجة وحجمها ومدى خطورتها، لاسيما في الحالات التي تتطلب معالجة واسعة النطاق أو بيانات حساسة تستوجب رقابة داخلية معززة لضمان الامتثال لأحكام حماية المعطيات الشخصية.

يتمثل الدور الأساسي لمندوب حماية المعطيات في ضمان الامتثال المسبق لأحكام القانون، من خلال مراقبة عمليات جمع البيانات ومعالجتها والتأكد من مشروعيتها، وتقديم الاستشارات القانونية والتقنية للإدارة، إضافة إلى التنسيق مع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي عند الاقتضاء، كما يساهم هذا المندوب في ترسيخ ثقافة حماية البيانات داخل المؤسسة عبر التوعية والتكوين المستمر للموظفين⁽³⁰⁾.

ويعكس هذا الاستحداث تحولاً مهماً في فلسفة الحماية القانونية للمعطيات الشخصية، إذ انتقل المشرع من نموذج يعتمد أساساً على الرقابة الخارجية اللاحقة إلى نموذج مزدوج يجمع بين الرقابة الخارجية والرقابة الداخلية الوقائية، بما يضمن حماية أكثر فعالية للمعطيات ويقلل من مخاطر الانتهاكات قبل وقوعها.

2.1.2- الضبطية القضائية

تعد الضبطية القضائية، بصرف النظر عن انتماء أجهزتها أو أسلاكها، السلطة المكلفة بالاختصاص العام في مكافحة جميع أنواع الجرائم، بما في ذلك الجرائم الإلكترونية، رغم ما تثيره هذه الأخيرة من إشكالات تتعلق أساساً بصعوبة الكشف عن مرتكبيها وسهولة محو آثارها لأنها تحدث في بيئة

(29) المادة 41 مكرر من القانون رقم 11-25، المرجع السالف الذكر.

(30) انظر المادة 41 مكرر 1 من القانون رقم 11-25، المرجع السالف الذكر.

وأيضاً مداولة رقم 1 صادرة عن السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بتاريخ 24 ديسمبر سنة 2025، تتضمن التعريف بمندوب حماية المعطيات ذات الطابع الشخصي وتحديد مهامه وكيفيةاته.

افتراضية تمارس فيها الجريمة على نطاق واسع من حيث المكان الذي قد يتجاوز حدود الدولة الواحدة، وهو ما يمكن المجرمين من الإفلات من العقاب.

تمارس الضبطية القضائية مهام التحري والبحث عن مختلف الجرائم وملاحقة مرتكبيها تحت إشراف جهاز النيابة العامة، وهذا طبقا لنص المادة 50 من القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي.

إن طبيعة البيئة الرقمية وما تتمتع به من سمات، بما في ذلك التفاعلية والانتشار والتدفق المستمر للمعلومات، يثير صعوبة كبيرة في التحكم فيها من طرف الضبطية القضائية وأجهزة العدالة الجنائية التي تبقى عاجزة بدورها عن الكشف عن هذه الجرائم، باعتبار أن الإجراءات التي يتم اتخاذها من أجل حماية المعطيات ذات الطابع الشخصي قد لا تكون كافية بالنظر إلى طبيعة تلك البيئة، مما يشكل تحديا حقيقيا بالنسبة للسلطات المختصة من أجل مواجهة ظاهرة الاعتداءات على تلك المعطيات لاسيما مع التطور العلمي والتكنولوجي الذي يكشف عنه مجال المعلوماتية الرقمية.

بناء على ما سبق، يتضح لنا مدى حرص المشرع الجزائري على إعطاء كافة الضمانات الإجرائية من أجل إضفاء الحماية اللازمة على المعطيات ذات الطابع الشخصي، وهذا من خلال منح السلطة الوطنية لحماية المعطيات استقلالية إدارية ومالية مطلقة، بغية ضمان الشفافية والمساءلة، وتطبيق القانون بحيادية، مما يسمح لها بممارسة مهام رقابية وقمعية بحرية دون تأثير أو ضغوط من الأطراف الأخرى لضمان عدم المساس بحقوق وحرريات الأفراد، كما أناط القيام بهذا الدور للضبطية القضائية لتكون حماية البيانات الشخصية أكثر نجاعة رغم أن الإجراءات التي يتم اتخاذها من أجل حماية المعطيات ذات الطابع الشخصي قد لا تكون كافية بالنظر إلى طبيعة تلك البيئة، مما يقتضي البحث عن أساليب أكثر حداثة وتطورا تتناسب مع تلك البيئة، بغية المساهمة في تعزيز ثقة المواطنين في آليات حماية حقوقهم الأساسية في عالم التحول الرقمي.

3.2- ازدواجية الحماية المقررة للمعطيات الشخصية

كرس المشرع الجزائري في إضفاء حماية مزدوجة مقررة للمعطيات الشخصية، وهذا نظرا لحساسية هذه المعطيات وخصوصيتها، وهو ما نبينه من خلال التطرق للجزاءات الإدارية المترتبة عن انتهاك المعطيات ذات الطابع الشخصي، وصور الجرائم المتعلقة بالمعطيات الشخصية.

1.3.2- الجزاءات الإدارية المقررة لحماية المعطيات ذات الطابع الشخصي

خول المشرع الجزائري السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي صلاحية اتخاذ الإجراءات الإدارية المناسبة ضد المسؤول عن معالجة البيانات في حال الإخلال بالالتزامات المنصوص عليها في القانون رقم 18-07، وتشمل الجزاءات الإدارية التي يمكن أن تفرض على المسؤول عن

معالجة المعطيات الشخصية الإنذار أو التوبيخ، والغرامات المالية، أو سحب الترخيص أو تصريح المعالجة بشكل مؤقت أو دائم، مع إمكانية الطعن في هذه القرارات أمام الجهة القضائية المختصة⁽³¹⁾، كما يخول القانون السلطة الوطنية صلاحية معاينة الأماكن المرتبطة بالمعالجة⁽³²⁾ وفرض عقوبات وغرامة قدرها 500.000 دج ضد كل من يرفض، بدون سبب قانوني⁽³³⁾، احترام حقوق الأفراد في الإعلام، والولوج، والتصحيح، والاعتراض، أو الامتناع عن تبليغ السلطة بالمعطيات اللازمة، وفي الحالات التي تشكل فيها المعالجة تهديدا للأمن الوطني أو تتعارض مع القيم الأخلاقية والآداب العامة، يمكن للسلطة سحب الترخيص أو تصريح المعالجة دون المساس بالعقوبات الجزائية المقررة⁽³⁴⁾.

2.3.2- صور الجرائم الماسة بالمعطيات الشخصية

نظرا للطبيعة الخاصة للجرائم المتعلقة بالمعطيات الشخصية، خصها المشرع بإجراءات محددة تهدف إلى ضبط هذه الجرائم وتحريك الدعوى العمومية ضد مرتكبيها، ويتم توثيق الجرائم المنصوص عليها في القانون بموجب محاضر رسمية تُرفع فورا إلى وكيل الجمهورية المختص إقليميا، لضمان متابعة التحقيق واتخاذ الإجراءات القانونية اللازمة، وتشمل هذه الجرائم نوعين رئيسيين: الجرائم التي تمس القواعد الموضوعية لحماية المعطيات الشخصية (أولا)، والجرائم المرتبطة بالقواعد الإجرائية المنظمة لكيفية معالجتها (ثانيا)، وذلك بهدف صون حقوق الأفراد وحرياتهم وحماية خصوصيتهم.

أولا: الجرائم الماسة بالقواعد الموضوعية للمعالجة

تتصب الجرائم الماسة بالقواعد الموضوعية على محل الجريمة ذاته، والمتمثل في المعطيات ذات الطابع الشخصي، وتتخذ عدة صور من بينها:

أ- جريمة المعالجة غير المشروعة للمعطيات ذات الطابع الشخصي

تعد المعالجة غير المشروعة للمعطيات ذات الطابع الشخصي من بين الجرائم المنصوص عليها في القانون رقم 07-18، والتي يؤدي اقترافها إلى توقيع عقوبات مختلفة على مرتكبيها سواء تم الفعل غير المشروع بصفة انفرادية من طرف المسؤول عن المعالجة أو كان بالاشتراك مع الغير، ولكي نعطي فكرة واضحة عن هذه الجريمة نقوم بتعريفها (1)، وذكر صورها (2).

