

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et populaire
Ministère de l'Enseignement Supérieur et
de la Recherche Scientifique.

Université de Ghardaïa

Faculté de Droit et des Sciences Politiques

Département de Droit



وزارة التعليم العالي و البحث العلمي

جامعة غرداية

كلية الحقوق والعلوم السياسية

قسم الحقوق

شهادة تصحيح

يشهد الأستاذ بن أوزينة محمد بصفته (ها) رئيسا للجنة مناقشة مذكرة

الماستر لـ:

الطالب (ة): عبد الستار إلهام تحت رقم التسجيل: 212139091287

الطالب (ة): إيدابير فاطيمة الزهراء تحت رقم التسجيل: 202039082204

تخصص: ماستر قانون خاص دفعة 2026 لنظام (ل م د)

أن المذكرة المعنونة بـ:

الحماية القانونية للبيانات الشخصية وفق القانون رقم 25-11 المعدل والمتمم المتعلق بحماية

الأشخاص الطبيعيين في مجال معالجة المعطيات ذات طابع الشخصي.

تم تصحيحها من طرف الطالبتين وهي صالحة للإيداع.

غرداية في 2026/06/30

إمضاء الأستاذ رئيس اللجنة المكلف بمتابعة التصحيح:

رئيس القسم:

د/..... **البيكتور حمودين داود**

رئيس قسم الحقوق

ملاحظة: تترك هذه الشهادة لدى القسم.



جامعة غرداية

كلية الحقوق والعلوم السياسية



قسم: الحقوق

عنوان المذكرة

الحماية القانونية للبيانات الشخصية وفق قانون
رقم 25-11 المعدل والمتمم المتعلق بحماية الأشخاص
الطبيعيين في مجال معالجة المعطيات ذات طابع الشخصي

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر أكاديمي حقوق

تخصص: قانون خاص

تحت إشراف الأستاذ:

د. أحمد البرج

إعداد الطالبتين:

-الهام عبد الستار

- فاطيمة الزهراء ايدابير.

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الجامعة	الصفة
د. محمد بن أوزينة	أستاذ	غرداية	رئيسا
د. أحمد البرج	محاضر أ	غرداية	مشرفا
د. مروان دهمة	محاضر أ	غرداية	مناقشا

نوقشت بتاريخ: 2026/06/06

السنة الجامعية:

2026 / 2025 م - 1446/1447هـ



جامعة غرداية

كلية الحقوق والعلوم السياسية

قسم: الحقوق

عنوان المذكرة



الحماية القانونية للبيانات الشخصية وفق قانون
رقم 25-11 المعدل والمتمم المتعلق بحماية الاشخاص
الطبيعي

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر أكاديمي حقوق

تخصص: قانون خاص

تحت اشراف الاستاذ:

د. أحمد البرج

إعداد الطالبتين:

- الهام عبد الستار

- فاطيمة الزهراء ايدابير

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الجامعة	الصفة
	استاذ	غرداية	رئيسا
د. أحمد البرج	محاضر أ	غرداية	مشرفا
	محاضر أ	غرداية	مناقشا

نوقشت بتاريخ:

السنة الجامعية:

2025 / 2026 م - 1446هـ / 1447هـ

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الشكر والعرفان

من باب العمل بقول النبي صلى الله عليه وسلم:

(من صنع إليكم معروفا فكافئوه)

الشكر أولاً وآخراً، ودائماً وأبدًا، لله سبحانه وتعالى، المعين على كل خير، والموفق لإتمام هذا العمل، فاللهم لك الحمد حتى ترضى، ولك الحمد إذا رضيت، ولك الحمد بعد الرضا. وإننا نتقدم بأسمى عبارات الشكر والعرفان، النابعة من القلب، لكل من أسهم في هذا الإنجاز. ولا يسعني، بعد أن أنجزت هذه الدراسة بعون الله وتوفيقه، إلا أن أتقدم بجزيل الشكر وعظيم الامتنان لأستاذي الفاضل البرج أحمد التي أشرف على هذا العمل وحرص على قراءة كل كلمة فيه.

كما نتوجه بالشكر والتقدير لأعضاء لجنة المناقشة الموقرين، على ما تفضلوا به من جهد وتوجيه. ولا يفوتنا أن نشكر طلبة الماجستير بكلية الحقوق والعلوم السياسية على تجاوبهم وتعاونهم الكريم. وجزيل الشكر وعظيم الامتنان نرفعه لكل من كان لنا عوناً، وساعدنا من قريب أو بعيد، بالنصيحة أو بالدعم، في سبيل إنجاح هذا العمل

الاهداء

إلى من يحملون في قلوبهم مسيرتي، ويضيئون بوجودهم ودعواتهم عتمة
طريقي...

إلى منبع العطاء وبسمة الحياة.. أمي الغالية، إليك يا من سهرت لينا
التعب، ودعوت ليصعد الأمل. إلى طهر دعواتك التي كانت ملاذي وسندي
في كل خطوة.

إلى منبع الفخر والظهر الذي لا ينحني.. أبي العزيز، إلى من علمني أن
القمم تُنال بالصبر، وأن الطموح لا سقف له. إليك يا من حصدت الشوك
لأجني أنا الثمار.

إلى شركاء العمر وسند الأيام.. إخوتي وأخواتي، إلى من تقاسمت معهم
الأيام بخلوها ومزّها، وكانت كلماتهم لي دافعاً مستمراً للاستمرار والتميز.

إلى منبع البركة والوقار.. جدي العزيز، حفظك الله ورعاك وأطال في
عمرك، لتظل ظلاً ظليلاً نستظل به.

إلى الروح الطاهرة التي غادرتنا ومسكنها القلب.. جدتي رحمها الله، إلى
من كنت أتمنى أن تشهد معي هذه اللحظة، أهدي إليك هذا النجاح، سائلاً
المولى أن يجعله نوراً لروحك الطاهرة في جنات النعيم.

إلى من صمدت وعافرت.. إلى "نفسي"، إلى الذات التي لم تنكسر أمام
العقبات، وتحذت الصعاب لتصل إلى هذا اليوم. أهدي هذا الجهد تقديراً
لشغفي وصبري.

فاطيمة الزهراء ايدابير.

الاهداء

"قل اعملوا فسيرى الله عملكم ورسوله والمؤمنون" صدق الله العظيم
الهي لا يطيب الليل إلا بشكرك ولا يطيب النهار إلا بطاعتك... ولا تطيب
اللحظات إلا بذكرك... ولا تطيب الاخوة إلا بعفوك... ولا تطيب الجنة إلا
برؤيتك سبحانك لا إله إلا أنت.
إلى من بلغ الرسالة وأدى الأمانة... ونصح الأمة... إلى نبي الرحمة ونور
العالمين... سيدنا محمد صلى الله عليه وسلم.
إلى من كلله الله بالهيبة والوقار... إلى من علمني الطاعة بدون انتظار
... إلى من أحمل اسمه بكل افتخار.. أرجو الله ان يمد في عمرك لتري ثمار
الذي قد حان قطفها بعد طول انتظار وستبقى كلماتك نجوم اهتدى بها
اليوم وفي الغد أبي الغالي العزيز.
إلى ملاكي في الحياة.... إلى معنى الحب و الحنان إلى بسمه الحياة
وسر الوجود إلى من كان دعائها سر نجاحي وحنانها بلسم جروحي
..... إلى أغلى الحبايب أمي الحبية.
إلى من ترعرعت معهم تحت سقف واحد تجمعنا المحبة والاخلاص
وقاسمت معهم الحياة إلى اخوتي.
إلى جدتي العزيزة التي كان دعائها سندي وقوتي، وإلى خالاتي واخوالي
الاعزاء الذين غمروني بالمحبة والدعم اهديكم هذا العمل المتألق بكل شكر
وامتنان حفظكم الله ودام وجودكم في حياتي.
إلى الذي كان لنا عوناً في بحثنا هذا ونورا يوضئ الظلمة إلى من
زرع التفاؤل في دربنا فله مني كل الشكر والتقدير استاذي.
وإلى جميع الاصدقاء و الاحباب من قريب ومن بعيد، وإلى جميع الاساتذة
كلية الحقوق والعلوم السياسية

الهام عبد الستار

قائمة المختصرات

المختصر	المقصود به
GDPR	General Data Protection Regulation
IAPP	International Association of Privacy Professionals
AI	Artificial Intelligence
ق.م	القانون المدني
ق.إ.م.إ	قانون الإجراءات المدنية والإدارية
ج.ر	الجريدة الرسمية
ص	الصفحة
ط	الطبعة

مقدمة

بفعل الثورة الرقمية يشهد العالم المعاصر تحولات عميقة ومتسارعة وتنامي الاعتماد على تكنولوجيات الإعلام والاتصال، حيث لم تعد البيانات مجرد عنصر تقني محايد، بل أصبحت موردًا استراتيجيًا ذا قيمة اقتصادية وقانونية واجتماعية بالغة.

ومن هنا تبرز أهمية التعمق في دراسة الحماية القانونية للبيانات الشخصية، ليس فقط من خلال استعراض النصوص القانونية المنظمة لها، بل من خلال تحليلها في ضوء التطورات التكنولوجية الراهنة، وتقييم مدى نجاعتها في تحقيق التوازن بين متطلبات المعالجة الرقمية وحماية حقوق الأفراد..

وعليه، فإن موضوع الحماية القانونية للبيانات الشخصية يندرج ضمن الإشكاليات القانونية المعاصرة التي تتقاطع فيها عدة مجالات، من بينها القانون الخاص، والقانون الجنائي، وقانون التكنولوجيا، مما يجعله موضوعًا خصبًا للبحث والتحليل، ويستدعي مقاربة علمية دقيقة تأخذ بعين الاعتبار خصوصية البيئة الرقمية وتعقيداتها المتزايدة.

وتتجلى أهمية هذا الموضوع في كونه يعالج إحدى أهم القضايا القانونية المعاصرة المرتبطة بحماية الحقوق والحريات الأساسية في البيئة الرقمية، وعلى رأسها الحق في الخصوصية. كما تبرز أهمية الدراسة في إبراز مدى قدرة المشرع على تحقيق التوازن بين متطلبات التطور التكنولوجي، خاصة في ظل تنامي استخدام الذكاء الاصطناعي، وبين ضرورة حماية الأفراد من المخاطر المرتبطة بمعالجة بياناتهم.

أما من حيث أسباب اختيار الموضوع، فتتوزع بين أسباب علمية وأخرى عملية. فمن الناحية العلمية، يندرج هذا الموضوع ضمن مجالات البحث الحديثة التي تشهد تطورًا مستمرًا. وتهدف هذه الدراسة إلى تحقيق جملة من الأهداف، من أبرزها تحليل الإطار القانوني المنظم لحماية البيانات الشخصية في التشريع الجزائري، وبيان مدى انسجامه مع المعايير الدولية، خاصة في ظل التطورات التكنولوجية الحديثة.

وفي إطار تدعيم الدراسة علميًا، يجدر التطرق إلى أهم الدراسات السابقة التي تناولت موضوع حماية البيانات الشخصية، وذلك بغرض الوقوف على الجهود العلمية السابقة وتحديد الإضافة التي تسعى هذه الدراسة إلى تقديمها.

في هذا السياق، تناول الباحث Daniel J. Solove في كتابه الموسوم بـ Privacy Law Fundamentals، وهو كتاب أكاديمي صادر عن الرابطة الدولية لمتخصصي الخصوصية (IAPP) سنة 2024، موضوع الخصوصية الرقمية من منظور قانوني حديث، حيث ركز على تطور مفهوم الخصوصية وتعقيداته في البيئة الرقمية، خاصة في ظل تنامي المعالجة الآلية للبيانات، وتتقاطع هذه الدراسة مع موضوع بحثنا في تناولها للإشكالات المرتبطة بحماية البيانات الشخصية، إلا أنها تختلف عنها من حيث تركيزها على التأصيل النظري العام للخصوصية في الأنظمة الغربية، بينما تهدف دراستنا إلى تحليل الإطار القانوني الجزائري مع ربطه بالتطورات الرقمية الحديثة.

وفي السياق العربي، تناولت الباحثة مروة زين العابدين صالح في دراستها الموسومة بـ الحماية القانونية للبيانات الشخصية عبر الإنترنت، وهي أطروحة دكتوراه، موضوع الحماية القانونية للبيانات في البيئة الرقمية، مع التركيز على الجوانب الدولية والتنظيمية المرتبطة بالإنترنت، وتتقاطع هذه الدراسة مع موضوع بحثنا من حيث الاهتمام بحماية البيانات في المجال الرقمي، إلا أنها تختلف عنها في كونها اعتمدت مقارنة دولية عامة، بينما تركز دراستنا على القانون الجزائري ومستجداته الحديثة.

ومن خلال استعراض هذه الدراسات، يتضح أنها رغم أهميتها العلمية، إلا أنها ركزت في معظمها على القانون رقم 07-18 أو على جوانب جزئية من الموضوع، دون التوسع في تحليل الإشكالات المستحدثة التي أفرزها التطور التكنولوجي، خاصة ما يتعلق بالذكاء الاصطناعي، والقرارات الآلية، والحقوق الرقمية الجديدة، وهو ما تسعى هذه الدراسة إلى معالجته من خلال مقارنة قانونية حديثة تجمع بين التحليل الموضوعي والبعد التطبيقي

غير أن دراسة هذا الموضوع لا تخلو من صعوبات، من أبرزها حداثة النصوص القانونية المتعلقة بحماية البيانات الشخصية، مما يؤدي إلى محدودية الاجتهاد القضائي في هذا المجال. المراجع العربية المتخصصة التي تتناول الموضوع بشكل معمق في ضوء التطورات الحديثة. وانطلاقاً مما سبق، تبرز الإشكالية الرئيسية للدراسة في التساؤل حول مدى فعالية النظام القانوني الذي أقره المشرع الجزائري في توفير حماية حقيقية للبيانات الشخصية في ظل التحولات الرقمية المتسارعة.

ويمكن صياغة الإشكالية الرئيسية على النحو الآتي:

الى أي مدى حقق القانون 11-25 حماية فعالة للبيانات الشخصية في الجزائر؟

وتتفرع هذه الاشكالية الى تساؤلات فرعية متمثلة فيما يلي :

- كيف عالج القانون 11-25 نطاق المعالجة المشروعة للمعطيات الشخصية مع اهم

الحقوق المستحدثة التي كرسها؟

- هل تكفي الضمانات المؤسسية والجزائية التي اقرها القانون 11-25 لتحقيق حماية

فعالة للمعطيات الشخصية في ظل التحديات الرقمية الراهنة ؟

- لماذا تعد حماية البيانات الشخصية من اهم التحديات القانونية الرقمية وبما ترتبط

فعالية الحماية ؟

وللإجابة عن هذه الإشكالية، تم اعتماد المنهج الوصفي من خلال عرض المفاهيم

الأساسية المتعلقة بالبيانات الشخصية، والمنهج التحليلي من خلال تحليل النصوص القانونية

المنظمة لها، إضافة إلى المنهج المقارن من خلال الاستئناس ببعض التشريعات المقارنة، خاصة

الأوروبية، لاستخلاص أوجه القوة والقصور في التشريع الجزائري.

وتأسيساً على ذلك، تم اعتماد خطة بحث تقوم على تقسيم الدراسة إلى فصلين رئيسيين،

وذلك قصد الإحاطة بمختلف الجوانب القانونية المرتبطة بحماية البيانات الشخصية في ظل

التطورات الرقمية الحديثة.

حيث خُصص الفصل الأول لدراسة النظام الموضوعي لحماية نطاق معالجة الحقوق المستحدثة من خلال بيان مفهوم القانوني للمعطيات الشخصية، مع ضوابط مشروعيتها، إضافة إلى تحديد المركز القانوني لأطراف المعالجة البيانات ، وكذا الالتزامات المتدخلين في معالجة البيانات .

أما الفصل الثاني، فقد خُصص لدراسة الضمانات المؤسسية الجزائية ، وذلك من خلال التطرق إلى الآليات الرقابية الداخلية والخارجية، وبيان دور المسؤولية القانونية للمشرع الجزائي ، إلى جانب دراسة الحماية الجزائية لقانون 11-25 المعدل والمتمم متمثلة في المسائلة المترتبة عن مخالفة الأحكام القانونية المنظمة لحماية البيانات الشخصية، خاصة في ظل تنامي المخاطر المرتبطة بالمعالجة الرقمية والذكاء الاصطناعي.

وقد تم تقسيم كل فصل إلى مبحثين، كما تم توزيع كل مبحث إلى مطلبين، مع تفريع المطالب إلى فروع، بما يضمن التدرج المنطقي للأفكار وتحقيق التوازن المنهجي في معالجة مختلف عناصر الموضوع.

الفصل الأول:

النظام الموضوعي لحماية نطاق المعالجة الحقوق المستحدثة

تمهيد

أدى التطور المتسارع في تكنولوجيات الإعلام والاتصال إلى بروز واقع رقمي أصبحت فيه البيانات الشخصية محورًا أساسيًا في مختلف المعاملات، مما جعل حمايتها ضرورة قانونية ملحة، فلم تعد المخاطر المرتبطة بها تقتصر على الاعتداءات التقليدية، بل امتدت إلى ممارسات أكثر تعقيدًا كالمعالجة الآلية والتنميط الخوارزمي، وهو ما قد يمس مباشرة بحقوق الأفراد وحياتهم، خاصة الحق في الخصوصية.

وفي مواجهة هذه التحديات، برزت الحاجة إلى إرساء نظام قانوني موضوعي يحدد نطاق البيانات المشمولة بالحماية، ويضبط شروط مشروعيتها مع تكريس حقوق رقمية جديدة لفائدة الأفراد، كحق النفاذ والمحو والاعتراض، كما تقتضي فعالية هذا النظام تحديد المركز القانوني لمختلف أطراف المعالجة، بما يضمن توزيعًا متوازنًا للحقوق والالتزامات.

وعليه، سيتم تناول هذا الفصل من خلال دراسة النطاق المفاهيمي للمعطيات وضوابط مشروعيتها معالجتها، ثم بيان المركز القانوني لأطراف المعالجة، وذلك للوقوف على مدى فعالية الحماية القانونية المقررة في ظل البيئة الرقمية الحديثة

المبحث الأول: المفهوم القانوني للمعطيات الشخصية مع ضوابط مشروعيتها

تُعد دراسة النطاق المفاهيمي للمعطيات الشخصية وضوابط مشروعية معالجتها أساساً لفهم النظام القانوني لحمايتها، إذ لا يمكن إرساء حماية فعالة دون تحديد دقيق لمفهوم البيانات المشمولة بالحماية، وكذا القواعد التي تحكم معالجتها، وعليه، يقتضي هذا المبحث التطرق أولاً إلى تصنيف المعطيات المحمية في ظل تعديل القانون 11-25، ثم بيان القواعد النازمة لمشروعية المعالجة البيانات وبناءً على ذلك، سيتم تقسيم هذا المبحث إلى مطلبين: يتناول الأول تصنيف المعطيات المشمولة بالحماية، بينما يخصص الثاني لدراسة القواعد النازمة لمشروعية المعالجة.

