الجمهورية الجزائرية الديمقراطية الشّعبية
وزارة التّعليم العالي والبحث العلمي
جامعة الشاذلي بن جديد – الطـــارف –
كلية الحقوق والعلوم السياسية
قسم الحقوق

حماية البيانات الشخصية في ظل الادارة الالكترونية

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص: قانون عام معمق

من إعداد الطالبتين:

- عبير سدور
- بلقيس هميسي

إشراف الدكتورة:

كريمة أمزيان

لجنة المناقشة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
زيد الخيل توفيق	أستاذ محاضر–أ–	جامعة الشتذلي بن جديد –الطارف	رئيساً
أمزيان كريمة	أستاذ مساعد–أ–	جامعة الشتذلي بن جديد –الطارف	مشرفًا
العمري زقار منية	أستاذ محاضر–ب–	جامعة الشتذلي بن جديد –الطارف	ممتحنًا

السنة الجامعية: 2024 / 2025

الجمهورية الجزائرية الديمقراطية الشّعبية
وزارة التّعليم العالي والبحث العلمي
جامعة الشاذلي بن جديد – الطـــارف –
كلية الحقوق والعلوم السياسية
قسم الحقوق

حماية البيانات الشخصية في ظل الادارة الالكترونية

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص: قانون عام معمق

من إعداد الطالبتين:
- عبير سدور
- بلقيس هميسي

إشراف الدكتورة:
كريمة أمزيان

لجنة المناقشة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
زيد الخيل توفيق	أستاذ محاضر–أ–	جامعة الشتذلي بن جديد –الطارف	رئيساً
أمزيان كريمة	أستاذ مساعد–أ–	جامعة الشتذلي بن جديد –الطارف	مشرفًا
العمري زقار منية	أستاذ محاضر–ب–	جامعة الشتذلي بن جديد –الطارف	ممتحنًا

السنة الجامعية: 2024 / 2025

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

جامعة الشاذلي بن جديد
UNIVERSITE CHADLI BENDJEDID

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): .....سدور عبير.....

الحامل لبطاقة التعريف الوطنية رقم: .....110011241008280004.....

الصادرة بتاريخ: .....2026/06/29.....

عن دائرة: ....الطارف.....

المسجل بقسم: .....حقوق.....

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

حماية البيانات الشخصية في ظل الادارة الالكترونية.

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025/06./12

إمضاء المعني

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

جامعة الشاذلي بن جديد
UNIVERSITE CHADLI BENDJEDID

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): .....هميسي بلقيس.....

الحامل لبطاقة التعريف الوطنية رقم: .....110011245002410004.....

الصادرة بتاريخ: .....2024/03/16.....

عن دائرة: .....بوحجار بلدية عين الكرمة.....

المسجل بقسم: .....حقوق.....

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

حماية البيانات الشخصية في ظل الادارة الالكترونية

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025/06/12

إمضاء المعني


بسم الله الرحمن الرحيم

شكر وتقدير

قبل كل أحد وبعد كل أحد، الشكر للواحد الأحد، الفرد الصمد، الذي أمدّنا بالقوة والعون والسداد لإنجاز هذا العمل، وندعوه عز وجل أن يجعله خالصًا لوجهه الكريم.

كما نتقدم بالشكر الجزيل للأستاذة المشرفة كريمة أمزيان، التي لم تبخل علينا بأي معلومة أو توضيح في شتى مراحل إعداد هذه المذكرة، فجزاك الله خيرًا.

كما نتوجه بالشكر لأعضاء لجنة المناقشة، أساتذتنا بقسم الحقوق، على المجهودات المبذولة لإيصالنا إلى ما نحن عليه.

الإهداء

إلى كل من كلّل العرق جبينه، ومن علّمني أن النجاح لا يأتي إلا بالصبر والإصرار.

إلى النور الذي أنار دربي، والسراج الذي لا ينطفئ نوره في قلبي أبدًا، من بذل الغالي والنفيس، فاستمددت منه قوتي واعتزازي بذاتي: والدي العزيز سدور العياشي.

إلى من جعل الجنة تحت أقدامها، وسهّلت الشدائد بدعائها، إلى الإنسانة العظيمة التي طالما تمنّيت أن أقرّ عينيها في يومي هذا: أمي الغالية عقاب عريفة.

إلى ضلعي الثابت وأمان أيامي، إلى من شددت عضدي بهم فكانوا ينابيع أرتوي منها من خبرة أمي وصفوتها.

إلى قرة عيني: سامي، أسامة، رانيا، نور، رودينة.

ولكل من كان عونًا وسندًا في هذا الطريق، للأصدقاء الأوفياء: خولة، ندى.

كما أشير إلى زميلتي في هذا البحث: بلقيس.

فالحمد لله شكرًا وحبًا وامتنانًا على البدء والختام، وآخر دعوانا أن الحمد لله رب العالمين.