(31) المادة 46 من القانون رقم 07-18، المرجع السالف الذكر.

(32) المادة 49 من القانون رقم 07-18، المرجع السالف الذكر.

(33) المادة 47 من القانون رقم 07-18، المرجع السالف الذكر.

(34) المادة 48 من القانون رقم 07-18، المرجع السالف الذكر.

- المقصود بجريمة المعالجة غير المشروعة للمعطيات ذات الطابع الشخصي

حدد المشرع الجزائري عند معالجة المعطيات الشخصية من قبل أشخاص طبيعيين أو معنويين مجموعة من الأفعال المشكلة انتهاكا للقواعد الواجب احترامها، وتكون العقوبة على الأشخاص المعنوية وفق القواعد العامة للعقوبات، مع إمكانية فرض عقوبات تكميلية على المخالفين، كما يمكن أن يتضمن ذلك أيضا مسح كل أو جزء من المعطيات الشخصية المسفرة عن ارتكاب الجريمة.

ويمكن تعريف المعالجة الآلية بأنها كل العمليات المنجزة جزئيا أو كليا وذلك باستعمال وسائل تقنية، كتسجيل البيانات أو تطبيق عمليات منطقية أو حسابية عليها، أو تعديلها، أو مسحها، أو استخراجها، أو نشرها، ويقصد بالمسؤول عن المعالجة كل شخص طبيعي أو معنوي أو أي كيان آخر يقوم منفردا أو مشتركا مع الغير بتحديد أغراض المعالجة ووسائل تنفيذها.

ولابد على هذا المسؤول من اتخاذ التدابير التقنية والتنظيمية المناسبة لحماية المعطيات من التلف أو الضياع العرضي، أو من أي استعمال غير مشروع، مثل النشر أو الوصول غير المصرح به، خاصة عند نقل البيانات عبر الشبكات، كما يجب أن تضمن هذه التدابير مستوى مناسب من الأمن والسلامة ما يتناسب مع المخاطر المرتبطة بطبيعة المعطيات وطرق معالجتها⁽³⁵⁾.

وتتم معاقبة بالحبس وغرامة مالية كل من يقوم بمعالجة المعطيات الحساسة دون موافقة صريحة من الشخص المعني، وفي الحالات غير المصرح بها قانونا، كما يعاقب كل من يستعمل معالجة البيانات لأغراض غير تلك المصرح بها أو المرخصة له، بالحبس أو الغرامة أو كلاهما، وفقا لخطورة المخالفة، ويشمل مفهوم إنجاز إنشاء المعالجة أو تعديلها أو إلغائها، بحيث تكون الجريمة محققة إذا أقدم المسؤول على أي من هذه الأفعال دون تصريح مسبق أمام السلطة الوطنية، سواء قام بها شخصا أو وكل غيره للقيام بها⁽³⁶⁾.

- صور الجرائم المتعلقة بجريمة المعالجة غير المشروعة للمعطيات ذات الطابع الشخصي

نظرا لكون جريمة المعالجة غير المشروعة للمعطيات تشمل صورا عديدة وهذا في مفهوم المادة 3 من القانون رقم 18-07، فسنتصر على ذكر بعضها:

(35) حسب المادة 38 من القانون رقم 18-07، المرجع السالف الذكر.

(36) نبيلة رزاق، المرجع السابق، ص 2002.

- جريمة جمع المعطيات باستخدام طرق تدليسية وغير نزيهة وغير مشروعة

يدخل الجمع أو التجميع للمعطيات ذات الطابع الشخصي ضمن المعنى العام للمعالجة، حيث تعده المادة 3 من القانون رقم 07-18 من بين صور وكيفيات المعالجة، ويعرف الجمع بأنه عملية الإلزام المسبق بالمعطيات وتنظيمها من أجل استعمالها فيما بعد⁽³⁷⁾.

ويقصد بجريمة جمع البيانات بطرق تدليسية وغير نزيهة وغير مشروعة بأنها فعل جمع معلومات شخصية بطرق غير قانونية أو غير أخلاقية أو غير شفافة، وتعتبر الطرق التدليسية في جمع البيانات من الجرائم المعاقب عليها قانونا، وهذا طبقا لنص المادتين 59 و 65 من القانون السالف الذكر.

- جريمة الاستعمال غير المشروع للمعطيات

يعد الاستعمال غير المشروع للمعطيات المعالجة جريمة يعاقب عليها القانون، لأنها تمت بدون موافقة أو علم الشخص المعني الذي وقع الاعتداء على بياناته، ونظرا لكون هذه الجريمة تشكل اعتداء على حرمة خصوصية الأفراد، فقد تشدد المشرع نسبيا في رصد العقوبات المخصصة لها، ويظهر ذلك في توقيع عقوبة الحبس وهي عقوبة سالبة للحرية، علاوة على فرض غرامة مالية وهذا دون الاعتداد بنية مرتكبها، سواء أكان ذلك الفعل صدر عمدا أو عن إهمال، أو تم ارتكاب هذه الجريمة من طرف شخص واحد أو أشخاص معينين، كالمسؤول عن المعالجة أو المعالج من الباطن⁽³⁸⁾.

ب- الجرائم المتعلقة بحقوق الشخص المعني

تقتضي حماية الحياة الخاصة للأشخاص المعنيين بمعالجة المعطيات توفير مجموعة من الحقوق والضمانات في مواجهة المسؤول عن المعالجة، وهو ما تم تكريسه في القانون رقم 07-18، حيث اعتبر المشرع الجزائي كل اعتداء على تلك الحقوق فعلا مجرما ويعرض مرتكبه للعقوبات المنصوص عليها قانونا، كإجراء المعالجة دون موافقة الشخص المعني أو لم تكن ضمن الحالات الضرورية المنصوص عليها قانونا⁽³⁹⁾.

ويتم تطبيق ذات العقوبة على كل مكلف بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني، لاسيما عندما تكون هذه المعالجة متعلقة بالإشهار التجاري أو عندما يكون الاعتراض مبنيا على مسوغات قانونية.

⁽³⁷⁾ فريد روابح، جرائم الجمع غير المشروع للمعطيات الشخصية الرقمية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، مج9، العدد 1، جامعة عباس لغرور، خنشلة، أبريل 2022، ص 86.

⁽³⁸⁾ المادة 69 من القانون رقم 07-18، المرجع السالف الذكر.

⁽³⁹⁾ المادة 55 من القانون رقم 07-18، المرجع السالف الذكر.

ثانيا: الجرائم الماسة بالقواعد الإجرائية الشكلية للمعالجة

يلتزم الشخص المكلف بمعالجة المعطيات ذات الطابع الشخصي بمجموعة من القواعد الإجرائية التي تستهدف حماية الأشخاص الطبيعيين، ومن ثم فإن مخالفة هذه الشكليات يعد جريمة معاقب عليها، من بينها مخالفة الإجراءات المسبقة عن المعالجة (أ)، وخرق الالتزام بسرية وسلامة المعالجة للمعطيات الشخصية (ب)، ونقل المعطيات ذات الطابع الشخصي نحو دولة أجنبية (ج)، وأخيرا الجرائم المتعلقة بإجراءات الحماية والتعاون مع السلطة الوطنية (د).

أ- الجرائم المتعلقة بالإجراءات المسبقة عن المعالجة

ينبغي على المسؤول عن المعالجة أن يقدم تصريحاً مسبقاً بذلك أو أن يحصل على ترخيص من قبل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وهذا قبل إجراء معالجة المعطيات ذات الطابع الشخصي، إلا إذا كان هناك ما يجيز عدم اللجوء إلى هذا الإجراء⁽⁴⁰⁾، ومن ثم كل معالجة يجريها المسؤول عن المعالجة في غياب التصريح أو الترخيص تعد جريمة معاقب عليها وفق المادة 56 من القانون رقم 07-18، ويعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 20.000 دج إلى 500.000 دج.