المطلب الأول: تصنيف المعطيات المحمية في ظل تعديل القانون 11-25

تُعد مسألة تحديد نطاق المعطيات الشخصية المشمولة بالحماية من المسائل الجوهرية في مجال حماية البيانات، إذ تمثل الخطوة الأولى نحو إرساء حماية قانونية فعالة. فكلما كان مفهوم المعطيات الشخصية واضحاً ودقيقاً، أمكن ضبط مجال تطبيق القانون وتحديد الحالات التي تستوجب الحماية، وقد اتجهت التشريعات الحديثة، ومنها التشريع الجزائري، إلى تبني مفهوم واسع للبيانات الشخصية، لا يقتصر على المعطيات المباشرة، بل يشمل أيضاً المعطيات التي يمكن من خلالها التعرف على الشخص بصفة غير مباشرة¹.

وفي ظل التطورات الرقمية المتسارعة، لم يعد التصنيف التقليدي للمعطيات كافياً، مما دفع المشرع إلى توسيع نطاق الحماية ليشمل فئات جديدة من البيانات التي تكتسي طابعاً خاصاً نظراً لحساسيتها أو لارتباطها بفئات تحتاج إلى حماية إضافية. وعليه، أصبح من الضروري التمييز بين المعطيات الشخصية التقليدية، والمعطيات ذات الطبيعة الخاصة، فضلاً

¹ بوعزيز خليفة، حماية المعطيات الشخصية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2021، ص 15.

عن المعطيات المتعلقة بالفئات المستضعفة، لما يترتب عن ذلك من اختلاف في مستوى الحماية القانونية المقررة لكل منها.

وبناءً على ذلك، سيتم تناول هذا المطلب من خلال ثلاثة فروع، حيث يُخصص الفرع الأول لدراسة المعطيات الشخصية التقليدية، بينما يتناول الفرع الثاني المعطيات ذات الطبيعة الخاصة، في حين يُعنى الفرع الثالث بالمعطيات المتعلقة بالأطفال مع الفئات المستضعفة.

الفرع الأول: المعطيات الشخصية التقليدية

تُعد المعطيات الشخصية التقليدية الأساس الذي تقوم عليه منظومة الحماية القانونية للبيانات، إذ تمثل النطاق الأولي الذي ينصرف إليه تطبيق القواعد القانونية المنظمة لمعالجة البيانات. ويقصد بها تلك المعطيات التي ترتبط بالشخص الطبيعي بشكل مباشر أو غير مباشر، بما يسمح بتحديد هويته أو التعرف عليه، سواء تعلق الأمر ببيانات بسيطة أو مركبة.

وقد اختلف الفقه في تعريف المعطيات الشخصية، حيث ذهب اتجاه إلى تعريفها بأنها كل معلومة تتعلق بشخص معين، مثل الاسم واللقب والعنوان ورقم الهاتف والبريد الإلكتروني، وهي بيانات تمكن من التعرف المباشر على الشخص¹، في حين اتجه رأي آخر إلى توسيع هذا المفهوم، معتبراً أن المعطيات الشخصية لا تقتصر على البيانات المباشرة، بل تشمل كذلك كل المعلومات التي يمكن أن تؤدي، بطريقة غير مباشرة، إلى تحديد هوية الشخص، كالمعرفات الرقمية أو البيانات المرتبطة بسلوكه أو نشاطه²، ويُعد هذا الاتجاه الأخير أكثر انسجاماً مع طبيعة البيئة الرقمية، التي أصبح فيها التعرف على الأشخاص يتم عبر وسائل تقنية معقدة.

أما على المستوى التشريعي، فقد تبنى المشرع الجزائري مفهوماً واسعاً للمعطيات الشخصية، وهو ما أكدته المادة 03 من القانون رقم 18-07، التي عرفت المعطيات الشخصية

¹ أحيممة علالي، الحماية الجنائية للمعطيات الشخصية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2019، ص 09.

² بوعزيز خليفة، مرجع سابق، ص 16.

بأنها كل معلومة تتعلق بشخص طبيعي معرف أو قابل للتعريف، بصورة مباشرة أو غير مباشرة،¹ حيث اعتبرها كل معلومة، مهما كان شكلها أو طبيعتها، تتعلق بشخص طبيعي معرف أو قابل للتعريف، بشكل مباشر أو غير مباشر، وهو ما يعكس إرادة واضحة في توسيع نطاق الحماية القانونية، كما يتماشى هذا التعريف مع ما استقر عليه التشريع المقارن، خاصة الأوروبي، الذي يعتمد معيار إمكانية التعريف كعنصر أساسي في تحديد مفهوم البيانات الشخصية، ويشمل هذا النوع من المعطيات مجموعة واسعة من البيانات، من بينها: الاسم، اللقب، تاريخ ومكان الميلاد، العنوان، رقم الهاتف، البريد الإلكتروني، الحالة العائلية، الوضع المهني، وغيرها من المعلومات التي تشكل هوية الشخص أو جزءاً منها. ولا يقتصر الأمر على البيانات الثابتة، بل يمتد ليشمل البيانات المتغيرة المرتبطة بسلوك الشخص في البيئة الرقمية. مما يوسع من نطاق الحماية ويجعلها أكثر شمولاً، غير أن التمييز بين المعطيات الشخصية التقليدية وغيرها من المعطيات يثير إشكالاً عملياً، خاصة في ظل التداخل بين البيانات العادية والبيانات الحساسة، إذ قد تتحول بعض المعطيات البسيطة، عند تجميعها أو تحليلها، إلى معلومات ذات طابع حساس تمس الحياة الخاصة للفرد. وهو ما يفرض ضرورة اعتماد معيار مرن في التمييز، يأخذ بعين الاعتبار طبيعة البيانات وسياق استخدامها، وليس فقط شكلها الظاهري.²

وعليه، فإن المعطيات الشخصية التقليدية، رغم بساطتها الظاهرة، تظل ذات أهمية بالغة في مجال الحماية القانونية، باعتبارها المدخل الأساسي لفهم باقي أنواع المعطيات، كما تشكل الأساس الذي تُبنى عليه بقية الضوابط القانونية المتعلقة بمعالجة البيانات الشخصية.

الفرع الثاني: المعطيات ذات الطبيعة الخاصة

¹ المادة 03 من القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ج ج ، العدد 34، الصادرة بتاريخ 10 يونيو 2018.

² حسن عبد الباسط جميعي، حماية الخصوصية في مواجهة نظم المعلومات الحديثة، دار الفكر الجامعي، الإسكندرية، مصر، 2020، ص 56.

تتميز بعض المعطيات الشخصية بطابع خاص يضيف عليها درجة عالية من الحساسية، نظراً لارتباطها المباشر بالجوانب الأكثر خصوصية في حياة الإنسان، وهو ما يجعل معالجتها أو الكشف عنها دون ضوابط صارمة من شأنه أن يمس بكرامة الفرد وحقوقه الأساسية، ولهذا، اتجهت التشريعات الحديثة إلى إفراد هذا النوع من البيانات بحماية قانونية مشددة تختلف عن تلك المقررة للمعطيات الشخصية التقليدية.

ويقصد بالمعطيات ذات الطبيعة الخاصة تلك البيانات التي تكشف عن معلومات دقيقة تتعلق بالشخص، مثل أصله العرقي أو الإثني، وآرائه السياسية، ومعتقداته الدينية أو الفلسفية، وانتمائه النقابي، فضلاً عن البيانات المتعلقة بصحته أو حياته الخاصة، كما تدرج ضمنها المعطيات البيومترية التي تقوم على الخصائص الفيزيولوجية أو السلوكية للفرد، كالبصمة والتعرف على الوجه والصوت، إضافة إلى المعطيات الجينية المرتبطة بالبنية الوراثية، والتي تتيح التعرف الدقيق على الشخص بصورة شبه قطعية¹، وقد تبني المشرع الجزائري هذا التوجه، حيث أخضع هذه الفئة من المعطيات لنظام قانوني صارم يقوم في الأصل على مبدأ الحظر، مع السماح بمعالجتها في حالات استثنائية محددة، كالحصول على موافقة صريحة من الشخص المعني أو وجود مبرر قانوني أو مصلحة عامة تقتضي ذلك ويعكس هذا التنظيم وعياً بخطورة هذه البيانات، خاصة لما قد يترتب عن إساءة استخدامها من ممارسات تمييزية أو انتهاك للحياة الخاصة ويستفاد من المادة 07 من القانون رقم 07-18 أن المشرع اعتمد مبدأ الحظر كأصل عام في معالجة البيانات الحساسة، مع السماح بها استثناءً عند وجود موافقة صريحة أو مبرر قانوني مشروع.²

وفي الإطار المقارن، كرّس التشريع الأوروبي بدوره حماية معززة لهذه المعطيات، حيث وضع شروطاً دقيقة لمعالجتها، من بينها ضرورة تحديد الغرض بشكل واضح، واعتماد تدابير

¹بوعزيز خليفة، مرجع سابق، ص 18.

²المادة 07 من القانون رقم 07-18، مصدر سابق.

أمنية مشددة، وإجراء تقييم مسبق للأثر الذي قد تخلفه المعالجة على حقوق الأفراد¹، وقد توسع هذا الاتجاه ليشمل بشكل صريح المعطيات البيومترية والجينية، نظرًا لما تتيحه من إمكانيات متقدمة في التعرف على الأشخاص، غير أن التطور التكنولوجي، خاصة في مجال الذكاء الاصطناعي، أفرز إشكالات جديدة تتعلق باستخدام هذه البيانات في أنظمة التعرف الآلي والتحليل الخوارزمي، مما يثير تساؤلات حول مدى مشروعية هذه الاستخدامات وحدودها القانونية. كما أن خصوصية هذه المعطيات تكمن في صعوبة تغييرها أو إخفائها، الأمر الذي يزيد من خطورة تسريبها أو استغلالها بشكل غير مشروع، ويستدعي بالتالي تعزيز الضمانات القانونية والتقنية لحمايتها.

وعليه، فإن المعطيات ذات الطبيعة الخاصة تمثل فئة متميزة تستوجب حماية قانونية مضاعفة، تقوم على تقييد معالجتها وإخضاعها لضوابط دقيقة، بما يحقق التوازن بين متطلبات الاستعمال المشروع لهذه البيانات وضمان احترام الحقوق والحريات الأساسية للأفراد.

الفرع الثالث: المعطيات المتعلقة بالأطفال مع الفئات المستضعفة

تكتسي المعطيات الشخصية المتعلقة بالأطفال والفئات المستضعفة أهمية خاصة في مجال الحماية القانونية، نظرًا لخصوصية هذه الفئات وضعف قدرتها على تقدير المخاطر المرتبطة بمعالجة بياناتها أو الدفاع عن حقوقها في مواجهة الانتهاكات المحتملة، ومن ثم، فقد اتجهت التشريعات الحديثة إلى إقرار حماية معززة لهذه الفئة من المعطيات، تقوم على تشديد الضوابط القانونية وتقييد نطاق معالجتها.

ويقصد بالفئات المستضعفة، بالإضافة إلى الأطفال، كل الأشخاص الذين قد يكونون في وضعية هشاشة تجعلهم أكثر عرضة للاستغلال، كذوي الاحتياجات الخاصة، أو المرضى، أو الأشخاص الذين يعانون من ضعف في الإدراك أو التمييز، أما بالنسبة للأطفال، فإن

¹ Paul Voigt & Axel vondenBussche 'The EU General Data Protection Regulation (GDPR): A Practical Guide ' Springer ,Cham ,2023 ,p45

خصوصية وضعهم القانوني والاجتماعي تفرض ضرورة توفير حماية خاصة لمعطياتهم، بالنظر إلى عدم اكتمال أهليتهم القانونية، وقابليتهم للتأثر بمختلف الممارسات الرقمية،

وفي هذا السياق، أقر المشرع الجزائري جملة من الضوابط التي تهدف إلى حماية هذه الفئة، من خلال اشتراط الحصول على موافقة الولي أو الممثل القانوني في حالات معينة، خاصة عندما يتعلق الأمر بمعالجة بيانات الأطفال، إضافة إلى ضرورة مراعاة مصالحهم الفضلى عند اتخاذ أي إجراء يتعلق بمعطياتهم الشخصية¹. كما يفهم من الإطار العام للقانون أن حماية هذه الفئة لا تقتصر على الجانب الشكلي للموافقة، بل تمتد إلى فرض التزامات إضافية على المسؤولين عن المعالجة، لضمان عدم استغلال هذه البيانات بطريقة تضر بالأشخاص المعنيين.

وعلى المستوى المقارن، أولى التشريع الأوروبي أهمية بالغة لحماية بيانات الأطفال، حيث شدد على ضرورة توفير شروط خاصة لمعالجة بياناتهم، من بينها وضوح المعلومات المقدمة لهم، واعتماد لغة مبسطة تمكنهم من فهم طبيعة المعالجة، فضلاً عن تعزيز آليات الرقابة على الأنشطة الرقمية التي تستهدفهم²، ويعكس هذا التوجه إدراكاً لخطورة البيئة الرقمية على هذه الفئة، خاصة في ظل انتشار التطبيقات والمنصات التي تعتمد على جمع البيانات وتحليلها.

غير أن الإشكال الذي يطرح في هذا المجال يتمثل في صعوبة التوفيق بين متطلبات الاستفادة من الخدمات الرقمية، التي أصبحت ضرورية في الحياة اليومية، وبين ضرورة حماية هذه الفئات من المخاطر المرتبطة باستغلال بياناتها، كما أن غموض بعض النصوص القانونية أو عموميتها قد يحد من فعالية الحماية، خاصة في ظل غياب آليات تطبيق واضحة أو رقابة كافية على الممارسات الرقمية.

¹ المواد رقم 06,09,34، من القانون رقم 18-07، مصدر سابق.

² Paul Voigt & Axel vondenBussche, Op.cit., p. 52.

وعليه، فإن المعطيات المتعلقة بالأطفال والفئات المستضعفة تستوجب حماية قانونية خاصة تتجاوز القواعد العامة، وتستند إلى مقاربة وقائية قائمة على تشديد الضوابط، وتعزيز الرقابة، وضمان مراعاة المصلحة الفضلى لهذه الفئات، بما يحقق حماية فعالة لحقوقها في البيئة الرقمية.

المطلب الثاني: القواعد النازمة لمشروعية المعالجة البيانات

تُعد مشروعية معالجة البيانات الشخصية الركيزة الأساسية التي يقوم عليها نظام الحماية القانونية، إذ لا يكفي مجرد الاعتراف بحقوق الأفراد على بياناتهم، بل يتعين تأطير عمليات جمعها واستعمالها وفق ضوابط قانونية دقيقة تضمن عدم التعسف في استخدامها، وقد أدرك المشرع، في ظل التحولات الرقمية المتسارعة، أن المعالجة غير المقيدة للبيانات قد تؤدي إلى انتهاكات جسيمة للحقوق والحريات، مما استدعى وضع مجموعة من المبادئ والقواعد التي تحكم هذه العمليات وتحدد شروط صحتها.

وتقوم مشروعية المعالجة على جملة من الأسس، في مقدمتها ضرورة وجود سند قانوني يبرر عملية المعالجة، سواء تمثل ذلك في موافقة الشخص المعني، أو وجود التزام قانوني، أو تحقيق مصلحة مشروعة لا تتعارض مع حقوق الأفراد، كما تقتضي هذه المشروعية احترام مجموعة من المبادئ الأساسية، مثل مبدأ الشفافية¹.

وايضاً تحديد الغرض من المعالجة، والاقتصار على البيانات الضرورية فقط، إضافة إلى ضمان أمن وسرية البيانات أثناء معالجتها وتخزينها².

وقد تبني المشرع الجزائري هذه المبادئ، حيث وضع إطاراً قانونياً يحدد الشروط الواجب توافرها لاعتبار المعالجة مشروعة، مع إلزام المسؤولين عن المعالجة باحترام هذه الضوابط تحت

¹ حسن عبد الباسط جميعي، مرجع سابق، ص 59.

² حميمة علالي، مصدر سابق، ص 18.

طائلة المسؤولية القانونية¹، ويلاحظ أن هذا التنظيم يهدف إلى تحقيق توازن دقيق بين متطلبات استغلال البيانات في مختلف المجالات، خاصة الاقتصادية والتكنولوجية، وبين ضرورة حماية الأفراد من المخاطر المرتبطة بها حيث قام المشرع الجزائري بوضع آليات ردع من أجل حماية البيانات الشخصية لحماية الفرد وتمثلة في النص القانوني رقم 09-04 الذي تضمن القواعد الخاصة للوقاية من الجرائم التي تتصل بتكنولوجيا الاعلام والاتصال ومكافحتها².

غير أن التطور التكنولوجي، خاصة في مجال المعالجة الآلية والذكاء الاصطناعي، أفرز تحديات جديدة تتعلق بمدى كفاية هذه القواعد التقليدية، حيث أصبحت بعض عمليات المعالجة تتم بشكل معقد وغير شفاف، مما يصعب على الأفراد إدراك طبيعتها أو التحكم فيها وهو ما يفرض تعزيز هذه الضوابط من خلال إقرار آليات إضافية، تضمن مزيداً من الشفافية والمساءلة..

وعليه، فإن دراسة القواعد النازمة لمشروعية المعالجة تقتضي التطرق إلى مبدأ الرضائية كأساس أولي للمعالجة، ثم تحليل المبادئ العامة التي تحكمها، وأخيراً بيان الضوابط الأمنية والتقنية الكفيلة بضمان حماية البيانات أثناء معالجتها.

وبناءً على ذلك، سيتم تقسيم هذا المطلب إلى ثلاثة فروع: يُخصص الأول لدراسة مبدأ الرضائية، بينما يتناول الثاني المبادئ الأساسية للمعالجة، في حين يُعنى الثالث بالضوابط الأمنية والتقنية.

الفرع الأول: مبدأ الرضائية

يُعد مبدأ الرضائية حجر الأساس في مشروعية معالجة البيانات الشخصية، باعتباره يُجسد إرادة الشخص المعني في التحكم في بياناته، ويعكس انتقال الحماية القانونية من مجرد

¹ المواد 04، 06، 34 من القانون رقم 18-07، مصدر سابق..

² القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل 05 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال.

منع الاعتداء إلى تمكين الفرد من سلطة تقريرية فعلية على معطياته، فالأصل أن أي معالجة للبيانات الشخصية تظل غير مشروعة ما لم تستند إلى موافقة صادرة عن صاحبها أو إلى أساس قانوني بديل يبررها.

و تُعرّف الموافقة في الفقه الحديث بأنها تعبير حر ومحدد ومستدير عن إرادة الشخص المعني، يقبل بموجبه معالجة بياناته لغرض معين، ويستفاد من هذا التعريف أن الموافقة لا تُعتبر صحيحة إلا إذا استوفت مجموعة من الشروط الجوهرية، في مقدمتها أن تكون حرة، أي صادرة دون ضغط أو إكراه، وألا تكون نتيجة عدم توازن واضح بين الأطراف، كما هو الحال في العلاقة بين المستخدم والمنصات الرقمية الكبرى¹.