عبير

الإهداء

الحمد لله وكفى، والصلاة على المصطفى وآله ومن وفى، أما بعد:

إلى التي بحنانها ارتويت، وبدفئها احتميت، ولحقها ما وفيت، إلا من يشتهي اللسان نطقها، إلى من كانت تتمنى رؤيتي وأنا أحقق هذا النجاح، ويشاء الله أن يأتي هذا اليوم: أمي الغالية، حفظها الله.

إلى من شق لي بحر العلم والتعلم، إلى من احترقت كالشمعة لتُضيء دروب النجاح، ركيزة عمري، كبريائك، وكرامتك: أبي، أطال الله في عمره.

إلى رفيق الدرب وصديق الأيام، حاميها بحلوها ومرّها، طالما كان الداعم الأكبر في كل شيء: زوجي الغالي، فشكرًا كثيرًا على ثقتك بنجاحي ودفعك لي نحو الأفضل.

إلى من حلّت بركة وجوده في حياتي، ومن ملأت ضحكاته الجميلة عمري، إلى زينة حياتي وبهجتها، والطفولة التي ملأت عالمي وأبهجت شوارحي: إلى عيون ابني الغالي.

إلى من ساندوا خطاي المتعثرة، ومن يؤمنون بي حين يخذلني الجميع، إلى سندي وقوتي وملاذي: إخوتي.

إلى من كانت لها بالغ الأثر في كثير من العقبات والصعاب، من ساندتني، صاحبة الكلمة التي سارت بي نحو النجاح: أم زوجي، أمي الثانية.

كما لا أنسى بالذكر زميلتي في هذا العمل: سدور عبير، أهديهم جميعًا هذا البحث

بلقيس.

مقدّمة

في ظل الثورة الرقمية التي يشهدها العالم، أصبحت الإدارة الإلكترونية خيارا استراتيجيا تبنته العديد من الدول، بما فيها الجزائر، من أجل تحسين جودة الخدمات العمومية، وتقريب الإدارة من المواطن، وتطوير أساليب المرافق العامة. وقد رافق هذا التحول الجذري اعتماد تقنيات حديثة لمعالجة البيانات والمعلومات، والتي تشمل في كثير من الأحيان بيانات شخصية حساسة تتعلق بهوية الأفراد وحياتهم الخاصة. ونظرا لما تتيحه هذه المعطيات من فرص للاستغلال غير المشروع أو المساس بحرمة الحياة الخاصة، أصبح من الضروري توفير إطار قانوني وتنظيمي يحمي هذه البيانات ويضمن معالجتها في ظل احترام حقوق وحريات الأفراد.

وفي هذا الإطار جاء القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي ليشكل خطوة هامة في مسار تعزيز حماية الخصوصية الرقمية في الجزائر، خاصة في ظل توسيع استخدام تقنيات الإدارة الإلكترونية. يهدف هذا القانون إلى وضع القواعد القانونية التي تنظم كيفية جمع، حفظ، استعمال، ومعالجة البيانات الشخصية، مع فرض التزامات صارمة على الهيئات المعنية، سواء كانت عامة أو خاصة، واحترام حقوق الأفراد المعنيين بهذه البيانات. كما نص القانون على إنشاء سلطة مستقلة تُعنى بمراقبة مدى الالتزام بأحكامه، وهي السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

1-**أهمية الموضوع:** تتمثل في أهمية علمية وأخرى عملية

- **الأهمية العلمية:**

- يسهم الموضوع في إثراء الدراسات القانونية الجزائرية حول حماية الحياة الخاصة في البيئة الرقمية، والتي لا تزال محدودة نسبيا.
- يسلط الضوء على تقاطع مهم بين القانون وتكنولوجيا المعلومات، وهو ما يندرج ضمن فقه قانوني حديث يستجيب لتطور العصر.

- يساهم في تحليل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي من زوايا ارتباطه بالإدارة الإلكترونية.
- يبرز دور السلطات التنظيمية مثل السلطة الوطنية لحماية المعطيات ويقيّم مدى فعاليتها القانونية والعملية.

➢ **الأهمية العملية:**

- يواكب التحولات الرقمية في الإدارة الجزائرية ويسلط الضوء على التحديات المدنية في حماية بيانات المواطنين.
- يلفت انتباه الهيئات الإدارية إلى ضرورة تبني مقاربات قانونية وتقنية لحماية المعطيات التي تتعامل معها يوميا.
- يساهم في تعزيز الوعي بأهمية الخصوصية الرقمية لدى المواطن ومؤسسات الدولة.
- يبرز أهمية تطوير البنية التحتية التقنية والتشريعات للإدارة الإلكترونية لضمان أمن المعلومات والثقة الرقمية.