تتحقق هذه الجريمة عند مخالفة القواعد القانونية المنظمة لمعالجة المعطيات ذات الطابع الشخصي، وذلك بارتكاب أحد الأفعال التي تمس بالإجراءات المسبقة المفروضة قانوناً، ويتجلى ذلك أساساً عند قيام المسؤول عن المعالجة بإجراء معالجة للبيانات الشخصية أو يأمر بالقيام بها دون الحصول مسبقاً على التصريح أو الترخيص اللازم من السلطة المختصة، وهو ما يشكل مخالفة للأحكام التي أقرتها المادة 12 من القانون ذاته، كما تتحقق الجريمة كذلك في حالة تقديم معلومات أو تصريحات غير صحيحة إلى الجهة المختصة، أو الاستمرار في مزاولة نشاط معالجة المعطيات رغم سحب وصل التصريح أو إلغاء الترخيص الممنوح، وفقاً لما ورد في الفقرة الثانية من المادة 56 من نفس القانون كما يعتبر مرتكباً لجرائم الإخلال بالإجراءات المسبقة للمعالجة كل من يقوم، خارج الحالات التي يسمح بها القانون، بتسجيل أو الاحتفاظ بمعطيات ذات طابع شخصي ضمن الأنظمة المعلوماتية تتعلق بالجرائم المنسوبة إلى شخص معين، أو التدابير الأمنية المتخذة ضده، أو الأحكام القضائية الصادرة في حقه، وتعد معالجة هذا النوع من البيانات فعلاً مجرمًا يعاقب عليه القانون بموجب أحكام المادة 68 من القانون

(40) المادة 12 من القانون رقم 07-18، المرجع نفسه.

رقم 07-18⁽⁴¹⁾، نظرا لما تتميز به هذه المعطيات من حساسية خاصة، إذ يمنع التعامل معها داخل القطاع الخاص، وتبقى صلاحية معالجتها حكرا على الجهات القضائية المختصة⁽⁴²⁾.

ب- خرق الالتزام بسرية وسلامة المعالجة للمعطيات الشخصية

يحصل خرق هذا الالتزام عندما يتقاعس المسؤول عن معالجة المعطيات عن اعتماد التدابير التقنية والتنظيمية الكفيلة بضمان سرية وسلامة المعطيات ذات الطابع الشخصي، من أي شكل من أشكال المعالجة غير المشروعة التي قد تطالها، أو من الإلتلاف العرضي أو غير المشروع، أو الضياع العرضي أو التلف، إضافة إلى منع نشرها أو تمكين الغير من الوصول إليها دون ترخيص قانوني، لاسيما عندما تتطلب المعالجة إرسال معطيات عبر الشبكات المعلوماتية.

وطبقا لنص المادتين 38 و39 من القانون رقم 07-18، تتمثل التدابير التنظيمية في منع اطلاع الغير الذين لا يرخّص لهم بذلك، أو لتفادي ضياعها، أما التدابير التقنية فهي التي تتيح ضمان سرية وسلامة المعالجة الآلية، من بينها إجراءات التشفير أو وضع كلمات المرور التي تمنع من الوصول إليها باستثناء الشخص المخول له بذلك، أو تزويد النظام المعلوماتي ببرامج أمنية تحول دون الدخول إليه، أو وضع برامج خاصة لمنع تخريب المعالجة أو إحداث أي تغيير أو تلف فيها.

وعلى هذا الأساس، ينبغي على المسؤول عن المعالجة اتخاذ جميع التدابير التقنية والتنظيمية الكفيلة بضمان الحماية اللازمة للمعطيات، إذ أن أي إهمال أو تقاعس من جانبه يؤدي حتما إلى إلحاق أضرار بالمعطيات وبالتالي الإضرار بأصحابها⁽⁴³⁾.

كما ألزم المشرع الجزائري على المسؤول عن المعالجة في حالة ما إذا لم يتول بنفسه بإجراء المعالجة، أن يختار بحرص شديد معالج من الباطن، الذي ينبغي عليه هو الآخر أن يعطي ضمانات كافية لاتخاذ التدابير الملائمة لضمان سرية وسلامة المعالجة، شريطة أن تقدم تلك الضمانات في شكل

⁽⁴¹⁾ بنصها: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 60.000 دج، كل من قام في غير الحالات المنصوص عليها قانونا بوضع أو حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن".

⁽⁴²⁾ كاملة بوعكة، الحماية القانونية للأشخاص في مجال معالجة المعطيات ذات الطابع الشخصي في ضوء القانون 18-07، المجلة الجزائرية للقانون والأعمال، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، ديسمبر 2020، ص 65.

⁽⁴³⁾ عز الدين طباش، الحماية الجزائرية للمعطيات الشخصية في التشريع الجزائري: دراسة في ظل قانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، مج9، العدد 2، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، ديسمبر 2018، ص ص 46، 47.

عقد أو أي سند آخر يتم إنشاؤه بالكتابة أو أي شكل آخر⁽⁴⁴⁾. ومن ثم فإن خرق هذه الالتزامات يؤدي إلى قيام الجريمة طبقا لنص المادة 65 من القانون رقم 18-07.

ج- جريمة نقل المعطيات ذات الطابع الشخصي نحو دولة أجنبية

يعد نقل المعطيات نحو بلد أجنبي من قبل المسؤول عن المعالجة في حالة تم ذلك دون ترخيص من السلطة الوطنية، خرقا للقواعد الشكلية لمعالجة المعطيات الشخصية وفقا لمقتضيات المادة 44 من القانون رقم 18-07⁽⁴⁵⁾، كما أن هذا الفعل يعتبر جريمة عمدية معاقب عليها طبقا لنص المادة 67 من نفس القانون، لكونه يشكل تهديدا خطيرا للأفراد في حماية حياتهم الخاصة.

عليه، يلزم لتحقيق هذه الجريمة توافر كل من الركن المادي المتمثل في فعل النقل (التحويل)، وهو إخراج المعطيات الشخصية من نطاق المعالجة الأولية إلى بلد أجنبي غير بلد الشخص المعني أو بلد المعالجة الأصلي، سواء كانت دولة أجنبية أو منظمة دولية، والركن المعنوي (القصد الجنائي)، وهو علم مرتكب الفعل بحقيقة المعطيات الشخصية، وبأنها ستنتقل لدولة أجنبية، وبأن هذا النقل يتم دون سند قانوني أو موافقة صريحة، مع اتجاه إرادة صاحبها لارتكاب هذا الجرم.

د- الجرائم المتعلقة بإجراءات الحماية والتعاون مع السلطة الوطنية

يقع على عاتق المسؤول عن معالجة المعطيات الشخصية التزام قانوني يتمثل في ضرورة اتخاذ جميع التدابير وإجراءات التعاون مع السلطة الوطنية التي تسمح لها بممارسة اختصاصها، فكل إغفال أو تقصير في اتخاذ هذه الإجراءات التي تهدف إلى حماية المعطيات الشخصية محل المعالجة فإنه يشكل جريمة يعاقب عليها قانونا؛ ومن صور هذا الإخلال:

- جريمة الامتناع عن التعاون مع السلطة الوطنية بالعرقلة أو الاعتراض على إجراء عمليات التحقيق والمعاينة التي تقوم بها هذه السلطة في عين المكان.
- رفض تزويد أعضاء السلطة أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية التي تسمح لهم بأداء المهام الموكلة إليهم من طرف السلطة الوطنية أو عند تعمد إخفاء أو إزالة الوثائق أو المعلومات المذكورة.

(44) المادة 39 من القانون رقم 18-07، المرجع السالف الذكر.