كما يشترط أن تكون محددة، بحيث ترتبط بغرض واضح ومشروع، فلا يجوز تعميم الموافقة أو استعمالها لغايات غير محددة سلفاً.

ويقتضي كذلك أن تكون الموافقة مستتيرة، أي مبنية على إعلام مسبق وكاف يتيح للشخص المعني فهم طبيعة المعالجة وحدودها، بما في ذلك هوية المسؤول عن المعالجة، وأهدافها، ومدة الاحتفاظ بالبيانات، والحقوق المرتبطة بها، ويترتب على ذلك التزام قانوني على عاتق المسؤول عن المعالجة بتقديم معلومات واضحة ومفهومة، خاصة في البيئة الرقمية التي تتسم بتعقيد شروط الاستخدام².

أما من حيث الشكل، فقد تكون الموافقة صريحة، وذلك من خلال تعبير واضح لا لبس فيه، خاصة في حالة معالجة البيانات الحساسة، أو ضمنية تُستفاد من سلوك الشخص المعني، غير أن هذا النوع الأخير يثير إشكالات عملية، إذ قد لا يعكس إرادة حقيقية، خاصة في ظل

¹ حسن عبد الباسط جمعي، مرجع سابق، ص 79.

² European Data Protection Board (EDPB), 'Guidelines on Consent under GDPR', 2023, p08

ما يُعرف بـ"الإجبار التعاقدى الرقمي"، حيث يُضطر المستخدم إلى القبول بشروط معقدة للاستفادة من الخدمة¹.

وقد كرس المشرع الجزائري هذا المبدأ من خلال اشتراط الموافقة المسبقة كقاعدة عامة لمعالجة البيانات الشخصية، مع إقرار حق الشخص المعني في سحب موافقته في أي وقت، وهو ما يعزز من سيطرته المستمرة على بياناته، غير أن فعالية هذا المبدأ تظل مرتبطة بمدى احترام شروطه الموضوعية والشكلية، ومدى قدرة الأفراد على فهم تبعات موافقتهم في بيئة رقمية معقدة².

وفي السياق المقارن، شددت التشريعات الحديثة، خاصة الأوروبية، على ضرورة أن تكون الموافقة قابلة للإثبات، وأن تُعبر عن إرادة حقيقية، وهو ما أدى إلى التشكيك في فعالية الموافقة التقليدية، والدعوة إلى تجاوزها نحو آليات أكثر حماية، كتعزيز مبدأ "الخصوصية عبر التصميم" والحد من الاعتماد المطلق على رضا المستخدم³.

وعليه، فإن مبدأ الرضائية، رغم أهميته، لم يعد كافياً بمفرده لضمان مشروعية المعالجة، بل يتعين دعمه بضمانات أخرى تكفل تحقيق حماية فعلية للبيانات الشخصية في ظل التطورات الرقمية المتسارعة.

الفرع الثاني: المبادئ الأساسية للمعالجة

تقوم مشروعية معالجة البيانات الشخصية، إلى جانب مبدأ الرضائية، على مجموعة من المبادئ الأساسية التي تشكل الإطار العام المنظم لهذه المعالجة، وفي مقدمتها مبدأ الشفافية،

¹ حسن عبد الباسط جميعي، مرجع سابق، ص 84.

² المواد 34'06,04 من القانون رقم 07-18، مصدر سابق.

³ مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2021، ص 94.

ومبدأ تحديد الغاية، ومبدأ تقليل البيانات، وتُعد هذه المبادئ ضمانات جوهرية تهدف إلى الحد من التعسف في استعمال البيانات، وتعزيز ثقة الأفراد في البيئة الرقمية.

يُقصد بمبدأ الشفافية ضرورة أن تتم معالجة البيانات الشخصية بطريقة واضحة ومفهومة بالنسبة للشخص المعني، بحيث يتم إعلامه بكيفية جمع بياناته، والأغراض التي سَتُستعمل من أجلها، والجهات التي يمكن أن تُنقل إليها، ويُعد هذا المبدأ تجسيداً لحق الفرد في المعرفة، ويشكل شرطاً أساسياً لممارسة باقي الحقوق المرتبطة بالبيانات، غير أن التطبيق العملي لهذا المبدأ يواجه صعوبات، خاصة في ظل تعقيد سياسات الخصوصية وطولها، مما يجعلها في كثير من الأحيان غير مقروءة أو غير مفهومة بالنسبة للمستخدم العادي¹.

أما مبدأ تحديد الغاية، فيقضي بضرورة جمع البيانات ومعالجتها لأغراض محددة ومشروعة ومعلنة مسبقاً، بحيث لا يجوز استخدامها لاحقاً في أغراض أخرى غير متوافقة مع تلك التي جُمعت من أجلها، ويهدف هذا المبدأ إلى منع التوسع غير المشروع في استعمال البيانات، خاصة في ظل الممارسات الرقمية التي تعتمد على إعادة توظيف البيانات لأغراض تجارية أو تحليلية دون علم أصحابها²، ويكتسي هذا المبدأ أهمية خاصة في سياق الذكاء الاصطناعي، حيث يتم استخدام البيانات لأغراض متعددة قد تتجاوز الغاية الأصلي.

في حين يقوم مبدأ تقليل البيانات على ضرورة الاقتصار في جمع ومعالجة البيانات على الحد الأدنى اللازم لتحقيق الغرض المحدد، بحيث لا يتم جمع بيانات زائدة أو غير ضرورية، ويُعد هذا المبدأ من أهم الآليات الوقائية التي تحد من مخاطر انتهاك الخصوصية، إذ كلما قلَّ حجم البيانات المعالجة، تقلَّ احتمالات إساءة استخدامها أو تسريبها³.

¹ European Data Protection Board (EDPB), Op.cit., p.06

² Christopher Kuner, 'Transborder Data Flows and Data Privacy Law', Oxford University Press, 2023, p134.

³ مروة زين العابدين صالح، مرجع سابق، ص 101.

وقد تبنى المشرع الجزائري هذه المبادئ ضمن الإطار القانوني المنظم لحماية البيانات الشخصية، حيث ألزم المسؤولين عن المعالجة بضرورة احترامها تحت طائلة المسؤولية القانونية، بما يعكس سعيه إلى تحقيق توازن بين متطلبات استغلال البيانات وضمان حماية حقوق الأفراد وحرياتهم، كما تتوافق هذه المبادئ مع ما استقر عليه التشريع المقارن، خاصة التشريع الأوروبي، الذي اعتبرها من الأسس الجوهرية التي تقوم عليها مشروعية معالجة البيانات الشخصية.

غير أن التحدي الحقيقي لا يكمن في إقرار هذه المبادئ، بل في مدى فعاليتها في التطبيق، خاصة في ظل التطور التكنولوجي المتسارع، حيث أصبحت بعض تقنيات المعالجة، كالخوارزميات الذكية، تعمل بطريقة معقدة وغير شفافة، مما يصعب مراقبتها أو التحقق من احترامها لهذه المبادئ، وهو ما يستدعي تعزيز الرقابة القانونية والتقنية، وتطوير آليات جديدة تضمن احترام هذه المبادئ في الواقع العملي.

وعليه، فإن مبادئ الشفافية وتحديد الغاية وتقليل البيانات تشكل حجر الزاوية في ضمان مشروعية معالجة البيانات الشخصية، غير أن فعاليتها تظل رهينة بمدى تطبيقها الفعلي في البيئة الرقمية.

الفرع الثالث: الضوابط الأمنية التقنية

تُعد الضوابط الأمنية التقنية أحد أهم الركائز التي يقوم عليها نظام حماية البيانات الشخصية، إذ لا تقتصر الحماية على الجوانب القانونية الشكلية، بل تمتد لتشمل ضمان أمن البيانات أثناء جمعها ومعالجتها وتخزينها، فالتطور التكنولوجي، رغم ما يوفره من مزايا، أفرز في المقابل مخاطر متزايدة، كالهجمات السيبرانية، وتسريب البيانات، والوصول غير المشروع

إلى الأنظمة المعلوماتية، وهو ما يجعل تأمين البيانات ضرورة حتمية لضمان فعاليتها القانونية¹.

ويقصد بالضوابط الأمنية التقنية مجموعة التدابير والإجراءات التي يتعين على المسؤول عن المعالجة اتخاذها لحماية البيانات الشخصية من الضياع أو التغيير أو الإفشاء غير المشروع، وتشمل هذه التدابير، على وجه الخصوص، تقنيات التشفير، وأنظمة الحماية المعلوماتية، وآليات التحكم في الوصول، إضافة إلى اعتماد بروتوكولات أمنية تضمن سلامة البيانات وسريتها، كما تمتد هذه الضوابط إلى مرحلة تخزين البيانات، حيث يجب تأمينها ضد المخاطر التقنية والاختراقات المحتملة².

وقد ألزم المشرع الجزائري المسؤولين عن المعالجة باتخاذ التدابير اللازمة لضمان أمن البيانات، بما يتناسب مع طبيعتها ومستوى حساسيتها، وهو ما يعكس تبني مقاربة وقائية تهدف إلى الحد من المخاطر قبل وقوعها³، ويستفاد من ذلك أن مستوى الحماية المطلوب ليس موحدًا، بل يختلف بحسب نوع البيانات، حيث تستوجب المعطيات الحساسة مستوى أعلى من الحماية مقارنة بالبيانات العادية.

وفي السياق المقارن، شهدت التشريعات الحديثة تطورًا ملحوظًا في هذا المجال، حيث تم إدماج مفاهيم جديدة مثل "الأمن حسب التصميم" و"الأمن الافتراضي"، التي تقوم على إدراج متطلبات الحماية منذ المراحل الأولى لتصميم الأنظمة المعلوماتية، بدل الاكتفاء بمعالجتها لاحقًا⁴، كما تم تعزيز الالتزامات المفروضة على المسؤولين عن المعالجة، من خلال إلزامهم بالإبلاغ عن خروقات البيانات، واتخاذ إجراءات فورية للحد من آثارها.

¹ عبد القادر بوعلام، "حماية البيانات الشخصية في ظل التطور التكنولوجي"، مجلة العلوم القانونية، 2023، ص 67.

² نفس مرجع سابق، ص 68.

³ المواد 04، 06، 34. من القانون رقم 18-07، مصدر سابق..

⁴ Alessandro Mantelero, "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment", Computer Law & Security Review, Vol. 34, Issue 4, 2018, p. 30.

غير أن الإشكال المطروح لا يتعلق فقط بوجود هذه الضوابط، بل بمدى فعاليتها في الواقع العملي، خاصة في ظل التطور المستمر لأساليب الاختراق والهجمات الإلكترونية، كما أن ضعف الوعي الأمني لدى بعض الفاعلين، وعدم تحديث الأنظمة المعلوماتية بشكل دوري، قد يؤدي إلى تقويض هذه الحماية، رغم وجود إطار قانوني منظم لها.

ويلاحظ أن المشرع الجزائري حاول مواكبة التطورات الرقمية الحديثة من خلال القانون رقم 11-25 المعدل والمتمم للقانون 07-18، خاصة فيما يتعلق بتعزيز آليات الرقابة على المعالجة الرقمية للبيانات الشخصية.¹

وعليه، فإن الضوابط الأمنية التقنية تمثل عنصراً أساسياً في تحقيق الحماية الفعلية للبيانات الشخصية، غير أن فعاليتها تظل رهينة بمدى التزام المسؤولين عن المعالجة بتطبيقها، وتطويرها بما يتماشى مع التحديات التكنولوجية المتجددة.

¹ المادة 41 مكرر من القانون رقم 11-25 المؤرخ في 24 يوليو 2025، المعدل والمتمم للقانون رقم 07-18 ج ر ج ج، العدد 48، الصادرة بتاريخ 29 يوليو 2025.

المبحث الثاني: المركز القانوني لأطراف المعالجة البيانات

لا تكتمل الحماية القانونية للبيانات الشخصية بمجرد تحديد نطاقها وضوابط معالجتها، بل تقتضي أيضاً تحديد المركز القانوني لمختلف الأطراف المتدخلة في عملية المعالجة، لما لذلك من أثر مباشر في توزيع الحقوق والالتزامات وضمان احترام القواعد القانونية المنظمة لها، فمع تعدد الفاعلين في البيئة الرقمية، لم يعد الأمر يقتصر على العلاقة الثنائية بين الشخص المعني والجهة المعالجة، بل أصبح يشمل أطرافاً متعددة تتداخل أدوارها ومسؤولياتها.

وعليه، فإن دراسة المركز القانوني لأطراف المعالجة تقتضي التطرق، في مطلب أول، إلى الحقوق الرقمية للشخص المعني، ثم في مطلب ثانٍ إلى الالتزامات المفروضة على مختلف المتدخلين في عملية المعالجة، وذلك بهدف تقييم مدى تحقيق التوازن بين حماية الأفراد ومتطلبات المعالجة الرقمية.

المطلب الأول: الحقوق الرقمية للشخص المعني

يُعد الشخص المعني بالبيانات محور الحماية القانونية في نظام حماية المعطيات الشخصية، إذ كرس له المشرع مجموعة من الحقوق الرقمية التي تمكنه من التحكم في بياناته ومراقبة كيفية معالجتها، وتمثل هذه الحقوق ترجمة عملية لمبدأ سيادة الفرد على معطياته، كما تعكس انتقال الحماية من مجرد منع الاعتداء إلى تمكين إيجابي يضمن للفرد التدخل في مختلف مراحل المعالجة¹.

¹ بوعزيز خليفة، مرجع سابق، ص 28.

وتكتسي هذه الحقوق أهمية خاصة في البيئة الرقمية، حيث تتسم عمليات المعالجة بالتعقيد والسرعة، مما قد يؤدي إلى تهميش دور الشخص المعني إذا لم تُمنح له أدوات قانونية فعالة، وقد استلهم المشرع الجزائري في هذا المجال الاتجاهات الحديثة، خاصة الأوروبية، من خلال تكريس مجموعة من الحقوق التي تضمن الشفافية والتحكم والمساءلة.¹

وعليه، سيتم تناول هذه الحقوق من خلال ثلاثة فروع: يُخصص الأول للحقوق المعلوماتية، بينما يتناول الثاني حقوق التصويب والمحو، في حين يُعنى الثالث بحق الاعتراض مع عدم الخضوع للقرارات الآلية.

الفرع الأول: الحقوق المعلوماتية

تُعد الحقوق المعلوماتية من أهم الآليات التي تضمن شفافية معالجة البيانات الشخصية، إذ تمكّن الشخص المعني من معرفة كيفية التعامل مع بياناته، وتتيح له الاطلاع عليها عند الحاجة، ويأتي في مقدمة هذه الحقوق حق الإعلام، الذي يفرض على المسؤول عن المعالجة إعلام الشخص المعني بجميع المعلومات الأساسية المتعلقة بعملية المعالجة، كهوية المسؤول، وأغراض المعالجة، وطبيعة البيانات، والجهات التي يمكن أن تُنقل إليها.

ويُعتبر هذا الحق شرطاً أساسياً لممارسة باقي الحقوق، إذ لا يمكن للشخص المعني أن يدافع عن بياناته أو يعترض على معالجتها دون علم مسبق بها. غير أن التطبيق العملي لهذا الحق يواجه تحديات، خاصة في ظل تعقيد سياسات الخصوصية، التي غالباً ما تكون طويلة وغير مفهومة بالنسبة للمستخدم العادي.²

أما حق النفاذ، فيُمكّن الشخص المعني من الحصول على تأكيد بشأن ما إذا كانت بياناته تخضع للمعالجة، والاطلاع عليها، والحصول على نسخة منها، ويُعد هذا الحق تجسيداً

¹ عبد الفتاح بيومي حجازي، الحق في الخصوصية والمسؤولية المدنية في عصر الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2019، ص 102.

² European Data Protection Board (EDPB), Op.cit., p. 10.

لمبدأ الشفافية، كما يشكل وسيلة للتحقق من مدى مشروعية المعالجة وصحة البيانات المستخدمة¹.

في حين يُعتبر حق قابلية نقل البيانات من الحقوق الحديثة التي أفرزتها البيئة الرقمية، حيث يتيح للشخص المعني نقل بياناته من نظام إلى آخر بطريقة منظمة وقابلة للقراءة، مما يعزز من حريته في اختيار الخدمات الرقمية، ويحد من احتكار البيانات من قبل بعض الجهات²، وقد كرس المشرع الجزائري هذه الحقوق ضمن الإطار القانوني لحماية البيانات الشخصية، مما يعكس توجهًا نحو تمكين الأفراد من السيطرة على بياناتهم، غير أن فعالية هذه الحقوق تظل مرتبطة بمدى وضوح الإجراءات المتبعة لممارستها، وسهولة الوصول إليها.

الفرع الثاني: حقوق التصويب والمحو

تُعد حقوق التصويب والمحو من أهم الآليات التي تُمكن الشخص المعني من التدخل المباشر في البيانات المتعلقة به، بما يضمن دقتها ويحد من آثار معالجتها غير المشروعة، فهذه الحقوق لا تقتصر على مجرد الاطلاع، بل تمنح للفرد سلطة تصحيح بياناته أو حذفها متى كانت غير صحيحة أو لم يعد هناك مبرر للاحتفاظ بها.

01/ حق التصويب : و يتمثل في تمكين الشخص المعني من طلب تعديل أو تصحيح البيانات غير الدقيقة أو غير المكتملة، بما يعكس وضعه الحقيقي، ويكتسي هذا الحق أهمية خاصة في ظل الاعتماد المتزايد على البيانات في اتخاذ القرارات، إذ قد يؤدي وجود بيانات خاطئة إلى الإضرار بالمركز القانوني أو المهني للفرد³، كما يُعد هذا الحق امتدادًا لمبدأ دقة البيانات، الذي يفرض على المسؤول عن المعالجة التأكد من صحة المعلومات التي يتعامل معها.

¹Daniel J. Solove «Privacy Law Fundamentals» IAPP، 2024، p77

²Christopher Kuner, Op.cit., p. 145.

³حميمة علالي، مرجع سابق، ص 25

02/ حق المحو: أو ما يُعرف بالحق في النسيان الرقمي، فيخول للشخص المعني طلب حذف بياناته الشخصية في حالات معينة، كأن تكون المعالجة غير مشروعة، أو أن تزول الغاية التي جُمعت من أجلها البيانات، أو عند سحب الموافقة التي كانت أساس المعالجة¹. ويُعد هذا الحق من أبرز الحقوق الحديثة التي أفرزتها البيئة الرقمية، حيث أصبح من الضروري تمكين الأفراد من إزالة آثارهم الرقمية التي قد تستمر لفترات طويلة دون مبرر.

غير أن تطبيق هذا الحق يثير إشكاليات عملية، خاصة في ظل تعارضه مع بعض المصالح الأخرى، كحرية التعبير أو متطلبات الاحتفاظ بالبيانات لأغراض قانونية أو أمنية، كما أن الطابع التقني للبيئة الرقمية يجعل من عملية الحذف الكامل للبيانات أمراً معقداً، خاصة في ظل إمكانية نسخها أو تداولها عبر عدة منصات².