2- أهداف الدراسة:

تهدف هذه الدراسة إلى:

- بيان مفهوم البيانات الشخصية وخصائصها القانونية.
- تسليط الضوء على الإدارة الإلكترونية وطبيعتها ومجالات تطبيقها في الجزائر.
- تحليل الإطار القانوني الجزائري المنظم لحماية البيانات الشخصية، خاصة القانون 18-07.
- إبراز دور السلطات المختصة، وعلى رأسها السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، في تنظيم وتفعيل الحماية.
- الوقوف على الآليات التقنية المعتمدة لحماية البيانات الشخصية من الاعتداءات.
- تقديم رؤية متكاملة حول التحديات والآفاق في مجال حماية البيانات في ظل الإدارة الإلكترونية.

3- أسباب اختيار الموضوع: تتراوح بين أسباب ذاتية وأخرى موضوعية

➢ **الأسباب الذاتية:**

- الاهتمام الشخصي المتزايد بالمجالات القانونية الحديثة، خصوصا تلك التي تتقاطع مع التكنولوجيا الرقمية، وعلى رأسها حماية البيانات الشخصية.
- الرغبة في فهم التحديات العملية التي تواجه الإدارة الإلكترونية في الجزائر، خاصة من الزاوية القانونية والتنظيمية.
- طموحنا في المساهمة الأكاديمية في إثراء هذا الموضوع، الذي لا يزال يحتاج إلى دراسات معمقة في البيئة الجزائرية.
- تطلعنا إلى ربط الجانب النظري بالواقع العملي من خلال دراسة تطبيقية تعكس الواقع الإداري والقانوني المحلي.

➢ **الأسباب الموضوعية:**

- التحول الرقمي الذي تشهده الإدارة الجزائرية، وما يرافقه من تخزين واسع للبيانات الشخصية، يستدعي أثرا قانونيا وتقنيا لحمايتها.
- صدور القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة البيانات ذات الطابع الشخصي، مما وفر أرضية مناسبة للبحث والتحليل.
- ضعف الثقافة القانونية المتعلقة بحماية الخصوصية الرقمية، سواء لدى المواطن أو حتى في بعض الهيئات الإدارية.
- الحاجة إلى تسليط الضوء على دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كهيئة جديدة لم تحظ بعد بالاهتمام الأكاديمي الكافي.
- التزايد الملحوظ في التهديدات الإلكترونية وتوسع الجرائم المعلوماتية التي تستهدف البيانات الشخصية.

4- الإشكالية: مما سبق تتمثل إشكالية الدراسة في الآتي

كيف يمكن تحقيق التوازن بين متطلبات التحول نحو الإدارة الإلكترونية وضمان حماية البيانات الشخصية للمواطنين؟:

5- المنهج المعتمد: تم الاعتماد على المنهج الوصفي التحليلي كأداة رئيسية في هذه الدراسة، حيث تم استخدامه لغرض شرح المفاهيم الأساسية المرتبطة بالبيانات الشخصية والإدارة الإلكترونية وشرح خصائصها القانونية والتقنية، كما مكّن هذا المنهج من تحليل النصوص القانونية والتنظيمية ذات الصلة، لا سيما القانون رقم 18-07، وذلك بهدف تقييم مدى كفاءتها في حماية المعطيات الشخصية ضمن بيئة رقمية متغيرة.

6- تبرير الخطة

جاءت الخطة بناءً على تسلسل منطقي ومنهجي يراعي الإحاطة الشاملة بجوانب الموضوع المختلفة التي قسمناها إلى فصلين:

الفصل الأول تحت عنوان الإطار المفاهيمي والقانوني لحماية البيانات الشخصية في ظل الإدارة الإلكترونية، والذي يتناول الإطار النظري للموضوع من خلال التعريف بالبيانات الشخصية والإدارة الإلكترونية وبيان خصائص كل منهما وعلاقتهما ببعض، كما يُخصص لدراسة الإطار القانوني والتنظيمي في الجزائر، خاصة قانون 18-07 والنصوص المرافقة له، والعقبات المرتبطة بانتهاك البيانات في المبحث الثاني.

أما الفصل الثاني فجاء تحت عنوان الآليات العملية لحماية البيانات الشخصية في ظل الإدارة الإلكترونية، حيث تطرقنا إلى الآليات المؤسساتية التي تبرز دور السلطة الوطنية وسلطات الضبط القطاعية والمؤسسات العامة والخاصة في ضمان الحماية، وفي المبحث الثاني تحدثنا عن الآليات التقنية والتدابير الوقائية المستخدمة لحماية البيانات، من خلال الوسائل الفنية، وسياسة أمن المعلومات، والتشفير، والتدابير التوعوية.