(45) بنصها: "لا يجوز للمسؤول عن المعالجة نقل المعطيات ذات الطابع الشخصي إلى دولة أجنبية إلا بترخيص من السلطة الوطنية، وفقا لأحكام هذا القانون، وإذا كانت هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص، إزاء المعالجة التي تخضع لها المعطيات، أو التي قد تخضع لها؛ تقدر السلطة الوطنية المستوى الكافي من الحماية التي تضمنها دولة معينة، لاسيما وفقا للمقتضيات القانونية المعمول بها في هذه الدولة، ولإجراءات الأمن المطبقة فيها، وللخصائص المتعلقة بالمعالجة مثل غاياتها ومدتها وكذا طبيعة وأصل ووجهة المعطيات المعالجة".

- إرسال بيانات أو معلومات غير مطابقة لما هو مدون في السجلات أو الأنظمة المعتمدة وقت تقديم الطلب أو عدم تقديمها بصورة واضحة ومباشرة بما يعرقل عملية الرقابة⁽⁴⁶⁾.

- كما يعتبر جريمة متعلقة بالاعتداء على المعطيات امتناع مقدم الخدمة عن إبلاغ السلطة الوطنية والشخص المعني بأي خرق أو انتهاك يمس المعطيات الشخصية⁽⁴⁷⁾.

3-تقييم واقع حماية البيانات الشخصية في البيئة الرقمية

بالرغم من محاولة المشرع الجزائري إضفاء نوع من الحماية القانونية على المعطيات ذات الطابع الشخصي، وهذا عبر تكريس مجموعة من الآليات القانونية المنصوص عليها في القانون رقم 07-18 المتعلق بحماية المعطيات ذات الطابع الشخصي، إلا أنها تبقى في نظرنا غير كافية، حيث أن الواقع العملي أثبت قصورها ومحدوديتها، وهذا بالنظر للتحديات التي أصبحت تطل حماية البيانات الشخصية، مما يقتضي التركيز على بديل آخر يسمح بتوفير أقصى قدر من الحماية للبيانات الشخصية، والمتمثل في الحماية التقنية.

1.3- المخاطر التي تهدد البيانات الشخصية

بالرغم من الامتيازات العديدة التي أتاحتها التعامل في البيئة الرقمية فيما يتعلق بخصوصية البيانات الرقمية ومن بينها سهولة القيام بمختلف العمليات الإلكترونية كتخزين البيانات الشخصية للأفراد أو معالجتها أو نقلها عبرها، إلا أنه وبالمقابل تواجهه سلسلة من التهديدات من بينها:

1.1.3- المخاطر المتعلقة بتجميع البيانات الشخصية

يتطلب إجراء عمليات المعالجة جمع البيانات الشخصية والتي يقصد بها: "أي عمل من أعمال جمع وترتيب عناصر البيانات الخاصة بشخص ما، ووضعها في بطاقة معلومات ورقية كانت أو إلكترونية"⁽⁴⁸⁾، غير أن القيام بهذه العملية قد لا يخلو من وقوع مخاطر الاعتداء على خصوصية تلك البيانات المجمعة، لاسيما إذا كانت هذه الأخيرة تتسم بكونها حساسة، مثل قيام الجهات الحكومية أو الهيئات الخاصة بتجميع بيانات مفصلة ودقيقة خاصة بالمتعاملين معها، وهو ما قد يؤدي لاستخدام تلك

(46) المادة 61 من القانون رقم 07-18، المرجع السالف الذكر.

(47) المادة 66 من القانون رقم 07-18، المرجع نفسه.

(48) هبة رمضان رجب، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية، مجلة العلوم القانونية والاقتصادية، مج66، العدد3، كلية الحقوق، جامعة عين شمس، مصر، جانفي 2024، ص 437.

البيانات المحفوظة بطريقة غير مشروعة، خاصة وأن تلك الجهات تقوم بربط الأجهزة المشتركة عبر شبكات وروابط إلكترونية عامة لتسهيل عملية تداول البيانات الشخصية فيما بينها⁽⁴⁹⁾.

كما قد يتم انتهاك خصوصية البيانات الخاصة بالأفراد بتجميعها دون علمهم أو موافقتهم ، وذلك باستخدام الوسائل التقنية الحديثة المتاحة عبر شبكة الإنترنت، مثل ملفات تعريف الارتباط (Cookies) التي تعتمد عليها الشركات التجارية لأغراض الدعاية والتسويق لخدماتها ومنتجاتها⁽⁵⁰⁾ ، فبالرغم مما توفره من فوائد ومزايا عديدة إلا أنه قد يساء استخدامها في أغراض غير مشروعة من خلال الاعتداء على خصوصية الأفراد والاطلاع على بياناتهم الشخصية وهو ما يندرج تحت الأفعال المجرمة قانونا، أما أنظمة جمع المعلومات أو ما يعرف ببرمجيات التتبع والالتقاط فهي تعد الوسيلة الأخطر، خصوصا إذا ما تم استخدامها في المجال الأمني، فهذه الوسيلة تمكن مستخدمها من تجميع كميات كبيرة من المعلومات السرية ومعالجتها بدقة وسرعة فائقتين، غير أنها بالمقابل قد تكون المعلومات المتواجدة فيها محل استغلال غير مشروع بسبب سهولة تعرضها للاختراق وأعمال التجسس الإلكتروني⁽⁵¹⁾.

ومن جهة أخرى، تقوم أغلب وسائل التواصل الاجتماعي بتجميع بيانات خاصة بالمستخدمين، من أجل استغلالها في عمليات التسويق المباشر لمنتجاتها وخدماتها، وهو الأمر الذي يؤدي إلى تعرضها لهجمات القرصنة، أو انتحال الأفراد الموجودين في هذه المواقع شخصيات أخرى وهمية للتدليس عليها ما يسبب في تضليل المستخدمين أو استغلال بياناتهم بطريقة غير قانونية.

2.1.3- المخاطر المتعلقة بتدفق البيانات عبر الأنترنت

تعد الأنترنت مصدرا خطيرا آخرًا للتعدي على البيانات الشخصية، نظرا لكونها تشكل وعاء ضخما لتدفق البيانات عبرها من طرف جميع المستخدمين، إذ هي عبارة عن شبكة تتكون من العديد من الحواسيب والأجهزة الرقمية المتصلة فيما بينها، ويكون ذلك عبر وسائل الاتصالات السلكية أو اللاسلكية، ليمتد تواصل الشبكة لمختلف أنحاء العالم⁽⁵²⁾، وبالتالي يكون من السهل اختراق البيانات الشخصية المخزنة فيها وتخريبها أو تحويلها وذلك من خلال استعمال برامج فيروسية، أو القيام بأعمال القرصنة الإلكترونية "الهاكرز" وكذا استعمال برامج ذكية لجمع معلومات خاصة عن المستخدمين، أو من خلال

(49) محمود عبد الرحمان، التطورات الحديثة لمفهوم الحق في الخصوصية: الحق في الخصوصية المعلوماتية، مجلة كلية القانون الكويتية العالمية، العدد 9، مارس 2015، ص 109.

(50) الكوكيز (ملفات تعريف الارتباط) عبارة عن ملفات نصية تضعها معظم مواقع الويب عند زيارة موقعها، بغرض جمع معلومات عن المستخدمين، بحيث تمكن الموقع من الرجوع إليها عند الحاجة. انظر: سياسة ملفات الكوكيز، متاح على الموقع الإلكتروني: <https://www.ef.dz › cookie-policy>، تاريخ الاطلاع: 2025/07/15 على سا 22:00

(51) هبه رمضان رجب، المرجع السابق، ص 424.

(52) جميل عبد الباقي، القانون الجنائي والأنترنت، دار الفكر العربي، القاهرة، مصر، 2001، ص 4.

ظهورها كروابط مزيفة تتسلل إلى حسابات المستخدم وتعمل على التجسس عليه بمجرد النقر عليها من طرفه، أو حتى من أجل ارتكاب جرائم أخرى كالسرقة المعلوماتية والنصب⁽⁵³⁾.