وقد كرس المشرع الجزائري هذه الحقوق ضمن الإطار القانوني لحماية البيانات الشخصية، حيث منح للشخص المعني إمكانية طلب تصحيح بياناته أو حذفها، وهو ما يعزز من حمايته في مواجهة المعالجة غير المشروعة، غير أن فعالية هذه الحقوق تبقى رهينة بمدى وضوح الإجراءات العملية لممارستها، وكذا بمدى التزام الجهات المعالجة بتنفيذ هذه الطلبات في آجال معقولة³..

وعليه فإن حقوق التصويب والمحو تمثل ضماناً أساسية لحماية البيانات الشخصية، غير أنها تظل بحاجة إلى تفعيل عملي وآليات رقابية فعالة لضمان تحقيق الغاية المرجوة منها.

¹بوعزيز خليفة، مرجع سابق، ص 32.

²مفيدة مباركية، "الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري"، مجلة الشريعة والاقتصاد، جامعة قسنطينة، العدد 13، 2018، ص 470.

³المواد 04، 06، 34 من القانون رقم 18-07، مصدر سابق.

الفرع الثالث: الحق في الاعتراض مع عدم الخضوع للقرارات الآلية

يُعد الحق في الاعتراض وعدم الخضوع للقرارات الآلية من أبرز الحقوق الرقمية الحديثة التي أفرزها التطور التكنولوجي، خاصة مع انتشار أنظمة المعالجة الآلية المعتمدة على الخوارزميات والذكاء الاصطناعي، ويهدف هذا الحق إلى تمكين الشخص المعني من رفض معالجة بياناته في حالات معينة، وكذا حمايته من القرارات التي تُتخذ بشكل آلي دون تدخل بشري، والتي قد تؤثر على مركزه القانوني أو الشخصي.

ويتمثل الحق في الاعتراض في تمكين الشخص المعني من رفض معالجة بياناته الشخصية، خاصة إذا كانت هذه المعالجة قائمة على مصلحة مشروعة للمسؤول عن المعالجة، أو لأغراض التسويق المباشر، ويُعد هذا الحق وسيلة لتحقيق التوازن بين مصالح الجهات المعالجة وحقوق الأفراد، حيث يُلزم المسؤول عن المعالجة بالتوقف عن المعالجة متى ثبت أن مصلحة الشخص المعني أولى بالحماية¹.

أما الحق في عدم الخضوع للقرارات الآلية، فيُقصد به حق الشخص في ألا يكون محل قرار يُتخذ بناءً على معالجة آلية بحتة، دون تدخل بشري، متى كان لهذا القرار أثر قانوني أو تأثير جوهري عليه. وتبرز أهمية هذا الحق في مواجهة الأنظمة الخوارزمية التي تعتمد على تحليل البيانات لاتخاذ قرارات تتعلق بالتوظيف أو القروض أو الخدمات الرقمية، والتي قد تتطوي على مخاطر التمييز أو الخطأ².

وقد أصبح هذا الحق أكثر إلحاحًا في ظل توسع استخدام تقنيات الذكاء الاصطناعي، التي تعتمد على معالجة كميات هائلة من البيانات، مما قد يؤدي إلى اتخاذ قرارات غير شفافة أو غير قابلة للتفسير، وهو ما يطرح إشكالية "الصندوق الأسود" للخوارزميات، حيث يصعب فهم كيفية اتخاذ القرار أو الطعن فيه.

¹بوعزيز خليفة، مرجع سابق، ص 35

²مفيدة مباركية، مرجع سابق، ص 475

وفي هذا الإطار، سعى المشرع الجزائري إلى توفير حماية نسبية من خلال تمكين الشخص المعني من الاعتراض على بعض أشكال المعالجة، غير أن النصوص القانونية لا تزال بحاجة إلى مزيد من التفصيل فيما يتعلق بالقرارات الآلية، خاصة في ظل التطورات المتسارعة في هذا المجال¹، وفي المقابل، اتجهت التشريعات المقارنة إلى تكريس هذا الحق بشكل صريح، مع إلزام المسؤولين عن المعالجة بتوفير تدخل بشري وإمكانية مراجعة القرار.

وعليه، فإن الحق في الاعتراض وعدم الخضوع للقرارات الآلية يمثل ضماناً أساسية لحماية الأفراد في مواجهة المخاطر المرتبطة بالنكاء الاصطناعي، غير أن فعاليته تظل مرتبطة بمدى تطوير الإطار القانوني بما يتماشى مع هذه التحولات التكنولوجية.

المطلب الثاني: التزامات المتدخلين في المعالجة البيانات

لا تقتصر الحماية القانونية للبيانات الشخصية على تمكين الشخص المعني من حقوق رقمية، بل تمتد لتشمل فرض التزامات قانونية دقيقة على مختلف المتدخلين في عملية المعالجة، وعلى رأسهم المسؤول عن المعالجة والمعالج من الباطن، ويهدف هذا التوجه إلى تحقيق توازن بين حرية استغلال البيانات من جهة، وضمان احترام الحقوق والحريات الأساسية للأفراد من جهة أخرى.

وعليه، سيتم تناول هذه الالتزامات من خلال ثلاثة فروع: يُخصص الأول لدراسة الالتزامات الإدارية، بينما يتناول الثاني مبدأ الخصوصية، في حين يُعنى الثالث النظام القانوني للمسؤول عن المعالجة.

الفرع الأول: الالتزامات الإدارية

تُعد الالتزامات الإدارية من الآليات الأساسية التي اعتمدها المشرع لضمان شفافية معالجة البيانات الشخصية وإخضاعها لرقابة مسبقة ولاحقة، فهذه الالتزامات لا تهدف فقط إلى

¹ المواد 04، 06، 34 من القانون رقم 18-07، مصدر سابق.

الفصل الأول: النظام الموضوعي للحماية نطاق المعالجة والحقوق المستحدثة

تنظيم النشاط المرتبط بالمعالجة، بل تسعى إلى تمكين السلطة المختصة من تتبع العمليات التي تتم على البيانات، والتأكد من مطابقتها لأحكام القانون¹.

ويأتي في مقدمة هذه الالتزامات واجب التصريح، حيث يُلزم المسؤول عن المعالجة بإخطار الجهة المختصة بعمليات المعالجة التي ينوي القيام بها، من خلال تقديم معلومات تتعلق بطبيعة البيانات، والغرض من معالجتها، والوسائل المستعملة في ذلك. ويُعد هذا الإجراء وسيلة لإعلام السلطة الرقابية مسبقاً، مما يسمح لها بالتدخل عند الاقتضاء لمنع أي معالجة غير مشروعة².

أما الترخيص المسبق، فيُفرض في بعض الحالات التي تتسم بحساسية خاصة، كمعالجة البيانات ذات الطابع الحساس أو تلك التي قد تشكل خطراً على حقوق الأفراد، وفي هذه الحالات، لا يكفي مجرد التصريح، بل يتعين الحصول على إذن مسبق من السلطة المختصة قبل الشروع في المعالجة، وهو ما يعكس تشديداً في الرقابة على هذا النوع من العمليات³.

إلى جانب ذلك، يلتزم المسؤول عن المعالجة بمسك سجلات خاصة تتضمن جميع العمليات المتعلقة بالبيانات الشخصية، بما في ذلك نوع البيانات المعالجة، وأغراض المعالجة، والجهات التي تم نقل البيانات إليها، ومدة الاحتفاظ بها، وتُعد هذه السجلات أداة مهمة لضمان الشفافية، كما تمكّن من إجراء عمليات المراقبة والتدقيق عند الحاجة⁴.

وقد كرس المشرع الجزائري هذه الالتزامات ضمن الإطار القانوني لحماية البيانات الشخصية، بهدف إخضاع المعالجة لنظام رقابي فعال يحد من التجاوزات، غير أن فعالية هذه

¹ تبينة حكيم، "السلطات الإدارية المستقلة ودورها في حماية البيانات الشخصية"، مجلة الحقوق، جامعة الجزائر، العدد 02، 2021، ص 110.

² حميمة علالي، مرجع السابق، ص 30

³ بوعزيز خليفة، مرجع السابق، ص 40

⁴ تبينة حكيم، مرجع سابق، ص 112.

الالتزامات تظل مرتبطة بمدى تطبيقها العملي، خاصة في ظل ضعف الوعي القانوني لدى بعض الفاعلين، أو غياب رقابة صارمة على تنفيذها.

وفي السياق المقارن، شهدت هذه الالتزامات تطوراً ملحوظاً، حيث تم الانتقال من نظام التصريح المسبق إلى نظام المساءلة، الذي يقوم على تحميل المسؤول عن المعالجة عبء إثبات امتثاله للقانون، وهو ما يعكس تحولاً نحو رقابة ذاتية مدعومة برقابة مؤسساتية¹.

وعليه، فإن الالتزامات الإدارية تمثل خطوة أساسية في تنظيم معالجة البيانات الشخصية، غير أن فعاليتها تتوقف على مدى تكاملها مع باقي الآليات القانونية والتقنية، وكذا على وجود رقابة فعالة تضمن احترامها في الواقع.

الفرع الثاني: مبدأ الخصوصية

يُعد مبدأ الخصوصية عبر التصميم من أهم المفاهيم الحديثة في مجال حماية البيانات الشخصية، إذ يقوم على إدماج متطلبات الحماية منذ المراحل الأولى لتصميم الأنظمة والتطبيقات، بدل الاكتفاء بمعالجتها بعد وقوع الانتهاك، ويعكس هذا التوجه انتقالاً نوعياً من الحماية اللاحقة إلى الحماية الوقائية، بما يضمن تقليل المخاطر المرتبطة بمعالجة البيانات قبل حدوثها.

ويقتضي هذا المبدأ أن يأخذ المسؤول عن المعالجة بعين الاعتبار حماية البيانات الشخصية عند تطوير الأنظمة المعلوماتية أو اعتماد وسائل جديدة للمعالجة، وذلك من خلال تقليل حجم البيانات المجمعة، وتحديد أغراضها بدقة، وضمان أمنها منذ البداية، كما يرتبط هذا المبدأ بمفهوم "الخصوصية الافتراضية"، الذي يعني أن تكون أعلى درجات الحماية مفعلة بشكل تلقائي دون تدخل من المستخدم².

¹Christopher Kuner, Op.cit., p. 150.

²عبد القادر بوعلام، مرجع سابق، ص 88

وإلى جانب ذلك، يبرز تقييم أثر المعالجة كآلية مكتملة لهذا المبدأ، حيث يتمثل في إجراء دراسة مسبقة لتحديد المخاطر المحتملة التي قد تترتب عن معالجة البيانات الشخصية، خاصة عندما تكون هذه المعالجة ذات طبيعة حساسة أو تعتمد على تقنيات حديثة كالذكاء الاصطناعي، ويهدف هذا التقييم إلى تحليل مدى تأثير المعالجة على حقوق الأفراد، واقتراح التدابير اللازمة للتقليل من هذه المخاطر¹.

وقد بدأ هذا التوجه يجد صدى في التشريعات الحديثة، التي لم تعد تكتفي بفرض التزامات عامة، بل اتجهت نحو إلزام المسؤولين عن المعالجة باتباع مقاربة استباقية تقوم على تقييم المخاطر واتخاذ تدابير وقائية، وفي هذا الإطار، يُلاحظ أن المشرع الجزائري، وإن لم ينص صراحة على مصطلح "الخصوصية عبر التصميم"، إلا أن بعض أحكامه توجي بتبني هذا الاتجاه من خلال التأكيد على ضرورة اتخاذ تدابير مناسبة لحماية البيانات وضمان أمنها².

غير أن تطبيق هذه الآليات يطرح تحديات عملية، خاصة في ظل نقص الخبرة التقنية لدى بعض الجهات المعالجة، أو ارتفاع تكاليف تطبيقها، مما قد يدفع بعض الفاعلين إلى إهمالها أو تطبيقها بشكل شكلي، كما أن غياب توجيهات دقيقة أو معايير واضحة قد يحد من فعاليتها، خاصة في البيئات الرقمية المعقدة.

وعليه، فإن الالتزام بالخصوصية عبر التصميم وتقييم أثر المعالجة يمثلان آليتين أساسيتين لتعزيز الحماية الوقائية للبيانات الشخصية، غير أن نجاحهما يظل مرتبطاً بمدى وعي الفاعلين بأهميتهما، وتوفير إطار قانوني وتقني يدعم تطبيقهما بشكل فعال.

¹ محمد عبد الله، "حماية البيانات الشخصية في ظل الذكاء الاصطناعي"، مجلة القانون الرقمي، 2024، ص 55

² القانون رقم 07-18، مصدر سابق.

الفرع الثالث: النظام القانوني المسؤول عن المعالجة

تُعد مسألة تحديد المركز القانوني لكلٍّ من المسؤول عن المعالجة والمعالج من الباطن من القضايا الجوهرية في نظام حماية البيانات الشخصية، لما لها من أثر مباشر في توزيع المسؤوليات وتحديد نطاق الالتزامات القانونية، فتعقد عمليات المعالجة في البيئة الرقمية، وتعدد الأطراف المتدخلة فيها، يفرضان ضرورة وضع إطار قانوني واضح يحدد دور كل طرف، تفادياً لفراغ المسؤولية أو تداخلها.

وقد عزز القانون رقم 11-25 هذا التوجه من خلال استحداث التزامات جديدة تتعلق بمسك سجل نشاطات المعالجة، وتعيين مندوب لحماية البيانات الشخصية.¹

ويقصد بـ المسؤول عن المعالجة الشخص الطبيعي أو المعنوي الذي يحدد أغراض ووسائل معالجة البيانات الشخصية، ويُعد الطرف الرئيسي الذي يتحمل عبء ضمان مشروعية المعالجة واحترام حقوق الأشخاص المعنيين، ومن ثم، فإنه يلتزم بجملة من الواجبات، منها احترام مبادئ المعالجة، وضمان أمن البيانات، وتمكين الأشخاص من ممارسة حقوقهم، إضافة إلى تحمل المسؤولية القانونية في حالة الإخلال بهذه الالتزامات.²

أما المعالج من الباطن، فهو الشخص الذي يقوم بمعالجة البيانات لحساب المسؤول عن المعالجة، دون أن تكون له سلطة تحديد أغراضها أو وسائلها، ورغم أن دوره يبدو تقنياً في الظاهر، إلا أن مسؤوليته ليست منعدمة، إذ يلتزم بدوره باحترام التعليمات الصادرة عن المسؤول، وضمان سرية البيانات، واتخاذ التدابير الأمنية اللازمة لحمايتها.³

ويقوم النظام القانوني الحديث على مبدأ توزيع المسؤوليات بين هذين الطرفين، بحيث لا يتحمل أحدهما عبء المسؤولية بشكل مطلق، بل يتم تحديدها وفقاً لدور كل منهما في عملية

¹ القانون رقم 11-25 مصدر سابق، المادة 41 مكرر

² بوعزيز خليفة، مرجع سابق، ص 45

³ حميمة علالي، مرجع سابق، ص 34

المعالجة، ويُعد هذا التوزيع ضروريًا لضمان فعالية الحماية، خاصة في الحالات التي يتم فيها إسناد جزء من المعالجة إلى أطراف خارجية، كما هو الحال في خدمات الحوسبة السحابية.

وقد أخذ المشرع الجزائري بهذا التوجه، حيث ميز بين المسؤول عن المعالجة والمعالج من الباطن، وأخضع كل منهما لالتزامات محددة، مع تحميل المسؤول عن المعالجة الدور الرئيسي في ضمان الامتثال لأحكام القانون¹، كما أقر ضرورة وجود إطار تعاقدى ينظم العلاقة بين الطرفين، يحدد طبيعة المعالجة، ومدتها، والتزامات كل طرف، بما يضمن حماية البيانات من أي استغلال غير مشروع.

غير أن التطبيق العملي لهذا النظام يثير عدة إشكالات، خاصة في الحالات التي تتعدد فيها الجهات المتدخلة في المعالجة، أو عندما يتم نقل البيانات خارج الإقليم الوطني، مما يصعب تحديد المسؤولية بدقة، كما أن بعض الفاعلين قد يلجؤون إلى توزيع الأدوار بشكل معقد بهدف التهرب من المسؤولية، وهو ما يستدعي تعزيز الرقابة القانونية وتوضيح القواعد المنظمة لهذه العلاقة.

وعليه، فإن تحديد النظام القانوني للمسؤول عن المعالجة والمعالج من الباطن يمثل عنصرًا أساسيًا في تحقيق الحماية الفعلية للبيانات الشخصية، من خلال ضمان توزيع عادل وواضح للمسؤوليات، بما يمنع الإفلات من المساءلة ويعزز ثقة الأفراد في البيئة الرقمية.

¹ القانون رقم 18-07، مصدر سابق.

خلاصة الفصل

خلصت الدراسة في هذا الفصل إلى أن المشرع الجزائري سعى إلى تكريس حماية قانونية للبيانات الشخصية من خلال تحديد نطاق المعطيات المشمولة بالحماية، ووضع ضوابط قانونية تحكم مشروعية معالجتها، إلى جانب تكريس مجموعة من الحقوق الرقمية لفائدة الشخص المعني بالبيانات، كحق الإعلام والنفاد والتصحيح والمحو.

كما تبين أن القانون رقم 07-18 المعدل والمتمم بالقانون رقم 11-25 عزز التزامات المسؤولين عن المعالجة، من خلال تدعيم آليات الأمن والرقابة والامتثال، بما ينسجم مع التطورات الرقمية الحديثة.

غير أن الدراسة كشفت في المقابل عن وجود بعض النقائص المتعلقة بمواكبة التطورات المرتبطة بالذكاء الاصطناعي والمعالجة الآلية للبيانات، وهو ما يبرز الحاجة إلى تطوير المنظومة القانونية الجزائرية بما يضمن حماية أكثر فعالية للبيانات الشخصية في البيئة الرقمية.

الفصل الثاني

الضمانات المؤسسية الجزائية

تمهيد:

لا تقتصر الحماية القانونية للبيانات الشخصية على مجرد الاعتراف بالحقوق والالتزامات المنظمة لعمليات المعالجة، بل تقتضي أيضًا توفير آليات مؤسسية وقانونية فعالة تضمن احترام هذه الأحكام في الواقع العملي، فمهما بلغ مستوى التنظيم الموضوعي لحماية البيانات الشخصية، فإن فعاليته تبقى رهينة بوجود أجهزة رقابية قادرة على متابعة عمليات المعالجة، والتدخل عند وقوع المخالفات، إلى جانب تقرير الجزاءات القانونية تكفل ردع الانتهاكات التي قد تمس بحقوق الأفراد وحياتهم.

وفي ظل التوسع المتزايد لاستخدام الوسائل الرقمية والاعتماد المتنامي على المعالجة الآلية للبيانات، برزت الحاجة إلى تطوير منظومة رقابية أكثر فعالية، تقوم على التوازن بين متطلبات التطور التكنولوجي وضرورة حماية الحياة الخاصة للأفراد، ومن هذا المنطلق، سعى المشرع الجزائري، لاسيما من خلال القانون رقم 18-07 المعدل والمتمم بالقانون رقم 25-11، إلى تدعيم الحماية المؤسسية للبيانات الشخصية، عبر تعزيز دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، واستحداث آليات رقابية جديدة، إلى جانب تشديد المسؤولية القانونية المترتبة عن المعالجة غير المشروعة للبيانات.