الفصل الأول

الإطار المفاهيمي والقانوني لحماية البيانات الشخصية في ظل الادارة الالكترونية

تمهيد

تعد البيانات الشخصية معلومات فردية مهمة لتحديد الهوية، وفي ذلك أهمية متزايدة نتيجة للتطور الذي شهدته وسائل الاتصال ومنها الإنترنت، مما أدى إلى الانتقال من الأنشطة التقليدية إلى الأنشطة الإلكترونية. إذ أصبح الاعتماد على تقنية المعلومات والاتصال أحد الأسس لتحقيق التنمية الاقتصادية والاجتماعية. ونتيجة لذلك، ظهر ما يعرف بالأعمال الإلكترونية وانتشرت تطبيقاتها المختلفة. هذا التطور جعل حماية البيانات الشخصية ضرورة حتمية لحفظ خصوصية الأفراد وحقوقهم في التحكم بمعلوماتهم.

إذ يُعتبر مفهوم البيانات الشخصية والإدارة الإلكترونية أساسين في عالمنا اليوم، حيث أصبحت التكنولوجيا جزءا لا يتجزأ من حياتنا اليومية والعمليات الإدارية.

في هذا الفصل سنتطرق إلى ماهية البيانات الشخصية والإدارة الإلكترونية في المبحث الأول، حيث نتناول مفهوم البيانات الشخصية وخصائصها، إلى جانب أنواعها وأهمية حمايتها، مع التطرق إلى مفهوم الإدارة الإلكترونية وخصائصها، والاستراتيجية الجزائرية الرقمية، ومظاهر التحول الإلكتروني، إضافة إلى متطلبات تطبيقاتها.

أما المبحث الثاني فيسلط الضوء على الإطار القانوني لحماية البيانات الشخصية في التشريع الجزائري، ولتعزيز هذه الحماية نتناول حمايتها في القوانين الجزائرية وفي التشريعات الخاصة.

المبحث الأول: ماهية البيانات الشخصية والإدارة الالكترونية:

أدى التطور التكنولوجي الهائل إلى تغيير جذري في طبيعة التعاملات الإدارية والقانونية، حيث أصبحت البيانات تعالج وتخزن وتتداول بشكل الكتروني واسع، مما أبرز أهمية البيانات الشخصية والإدارية الالكترونية كمحور رئيس في المنظومة القانونية الحديثة، ولم يعد من الممكن الحديث عن حماية الخصوصية أو تنظيم العلاقة بين الأفراد والإدارة دون فهم دقيق لماهية هذه البيانات.

ويهدف هذا المبحث إلى توضيح المفهوم القانوني للبيانات الشخصية والإدارية الالكترونية، من خلال تقسيمه إلى مطلبين رئيسين:

المطلب الأول: مفهوم البيانات الشخصية وخصائصها:

يعد فهم البيانات الشخصية الالكترونية خطوة أساسية لفهم أبعاد الحماية القانونية المقررة لها خاصة في ظل تزايد الاعتماد على الوسائل الرقمية في جمع ومعالجة البيانات ويهدف هذا المطلب إلى بيان المفهوم القانوني للبيانات الشخصية الالكترونية، واستعراض أبرز خصائصها، والتفرقة بين أنواعها، وذلك من خلال ثلاثة فروع يتناول الأول مفهوم البيانات الشخصية الالكترونية، بينما يركز الثاني على خصائصها، ويخصص الفرع الثالث لبيان أنواع هذه البيانات.

الفرع الأول: تعريف البيانات الشخصية

يعد تحديد مفهوم البيانات الشخصية أمرا ضروريا للتمييز بينها وبين غيرها من أنواع البيانات، إذ تشكل الأساس الذي تبنى عليه قواعد الحماية القانونية في البيئة الرقمية. ويهدف هذا الفرع إلى توضيح المعنى المقصود بالبيانات الشخصية عن معالجتها الكترونيا.

أولا– تعريف البيانات الشخصية لغة:

1– البيانات: كل ما يمكن تخزينه ومعالجته وتوليد ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وما إليها.[1]

2– الشخصية: الصفات تميز الشخص عن غيره، ويقال عن الفرد انه ذو شخصية قوية إذا كان يتمتع بصفات فريدة ومميزة[2]

ثانيا– تعريف البيانات الشخصية اصطلاحا:

1– تشريعا: تتأثر التشريعات الوطنية بالنصوص الدولية المتعلقة بحماية المعطيات الشخصية وأن اختلفت في توقيت إصدارها وتباينت في تحديد نوعية المعطيات المشمولة بالحماية، ومن أبرز هذه النصوص نذكر على سبيل المثال ما يلي:

- **القانون الفرنسي:**

يذهب المشرع الفرنسي في المادة 02 من القانون رقم 801 لسنة 2004 الخاص بحماية البيانات الشخصية في تعريفها: "البيانات الشخصية في أي معلومات تتعلق بشخص طبيعي محدد، أو يمكن تحديد هوية بشكل مباشر أو غير مباشر بالرجوع إلى رقم تعريف أو عنصر أو عدة عناصر خاصة به لتحديد إذا كان الشخص قابلا للتحديد.[3]

1 معجم المعني، متاح على الرابط: https:// www.almaandy.com ، تاريخ الزيارة: 1/2/2025، على الساعة: 14:30.