إضافة لما تم ذكره فقد تتعرض المعلومات المعالجة إلكترونيا لمختلف الممارسات والأفعال غير المشروعة كالتجسس والتلاعب والسرقة بغرض الحصول على أموال أو خدمات غير مستحقة، حيث أن التصفح والولوج عبر شبكة الأنترنت يترك وراءه لدى المواقع المزارة كمية ضخمة من البيانات تتمثل فيما يلي:

- استعمال عنوان الكمبيوتر العائد للزبون (IP)، لأن كل حاسوب متصل بالأنترنت يتم منحه عنوانا يتكون من 32 رقما، وكذلك المعلومات الخاصة بالمتصفح ووقت وتاريخ زيارة الموقع، والاحتفاظ بهذه البيانات داخل المواقع يشكل تهديدا لخصوصية الأفراد في العالم الافتراضي⁽⁵⁴⁾.

- المعلومات الأساسية عن المتصفح ونظام التشغيل وتجهيزات النظام المادية المستخدمة من قبل الزبون.

- مواقع الأنترنت وعناوين الصفحات السابقة التي زارها المستخدم، وهو ما يجعلها محل اطلاع من طرف الغير في حال عدم إخفائها أو حذفها.

- وقد تحتوي كذلك على معلومات عن محركات البحث التي تم استخدامها بغرض الوصول إلى صفحات معينة، وتبعاً لنوع المتصفح المستخدم قد يظهر عنوان البريد الإلكتروني الخاص بهذا الأخير، ومن ثم يظهر مدى تعقيد المعلومات الشخصية المتاحة على الإنترنت، وضرورة اتخاذ تدابير الحماية الدقيقة من الاستغلال غير المشروع⁽⁵⁵⁾.

3.1.3- المخاطر المترتبة عن حوسبة البيانات الشخصية

لقد اتسع نطاق استعمال الحواسيب في مختلف مجالات الحياة، وغزا جميع المؤسسات والإدارات الحكومية والشركات الخاصة التي أصبحت تستخدمه في عملية معالجة المعلومات الشخصية، ورغم الأثر الإيجابي الواسع لهذه الأجهزة والتكنولوجيات إلا أنه خلف آثارا سلبية ملموسة تتمثل في:

(53) عائشة بن قارة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم ونشر الأبحاث، مج2، العدد 5، المركز القومي للبحوث، فلسطين، جوان 2016، ص 42.

(54) المختار بن قوية، المرجع السابق، ص 247.

(55) عائشة بن قارة مصطفى، المرجع السابق، ص 42.

- إمكانية جعل فرص الوصول إلى هذه البيانات على نحو غير مصرح به عن طريق أساليب التلاعب والتحايل، وهو مازاد من مخاطر استغلال هذه البيانات التي من شأنها أن تفتح مجالا أوسع لإساءة استخدام هذه الأخيرة أو توجيهها لأغراض منحرفة⁽⁵⁶⁾.

- ظهور ما يعرف بـ "بنوك المعلومات"، إذ اتجهت كل دول العالم بمختلف مؤسساتها وفي سبيل تسهيل استخدام المعلومات وتعزيز نطاق الاستفادة من البيانات سواء لأغراض تنظيمية أو إدارية إلى إنشاء قواعد بيانات لتنظيم عملها، لتصبح في بنوك المعلومات مجمعة متوافرة، ومتاحة أكثر من ذي قبل للاستخدام في أغراض الرقابة على الأفراد بعد أن كانت المعلومات الشخصية منعزلة، متفرقة، ويصعب التوصل إليها⁽⁵⁷⁾.

2.3- الحماية التقنية كآلية وقائية (مكملة) لحماية المعطيات ذات الطابع الشخصي

تشكل الحماية التقنية العمود الفقري لأي استراتيجية أمنية متكاملة، حيث تهدف إلى تقليل المخاطر الناشئة عن التهديدات السيبرانية وضمان استمرارية العمليات المعلوماتية.

1.2.3- تعريف الحماية التقنية للمعطيات ذات الطابع الشخصي

يقصد بالحماية التقنية مجموعة من الأدوات، والبروتوكولات، والخوارزميات التي تُستخدم لتعزيز أمن البيانات قبل وقوع الخطر، مثل: التشفير المتقدم (Encryption)؛ أنظمة الكشف عن التسلل (IDS/IPS)؛ الهوية والمصادقة متعددة العوامل (MFA)⁽⁵⁸⁾.

وتتمحور طبيعة عمل الحماية التقنية للمعطيات الشخصية حول تطبيق تقنيات وأدوات لحماية البيانات، حيث تعمل هذه الوسائل على حماية البيانات من خلال منع الوصول غير المصرح به إليها والتلاعب بها والضياع، والتقليل من مخاطر الاحتيال وسرقة الهوية، وكذا ضمان استخدام البيانات الشخصية للأغراض التي جُمعت من أجلها فقط، دون إساءة استخدامها لأغراض تجارية أو غير مشروعة، وهذا ضمن إطار قانوني صارم يهدف للحفاظ على الخصوصية والحريات العامة، وتتضمن الحماية التقنية أدوات تستخدم لهذا الغرض مثل: التشفير، وحماية الشبكات، وتأمين أجهزة المستخدمين،

⁽⁵⁶⁾ محمد عبد المحسن المقاطع، حماية الأفراد وضماناتها في مواجهة الحاسوب الآلي، مطبوعات جامعة الكويت، الكويت، 1992، ص 40.

⁽⁵⁷⁾ شمس الدين إبراهيم أحمد، وسائل مواجهة الاعتداءات على الحياة الشخصية في مواجهة تقنية المعلومات في القانون السوداني والمصري: دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2005، ص 53.

⁽⁵⁸⁾ خالد ظاهر عبد الله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، ج1، العدد 38، كلية الشريعة والقانون بدمنهور - جامعة الأزهر، مصر، جويلية 2022، ص 999.

وضوابط الوصول، وتتكامل مع التدابير القانونية والإجرائية التي تفرضها التشريعات مثل التشريع الجزائري.

2.2.3- الوسائل المستخدمة في حماية أمن المراسلات والمواقع الإلكترونية

بالرغم من التقدم الكبير الذي أحرزته تقنيات التحقق من الشخصية في مجال حماية البيانات، إلا أن فعاليتها أصبحت مع مرور الوقت محدودة، وذلك نظرا للتطور المسجل في وسائل ارتكاب الجريمة المعلوماتية، وكذا تنوع الأساليب التي يلجأ إلى المجرمون لاختراق الحسابات الشخصية غير تلك التي تقوم على السطو وسرقة كلمات المرور، لذلك سعى المتخصصون في المجال الإلكتروني الرقمي إلى ابتكار وسائل حديثة تعمل على تعزيز حماية أمن وسرية المراسلات والمعلومات عن طريق تشفيرها (أولا)، وبحماية أمن الشبكات والأنظمة الداخلية (ثانيا)، وإدارة الوصول والهوية (ثالثا)، وأخيرا النسخ الاحتياطي واستعادة البيانات (رابعا).

أولا: التشفير

التشفير أو التعمية أو الكتابة السرية كلها مصطلحات تدل على تلك الوسيلة التقنية المستعملة لحماية أمن المعلومات ضد الأعمال غير المشروعة كالقرصنة والاختراق وبث الفيروسات التي تقع في المنصات الرقمية الموجودة في شبكة الأنترنت والحواسيب الإلكترونية، بهدف الاعتداء على المعلومات الاسمية وبيانات وسائل الدفع الإلكتروني كبطاقات الائتمان الممغنطة.

ويقصد به أيضا فن حماية المعلومات عن طريق تحويلها إلى رموز أو إشارات معينة غير مقروءة وغير مفهومة، باستخدام خوارزميات رياضية محددة، لا يمكن حلها إلا من خلال مفتاح سري يمتلكه الشخص المصرح له فقط يقوم بتحويل تلك الرموز إلى نص عادي مقروء⁽⁵⁹⁾، وهو تغيير لمظهر المعلومات يهدف لإخفاء معناها الحقيقي، فلا يمكن للغير الاطلاع عليها أو العبث بمحتوياتها بتغيير شكلها إلى صورة لا يمكن فهمها إلا بعد إرجاعها إلى صورتها الأصلية، ولا يمكن أن يتم ذلك إلا باستخدام مفتاح معين وهو مفتاح التشفير الذي لا يملكه إلا صاحب الحق في الاطلاع على المعلومات التي تعتبر حساسة للغاية⁽⁶⁰⁾.