وعليه، سيتم في هذا الفصل دراسة الضمانات المؤسسية الجزائية ، وذلك من خلال التطرق في المبحث الأول إلى الآليات الرقابية المؤسسية، ثم دراسة المسؤولية القانونية والسياسة العقابية للمشرع الجزائري في المبحث الثاني.

المبحث الأول: الآليات الرقابية المؤسسية

تقتضي الحماية الفعلية للبيانات الشخصية وجود آليات رقابية تضمن احترام القواعد القانونية المنظمة لعمليات المعالجة، خاصة في ظل تزايد المخاطر المرتبطة بالتطور الرقمي والمعالجة الآلية للبيانات، ولهذا، اتجه المشرع الجزائري، لاسيما من خلال القانون رقم 07-18 المعدل والمتمم بالقانون رقم 11-25، إلى تعزيز منظومة الرقابة عبر إقرار آليات داخلية وخارجية تهدف إلى ضمان الامتثال لأحكام حماية البيانات الشخصية.

وعليه، سيتم التطرق في هذا المبحث إلى الرقابة الداخلية في المطلب الأول، ثم دراسة الرقابة الخارجية في المطلب الثاني.

المطلب الأول: الرقابة الداخلية

لم تعد حماية البيانات الشخصية مسؤولية السلطة الرقابية وحدها، بل أصبحت تقوم كذلك على آليات رقابة داخلية تُمارس داخل الهيئات والمؤسسات التي تتولى معالجة البيانات، ويعكس هذا التوجه التحول نحو مفهوم الامتثال الذاتي، الذي يقوم على تحميل المسؤول عن المعالجة التزامًا دائمًا بضمان احترام قواعد حماية البيانات داخل المؤسسة نفسها¹.

وفي هذا السياق، استحدثت التشريعات الحديثة مجموعة من الفاعلين والآليات الجديدة، من أبرزها مندوب حماية البيانات، والممثل القانوني للهيئات الأجنبية، إضافة إلى مدونات السلوك وسياسات الامتثال الذاتي، باعتبارها أدوات تهدف إلى تعزيز الوقاية وتقليل مخاطر المعالجة غير المشروعة للبيانات الشخصية.

¹ محمد الأمين بوسماحة، "حماية المعطيات الشخصية في البيئة الرقمية"، مجلة الباحث للدراسات القانونية، جامعة باتنة، العدد

الفرع الأول: مندوب حماية المعطيات قانونيا

يُعد مندوب حماية المعطيات الشخصية من أبرز الآليات الحديثة التي استحدثتها التشريعات المعاصرة في مجال حماية البيانات، وذلك بالنظر إلى الدور المحوري الذي يؤديه في ضمان امتثال الهيئات والمؤسسات للقواعد القانونية المنظمة لمعالجة البيانات الشخصية، ويقوم هذا النظام على فكرة الرقابة الداخلية الوقائية، من خلال تعيين شخص يتولى متابعة مدى احترام قواعد الحماية داخل الهيئة المعالجة، بدل الاكتفاء بالتدخل الخارجي اللاحق من قبل السلطة المختصة.

وقد برز هذا النظام بشكل واضح في التشريع الأوروبي، خاصة في إطار اللائحة العامة لحماية البيانات، التي اعتبرت مندوب حماية البيانات عنصراً أساسياً في تكريس مبدأ الامتثال والمساءلة، وتأثر المشرع الجزائري بهذا التوجه، حيث عزز القانون رقم 11-25 المعدل والمتمم للقانون رقم 07-18 مكانة هذا الفاعل، من خلال استحداث أحكام جديدة تتعلق بتعيينه وتحديد مهامه واختصاصاته¹.

ويُقصد بمندوب حماية المعطيات الشخص الذي تعهد إليه مهمة السهر على احترام قواعد حماية البيانات داخل المؤسسة أو الهيئة المعالجة، من خلال مراقبة مدى مطابقة عمليات المعالجة لأحكام القانون، وتقديم الاستشارات والتوجيهات المتعلقة بحماية البيانات الشخصية²، ويتميز هذا المندوب بطابع وقائي واستشاري في آن واحد، إذ لا يقتصر دوره على الكشف عن المخالفات، بل يمتد إلى المساهمة في منع وقوعها منذ البداية، وفيما يتعلق بالتعيين، فقد اتجه المشرع الجزائري إلى إلزام بعض الهيئات بتعيين مندوب لحماية البيانات، خاصة عندما تكون عمليات المعالجة واسعة النطاق أو تتعلق بمعطيات حساسة.

¹ القانون رقم 11-25 المؤرخ في 24 يوليو 2025، المعدل والمتمم للقانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في

مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ج ج، العدد 48، الصادرة بتاريخ 29 يوليو 2025، المادة 41 مكرر.

² عبد القادر بوعلام، مرجع سابق، ص 91.

ويُفهم من أحكام القانون رقم 11-25 أن هذا التعيين يهدف إلى تدعيم الرقابة الداخلية وضمان احترام قواعد الأمن والسرية أثناء المعالجة¹.

أما من حيث المهام، فيتولى مندوب حماية المعطيات عدة وظائف، من أهمها مراقبة احترام التشريع المتعلق بحماية البيانات الشخصية، وتوعية العاملين داخل المؤسسة بمقتضيات الحماية، وتقديم الرأي بشأن عمليات المعالجة الجديدة، إضافة إلى التعاون مع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي²، كما يساهم في إعداد سجل نشاطات المعالجة ومتابعة مدى احترام التدابير التقنية والتنظيمية المتعلقة بآمن البيانات.

غير أن فعالية هذا النظام تبقى مرتبطة بمدى استقلالية المندوب وتوفير الإمكانيات اللازمة لأداء مهامه، إذ قد يؤدي خضوعه المباشر لإدارة المؤسسة إلى التأثير على حياده، خاصة في الحالات التي تتعارض فيها متطلبات الامتثال مع المصالح الاقتصادية للهيئة المعالجة³، كما أن غياب ثقافة الامتثال الرقمي داخل بعض المؤسسات قد يحد من فعالية هذا الدور في الواقع العملي .

ومن ثم، يمكن القول إن استحداث مندوب حماية المعطيات يمثل خطوة مهمة نحو تكريس الحماية الوقائية للبيانات الشخصية، غير أن نجاح هذه الآلية يظل مرهوناً بمدى وضوح الإطار القانوني المنظم لها، وكذا بفعالية الرقابة التي تمارسها السلطة المختصة على أداء هذا المندوب⁴.

الفرع الثاني: التزامات الممثل القانوني للهيئات الأجنبية

أدى الطابع العابر للحدود الذي أصبحت تتسم به معالجة البيانات الشخصية إلى بروز إشكالات قانونية جديدة، خاصة عندما يتعلق الأمر بمؤسسات أو هيئات أجنبية تقوم بمعالجة

¹المادة 41 مكرر 02 من القانون رقم 11-25، مصدر سابق.

²تبيينة حكيم، مرجع سابق، ص 117.

³محمد الأمين بوسماحة، مرجع سابق، ص 55.

⁴Paul Voigt & Axel von dem Bussche, Op.cit., p. 145.

بيانات أشخاص موجودين داخل الإقليم الوطني، ففي ظل التطور التكنولوجي وانتشار الخدمات الرقمية العابرة للحدود، لم تعد معالجة البيانات مرتبطة بوجود مادي للمؤسسة داخل الدولة، وهو ما فرض على التشريعات الحديثة البحث عن آليات قانونية تضمن إخضاع هذه الهيئات للقواعد الوطنية المتعلقة بحماية البيانات الشخصية.

وفي هذا السياق، اتجه المشرع الجزائري، أسوة بالتشريعات المقارنة، إلى تكريس نظام الممثل القانوني للهيئات الأجنبية، بهدف ضمان وجود مخاطب قانوني داخل الإقليم الوطني يمكن للسلطات المختصة والأشخاص المعنيين الرجوع إليه عند الاقتضاء، ويُعد هذا التوجه وسيلة لتفادي صعوبة متابعة الهيئات الأجنبية التي تمارس نشاط معالجة البيانات عن بُعد، دون أن يكون لها مقر فعلي داخل الجزائر¹.

ويقصد بالممثل القانوني الشخص الطبيعي أو المعنوي الذي تعينه الهيئة الأجنبية لتمثيلها داخل الدولة، ويتولى مهام التنسيق والتواصل مع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، إضافة إلى متابعة مدى احترام الالتزامات القانونية المرتبطة بمعالجة البيانات الشخصية²، كما يتحمل هذا الممثل دورًا مهمًا في تسهيل ممارسة الأشخاص المعنيين لحقوقهم، خاصة ما يتعلق بحقوق النفاذ والتصحيح والاعتراض.

وقد عزز القانون رقم 11-25 هذا التوجه من خلال إلزام بعض الهيئات الأجنبية التي تستهدف الأشخاص الموجودين داخل الجزائر بتعيين ممثل قانوني، وهو ما يعكس رغبة المشرع في توسيع نطاق الحماية القانونية وعدم قصرها على الهيئات الوطنية فقط³، ويُستفاد من هذا التنظيم أن المشرع يسعى إلى سد الفراغ القانوني الذي قد تستغله بعض الشركات الرقمية الأجنبية للتحلل من الالتزامات القانونية المتعلقة بحماية البيانات.

¹ محمد عبد الله، مرجع سابق، ص 61.

² عبد القادر بوعلام، مرجع سابق، ص 92.

³ المادة 41 مكرر 04 من القانون رقم 11-25، مصدر سابقا.

غير أن التطبيق العملي لهذا النظام قد يثير عدة صعوبات، خاصة فيما يتعلق بمدى فعالية متابعة الهيئات الأجنبية التي لا تمتلك أي وجود مادي داخل الدولة، أو في حالة تعارض القوانين الوطنية مع القوانين الأجنبية المنظمة للبيانات الشخصية، كما أن غياب تعاون دولي فعال في هذا المجال قد يحد من قدرة السلطة الوطنية على فرض احترام التشريع الجزائري خارج الحدود الوطنية.¹

ومن ثم، فإن نظام الممثل القانوني للهيئات الأجنبية يمثل آلية مهمة لتعزيز الحماية القانونية للبيانات الشخصية في البيئة الرقمية، غير أن فعاليتها تبقى مرتبطة بمدى تطوير آليات التعاون الدولي وتدعيم وسائل الرقابة العابرة للحدود.

الفرع الثالث: مدونات السلوك مع سياسات الامتثال الذاتي

أصبحت مدونات السلوك وسياسات الامتثال الذاتي من الآليات الحديثة التي تعتمد عليها التشريعات المعاصرة لتعزيز حماية البيانات الشخصية داخل المؤسسات والهيئات المعالجة، وذلك في إطار الانتقال من الرقابة التقليدية القائمة على التدخل الخارجي فقط، إلى رقابة داخلية تقوم على الوقاية والالتزام الطوعي بقواعد الحماية، ويعكس هذا التوجه تطور مفهوم حماية البيانات من مجرد التزام قانوني مفروض إلى ثقافة مؤسسية قائمة على احترام الخصوصية الرقمية،

ويقصد بمدونات السلوك مجموعة القواعد والمبادئ التي تضعها الهيئات أو القطاعات المهنية لتنظيم كيفية معالجة البيانات الشخصية داخل مجال نشاط معين، بما يضمن توافق الممارسات المهنية مع الأحكام القانونية المتعلقة بحماية البيانات². وتتميز هذه المدونات بطابعها المرن، إذ تسمح بتكييف قواعد الحماية وفق خصوصية كل قطاع، خاصة في المجالات التي تعتمد بشكل مكثف على المعالجة الرقمية للبيانات.

¹Paul Voigt & Axel von dem Bussche, Op.cit., p. 172.

²محمد الأمين بوسماحة، مرجع سابق، ص 59

أما سياسات الامتثال الذاتي، فتتمثل في الإجراءات والتدابير الداخلية التي تعتمد عليها المؤسسات لضمان احترام قواعد حماية البيانات الشخصية، من خلال وضع أنظمة رقابة داخلية، وتحديد المسؤوليات، وتكوين العاملين، واعتماد تدابير تقنية وتنظيمية لحماية البيانات¹، ويقوم هذا النظام على مبدأ المساءلة، الذي يفرض على المسؤول عن المعالجة إثبات مدى امتثاله للأحكام القانونية المنظمة للمعالجة.

وقد اتجه المشرع الجزائري، من خلال القانون رقم 11-25 المعدل والمتمم للقانون رقم 07-18، إلى تعزيز هذا التوجه، عبر تدعيم آليات الامتثال الداخلي وربطها بمسؤولية المسؤول عن المعالجة ومندوب حماية المعطيات²، ويلاحظ أن هذا التنظيم يهدف إلى تقليل المخاطر المرتبطة بالمعالجة غير المشروعة، خاصة في ظل التطور السريع للتقنيات الرقمية وتزايد الاعتماد على الذكاء الاصطناعي في معالجة البيانات.

غير أن فعالية هذه الآليات تبقى مرتبطة بمدى التزام المؤسسات بتطبيقها بصورة جدية، إذ قد تتحول مدونات السلوك في بعض الحالات إلى مجرد وثائق شكلية لا تُفَعَّل عملياً داخل المؤسسة³، كما أن غياب ثقافة قانونية رقمية لدى بعض الفاعلين قد يحد من فعالية الامتثال الذاتي، خاصة في المؤسسات التي تفتقر إلى الخبرة التقنية والقانونية الكافية.

ومن ثم، فإن مدونات السلوك وسياسات الامتثال الذاتي تمثلان آليتين مهمتين لتعزيز الحماية الوقائية للبيانات الشخصية⁴، غير أن نجاحهما يظل مرهوناً بمدى وجود رقابة فعلية تضمن احترام هذه السياسات وعدم الاكتفاء بها كالتزام شكلي فقط.

¹ عبد القادر بوعلام، مرجع سابق، ص 95.

المادة 41 مكرر 02 من القانون رقم 11-25، مصدر سابق.

³ تبيينة حكيم، المرجع سابق، ص 121.

⁴ Paul Voigt & Axel von demBussche, Op.cit., p. 181

المطلب الثاني: الرقابة الخارجية

وفي هذا الإطار، اتجه المشرع الجزائري، من خلال القانون رقم 18-07 المعدل والمتمم بالقانون رقم 25-11، إلى تكريس نظام رقابي خارجي تتولاه السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، حيث منحها مجموعة من الصلاحيات التنظيمية والرقابية والردعية، بهدف ضمان التطبيق الفعلي لأحكام القانون وتعزيز حماية الحياة الخاصة للأفراد.

وعليه، سيتم التطرق في هذا المطلب إلى الطبيعة القانونية للسلطة مع ضمانات استقلاليتها في الفرع الأول، ثم دراسة الصلاحيات الضبطية في الفرع الثاني، وأخيرًا بيان سلطتها في توقيع الجزاءات الإدارية المالية في الفرع الثالث.

الفرع الأول: الطبيعة القانونية للسلطة مع ضمانات استقلاليتها

تُعد السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي الآلية الأساسية التي اعتمدها المشرع الجزائري لضمان التطبيق الفعلي لأحكام حماية البيانات الشخصية، وذلك بالنظر إلى الدور المحوري الذي تؤديه في مراقبة عمليات المعالجة والتأكد من مدى احترام القواعد القانونية المنظمة لها، ويعكس إنشاء هذه السلطة توجه المشرع نحو تكريس رقابة مؤسسية متخصصة تتلاءم مع خصوصية البيئة الرقمية وما تفرضه من تحديات قانونية وتقنية متزايدة.

وقد أنشأ المشرع الجزائري هذه السلطة بموجب القانون رقم 18-07، ومنحها الشخصية المعنوية والاستقلال المالي، وهو ما يستفاد من أحكام المادة 22 من القانون المذكور¹، ويظهر هذا التنظيم أن المشرع لم يعتبرها مجرد هيئة إدارية تابعة للسلطة التنفيذية، بل منحها وضعًا قانونيًا خاصًا يهدف إلى ضمان قدر من الاستقلالية في ممارسة مهامها الرقابية.

¹ القانون رقم 18-07، مصدر سابق، المادة 22.

وتتدرج السلطة الوطنية ضمن فئة السلطات الإدارية المستقلة، باعتبارها تمارس وظائف رقابية وتنظيمية في مجال حماية البيانات الشخصية بعيداً عن التبعية الإدارية المباشرة، ويكتسي هذا الاستقلال أهمية خاصة، لأن فعالية الرقابة على معالجة البيانات تقتضي أن تكون الهيئة المكلفة بها بعيدة عن أي تأثير قد يمس بحيادها أو يحد من قدرتها على اتخاذ القرارات المناسبة.¹

وفي سبيل تدعيم هذه الاستقلالية، حرص المشرع الجزائري على تحديد تشكيلة السلطة وكيفية تعيين أعضائها، مع منحها صلاحيات خاصة في مجال المراقبة والتحقيق وإبداء الرأي، كما عزز القانون رقم 11-25 هذا التوجه من خلال استحداث أقطاب جهوية تابعة للسلطة الوطنية، بهدف توسيع نطاق الرقابة وتقريبها من مختلف الهيئات المعالجة عبر التراب الوطني.²

غير أن الاستقلال القانوني لا يكفي وحده لضمان فعالية هذه السلطة، إذ تبقى الاستقلالية العملية مرتبطة بتوفير الإمكانيات البشرية والتقنية والمالية اللازمة لممارسة مهامها، فضعف الوسائل التقنية أو قلة الموارد البشرية المتخصصة قد يؤثر سلباً على قدرتها في مواكبة التطور السريع لوسائل المعالجة الرقمية، خاصة في ظل الاعتماد المتزايد على تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة.

كما يُلاحظ أن فعالية السلطة الوطنية ترتبط كذلك بمدى وضوح علاقتها بباقي الهيئات الإدارية والقضائية، لتفادي تداخل الاختصاصات أو ببطء إجراءات التدخل عند وقوع الانتهاكات، وفي هذا الإطار، يرى جانب من الفقه أن تعزيز استقلالية هذه السلطة يقتضي دعم صلاحياتها الرقابية والردعية، مع تكريس ضمانات قانونية أوضح تكفل حيادها وفعاليتها.³

¹ تبينة حكيم، مرجع سابق، ص 125.

² المادة 27 مكرر من القانون رقم 11-25، مصدر سابق.

³ مسياد أمينة، "آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون 07-18"، مجلة الباحث، جامعة سوق أهراس، العدد 05، 2021، ص 144.