2 – معجم الوسيط، متاح على الرابط: https:// www.almaandy.com ، تاريخ الزيار:ة 1/2/2025، على الساعة: 20.:45

3 – خلايفية هدى، تدتول البانات الشخصية على مواقع لتواصل الاجتماعي المخاطر والحماية القانونية، المجلة الاكادمية للبحث القانوني، كلية الحقوق، جامعة الاخوة منتوري، قسنطينة (01)، الجزائر، المجلد14، العدد01، 2023، ص284. والمتوفر على الموقع: https://asjp.cerist.dz ، اطلع عليها بتاريخ 2025/02/12 على الساعة 10:30.

- **القانون المصري:**

نصت المادة الأولى من القانون المصري رقم 151 لسنة 2020 المتعلق بحماية البيانات الشخصية على ما يلي:

لأغراض تطبيق أحكام هذا القانون، يُقصد بالمصطلحات والعبارات التالية المعاني المبينة قرين كل منها، وتُعد البيانات الشخصية هي تلك التي تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه بشكل مباشر أو غير مباشر، من خلال الربط بين هذه البيانات وأية معلومات أخرى، مثل الاسم أو الصوت أو الصورة أو رقم الهوية أو أي مُعرّف إلكتروني، أو أية بيانات أخرى تكشف عن الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص.[1]

- **التشريع الوطني:**

عرفها المشرع الجزائري في المادة 3 الفقرة 01 من القانون 18_07 المعطيات ذات الطابع الشخصي " كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه" الشخص المعني" بصفة مباشرة أو غير مباشرة، لا سيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية، والاقتصادية أو الثقافية أو الاجتماعية.[2]

[1] – وليد رمضان، عبد الرزاق محمود، "الحماية الدستورية والقانونية للبيانات الشخصية"، مجلة مصر المعاصر، كلية الحقوق، جامعة بني يوسف، ص385. https://espesl.jornalis.ekb.eyg، بتاريخ 2025/02/15 على الساعة: 11.30

[2] – المادة 03 الفقرة 01 من القانون رقم18/07 المؤرخ في 10جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد34، الصادرة في 13 جوان 2018.

ثالثا– تعريف البيانات الشخصية فقها:

عرفها الدكتور عادل عبد العزيز الرشيد: بأنها معلومات تتعلق بالحياة الخاصة للفرد، مثل هويته، جنسيته، ميوله، معتقداته، واتجاهاته بالإضافة إلى تعاملاته المالية والمعرفية، وبشكل عام. تشمل كل معلومة ترتبط بشخص محدد أو يمكن التعرف عليه من خلالها[1]

وعرفها الدكتور أيمن عبد الله فكري: بأنها المعلومات التي تتعلق بفرد معين، ويمكن من خلالها التعرف عليه بشكل مباشر أو غير مباشر[2]

ونجد الدكتور عادل عبد الصادق يعرف البيانات الشخصية بأنها أي معلومة تتعلق بشخص طبيعي يمكن التعرف عليه، وتكمن أهمية هذا التعريف في اعتماده على مفهوم واسع البيانات الشخصية، مما يساهم في توسيع نطاق تطبيق القانون، إذ أن حصر مفهوم البيانات الشخصية قد يفتح المجال أمام جهات متعددة لانتهاك خصوصية الأفراد، فقد لا تكشف البيانات المتفرقة في قواعد بيانات مختلفة عن هوية الشخص بشكل مباشر، لكنها قد تؤدي إلى ذلك عند ربطها ببعضها البعض، وبالتالي فإن الاكتفاء بحماية البيانات المرتبطة بالشخص بشكل مباشر فقط، قد يتيح فرصا لتجاوزات في استخدام البيانات الشخصية، لا سيما مع تطور تقنيات جمع البيانات ومشاركتها[3]

رابعا– تعريف البيانات الحساسة:

عرفها المشرع المصري: بأنها البيانات المتعلقة بالصحة النفسية أو البدنية أو البيانات والقياسات الحيوية (البيومترية)، أو المعلومات المالية، أو المعتقدات الدينية، أو الآراء السياسية، أو

[1] – عادل، عبد العزيز الرشيد، البيانات الضخمة (big.data) دراسة فقهية رسالة مقدمة الى قسم الفقه، كلية الشريعة، جامعة محمد بن سعود الاسلامية، سنة، 2022م، ص62.