(59) عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، مصر، 2009، ص 62.

(60) بوعزة هداية، فتحة يوسف، الحماية التقنية للمعلومات ودورها في تأمين نظام الدفع الإلكتروني، مج3، العدد 4، مجلة الدراسات والبحوث القانونية، تصدر عن مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، ديسمبر 2018، ص 398.

كما يقصد بتشفير البيانات كل تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها⁽⁶¹⁾، والغرض من إجراء التشفير هو ضمان حفظ البيانات الشخصية وعدم إتاحتها للغير للعبث بها أو الاطلاع عليها وذلك لكونها سرية أو خاصة جدا⁽⁶²⁾.

إذن يعد التشفير إجراء تقنيا ضروريا من أجل الحفاظ على أمن وسرية المعلومات، وهو بهذا الشكل يعمل على توفير عنصري الثقة والأمان في المعاملات الإلكترونية، حيث يتيح لصاحب الحق في الخصوصية من خلال أدوات وأساليب معينة بتحويل المعلومات من أجل إخفاء مضمونها والحيلولة دون الوصول إليها وتعديلها أو استخدامها غير المشروع، وهو ما يسمح بضمان سرية البيانات المشفرة والاعتراف بحق أصحابها في الخصوصية بتجريم الاعتداء عليها، ويشكل حماية فعالة ضد المخاطر المرتبطة بالمعالجة الإلكترونية للمعطيات.

ثانيا: أمن الشبكات والأنظمة

هي مجموعة من الممارسات والإجراءات والتقنيات التي تهدف لحماية الشبكات الرقمية، وأجهزتها، وتطبيقاتها من الوصول غير المصرح به للبيانات، من الاختراقات والهجمات الخبيثة وذلك عبر تطبيق سياسات وإجراءات وتقنيات تتمثل فيما يلي:

أ- حماية المواقع الإلكترونية والشبكات الداخلية من خلال جدران الحماية (Firewalls)

يقصد بجدار الحماية "الجدار الناري" مجموعة الأنظمة التي توفر وسيلة أمنية بين شبكة الأنترنت وشبكة المستخدم الداخلية والخروج منها للمرور عبر هذا الجدار الذي يتصدى لجميع محاولات الدخول للشبكة بدون صفة، ويقوم جدار الحماية بمراقبة حركة البيانات الواردة والصادرة و يمنع دخول الأخطار القادمة من شبكة الأنترنت إلى الشبكة الداخلية الخاصة بالمستخدم⁽⁶³⁾.

ويؤدي جدار الحماية الرئيسية دورا هاما في حماية شبكة الحاسب الآلي الداخلية وشبكة الأنترنت، يتمثل في رصد جميع البيانات الواردة والصادرة من الشبكة الداخلية والتأكد من مدى مطابقتها لشروط المستخدم التي يحددها البرنامج من قبل⁽⁶⁴⁾، حيث يقوم بإجراء مسح scanne شامل للمعلومات التي

(61) عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2002، ص 311.

(62) عصام عبد الفتاح مطر، المرجع السابق، ص 62.

(63) إسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت بين الشريعة والقانون: الكمبيوتر والأنترنت، ط3، جامعة الإمارات العربية المتحدة، العين، الإمارات العربية المتحدة، 2004، ص 976.

(64) طارق إبراهيم الدسوقي عطيه، الموسوعة الأمنية: الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، مصر، 2015، ص 556.

ترد من شبكة الأنترنت ويقوم بفحصها وتحليلها، وعندما يجد أي شك في المعلومات التي تصل إليه لمحاولة التسلل أو الاختراق إلى الأماكن المؤمنة فإنه يقوم بمنعها وطردها خارج الشبكة، أما إذا كانت المعلومات عادية وآمنة فإن الجهاز يسمح لها بالمرور والدخول إلى أجهزة الحواسيب الآلية⁽⁶⁵⁾.

يتم تطبيق هذا النظام بالخصوص في كثير من القطاعات الحساسة مثل البنوك، التي تتوفر على قاعدة ضخمة من البيانات الشخصية الحساسة للعملاء المتعلقة بمختلف العمليات المالية التي يقوم البنك بإجرائها وإدارتها، حيث تستعين من أجل حماية الشبكة الداخلية من تلك المخاطر بأنظمة خاصة من خلال إقامة جدار ناري يفصل بين الشبكة الداخلية وشبكة الأنترنت حتى لا يكون موقع البنك عرضة للمقتحمين.

ب- برامج مكافحة الفيروسات والبرامج الضارة: يتمثل دورها في حماية الأجهزة من التهديدات التي يمكن أن تتعرض لها البيانات الشخصية، ويوجد العديد من هذه البرامج التي يمكن تنزيلها عبر الأنترنت من بينها: Norton 360, Bitdefender, McAfee, Kaspersky, و Avast، حيث توفر حماية شاملة ضد البرمجيات الخبيثة والتصيد الاحتيالي.

ج- أنظمة كشف ومنع التسلل (IDS/IPS) لمراقبة حركة مرور الشبكة للكشف عن الأنشطة المشبوهة، وهي تعمل عبر تحليل الحزم وقواعد التوقيعات والسلوكيات غير الطبيعية وتُصنف إلى أنواع مثل الشبكي (NIPS) والمضيفي (HIPS) واللاسلكي (WIPS) وتُستخدم بشكل متكامل مع جدران الحماية لتوفير دفاع عميق ضد الانتهاكات والهجمات السيبرانية.

ثالثا: إدارة الوصول والهوية

هي عملية شاملة لإدارة وتأمين هويات المستخدمين، تهدف إلى ضمان حصول المستخدمين على إمكانية الوصول المناسبة إلى الأنظمة والبيانات لضمان الخصوصية والأمان، وتتضمن ما يلي:

أ- كلمات مرور قوية والمصادقة متعددة العوامل (MFA): هي طريقة للتحقق من هوية المستخدم من خلال طلب نموذجين مختلفين على الأقل من الإثباتات، مثل كلمة مرور الحساب عبر الأنترنت وبصمة الإصبع أو غيرها من البيانات البيومترية، وتوفر المصادقة متعددة العوامل (MFA) طبقات إضافية من الحماية تتجاوز ما يمكن أن توفره كلمات المرور وحدها.

ب- مبدأ الامتياز الأقل (PoLP): يعد مفهوم أمني أساسي في مجال الأمن السيبراني، حيث يستلزم منح المستخدمين، والتطبيقات، والأنظمة، أقل قدر ممكن من الصلاحيات (أذونات الوصول)

⁽⁶⁵⁾ أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مطابع الشرطة، القاهرة، مصر، 2005،

اللازمة لتنفيذ مهامهم المحددة فقط، بهدف تقليل مخاطر سوء الاستخدام، وتقليل الأضرار المحتملة في حالة الاختراق، والحد من انتشار البرامج الضارة.

رابعاً: النسخ الاحتياطي واستعادة البيانات

تتضمن إنشاء نسخ مكررة من البيانات وتخزينها في مكان آمن (في جهاز الحاسوب أو الهاتف أو في الموقع الإلكتروني) لاستعادتها عند حدوث فقدان بسبب أخطاء بشرية، أعطال، أو هجمات سيبرانية.