ومن ثم، فإن إنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي يمثل خطوة مهمة في سبيل تكريس الحماية المؤسسية للبيانات الشخصية، غير أن فعالية هذه الآلية تبقى رهينة بمدى توفير الضمانات العملية الكفيلة بتمكينها من أداء مهامها بصورة مستقلة وفعالة،¹

الفرع الثاني: الصلاحيات الضبطية

لا يمكن الحديث عن فعالية الحماية القانونية للبيانات الشخصية دون تمكين السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي من صلاحيات حقيقية تسمح لها بمراقبة عمليات المعالجة والتدخل عند وقوع المخالفات، فخصوصية البيئة الرقمية وما تتسم به من سرعة وتعقيد في تداول البيانات تفرض منح الهيئة الرقابية سلطات تتجاوز الدور الاستشاري التقليدي، لتشمل وظائف الضبط والتحقيق والمعاينة، بما يضمن التطبيق الفعلي لأحكام القانون.

وفي هذا الإطار، منح المشرع الجزائري للسلطة الوطنية جملة من الصلاحيات الضبطية التي تهدف إلى تنظيم نشاط معالجة البيانات الشخصية وضمان احترام المبادئ القانونية المؤطرة لها، ويتجلى ذلك من خلال اختصاصها بتلقي التصاريح وطلبات الترخيص المتعلقة بالمعالجة، وإبداء الرأي بشأن بعض العمليات ذات الطابع الحساس، إضافة إلى إصدار التوجيهات والتوصيات المتعلقة بحماية البيانات الشخصية²، ويلاحظ أن هذه الصلاحيات تعكس الطابع الوقائي للرقابة، إذ تهدف إلى الحد من المخاطر قبل وقوع الانتهاك.

كما خول المشرع للسلطة الوطنية صلاحيات تحقيق واسعة، تمكنها من مراقبة مدى امتثال المسؤولين عن المعالجة لأحكام القانون، وتشمل هذه الصلاحيات إمكانية إجراء التحريات والرقابة الميدانية، والاطلاع على الوثائق والسجلات المتعلقة بعمليات المعالجة، وكذا طلب المعلومات

¹ بوالخلفة فيصل، "حماية المعطيات ذات الطابع الشخصي بين النصوص التقليدية والتحديات الرقمية"، مجلة الدراسات القانونية، العدد 03، 2023، ص 88.

² المواد 22.16.15. من القانون رقم 07-18، مصدر سابق..

الضرورية من الهيئات المعنية¹، ويظهر من خلال هذه السلطات أن المشرع اتجه نحو تكريس رقابة فعلية تتجاوز الرقابة الشكلية أو الإدارية البسيطة.

ويكتسي الطابع التحقيقي لهذه الصلاحيات أهمية خاصة في المجال الرقمي، بالنظر إلى صعوبة اكتشاف بعض الانتهاكات المرتبطة بمعالجة البيانات، خاصة تلك التي تتم عبر الأنظمة المعلوماتية المعقدة أو تقنيات الذكاء الاصطناعي، ولهذا، فإن فعالية الرقابة تظل مرتبطة بقدرة السلطة الوطنية على مواكبة التطور التقني، من خلال توفير خبرات متخصصة ووسائل تقنية حديثة تمكنها من تتبع المخالفات الرقمية وإثباتها².

وقد عزز القانون رقم 11-25 هذه الصلاحيات من خلال تدعيم آليات المتابعة والرقابة، خاصة عبر استحداث سجل نشاطات المعالجة، وإلزام بعض الهيئات بتعيين مندوب لحماية المعطيات، الأمر الذي يسمح للسلطة الوطنية بالحصول على معطيات أدق حول كيفية معالجة البيانات داخل المؤسسات³.

يعكس هذا التوجه انتقال المشرع الجزائري من رقابة لاحقة محدودة إلى رقابة مستمرة تقوم على منطق الامتثال والوقاية.

غير أن فعالية هذه الصلاحيات تبقى مرتبطة بعدة عوامل، من بينها مدى استقلالية السلطة الوطنية، وكفاءة الموارد البشرية والتقنية الموضوعة تحت تصرفها، فضلاً عن مستوى التعاون الذي تبديه الهيئات المعالجة أثناء عمليات التحقيق والرقابة، كما أن غياب نصوص تنظيمية دقيقة تحدد بعض إجراءات الرقابة الرقمية قد يطرح صعوبات عملية، خاصة في ما يتعلق بمراقبة الخوارزميات أو المعالجة العابرة للحدود.

¹ المواد 23.24.25. من القانون رقم 18-07، مصدر سابق.

² عبد الهادي كحالوي، الحماية القانونية للبيانات الشخصية في التشريع الجزائري، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، 2022، ص 214.

³ المواد 41 مكرر 02 من القانون رقم 25-11، مصدر سابق.

ويؤخذ على التنظيم الجزائري كذلك محدودية التنسيق الدولي في مجال التحقيقات الرقمية، رغم أن جزءًا كبيرًا من عمليات معالجة البيانات يتم من خلال منصات وشركات أجنبية عابرة للحدود، وهو ما قد يحد من قدرة السلطة الوطنية على فرض احترام التشريع الجزائري خارج الإقليم الوطني، خاصة في ظل غياب اتفاقيات فعالة للتعاون الدولي في هذا المجال¹.

ومن ثم، فإن الصلاحيات الضبطية والتحقيقية التي منحها المشرع للسلطة الوطنية تمثل ركيزة أساسية لضمان فعالية الحماية القانونية للبيانات الشخصية، غير أن نجاح هذه الآلية يظل مرهونًا بمدى تطوير الوسائل التقنية والقانونية الكفيلة بمواكبة التحولات الرقمية المتسارعة.²

الفرع الثالث: سلطة توقيع الجزاءات الإدارية المالية

لم يعد نظام حماية البيانات الشخصية يقوم فقط على منح الأفراد حقوقًا قانونية أو فرض التزامات على المسؤولين عن المعالجة، بل أصبح يركز كذلك على وجود آليات ردعية فعالة تكفل احترام هذه القواعد وتضمن عدم الإفلات من المسؤولية. ولهذا، اتجهت التشريعات الحديثة إلى تمكين السلطات المختصة بحماية البيانات من صلاحيات توقيع جزاءات إدارية ومالية، باعتبارها وسيلة سريعة وفعالة لمواجهة المخالفات المرتبطة بمعالجة البيانات الشخصية.

وفي هذا الإطار، منح المشرع الجزائري للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي صلاحيات ردعية تهدف إلى ضمان الامتثال لأحكام القانون، وذلك من خلال تمكينها من اتخاذ تدابير إدارية ضد الهيئات أو الأشخاص الذين يثبت إخلالهم بالقواعد المنظمة لمعالجة البيانات الشخصية³، ويلاحظ أن هذا التوجه يعكس انتقال السلطة الوطنية من مجرد هيئة

¹ عمر مؤيد محمود، "الحماية القانونية للبيانات الشخصية في ظل التشريعات الرقمية الحديثة"، مجلة Gateway Journal، العدد 04، 2025، ص 77.

² مسياد أمينة، مرجع سابق، ص 149.

³ القانون رقم 18-07، مصدر سابق، المواد 22، 23، 24.

استشارية أو رقابية إلى هيئة ضبط إداري تتمتع بسلطات فعلية في مجال حماية البيانات الشخصية.

وتتجسد هذه الجزاءات في عدة صور، من بينها توجيه الإنذارات والتنبيهات، والأمر بتوقيف بعض عمليات المعالجة مؤقتًا أو نهائيًا، إضافة إلى إمكانية سحب الترخيص أو رفض منح التصريح في الحالات التي تشكل فيها المعالجة خطرًا على حقوق الأفراد وحياتهم¹، كما يمكن للسلطة الوطنية أن تأمر باتخاذ تدابير تصحيحية تهدف إلى إعادة المعالجة إلى الإطار القانوني السليم، وهو ما يعكس الطابع الوقائي والعلاجي لهذه الجزاءات في آن واحد.

وقد عزز القانون رقم 11-25 هذه الصلاحيات من خلال تدعيم آليات الرقابة والامتثال، وربط بعض الالتزامات الجديدة بجزاءات إدارية ومالية، خاصة ما يتعلق بعدم مسك سجل نشاطات المعالجة أو الإخلال بالالتزامات مندوب حماية المعطيات²، ويظهر من ذلك أن المشرع الجزائري اتجه نحو تشديد الرقابة على المؤسسات التي تتعامل مع البيانات الشخصية، خاصة في ظل تنامي المخاطر المرتبطة بالمعالجة الرقمية والذكاء الاصطناعي.

ويكتسي الجزاء المالي أهمية خاصة في مجال حماية البيانات الشخصية، بالنظر إلى الطبيعة الاقتصادية للبيانات في العصر الرقمي، إذ أصبحت بعض المؤسسات تحقق أرباحًا ضخمة من استغلال البيانات الشخصية، الأمر الذي يجعل العقوبات التقليدية غير كافية لتحقيق الردع المطلوب، ومن ثم، فإن فرض غرامات مالية يشكل وسيلة فعالة لإجبار الهيئات المعالجة على احترام قواعد الحماية وعدم التعامل مع البيانات باعتبارها مجرد مورد اقتصادي خارج الرقابة القانونية³.

¹ مسياد أمينة، مرجع سابق، ص 151.

² المادة 41 مكرر 02 من القانون رقم 11-25، مصدر سابق.

³ بوخالفة فيصل، مرجع سابق، ص 94.

غير أن فعالية هذه الجزاءات تبقى مرتبطة بعدة عوامل، من أهمها وضوح المعايير المعتمدة في تقدير العقوبات، ومدى تناسبها مع خطورة المخالفة المرتكبة، إضافة إلى قدرة السلطة الوطنية على تنفيذ قراراتها بصورة فعالة، كما يُلاحظ أن التنظيم الجزائي لا يزال بحاجة إلى مزيد من التدقيق فيما يتعلق بسقف الغرامات الإدارية ومعايير تحديدها، مقارنة ببعض التشريعات المقارنة، خاصة اللائحة الأوروبية لحماية البيانات (GDPR)، التي اعتمدت نظامًا صارمًا للغرامات المالية¹.

ومن جهة أخرى، فإن منح السلطة الوطنية صلاحيات واسعة في توقيع الجزاءات يثير ضرورة تحقيق التوازن بين فعالية الحماية وضمانات المشروعية، وذلك من خلال إخضاع قراراتها للرقابة القضائية، تفاديًا لأي تعسف قد يمس بحقوق الأشخاص أو الهيئات المعنية، ويُعد هذا التوازن ضروريًا لضمان احترام مبدأ الشرعية وحماية الحقوق والحريات في إطار ممارسة السلطة الضبطية².

ومن ثم، فإن تمكين السلطة الوطنية من سلطة توقيع الجزاءات الإدارية والمالية يمثل ركيزة أساسية لتعزيز فعالية نظام حماية البيانات الشخصية، غير أن نجاح هذه الآلية يظل مرتبطًا بمدى تطوير الإطار القانوني المنظم لها، وتوفير الوسائل الكفيلة بضمان تنفيذها بصورة عادلة وفعالة.

¹ عمر مؤيد محمود، مرجع سابق، ص 82.

² Paul Voigt & Axel von dem Bussche, Op.cit., p. 201.

المبحث الثاني: المسؤولية القانونية للمشرع الجزائري

تقتضي الحماية الفعلية للبيانات الشخصية وجود نظام قانوني للمساءلة يضمن جبر الأضرار الناتجة عن المعالجة غير المشروعة، إلى جانب تقرير جزاءات قانونية تكفل ردع مختلف الانتهاكات المرتبطة بالبيانات الشخصية، ولهذا، سعى المشرع الجزائري من خلال القانون رقم 07-18 المعدل والمتمم بالقانون رقم 11-25 إلى تدعيم الحماية المدنية والجزائية للبيانات الشخصية بما يواكب تطورات البيئة الرقمية.

وعليه، سيتم التطرق في هذا المبحث إلى المسؤولية المدنية للمعالجة غير مشروعة في المطلب الأول، ثم دراسة الحماية الجزائية للقانون 11-25 المعدل والمتمم في المطلب الثاني.

المطلب الأول: المسؤولية المدنية للمعالجة غير المشروعة

أدى التطور المتسارع للتكنولوجيا الرقمية إلى توسع كبير في عمليات معالجة البيانات الشخصية، وهو ما نتج عنه في المقابل تزايد المخاطر المرتبطة بالاعتداء على الحياة الخاصة للأفراد أو إساءة استعمال معطياتهم الشخصية، ولم تعد الأضرار الناجمة عن المعالجة غير المشروعة تقتصر على الجانب المادي فقط، بل امتدت لتشمل أضراراً معنوية ومعلوماتية قد يصعب أحياناً إثباتها أو تقديرها، الأمر الذي دفع التشريعات الحديثة إلى تطوير قواعد المسؤولية المدنية بما يتلاءم مع خصوصية البيئة الرقمية.

وعليه، سيتم التطرق في هذا المطلب إلى طبيعة المسؤولية المدنية للمعالجة غير المشروعة في الفرع الأول، ثم دراسة خصوصيات الضرر المعلوماتي في الفرع الثاني، ثم دعوى التعويض الضرر في الفرع الثالث .

الفرع الأول: طبيعة المسؤولية المدنية للمعالجة غير المشروعة

تُعد المسؤولية المدنية من أهم الآليات القانونية التي تكفل حماية الأشخاص من الأضرار الناتجة عن الاعتداء على المعطيات ذات الطابع الشخصي، إذ تهدف إلى جبر الضرر الذي يلحق بالشخص المعني نتيجة المعالجة غير المشروعة لبياناته أو استعمالها بصورة مخالفة للقانون، وتبرز أهمية هذه المسؤولية في البيئة الرقمية بالنظر إلى اتساع نطاق تداول البيانات وسهولة نقلها واستغلالها عبر الوسائط الإلكترونية، الأمر الذي يزيد من احتمالات المساس بالحياة الخاصة للأفراد وحقوقهم الأساسية.

وقد اعتمد المشرع الجزائري في تنظيم المسؤولية المدنية عن أضرار المعالجة غير المشروعة على القواعد العامة للمسؤولية المدنية المنصوص عليها في القانون المدني، لاسيما المادة 124 منه، التي تقضي بأن كل فعل يرتكبه الشخص ويسبب ضرراً للغير يلزم مرتكبه بالتعويض، ويستفاد من ذلك أن قيام المسؤولية المدنية في مجال حماية البيانات الشخصية يقتضي توافر أركان الخطأ والضرر والعلاقة السببية بينهما.¹

ويتمثل الخطأ في هذا المجال في كل إخلال بالالتزامات القانونية المفروضة على المسؤول عن المعالجة، كجمع البيانات دون موافقة الشخص المعني، أو استعمالها لغير الغرض الذي جُمعت من أجله، أو الاحتفاظ بها لمدة تتجاوز المدة المسموح بها قانوناً، أو نقلها إلى الغير دون سند مشروع، كما قد يتحقق الخطأ نتيجة الإخلال بالتدابير الأمنية والتقنية المفروضة قانوناً لحماية البيانات من الاختراق أو التسريب أو الوصول غير المشروع إليها.²

ولا يقتصر الضرر الناتج عن انتهاك البيانات الشخصية على الأضرار المادية فقط، بل قد يشمل أضراراً معنوية تمس بالحياة الخاصة أو السمعة أو الاعتبار الشخصي، خاصة في الحالات المتعلقة بتسريب البيانات الصحية أو البنكية أو المعطيات الحساسة، ولهذا اتجه الفقه الحديث إلى

¹ المادة 124 من الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، ج ر ج ج، العدد 78، الصادرة

بتاريخ 30 سبتمبر 1975، المعدل والمتمم.

² المواد 15، 34، 35. قانون رقم 18-07، مصدر سابق..

التوسع في مفهوم الضرر القابل للتعويض ليشمل الأضرار الرقمية والمعلوماتية الناتجة عن انتهاك الخصوصية الإلكترونية.¹

كما يمكن أن تقوم المسؤولية المدنية على أساس عقدي متى وجدت علاقة تعاقدية بين الشخص المعني والجهة القائمة بالمعالجة، كما هو الحال في عقود الاشتراك مع شركات الاتصالات أو المؤسسات البنكية أو المنصات الرقمية، ففي هذه الحالة، يشكل الإخلال بالالتزامات المتعلقة بحماية البيانات إخلالاً بالعقد يترتب مسؤولية تعاقدية توجب التعويض عند تحقق الضرر، ويظهر ذلك مثلاً في حالة قيام مؤسسة مالية باستعمال بيانات زبائنها لأغراض تجارية دون رضاهم، أو نتيجة تسريب معلوماتهم البنكية بسبب ضعف أنظمة الحماية المعلوماتية المعتمدة لديها.²

ويلاحظ أن خصوصية البيئة الرقمية تجعل إثبات الضرر أو العلاقة السببية من المسائل المعقدة عملياً، خاصة في ظل الطابع غير المادي لبعض الأضرار المرتبطة بالبيانات الشخصية ولهذا، اتجهت بعض التشريعات المقارنة إلى التخفيف من عبء الإثبات وتعزيز حماية المتضررين، بالنظر إلى صعوبة تتبع عمليات المعالجة الرقمية وتحديد مصدر الضرر بدقة.³

الفرع الثاني: خصوصية الضرر المعلوماتي

يتميز الضرر الناتج عن انتهاك البيانات الشخصية بخصوصية تجعله مختلفاً عن الأضرار التقليدية المعروفة في نطاق المسؤولية المدنية، ذلك أن الاعتداء على المعطيات ذات الطابع الشخصي لا يترتب عنه دائماً ضرر مادي مباشر يمكن تقديره بسهولة، بل قد ينتج عنه ضرر معلوماتي أو معنوي يمس بالحياة الخاصة للأفراد وحقوقهم الأساسية، ولهذا أصبحت التشريعات

¹ بيومي حجازي عبد الفتاح، مرجع سابق، ص 167.

² حسين منصور محمد، المسؤولية الإلكترونية، مرجع سابق، ص 183.

³ زين العابدين صالح مروة، مرجع سابق، ص 214.

الحديثه تتجه نحو توسيع مفهوم الضرر القابل للتعويض ليشمل مختلف الأضرار المرتبطة بالمساس بالخصوصية الرقمية.