[2] – أيمن عبد الله،" الجرائم المعلوماتية، مكتب القانون والاقتصاد، الرياض، دراسة مقارنة في تشريعات العربية والأجنبية، 2014م، ص738.

[3] – عادل عبد الصادق، "البيانات الشخصية، الصراع على نمط الحادي والعشرون" المركز العربي الابحاث الفضاء الالكتروني، 11ديسمبر2018، ص31.

الوضع الأمني من البيانات الشخصية الحساسة كما تصنف بيانات الأطفال ضمن هذه الفئة الحساسة في جميع الأحوال[1]

ونجد الدكتور" يحي إبراهيم دهشان "يعرفها بأنها تعتبر البيانات التي تكشف عن الحالة النفسية أو العقلية أو البدنية أو الأجنبية، أو البيانات البيومترية (القياسات الحيوية)، أو المعلومات المالية، أو المعتقدات الدينية، أو الآراء السياسية، أو الوضع الأمني من البيانات الشخصية الحساسة كما تعد البيانات الشخصية الحساسة ايضا[2]

ويعرفها " الدكتور عادل عبد الصادق" بأنها تلك التي تتعلق بالجوانب الشخصية العميقة مثل العرق، الديانة المعتقدات، والسجل الجنائي وتعد أكثر خصوصية وخطورة من البيانات الأساسية كالاسم، تاريخ الميلاد والعنوان، مما يستدعي توفير مستوى أعلى من الحماية لبعض أنواعها مقارنة بغيرها [3]

وبالرجوع للمشرع الجزائري نجده يعرف " المعطيات الحساسة" في القانون 18_07 بأنها: معطيات ذات طابع شخصي تبين الأصل العرقي أو الاثني أو الآراء السياسة أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تلوث متعلقة بصحته بما فيها معطياته الجينية[4]

ومن مجمل التعريفات المقدمة يمكننا وضع تعريف للبيانات الشخصية بأنها "تلك المعلومات التي ترتبط بشخص طبيعي معينو التي يمكن تحديده بشكل مباشر او غير مباشر عن طريق ربط البيانات بالبيانات الأخرى كالاسم واللقب ووصورته ورقم الهوية الوطنية.

[1] – وليد رمضان عبد الرزاق محمود، المرجع السابق، ص ص 385،386.

[2] – يحي ابراهيم دهشان،" الجماية الجنائية للبانات في ظل التحول الرقمي" بدون ط، مدرسة القانون الجنائي، كلية الحقوق، جامعة الزقازيق، ص18.

[3] – عادل عبد الصادق، المرجع السابق، ص31.

[4] المادة3 الفقرة 6 من القانون18-07 المرجع السابق.

أما البيانات الحساسة هي تلك المعلومات التي تتعلق بشخص طبيعي والتي تبين معلوماته الصحية (الحالة النفسية أو العقلية أو البدنية أو الجينية) والمالية وانتماءاته الدينية والفلسفية والسياسية.

الفرع الثاني: أنواع البيانات الشخصية:

تعتبر البيانات الشخصية كل المعلومات التي تتيح التعرف على هوية الفرد، سواء كانت مرتبطة بصفاته الاجتماعية، الجينية، البيولوجية، أو حتى الوسائل والتقنيات التي يعتمدها، وتنقسم هذه البيانات إلى عدة أنواع، حيث تم تصنيفها إلى قسمين بناء على طبيعتها وكذلك وفقا للتصنيف القانوني المعتمد.

أولا – تصنيف المعطيات الشخصية من حيث طبيعتها: تصنف إلى:

1. المعطيات ذات الطبيعة الاسمية:

وتتمثل في الاسم والكنية، وهما ينادى ويعرف بهما المرء، وهما حقان شخصان يدخلان في الحياة الخاصة للشخص، إذ أنه بغيابهما يصعب التمييز بين الأشخاص ويتفرع الاسم إلى اسم أصلي، وشهرة، واسم مستعار. والاسم بمعناه الضيق يشير إلى اللقب أو الاسم العائلي، لذا أوجب القانون حماية الاسم الشخصي والعائلي وحتى الاسم المستعار[1]، يضاف إليهما العنوان والبريد الالكتروني وسجل السوابق العدلية، والصور الشخصية والحالة الاجتماعية، والسيرة الذاتية والسمعة وتاريخ الميلاد، ومحل الإقامة والعمل[2].

[1] –عبيزة منيرة، الحماية القانونية للبيانات الشخصية من الجرائم المعلوماتية في ضوء التشريع الجزائري، مجلة الاجتهاد القضائي، جامعة محمد لمين دباغين، سطيف2، الجزائر1 مجلد 15، العدد02، 30نوفمبر2023، ص183، المتوفر على الموقع https://asjp.cerist.dz بتاريخ 2025/02/10 على الساعة 13.00.