3.2.3- دور الوسائل التقنية في حماية المعطيات ذات الطابع الشخصي

شهد العالم في العقود الأخيرة تطور مذهلاً في ميدان الاتصالات والرقمنة وهذا بفضل الاختراعات والبرامج والخدمات اللاسلكية التي أصبحت توفرها الشركات الإلكترونية المختصة لزبائنها، مما انعكس ذلك بالإيجاب على مختلف مناحي الحياة، وأصبح الأفراد يتهافون على اقتناء أفضل البرامج والحواسيب والهواتف الرقمية وذلك من أجل الاستفادة من مزايا هذا التطور، لاسيما في مجال حفظ المعلومات والبيانات الشخصية، وبالرغم من أنه لا يمكن إنكار المستوى الهائل الذي بلغته التقنية في المجال الرقمي، حيث يبدو للوهلة الأولى أنها أصبحت تبدو الحل الأمثل والأكثر فاعلية في مواجهة الانتهاكات التي تطل البيانات الشخصية، إلا أن الملاحظ من خلال الواقع المعاش أن هذه الوسائل المستعملة في تأمين الخصوصية الإلكترونية قد أهدرت قيمتها في كثير من الأحيان - مما يتعذر معه القول بجودها بصفة مطلقة ودائمة-، وهذا نظراً لاعتبارين رئيسيين:

أولاً: الاعتبارات المتعلقة بأمن الدول

يتضح في بعض القضايا القانونية المتعلقة بانتهاك الخصوصية وبحجة حماية الأمن الوطني، حيث تبرر القيود على الخصوصية ويؤدي ذلك إلى الحد من حرية الأفراد الشخصية، فغالبا ما يضعف هذا الاعتبار موقف الأفراد أمام القانون، وقد اعتمدت الأجهزة الأمنية في سبيل ذلك على تتبع الجرائم الإلكترونية وتحليل تفاصيلها أحيانا دون الالتزام بالمعايير المقررة في نظم الاتصالات، كاستعمال التشفير لضمان حماية المعلومات. قد أصبح التأمين الكامل للبيانات الشخصية هو المبدأ الأساسي مع تقدم التقنيات الحديثة، حيث يعد أي انتهاك لها استثناء ينفذ بحذر، وهو ما يواجه اعتراض شركات الاتصالات والمستخدمين أحيانا، مما قد يقلل من فاعلية الاعتماد على الطرق التقنية الحديثة في حماية المعلومات، كما قد يضعف من خيار اللجوء إلى هذا الوسائل⁽⁶⁶⁾.

⁽⁶⁶⁾ من بين القضايا الشهيرة، ما يعرف بقضية شركة أبل، حيث تمسكت هذه الأخيرة بموقفها الرافض لطلب المباحث الفيدرالية في فك تشفير هاتف C5 جرى التحفظ عليه في قضية تتعلق بالإرهاب سنة 2016م، وكان من شأن موافقتها على هذا الطلب أن تهتز ثقة عملاء الشركة عبر العالم في نظامها المتعلق بتأمين أجهزة الاتصالات التي تسوقها، ولقد بررت الشركة رفضها بكونه مرتكزا على حقوق الأفراد في حماية الخصوصية، وبالتالي كانت الشركة تدفع باتجاه حماية

ولقد تضمن القانون رقم 07-18 النص على هذا الاستثناء، حيث أعطى المشرع السلطات القضائية والأمنية صلاحية التحري والولوج إلى المعطيات المعالجة وجميع الوثائق إذا اقتضت الضرورة الأمنية ذلك دون الاعتداد بالسري المهني أمام السلطة الوطنية، بشرط وجوب التقيد بالإجراءات القانونية المتبعة في ذلك⁽⁶⁷⁾.

ثانيا: التطور الهائل لأساليب التجسس وأنماط القرصنة الإلكترونية

نظرا للتطور الدائم والرهيب في مجال تقنيات التجسس والقرصنة الإلكترونية والوسائل المعتمدة في ذلك وهو ما تجاوز أنظمة الحماية الإلكترونية للبيانات الخاصة، حيث لم تعد وسائل الحماية التقنية التقليدية كافية لضمان أمن هذه البيانات، ما أدى إلى تطوير وابتكار وكذا انتشار آلاف الفيروسات الإلكترونية ونشرها على الشبكة المعلوماتية العالمية، وقادة بذلك إلى زيادة خطر اختراق البيانات، مما جعل مسألة حماية المعلومات أكثر صعوبة وتعقيدا من مجرد تخزينها فقط على الأجهزة أو الشبكات. وبناء على ذلك، وفي مجال حماية البيانات صار إيجاد وسائل تقنية وتطوير أدوات تتيح حماية المعلومات الشخصية واستغلالها بشكل آمن وسري يضمن أمنها الدائم هو التحدي الرئيسي للمتخصصين، بعيدا عن أي وصول غير مصرح به أو انتهاك للخصوصية، وهذا سواء تعلق الأمر بالأفراد أو الشركات التي قد تتعرض سمعتها ومكانتها للخطر في حال ما إذا تم تسريب بياناتها أو كشف كلمات المرور الخاصة بها، ومن أبرز الإجراءات الوقائية المقترحة والتي يوصى بها لتعزيز حماية البيانات: اختيار كلمات مرور طويلة وقوية، إدخال المعلومات من الأجهزة الشخصية بدلا من إدخالها من الأجهزة العامة، وتفاذي التعامل مع الشبكات العامة وكذا كمها في الإنترنت، إذ أن هذه الأخيرة يمكن ترك آثار الولوج بها والتي قد تستغل في الاختراق أو الاحتيال، كما يفضل الامتناع عن استخدام أجهزة مشتركة أو غير شخصية، إذ يمكن أن تحتفظ بسجلات الدخول وتتيح للآخرين الوصول إلى المعلومات، مما يزيد من مخاطر انتهاك الخصوصية والاطلاع وسرقة البيانات الشخصية دون ترخيص.

الخصوصية كي تحمي سوقها وسمعتها التكنولوجية، في حين كانت الحكومة الأمريكية تضغط في اتجاه انتهاك الخصوصية بدعوى حماية الأمن القومي، لاسيما وأنها قد تواجه المشكلة ذاتها في سياق جرائم أخرى في المستقبل. مشار إليه في: سليم حميداني، المظاهر القانونية لاختراق الخصوصية في العالم الرقمي، ورقة بحثية مقدمة ضمن فعاليات الملتقى الوطني الأول: الحق في الخصوصية في مواجهة التحديات الناشئة عن التكنولوجيا الرقمية واقع الحماية واعتبارات التقيد، المنعقد يومي (25-26) فيفري 2019، جامعة 8 ماي 1945، قالمة، ص 13.

⁽⁶⁷⁾ المادة 50 من القانون رقم 07-18، المرجع السالف الذكر.

4-خاتمة

بناء على ما تم التطرق إليه في هذه الدراسة، يمكن القول أن الحق في حماية البيانات الشخصية يعد من بين المسائل التي أصبحت تكتسي أهمية بالغة لارتباطها بالحياة الخاصة للأفراد وهو ما جعل المشرع الجزائري يقوم بتنظيمها سواء من خلال النص عليها في الدستور أو في القوانين الخاصة، لاسيما في ظل التطور التكنولوجي والرقمي الرهيب الذي أصبح يشهده العالم وما نتج عنه من انتهاكات ومخاطر، وعليه يمكن الخروج بمجموعة من النتائج والتوصيات تتمثل في الآتي:

- يتجلى انسجام المشرع الجزائري مع التطورات التكنولوجية والرقمية الحاصلة، وهو ما يظهر من خلال إصداره للقانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث جاء لسد فراغ تشريعي سابق، وفي إطار مواصلة تحديث وعصرنة الإدارة التي انتهجتها الجزائر، لاسيما فيما يتعلق بحماية المعطيات الشخصية بالنظر لخصوصيتها وحساسيتها؛

- بالرغم من السياسة التشريعية التي تبناها المشرع الجزائري والمتمثلة في سن قوانين متعلقة بتكنولوجيا المعلوماتية لاسيما القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المرتبطة بجرائم الإعلام والاتصال، وكذا التعديلات الجديدة التي طرأت على قانون العقوبات منذ سنة 2004، حيث شهد إدراج نصوص عقابية تتعلق بأنظمة المعالجة الآلية للمعطيات، إلا أن هذه القوانين في غالبيتها كانت تقتصر على حماية أنظمة المعالجة ذاتها أو للوقاية من بعض الجرائم التي يسهل ارتكابها بواسطة المعلوماتية، ولم تكن تتضمن الإشارة إلى مسألة الاعتداء على المعطيات الشخصية التي يمكن أن يرتكبها معالج المعطيات ذاته وليس الغير؛

- توفير مجموعة من الضمانات الموضوعية والإجرائية من أجل حماية المعطيات ذات الطابع الشخصي، بالمقابل ترتيب مجموعة من الالتزامات على عاتق المسؤول بالمعالجة في القانون رقم 07-18.