ويظهر الضرر المعلوماتي في صور متعددة، فقد يتمثل في كشف البيانات الصحية أو البنكية أو المعطيات الحساسة دون رضا الشخص المعني، أو في استغلال البيانات لأغراض تجارية أو إشهارية غير مشروعة، أو في المساس بسمعة الشخص واعتباره نتيجة نشر معلوماته الخاصة عبر الوسائط الرقمية، كما قد يتحقق الضرر بمجرد فقدان الشخص سيطرته على بياناته الشخصية، حتى ولو لم يثبت وقوع خسارة مادية مباشرة.¹

وتزداد خطورة هذا النوع من الأضرار في ظل التطور المتسارع للذكاء الاصطناعي وتقنيات التحليل الآلي للبيانات، حيث أصبحت البيانات الشخصية تُستغل في بناء ملفات رقمية دقيقة عن الأفراد، مما قد يؤدي إلى التمييز الإلكتروني أو التأثير على حرية الاختيار واتخاذ القرار، ولهذا لم تعد الحماية القانونية تقتصر على مواجهة الاعتداء المادي على البيانات، بل امتدت لتشمل حماية الحرية المعلوماتية والحق في الخصوصية الرقمية.²

غير أن خصوصية الضرر المعلوماتي تثير عدة صعوبات عملية، خاصة فيما يتعلق بإثبات الضرر والعلاقة السببية بين الخطأ والنتيجة الضارة، فعمليات المعالجة الرقمية غالباً ما تتم بصورة تقنية معقدة يصعب على الشخص المتضرر تتبعها أو إثبات مصدر التسريب أو الاختراق كما أن بعض الأضرار الرقمية قد تظهر آثارها بصورة غير مباشرة أو بعد فترة زمنية طويلة، وهو ما يزيد من تعقيد إثباتها أمام القضاء.³

ومن جهة أخرى، قد يواجه المتضرر صعوبة في إثبات الخطأ التقني المرتبط بالإخلال بواجبات الحماية والأمن المعلوماتي، خاصة عندما يتعلق الأمر بأنظمة إلكترونية معقدة أو

¹ بيومي حجازي عبد الفتاح، مرجع سابق، ص 174.

² Solove, Daniel J., Privacy Law Fundamentals, Op.cit., p. 77.

³ زين العابدين صالح مروة، مرجع لسابق، ص 221.

بمعالجة بيانات تتم عبر خوادم ومنصات رقمية عابرة للحدود، ولهذا اتجهت بعض التشريعات المقارنة إلى تخفيف عبء الإثبات في منازعات البيانات الشخصية، من خلال تحميل المسؤول عن المعالجة جزءاً من عبء إثبات احترامه للالتزامات القانونية والتقنية المفروضة عليه.¹

ويلاحظ أن المشرع الجزائري، رغم تكريسه لحق الشخص المتضرر في المطالبة بالتعويض عن الأضرار الناتجة عن المعالجة غير المشروعة، إلا أن التنظيم القانوني ما يزال بحاجة إلى تطوير القواعد الإجرائية الإثباتية بما يتلاءم مع خصوصية البيئة الرقمية، خاصة في ما يتعلق بالإثبات الإلكتروني والخبرة التقنية وتقدير الأضرار المعلوماتية.²

الفرع الثالث: دعوى التعويض الضرر

تُعد دعوى التعويض من أهم الآليات القضائية التي كرسها القانون لحماية الأشخاص المتضررين من المعالجة غير المشروعة للبيانات الشخصية، إذ تمكّن الشخص المعني من المطالبة بجبر الأضرار التي تلحق به نتيجة الاعتداء على معطياته أو استغلالها بصورة مخالفة للقانون، وتزداد أهمية هذه الدعوى في البيئة الرقمية بالنظر إلى خطورة الأضرار المعلوماتية واتساع نطاق تداول البيانات الشخصية عبر الوسائط الإلكترونية.

غير أن تحديد الجهة القضائية المختصة بالنظر في دعاوى التعويض المرتبطة بالبيانات الشخصية يختلف بحسب الطبيعة القانونية للجهة المتسببة في الضرر، وهو ما يعكس اعتماد المشرع الجزائري على المعيار العضوي في توزيع الاختصاص القضائي بين القضاء العادي والقضاء الإداري.

فإذا كان الضرر ناتجاً عن شخص طبيعي أو معنوي خاضع للقانون الخاص، كشركات الاتصالات أو المؤسسات البنكية أو المنصات الرقمية الخاصة، فإن الاختصاص ينعقد للقضاء

¹Voigt, Paul & von dem Bussche, Axel, Op.cit., p. 145.

²القانون رقم 18-07، مصدر سابق، المواد 64، 65.

العادي باعتباره صاحب الولاية العامة في منازعات المسؤولية المدنية، ويستند ذلك إلى أحكام المادة 124 من القانون المدني الجزائري التي تقضي بإلزام كل من تسبب بخطئه في إحداث ضرر للغير بالتعويض.¹

ويظهر ذلك مثلاً في حالة قيام شركة اتصالات بتسريب بيانات زبائنها أو استعمالها لأغراض تجارية دون موافقتهم، حيث يحق للمتضرر رفع دعوى تعويض أمام الجهات القضائية العادية للمطالبة بجبر الضرر الناتج عن هذا الاعتداء، كما يمكن تأسيس الدعوى في هذه الحالة على المسؤولية العقدية متى وجدت علاقة تعاقدية تربط الشخص المعني بالجهة القائمة بالمعالجة.²

أما إذا كان الضرر صادراً عن الدولة أو الجماعات المحلية أو المؤسسات العمومية ذات الصبغة الإدارية، فإن الاختصاص ينعقد للقضاء الإداري تطبيقاً للمادة 800 من قانون الإجراءات المدنية والإدارية، التي تمنح المحاكم الإدارية صلاحية الفصل في المنازعات التي تكون الإدارة طرفاً فيها. ويقوم هذا الاختصاص على أساس المعيار العضوي المعتمد في التشريع الجزائري.³

وفي هذه الحالة، تخضع المسؤولية لقواعد المسؤولية الإدارية، خاصة على أساس الخطأ المرفقي الناتج عن سوء تنظيم المرفق العام أو الإهمال في تأمين البيانات الشخصية، ومن التطبيقات العملية لذلك، تعرض قاعدة بيانات مستشفى عمومي لاختراق إلكتروني أدى إلى تسريب الملفات الطبية للمرضى، حيث تُرفع دعوى التعويض أمام المحكمة الإدارية بسبب تقصير الإدارة في حماية البيانات الصحية المخزنة ضمن منظومتها المعلوماتية.⁴

¹ المادة 124 من الأمر رقم 75-58، مصدر سابق.

² حسين منصور محمد، مرجع سابق، ص 191.

³ المادة 800 من القانون رقم 08-09 المؤرخ في 25 فبراير 2008، المتضمن قانون الإجراءات المدنية والإدارية، ج ر ج ج، العدد 21، الصادرة بتاريخ 23 أبريل 2008.

⁴ زرقيني راضية، الحماية الجزائية للمعطيات الشخصية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، 2022، ص 233.

كما يثار الإشكال بالنسبة للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، باعتبارها سلطة إدارية مستقلة وفق المادة 22 من القانون رقم 07-18، وهو ما يترتب عليه خضوع قراراتها لرقابة القضاء الإداري، ويقتضي الأمر هنا التمييز بين دعوى الإلغاء ودعوى التعويض؛ فإذا تعلق النزاع بالطعن في قرار إداري صادر عن السلطة الوطنية، كرفض منح ترخيص أو توقيع جزاء إداري، فإن الاختصاص ينعقد لمجلس الدولة باعتباره الجهة المختصة بالنظر في دعاوى الإلغاء الموجهة ضد قرارات السلطات الإدارية المستقلة، وذلك استنادًا إلى المادة 901 من قانون الإجراءات المدنية والإدارية.¹

أما إذا تعلق الأمر بالمطالبة بالتعويض عن الأضرار الناتجة عن نشاط السلطة الوطنية أو عن أحد قراراتها الإدارية، فإن النزاع يدخل ضمن اختصاص المحكمة الإدارية باعتباره من دعاوى القضاء الكامل، ويظهر ذلك مثلاً في حالة رفض منح ترخيص لمعالجة بيانات دون أساس قانوني مشروع، وترتب عن ذلك ضرر مالي للجهة المعنية.²

ويلاحظ أن فعالية دعوى التعويض في مجال البيانات الشخصية تظل مرتبطة بمدى تطوير القواعد الإجرائية والإثباتية بما يتلاءم مع خصوصية البيئة الرقمية، خاصة فيما يتعلق بالإثبات الإلكتروني والخبرة التقنية وصعوبة تحديد مصدر الاختراق أو التسريب المعلوماتي، ولهذا فإن حماية البيانات الشخصية لا تقتصر على تقرير الحق في التعويض، بل تقتضي أيضاً توفير آليات قضائية وتقنية فعالة تكفل ممارسة هذا الحق بصورة عملية وفعالة.³

المطلب الثاني: الحماية الجزائية لقانون 25-11 المعدل والمتمم

أفرز التطور الرقمي تزايداً ملحوظاً في الجرائم المرتبطة بالبيانات الشخصية، الأمر الذي دفع المشرع الجزائري إلى تدعيم الحماية الجزائية لمواجهة مختلف الأفعال التي تمس بسرية

¹ المادة 22 من القانون رقم 07-18، مصدر سابق والمادة 901 من القانون رقم 08-09، مصدر سابق.

² كحالوي عبد الهادي، مرجع سابق، ص 247.

³ بوخالفة فيصل، مرجع سابق، ص 107.

وسلامة المعطيات ذات الطابع الشخصي، ولم تعد الاعتداءات المرتبطة بالبيانات تقتصر على صور الاختراق أو التسريب التقليدية، بل امتدت لتشمل أنماطاً جديدة ترتبط بالمعالجة الآلية والذكاء الاصطناعي ونقل البيانات عبر الأنظمة الرقمية العابرة للحدود.

ولهذا، تضمن القانون رقم 07-18 المعدل والمتمم بالقانون رقم 11-25 مجموعة من النصوص التي تجرم المعالجة غير المشروعة للبيانات الشخصية، مع تشديد العقوبات المسؤولية الجزائية بما يتلاءم مع خصوصية البيئة الرقمية الحديثة.¹

وعليه، سيتم التطرق في هذا المطلب إلى التجريم والعقاب على انتهاك سرية المعطيات في الفرع الأول، ثم دراسة الجرائم المستحدثة في ظل الرقمنة في الفرع الثاني، وأخيراً بيان تشديد العقوبات المسؤولية الجزائية للشخص المعنوي في الفرع الثالث.

الفرع الأول: التجريم انتهاك سرية المعطيات

تُعد سرية وسلامة البيانات الشخصية من المبادئ الأساسية التي يقوم عليها نظام الحماية القانونية للمعطيات ذات الطابع الشخصي، ذلك أن أي اعتداء على هذه البيانات قد يؤدي إلى المساس بالحياة الخاصة للأفراد وحقوقهم وحررياتهم الأساسية، ولهذا اتجهت التشريعات الحديثة إلى إقرار حماية جزائية خاصة لمواجهة مختلف الأفعال التي تستهدف البيانات الشخصية، سواء تعلق الأمر بالكشف غير المشروع عنها، أو تعديلها، أو إتلافها، أو الوصول إليها دون ترخيص.

وقد كرس المشرع الجزائري هذا التوجه من خلال القانون رقم 07-18 المعدل والمتمم بالقانون رقم 11-25، حيث جرم مختلف صور المعالجة غير المشروعة للبيانات الشخصية، وقرر لها عقوبات جزائية تهدف إلى ردع الاعتداءات الواقعة على المعطيات ذات الطابع الشخصي. ويستفاد من أحكام هذا القانون أن الحماية الجزائية لا تقتصر على حماية البيانات في

¹ المواد 66 وما بعدها من القانون رقم 11-25، مصدر سابق.

حد ذاتها، بل تمتد كذلك إلى حماية حق الأفراد في الخصوصية المعلوماتية وضمان احترام الضوابط القانونية المنظمة للمعالجة.¹

ويتحقق الفعل الإجرامي في هذا المجال من خلال عدة صور، من بينها جمع البيانات الشخصية أو معالجتها دون موافقة الشخص المعني أو دون سند قانوني مشروع، أو استعمالها لأغراض مخالفة للغرض الذي جُمعت من أجله، أو الاحتفاظ بها لمدة تتجاوز الحدود المقررة قانونًا، كما تشمل الأفعال المجرمة إفشاء البيانات أو تمكين الغير من الاطلاع عليها بصورة غير مشروعة، خاصة إذا تعلق الأمر بالمعطيات الحساسة كالبيانات الصحية أو البيومترية أو المعلومات المرتبطة بالحياة الخاصة للأفراد،² كما جرم المشرع الأفعال المرتبطة بالإخلال بسلامة البيانات الشخصية، كإتلافها أو تعديلها أو حذفها أو تعطيل الوصول إليها بطرق غير مشروعة، لما قد يترتب عن ذلك من أضرار تمس بالأشخاص المعنيين أو تعرقل سلامة الأنظمة المعلوماتية.

وتزداد خطورة هذه الأفعال عندما ترتكب باستعمال وسائل تقنية متطورة أو في إطار هجمات إلكترونية تستهدف قواعد البيانات والمنصات الرقمية،³ ويلاحظ أن المشرع الجزائري حاول من خلال القانون رقم 11-25 تعزيز الحماية الجزائية للبيانات الشخصية عبر توسيع نطاق التجريم وتشديد العقوبات في بعض الحالات، خاصة عندما يتعلق الأمر بالمعالجة واسعة النطاق أو بالبيانات الحساسة أو بالأفعال التي تمس بعدد كبير من الأشخاص، وهو ما يعكس إدراكًا متزايدًا لخطورة الجرائم الرقمية وآثارها على الأمن المعلوماتي والحياة الخاصة للأفراد.⁴

¹ المواد 66 وما بعدها القانون رقم 18-07، مصدر سابق.

² زرقيني راضية، مرجع سابق، ص 254.

³ بن حمو محمد، "الحماية الجزائية للبيانات الشخصية في التشريع الجزائري"، مجلة الدراسات القانونية المقارنة، جامعة تلمسان،

العدد 02، 2023، ص 101.

⁴ المادة 72 مكرر من القانون رقم 11-25، مصدر سابق..

كما تتميز الجرائم المرتبطة بالبيانات الشخصية بطابع تقني خاص، إذ غالبًا ما ترتكب عبر أنظمة معلوماتية أو شبكات إلكترونية معقدة، الأمر الذي يثير صعوبات عملية في مجال الإثبات والكشف عن الجناة وتحديد الاختصاص القضائي، خاصة في الحالات التي تتجاوز فيها عمليات المعالجة الحدود الإقليمية للدولة ولهذا، أصبحت الحماية الجزائية للبيانات الشخصية مرتبطة بصورة وثيقة بمدى تطوير وسائل التحقيق الرقمي والخبرة التقنية وآليات التعاون الدولي في مواجهة الجرائم المعلوماتية.¹

ومن ثم، فإن التجريم والعقاب على انتهاك سرية وسلامة البيانات الشخصية يمثلان ركيزة أساسية لحماية الخصوصية الرقمية، غير أن فعالية هذه الحماية تبقى رهينة بمدى تطوير الإطار القانوني والتقني بما يواكب التحولات المتسارعة للبيئة الرقمية الحديثة.

الفرع الثاني: الجرائم المستحدثة في ظل الرقمنة

ومن أبرز الجرائم المستحدثة في هذا المجال جريمة نقل البيانات الشخصية إلى الخارج دون ترخيص أو دون توفر مستوى كافٍ من الحماية القانونية في الدولة المستقبلة للبيانات. وتكمن خطورة هذه الجريمة في أن نقل البيانات إلى جهات أجنبية قد يؤدي إلى فقدان السيطرة عليها أو إخضاعها لأنظمة قانونية لا توفر الضمانات الكافية لحماية الخصوصية، ولهذا قيد المشرع الجزائري عمليات نقل البيانات عبر الحدود بجملة من الشروط والضوابط القانونية، مع تجريم حالات النقل غير المشروع للمعطيات الشخصية،² وبرزت جرائم مرتبطة بالمعالجة الآلية واتخاذ القرارات الخوارزمية دون احترام حقوق الأشخاص المعنيين بالبيانات، خاصة في ظل استخدام أنظمة الذكاء الاصطناعي لتحليل البيانات الشخصية وتصنيف الأفراد بصورة آلية. وقد يؤدي هذا

¹ بوزيد آسيا، "الذكاء الاصطناعي وإشكالية المسؤولية الجزائية"، مجلة الفكر القانوني والسياسي، جامعة بسكرة، العدد 01، 2024، ص 74.

² المواد 44 إلى 47 من القانون رقم 18-07، مصدر سابق.

النوع من المعالجة إلى المساس بمبدأ الشفافية أو إلى التمييز الإلكتروني القائم على تحليل البيانات الحساسة، الأمر الذي يثير مخاطر قانونية متزايدة تتعلق بحماية الحقوق الرقمية للأفراد.¹

ومن الجرائم المستحدثة كذلك الأفعال التي تستهدف عرقلة عمل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أو الامتناع عن تنفيذ أوامرها وقراراتها، لما لذلك من تأثير مباشر على فعالية النظام الرقابي المكلف بحماية البيانات الشخصية. ويعكس هذا التجريم إدراك المشرع لأهمية الدور الذي تؤديه السلطة الوطنية في ضمان احترام القواعد القانونية المنظمة لمعالجة البيانات،² كما تزداد خطورة الجرائم المرتبطة بالبيانات الشخصية عندما ترتكب في إطار المعالجة واسعة النطاق أو باستعمال تقنيات متطورة يصعب تتبعها، خاصة مع اعتماد بعض المؤسسات على خوادم إلكترونية موزعة عبر عدة دول أو على تطبيقات رقمية تعتمد على التحليل الضخم للبيانات. ويؤدي ذلك إلى تعقيد عملية الكشف عن الجناة وتحديد القانون الواجب التطبيق والجهة القضائية المختصة،³

ويلاحظ أن المشرع الجزائري حاول مواكبة هذه التطورات من خلال تدعيم السياسة الجزائية المتعلقة بحماية البيانات الشخصية، غير أن بعض الجرائم المستحدثة المرتبطة بالذكاء الاصطناعي والمعالجة الخوارزمية ما تزال بحاجة إلى تنظيم أكثر تفصيلاً، خاصة في ظل التطور السريع للتقنيات الرقمية وصعوبة إخضاعها للقواعد التقليدية للمسؤولية الجزائية،⁴ ومن ثم، فإن مواجهة الجرائم المستحدثة المرتبطة بالمعالجة الرقمية للبيانات الشخصية لم تعد تقتصر على سن النصوص العقابية فقط، بل أصبحت تقتضي تطوير آليات التحقيق الرقمي، وتعزيز التعاون الدولي، وتوفير خبرات تقنية متخصصة قادرة على مواكبة الطبيعة المعقدة للجرائم المعلوماتية الحديثة.

¹بوزيد آسيا، مرجع سابق، ص 76.

²ال المادة 70 مكرر من القانون رقم 25-11، مصدر سابق.

³بن حمو محمد، مرجع سابق، ص 96.

⁴زرقيني راضية، مرجع سابق، ص 276.

الفرع الثالث: تشديد العقوبات المسؤولية الجزائية للشخص المعنوي

لم تعد الجرائم المرتبطة بالبيانات الشخصية تُرتكب فقط من طرف الأفراد، بل أصبحت في كثير من الأحيان مرتبطة بالمؤسسات والشركات التي تتولى جمع البيانات ومعالجتها واستغلالها ضمن أنشطة رقمية واسعة النطاق، ولهذا، لم يعد من الكافي الاكتفاء بالعقوبات التقليدية الموجهة للأشخاص الطبيعيين، بل أصبح من الضروري توسيع نطاق المسؤولية الجزائية ليشمل الأشخاص المعنوية كذلك، بالنظر إلى الدور الكبير الذي تؤديه في مجال معالجة البيانات الشخصية.