[2] –حمليل نوارة، حماية المعطياة الشخصية في مواجهة الادارة الالكترونية، المجلة النقدية للقانون و العلوم السياسية جامعة مولون معمري، تيزي وزو الجزائر، المجلة15 العدد2، ،30 ديسمبر2020، ص34 https://asjp.cerist.dz بتاريخ 2025/02/15 على الساعة 15:00.

2. البيانات غير الاسمية:

تحتوي المعلومات التعريفية غير المباشرة التي لايمكن تحديد هوية من خلالها إلى إن اقترنت بمعلومات أخرى، وتشمل أهم هذه البيانات الأرقام الشخصية كأرقام الهاتف والرقم الوطني ورقم بطاقة الهوية وكلمات المرور، وكذلك تشمل البيانات المالية مثل الدخل الشهري، بالإضافة إلى البيانات الصحية والمعطيات البيولوجية والقياسات الحيوية والمعطيات الوراثية وبصمة الإصبع والملامح الوراثية وكل ما يتعلق بهما على موافقة واضحة وصريحة منه وبرضاه[1] .

وقد أعطى المشرع لهذه الخصوصية أهمية بالغة، حيث صنف المعلومات الصحية ضمن المعطيات التي تخضع لحماية مشددة، وتم تعريف هذه المعلومات على أنها تتعلق بالحالة البدنية أو العقلية للشخص المعني وتشمل أيضا البيانات الجينية[2]الخاصة به، ووفقا لهذا التعريف، وبالمفهوم المخالف تعد المعلومات الجينية جزء من البيانات الطبية الحساسة مما يعني أن جميع المعلومات الطبية تندرج ضمن فئة البيانات الحساسة التي تتطلب حماية خاصة. وتشمل الحماية جميع البيانات الصحية المستخدمة لأغراض البحث، الدراسة، التقييم، وتحليل المعلومات المرتبطة بأنشطة العلاج والوقاية، وعلى الرغم من ذلك فإن المشرع استثنى بعض الحالات مثل:

– الدراسات التي تعتمد على بيانات جمعت مسبقا عندما تجرى من قبل الجهات المشرفة على على هذه المتابعة

– المعالجات الهادفة للتعويض أو الوقاية التي تقوم بها المسؤولة عن تامين المرضى.

– معالجة البيانات ذات الطابع الشخصي التي تهدف إلى المتابعة الطبية أو العلاجية الفردية للمرضى.

[1] –حمليل نوارة، المرجع السابق، ص36.

[2] –جوهر قوادري صامط، "الضوابط القانونية لمعالجة البيانات الشخصية، الكترونيا"، مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بوعلي الشلف المجلة06، العدد02، ،27ديسمبر2020، ص469،https://asjp.cerist.dz بتاريخ 2025/02/18 على الساعة: 11.30.

– المعالجات التي تتم داخل المؤسسات الصحية من قبل الأطباء المسؤولين عن البيانات الطبية[1]

وكل الاستثناءات تبرز التوازن الذي يحاول المشرع تحقيقه بين حماية الخصوصية الصحية وتوفير الظروف الملائمة للدراسة والعناية بالمريض من معلومات ذات صلة من قريب أو بعيد[2].

ثانيا– تصنيف المعطيات الشخصية من حيث حساسيتها:

1– معطيات حساسة: وهي معطيات تحمل طابعا شخصيا، تكشف عن الأصل العرقي او الاثنى أو الآراء السياسية، القناعات الدينية أو الفلسفية، الانتماء النقابي للفرد أو الشخص المعني، كما تشمل معلومات مرتبطة بوضعه الصحي، بما في ذلك بياناته الجينية. [3]

2– معطيات جينية : تعتبر المعطيات المتعلقة بالصفات الوراثية للأفراد أو لمجموعة من الأشخاص المرتبطين بقرابة أداة هامة لفهم الخصائص الجينية والمكتسبة، وقد أظهر المشرع التونسي دقة أكبر مقارنة بنظيره الجزائري، حيث لم يقتصر على تحليل الخصائص الجينية الوراثية فقط، بل توسع ليشمل الخصائص المكتسبة التي توفر معلومات إضافية ومميزة عن الفرد، ويتم تأكيد هذه الدراسات عادة من خلال تحليل عينة بيولوجية تعود للشخص المعنى، ما يفرز من جودة كفاية التحليل[4] .

[1] –المادة 05 من القانون رقم07–18، المصدر السابق

[2] –مريم لوكال، "الحماية القانونية الدولية و الوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي في ضوء قانون حماية المعطيات" رقم07–18 ، مجلة العلوم القانوني و السياسية، جامعة امحمد بو قزة بومرداس، الجزائر المجلد10، العدد1، افريل2019،ص1309 https://asjp.cerist.dz بتاريخ 2025/02/20 على الساعة 13.30.