- اتجه المشرع الجزائري نحو تدعيم الطابع الوقائي للحماية من خلال تعزيز آليات الرقابة والمتابعة والكشف المبكر عن أوجه الإخلال المرتبطة بمعالجة البيانات، وذلك عبر استحداث الأقطاب الجهوية المكلفة بمهام المراقبة والتدقيق لدى الهيئات والأشخاص المعالجين للمعطيات، إلى جانب تكريس مندوب حماية المعطيات ذات الطابع الشخصي باعتباره وسيلة داخلية لضمان الامتثال لقواعد الحماية القانوني للبيانات.

- أقر المشرع تنظيمًا أكثر دقة لعمليات نقل المعطيات الشخصية إلى الخارج، بما يحقق التوازن بين حماية البيانات ومتطلبات التعاون الدولي في هذا المجال.

- علاوة على الآليات الرقابية، كرس المشرع الجزائري آليات ردعية بهدف ضمان احترام قواعد حماية المعطيات، حيث تعد الجزاءات أداة ردعية أساسية في مواجهة أي إخلال بالالتزامات القانونية؛

- تشكل هذه الجزاءات امتدادا وظيفيا للآليات الإجرائية، باعتبارها الوسيلة التي تضمن فعالية النظام القانوني، وتمنع تحول القواعد التنظيمية إلى مجرد نصوص غير مطبقة؛

- رغم تكريس الآليات القانونية في حماية المعطيات ذات الطابع الشخصي إلا أنها أثبتت قصورها، وهذا بسبب التحديات والمخاطر التي أصبحت تفرضها البيئة الرقمية؛ مما يقتضي تعزيز هذه الآليات بحماية تقنية يكون دورها وقائيا ومكملا.

التوصيات

- هناك بعض المسائل المعقدة المرتبطة بالمفاهيم والمصطلحات المستعملة في القانون، بحيث قد تؤدي إلى خلق صعوبات في تعامل القضاء مع نصوصه، لذا ينبغي إقامة ندوات علمية لشرح مضمون هذا القانون، لاسيما فيما يتعلق بحصر أنواع المعطيات ذات الطابع الشخصي التي تكون محلا للحماية، وكذا تفسير الالتزامات المترتبة على المسؤولين عن المعالجة لضمان تطبيق فعال للقانون.

- تكثيف الحملات التحسيسية والتوعوية من طرف خبراء ومختصين بخصوص مخاطر التعامل في مجال المعطيات الشخصية؛

- وأخيرا تمديد نطاق حماية المعطيات كأحد عناصر الحق في الحياة الخاصة ليشمل الشخص المعنوي.

5- قائمة المراجع

أولا: الكتب

- 1- إسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت بين الشريعة والقانون: الكمبيوتر والأنترنت، ط3، جامعة الإمارات العربية المتحدة، العين، الإمارات العربية المتحدة، 2004.
- 2- أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مطابع الشرطة، القاهرة، مصر، 2005.
- 3- جميل عبد الباقي، القانون الجنائي والأنترنت، دار الفكر العربي، القاهرة، مصر، 2001.
- 4- شمس الدين إبراهيم أحمد، وسائل مواجهة الاعتداءات على الحياة الشخصية في مواجهة تقنية المعلومات في القانون السوداني والمصري: دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2005.
- 5- طارق إبراهيم الدسوقي عطيه، الموسوعة الأمنية: الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.
- 6- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2002.
- 7- عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، مصر، 2009.

المجلد: 12	العدد: 02	السنة: جوان 2026 م	ص: 237 - 269
------------	-----------	--------------------	--------------

8- محمد عبد المحسن المقاطع، حماية الأفراد وضماناتها في مواجهة الحاسوب الآلي، مطبوعات جامعة الكويت، الكويت، 1992.

ثانياً: المجالات

1- بوعزة هداية، فتحة يوسف، الحماية التقنية للمعلومات ودورها في تأمين نظام الدفع الإلكتروني، مج3، العدد 4، مجلة الدراسات والبحوث القانونية، تصدر عن مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، ديسمبر 2018.

2- خالد ظاهر عبد الله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، ج1، العدد 38، كلية الشريعة والقانون بدمنهور - جامعة الأزهر، مصر، جويلية 2022.

3- سهام بن دعاس، فوزية بن عثمان، ضمانات حماية المعطيات الشخصية في البيئة الرقمية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، مج 15، العدد 1، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، أفريل 2022.

4- عائشة بن قارة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم ونشر الأبحاث، مج2، العدد 5، المركز القومي للبحوث، فلسطين، جوان 2016.

5- عز الدين طباش، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري: دراسة في ظل قانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، مج9، العدد 2، كلية الحقوق لعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، ديسمبر 2018.

6- فريد روابح، جرائم الجمع غير المشروع للمعطيات الشخصية الرقمية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، مج9، العدد 1، جامعة عباس لغرور، خنشلة، أفريل 2022.

7- فيصل بوخالفة، حماية المعطيات ذات الطابع الشخصي بين النصوص التقليدية ومتطلبات التقنية، مجلة الدراسات والبحوث القانونية، مج 8، العدد 1، تصدر عن مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، جانفي 2023.

8- كاملة بوعكة، الحماية القانونية للأشخاص في مجال معالجة المعطيات ذات الطابع الشخصي في ضوء القانون 18-07، المجلة الجزائرية للقانون والأعمال، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، ديسمبر 2020.

9- محمود عبد الرحمان، التطورات الحديثة لمفهوم الحق في الخصوصية: الحق في الخصوصية المعلوماتية، مجلة كلية القانون الكويتية العالمية، العدد 9، مارس 2015.

10- المختار بن قوية، المعطيات الشخصية في ظل قانون 18-07 بين حتمية الرقمنة ومخاطر الاختراق، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مج 9، العدد 1، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، جوان 2024.

11- هبه رمضان رجب، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية، مجلة العلوم القانونية والاقتصادية، مج66، العدد3، كلية الحقوق، جامعة عين شمس، مصر، جانفي 2024.

12- يحي تومي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07: دراسة تحليلية، مج4، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، جانفي 2020.

13- يزيد بوحليط، عبد الرحمان فطناسي، الحماية الإدارية والجزائية في مجال المعطيات ذات الطابع الشخصي على ضوء القانون 07-18، مجلة أبحاث قانونية وسياسية، مج6، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحيى، جيجل، ديسمبر 2021.

ثالثا: المؤتمرات العلمية

سليم حميداني، المظاهر القانونية لاختراق الخصوصية في العالم الرقمي، ورقة بحثية مقدمة ضمن فعاليات الملتقى الوطني الأول: الحق في الخصوصية في مواجهة التحديات الناشئة عن التكنولوجيا الرقمية واقع الحماية واعتبارات التقييد، المنعقد يومي (25-26) فيفري 2019، جامعة 8 ماي 1945، قالمة،

رابعا: المواقع الإلكترونية

سياسة ملفات الكوكيز، متاح على الموقع الإلكتروني: <https://www.ef.dz › cookie-policy>، تاريخ الاطلاع: 2025/07/15 على سا 22:00

خامسا: النصوص القانونية

أ- الدستور

قانون رقم 01-16 مؤرخ في 26 جمادى الأولى عام 1437 الموافق 6 مارس سنة 2016، يتضمن التعديل الدستوري. ج. ر. ع 14، الصادر في 27 جمادى الأولى عام 1437 هـ الموافق 7 مارس سنة 2016م.

ب- النصوص التشريعية

قانون رقم 07-18 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. ج. ر. ع 34، الصادر في 25 رمضان عام 1439 هـ الموافق 10 يونيو سنة 2018م، معدل ومتمم.