وفي هذا الإطار، اتجه المشرع الجزائري إلى تشديد العقوبات المقررة لبعض الجرائم المرتبطة بالمعطيات ذات الطابع الشخصي، خاصة عندما يتعلق الأمر بالبيانات الحساسة أو بالمعالجة التي تمس عددًا كبيرًا من الأشخاص، ويظهر هذا التشديد من خلال رفع قيمة الغرامات المالية، وتشديد العقوبات السالبة للحرية في بعض الحالات التي تتسم بخطورة خاصة أو يترتب عنها ضرر جسيم بالأشخاص المعنويين بالبيانات.¹

كما لم يقتصر الأمر على العقوبات الأصلية فقط، بل أجاز المشرع توقيع عقوبات تكميلية قد تكون أكثر تأثيرًا بالنسبة للمؤسسات المخالفة، مثل غلق المؤسسة أو وقف نشاط المعالجة أو مصادرة الوسائل المستعملة في ارتكاب الجريمة، ويعكس هذا التوجه رغبة واضحة في دفع الهيئات والمؤسسات إلى احترام قواعد حماية البيانات وعدم التعامل مع العقوبات المالية باعتبارها مجرد أعباء ثانوية يمكن تجاوزها.²

ومن جهة أخرى، يلاحظ أن المسؤولية الجزائية للشخص المعنوي تكتسي أهمية خاصة في مجال الجرائم الرقمية، لأن أغلب عمليات المعالجة تتم داخل شركات وهيئات تعتمد على أنظمة معلوماتية معقدة، وقد يكون الانتهاك ناتجًا عن سياسة داخلية أو عن إهمال مؤسسي في تأمين

¹ ال المادة 72 مكرر من القانون رقم 11-25، مصدر سابق.

² المواد 72.71 من القانون رقم 07-18، مصدر سابق.

البيانات الشخصية، ولهذا أصبح من المنطقي مساءلة الشخص المعنوي متى ثبت أن الجريمة ارتكبت باسمه أو لفائدته أو نتيجة تقصير في الالتزامات المفروضة عليه قانوناً¹

ويظهر ذلك مثلاً في حالة قيام شركة رقمية باستغلال بيانات المستخدمين دون موافقتهم لأغراض تجارية أو إشهارية، أو في حالة إهمال مؤسسة مالية في حماية قواعد بياناتها مما يؤدي إلى تسريب المعلومات البنكية للزبائن. ففي مثل هذه الحالات، لا يقتصر الضرر على الأفراد المتضررين فقط، بل قد يمتد إلى زعزعة الثقة في البيئة الرقمية والمعاملات الإلكترونية ككل، ورغم أهمية هذا التشديد في تعزيز الحماية الجزائية للبيانات الشخصية، إلا أن فعالية السياسة العقابية تبقى مرتبطة بمدى قدرة السلطات المختصة على الكشف عن الجرائم الرقمية وإثباتها، خاصة في ظل الطبيعة التقنية المعقدة لبعض أنظمة المعالجة الحديثة، واعتماد بعض المؤسسات على تقنيات الذكاء الاصطناعي والخوادم العابرة للحدود.

ولهذا، فإن تطوير الحماية الجزائية للبيانات الشخصية يقتضي إلى جانب النصوص العقابية توفير وسائل تقنية وبشرية متخصصة قادرة على مواكبة التحولات المتسارعة للبيئة الرقمية².

¹قادري عبد الكريم، مرجع سابق، ص 133.

²بن حمو محمد، مرجع سابق، ص 104.

خلاصة الفصل

يتضح من خلال هذا الفصل أن الحماية الفعلية للبيانات الشخصية لا تتحقق بمجرد الاعتراف بالحقوق الرقمية أو تنظيم عمليات المعالجة، وإنما تقتضي تدعيمها بآليات رقابية ومؤسسية فعالة، إلى جانب إقرار نظام قانوني للمساءلة يضمن ردع مختلف الاعتداءات التي قد تمس بالبيانات الشخصية.

ولهذا، سعى المشرع الجزائري، من خلال القانون رقم 18-07 المعدل والمتمم بالقانون رقم 25-11، إلى تعزيز المنظومة الرقابية عبر تدعيم دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، واستحداث آليات جديدة تقوم على الرقابة الداخلية والامتثال الذاتي.

كما تبين أن المشرع اتجه إلى تكريس حماية مدنية وجزائية للبيانات الشخصية، من خلال تمكين الأشخاص المتضررين من المطالبة بالتعويض عن الأضرار الناتجة عن المعالجة غير المشروعة، إلى جانب تجريم الأفعال التي تمس بسرية وسلامة البيانات الشخصية، وتشديد العقوبات في بعض الجرائم المرتبطة بالمعالجة الرقمية.

غير أن الدراسة كشفت في المقابل عن وجود بعض النقائص العملية والتشريعية، خاصة ما يتعلق بصعوبة إثبات الضرر المعلوماتي، ومحدودية التنظيم القانوني لبعض الإشكالات المرتبطة بالذكاء الاصطناعي والمعالجة الخوارزمية، فضلاً عن التحديات التي تطرحها المعالجة العابرة للحدود، وهو ما يبرز حاجة التشريع الجزائري إلى مزيد من التطوير لمواكبة التحولات الرقمية المتسارعة وتعزيز فعالية حماية البيانات الشخصية في البيئة الإلكترونية الحديثة.

خاتمة

الخاتمة:

أصبحت حماية البيانات الشخصية من أبرز الإشكالات القانونية التي فرضتها التحولات الرقمية الحديثة، خاصة في ظل التوسع المتزايد لاستخدام الوسائل الإلكترونية والاعتماد المكثف على تقنيات الذكاء الاصطناعي والمعالجة الآلية للبيانات، فلم تعد البيانات الشخصية مجرد معطيات ذات طابع تقني، بل أضحت تمثل عنصراً أساسياً من عناصر الحياة الخاصة والهوية الرقمية للأفراد، الأمر الذي جعل حمايتها ضرورة قانونية وحقوقية تفرضها متطلبات العصر الرقمي.

ومن خلال هذه الدراسة، تبين أن المشرع الجزائري سعى إلى بناء إطار قانوني لحماية البيانات الشخصية، من خلال القانون رقم 07-18 المعدل والمتمم بالقانون رقم 25-11، حيث حاول تكريس مجموعة من المبادئ والضوابط القانونية المنظمة لعمليات المعالجة، مع إقرار حقوق رقمية لفائدة الشخص المعني بالبيانات، إلى جانب تدعيم آليات الرقابة والمسؤولية القانونية لمواجهة مختلف الانتهاكات التي قد تمس بسرية وسلامة المعطيات الشخصية.

كما أظهرت الدراسة أن المشرع الجزائري تأثر بصورة واضحة بالتوجهات الحديثة في التشريعات المقارنة، خاصة الأوروبية، سواء من حيث توسيع نطاق البيانات المشمولة بالحماية، أو من خلال استحداث آليات جديدة كمندوب حماية المعطيات، وسجل نشاطات المعالجة، والامتثال الذاتي، فضلاً عن تشديد الحماية الجزائية في مواجهة الجرائم المرتبطة بالبيانات الشخصية.

غير أن الدراسة كشفت في المقابل عن وجود بعض النقائص التي قد تحد من فعالية الحماية القانونية المقررة، خاصة في ظل التطور السريع للتقنيات الرقمية فالتشريع الجزائري، و رغم أهميته لا يزال بحاجة إلى مزيد من التطوير لمواكبة الإشكالات المستحدثة المرتبطة بالمعالجة

خاتمة

الخوارزمية والذكاء الاصطناعي والبيانات الضخمة، إضافة إلى ضرورة تدعيم آليات الرقابة والإثبات الرقمي وتعزيز التعاون الدولي في مجال حماية البيانات العابرة للحدود.

وانطلاقاً من ذلك، يمكن تسجيل أهم النتائج التي توصلت إليها الدراسة فيما يأتي:

1. تبني المشرع الجزائري مفهوماً واسعاً للبيانات الشخصية، بما يشمل البيانات الحساسة والبيومترية والجينية .

2. كرس القانون مجموعة من المبادئ القانونية المنظمة لمشروعية المعالجة، أهمها الرضائية والشفافية وتحديد الغرض .

3. عزز المشرع الحقوق الرقمية للشخص المعني بالبيانات، خاصة حق النفاذ والتصحيح والمحو والاعتراض .

4. استحدث القانون رقم 11-25 آليات جديدة للرقابة والامتثال، كمنصب مندوب حماية المعطيات وسجل نشاطات المعالجة .

5. اعتمد المشرع حماية مدنية وجزائية للبيانات الشخصية، مع تشديد العقوبات في بعض الجرائم الرقمية .

6. لا يزال التنظيم الجزائري يواجه بعض الصعوبات المرتبطة بالإثبات الرقمي ومواكبة تقنيات الذكاء الاصطناعي والمعالجة الآلية .

وبناءً على هذه النتائج، يمكن اقتراح جملة من التوصيات، من أهمها:

1. ضرورة مراجعة بعض أحكام القانون رقم 07-18 بما يواكب التطورات الحديثة في مجال الذكاء الاصطناعي والبيانات الضخمة .

خاتمة

2. تدعيم صلاحيات السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي وتوفير الإمكانيات التقنية والبشرية اللازمة لها .
 3. وضع تنظيم قانوني أكثر تفصيلاً للمعالجة الخوارزمية والقرارات الآلية .
 4. تعزيز التعاون الدولي في مجال مكافحة الجرائم المرتبطة بالبيانات الشخصية والمعالجة العابرة للحدود .
 5. نشر الثقافة القانونية الرقمية داخل المؤسسات والأوساط الاجتماعية، بما يضمن احترام قواعد حماية البيانات الشخصية .
 6. تكوين قضاة وخبراء متخصصين في المنازعات الرقمية والجرائم المعلوماتية .
- وفي الأخير، يمكن القول إن حماية البيانات الشخصية أصبحت من أهم التحديات القانونية التي تفرضها البيئة الرقمية الحديثة، وأن فعالية هذه الحماية لم تعد ترتبط فقط بوجود النصوص القانونية، بل بمدى قدرة التشريعات والآليات المؤسساتية على مواكبة التحولات التكنولوجية المتسارعة وتحقيق التوازن بين التطور الرقمي وحماية الحقوق والحريات الأساسية للأفراد.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أ- المصادر

أولا : النصوص القانونية

الأوامر

1. الأمر رقم 58-75 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني الجزائري، الجريدة الرسمية للجمهورية الجزائرية، العدد 78، الصادرة بتاريخ 30 سبتمبر 1975 .
2. الأمر رقم 09-08 المؤرخ في 25 فبراير 2008، المتضمن قانون الإجراءات المدنية والإدارية، الجريدة الرسمية للجمهورية الجزائرية، العدد 21، الصادرة بتاريخ 23 أبريل 2008 .

القوانين

1. القانون رقم 07-18 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادرة بتاريخ 10 يونيو 2018 .
2. القانون رقم 11-25 المؤرخ في 24 يوليو 2025، المعدل والمتمم للقانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 48، الصادرة بتاريخ 29 يوليو 2025 .
3. القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق ل 05 اوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال

والاتصال

ب- المراجع

- الكتب العربية

1. بيومي حجازي، عبد الفتاح، الحق في الخصوصية والمسؤولية المدنية في عصر الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2019 .

قائمة المصادر والمراجع

2. جميعي حسن عبد الباسط، حماية الخصوصية في مواجهة نظم المعلومات الحديثة، دار الفكر الجامعي، الإسكندرية، مصر، 2020 .
3. حسين منصور، محمد، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2021 .
4. الشوا، سامي، المسؤولية المدنية عن الاعتداء على البيانات الشخصية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2022 .
5. صقر نبيل، جرائم الإعلام الآلي في التشريع الجزائري، دار الهدى، عين مليلة، الجزائر، 2020 .
6. عبد الظاهر، أحمد، الحماية الجنائية للبيانات الشخصية عبر الإنترنت، دار النهضة العربية، القاهرة، مصر، 2021 .
- 7.

ثالثا: البحوث الجامعية

- أطروحات الدكتوراه

- 1- زرقيني راضية، الحماية الجزائية للمعطيات الشخصية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، 2022 .
- 2- زين العابدين صالح مروة، الحماية القانونية للبيانات الشخصية عبر الإنترنت، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2021 .
- 3- كحالوي عبد الهادي، الحماية القانونية للبيانات الشخصية في التشريع الجزائري، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، 2022 .

- مذكرات الماستر

- 1- بوعزيز خليفة، حماية المعطيات الشخصية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2021 .

قائمة المصادر والمراجع

- 2- علالي حميمة، الحماية الجنائية للمعطيات الشخصية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2019 .

رابعاً: المقالات العلمية

1. أمينة مسياد، "آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون 07-18"، مجلة الباحث، جامعة سوق أهراس، العدد 05، 2021 .
2. بوزيد آسيا، "الذكاء الاصطناعي وإشكالية المسؤولية الجزائية"، مجلة الفكر القانوني والسياسي، جامعة بسكرة، العدد 01، 2024 .
3. بوسماحة محمد الأمين، "حماية المعطيات الشخصية في البيئة الرقمية"، مجلة الباحث للدراسات القانونية، جامعة باتنة، العدد 01، 2024 .
4. بوخالفة فيصل، "حماية المعطيات ذات الطابع الشخصي بين النصوص التقليدية والتحديات الرقمية"، مجلة الدراسات القانونية، العدد 03، 2023 .
5. بن حمو محمد، "الحماية الجزائية للبيانات الشخصية في التشريع الجزائري"، مجلة الدراسات القانونية المقارنة، جامعة تلمسان، العدد 02، 2023 .
6. تبينة حكيم، "السلطات الإدارية المستقلة ودورها في حماية البيانات الشخصية"، مجلة الحقوق، جامعة الجزائر، العدد 02، 2021 .
7. بوعلام عبد القادر، "حماية البيانات الشخصية في ظل التحول الرقمي"، مجلة الدراسات القانونية، جامعة الجزائر 1، العدد 03، 2023 .
8. قادري عبد الكريم، "المسؤولية الجزائية للشخص المعنوي في الجرائم المعلوماتية"، مجلة العلوم القانونية والسياسية، جامعة الأغواط، العدد 02، 2023 .
9. محمود عمر مؤيد، "الحماية القانونية للبيانات الشخصية في ظل التشريعات الرقمية الحديثة"، مجلة Gateway Journal، العدد 04، 2025 .

قائمة المصادر والمراجع

10. عبد الله محمد، "الحماية القانونية للبيانات الشخصية في البيئة الرقمية"، مجلة القانون الرقمي، جامعة الجزائر 1، العدد 02، 2024.
11. مفيدة مباركية، "الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري"، مجلة الشريعة والاقتصاد، جامعة قسنطينة، العدد 13، 2018.

خامسا: المواقع الإلكترونية

1. السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، "القانون رقم 25-11 المعدل والمتمم للقانون 07-18"، متاح على الرابط: [الموقع الرسمي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي](#) تاريخ الاطلاع: 01 ماي 2026 .
2. [بوابة المجلات العلمية الجزائرية ASJP](#) تاريخ الاطلاع: 05 ماي 2026 .
3. [منصة ResearchGate](#) تاريخ الاطلاع: 06 ماي 2026 .

سادسا: المراجع الأجنبية

1. Alessandro Mantelero, "AI and Personal Data Protection", Computer Law & Security Review, 2024, p. 21.
2. Christopher Kuner, Transborder Data Flows and Data Privacy Law, Oxford University Press, Oxford, 2023.
3. Daniel J. Solove, Privacy Law Fundamentals, International Association of Privacy Professionals (IAPP), New Hampshire, 2024.
4. European Data Protection Board (EDPB), Guidelines on Consent under GDPR, 2023, p. 08.
5. Paul Voigt & Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, Cham, 2023.

فهرس المحتويات

فهرس المحتويات

رقم الصفحة	الموضوع
	شكر وعرفان
	إهداء
أ-ز	المقدمة
الفصل الأول: النظام الموضوعي للحماية نطاق المعالجة الحقوق المستحدثة	
9	تمهيد
10	المبحث الأول: مفهوم القانوني للمعطيات الشخصية مع ضوابط مشروعيتها
10	المطلب الأول: تصنيف المعطيات المحمية بعد تعديل القانون 11-25
16	المطلب الثاني: قواعد المنظمة لمشروعية معالجة البيانات
23	المبحث الثاني: المركز القانوني لأطراف المعالجة البيانات
23	المطلب الأول: الحقوق الرقمية للشخص المعني
28	المطلب الثاني: التزامات المتدخلين في المعالجة البيانات
34	ملخص الفصل
الفصل الثاني: الضمانات المؤسساتية والجزائية	
36	تمهيد
37	المبحث الأول: الآليات الرقابية المؤسساتية
37	المطلب الأول: الرقابة الداخلية
42	المطلب الثاني: الرقابة الخارجية
49	المبحث الثاني: المسؤولية القانونية للمشرع الجزائري
49	المطلب الأول: المسؤولية المدنية للمعالجة غير المشروعة
56	المطلب الثاني: الحماية الجزائية لقانون 11-25 المعدل والمتمم
64	خلاصة الفصل
66	الخاتمة
70	قائمة المصادر والمراجع

فهرس المحتويات

75	فهرسة المحتويات
78	الملخص

المخلص

الملخص:

تهدف هذه الدراسة إلى بيان مدى فعالية الحماية القانونية للبيانات الشخصية في ظل القانون رقم 07-18 المعدل والمتمم بالقانون رقم 11-25، وذلك من خلال تحليل الإطار القانوني المنظم لمعالجة البيانات الشخصية، والحقوق الرقمية المقررة للأشخاص المعنيين بالبيانات، إضافة إلى دراسة آليات الرقابة والمسؤولية المدنية والجزائية المرتبطة بحماية البيانات الشخصية في البيئة الرقمية.

وقد توصلت الدراسة إلى أن المشرع الجزائري سعى إلى مواكبة التطورات الرقمية الحديثة من خلال تدعيم الحماية القانونية للبيانات الشخصية، غير أن بعض التحديات لا تزال مطروحة، خاصة ما يتعلق بالذكاء الاصطناعي والمعالجة الخوارزمية والبيانات العابرة للحدود.

الكلمات المفتاحية:

البيانات الشخصية، الحماية القانونية، المعالجة الرقمية، الخصوصية، القانون 11-25، الذكاء الاصطناعي.

Abstract

This study aims to examine the effectiveness of the legal protection of personal data under Algerian Law No. 18-07 as amended and supplemented by Law No. 25-11. It analyzes the legal framework governing personal data processing, the digital rights granted to data subjects, as well as the institutional, civil, and criminal protection mechanisms related to personal data in the digital environment.

The study concludes that the Algerian legislator has attempted to adapt to modern digital developments by strengthening the legal protection of personal data. However, several challenges remain, particularly those related to artificial intelligence, algorithmic processing, and cross-border data transfers.

Keywords:

Personal Data, Legal Protection, Digital Processing, Privacy, Law No. 25-11, Artificial Intelligence.
Legal Regulation.