[3] – يوسف زروق والعيداني محمد، حماية المعطيات الشخصية في الجزائر في ضوء القانون 07/18 (المتعلق بحماية الاشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي) "مجلة معالم الدراسات القانونية والسياسية، جامعة الجلفة: العدد 05، 20ديسمبر2018، ص120، https://asjp.cerist.dz بتاريخ 2025/02/25 على الساعة 09.00.

[4] – حمليل نوارة، المرجع السابق، ص36.

2- معطيات صحية: تعد الحالة الصحية للفرد بجانب الرعاية الطبية والعلاج. الذي يتلقاه من

أهم الجوانب الحساسة والخصوصية في حياته الشخصية، وخاصة إذا كانت تلك الجوانب مرتبطة بأمراض خطيرة أو حالات حرجة، سواء نفسية أو عقلية. مثل هذه الأمور قد تدفع الشخص للانعزال والابتعاد عن الحياة العامة ولهذا السبب لا يجوز نشر أخبار تتعلق بمرض شخص ما أو تصويره في حالة صحية حرجة دون الحصول على بيانات حساسة ويمكن استنتاج أن المعلومات الطبية هي بالفعل ضمن البيانات الحساسة وتشمل هذه الحماية جميع البيانات الصحية التي تهدف الى البحث والدراسة وتقييم وتحليل المعلومات المرتبطة بأنشطة لعلاج والوقاية.[1]

الفرع الثالث: خصائص البيانات الشخصية وأهمية حمايتها

تتمتع البيانات الشخصية الالكترونية بعدد من الخصائص التي تميزها عن غيرها من أنواع البيانات لاسيما في بيئة المعالجة الرقمية وتكمن أهمية هذه الخصائص في أنها تؤثر مباشرة على كيفية جمع البيانات تخزينها وحمايتها قانونيا وبهذا الفرع إلى تسليط الضوء على أبرز واهم خصائص البيانات الشخصية الالكترونية وارتباطها الوثيق بضرورة حمايتها في البيئة الرقمية.

أولا – خصائصها:

تعد المعطيات الشخصية من الحقوق المرتبطة بالشخصية الإنسانية وبحياة الفرد الخاصة، ولابد أن تكون هذه البيانات متعلقة بشخص طبيعي، إذ لا تمنح مثل هذه الحقوق للشخصيات الاعتبارية، ومن أمثلتها حق الفرد في الاحتفاظ بأفكارها وسرية علاقاته، وهي حقوق لصيغة بالكرامة الإنسانية.[2]

[1] – جوهر قوادري صامت، الظوابط القانونية لمعالجة البيانت الشخصية الالكترونية، مجلة الدراسات اتقانونية المقارنة،كلية الحقوق والعلوم السياسية ،جامعة حسيبة بن بوعلي الشلف، المجلد 06،العدد02، 2020،ص 27، http://asjp.cerist.dz بتاريخ 2025/03/12 على الساعة 14.00

[2] – خالد سويلم، محمد سويلم، الحماية القانونية للبانات الشخصية الالكترونية، دراسة مقارنة" مجلة متخصصة في الدراسات والبحوث القانونية، كلية الحقوق، جامعة الزقازيق، ص1889، المتوفر على الموقع، https://jlaw.journals.ekb.ej بتاريخ 2025/02/26 على الساعة 14.00.

تتميز المعطيات الشخصية بقدرتها على التعريف بالشخص بشكل مباشر، مثل الاسم الكامل. الجنس، تاريخ ومكان الولادة، العنوان، أو السمات الجسدية كالصوت، الصورة، البصمات والجنسية. كما يمكن التعرف على الشخص بشكل غير مباشر من خلال مجموعة من المعايير المجتمعة، مثل: العمر، الوظيفة أو المواصفات الشخصية. هذه "البيانات تعد اسمية غير مباشرة"، لكنها تبقى ضمن نطاق البيانات الشخصية في نظر القوانين المعنية بحمايتها[1]

وقد اتفقت غالبية التشريعات على أن عناصر الهوية. سواء كانت بدنية أو فيزيولوجية أو جينية أو نفسية أو اقتصادية أو ثقافية أو اجتماعية، تندرج ضمن مفهوم المعطيات الشخصية. وهو ما يساعد على تحديد نطاق هذه البيانات بدقة[2]

مع تطور العالم الرقمي، بات على الأفراد السيطرة على بياناتهم الشخصية .. مثل الأسماء، العناوين، الصور، التوجهات، وغيرها من المعلومات التي يمكن من خلالها تمييز الشخص، سواء في الواقع أو عبر الانترنت لاسيما على مواقع التواصل الاجتماعي، وعلى الرغم من أن الاطلاع على هذه البيانات قد يبدو بسطا ولا يسب ضررا ظاهراً، إلا أنها تعد كنزا ثمينا بالنسبة الشركات والمؤسسات الاقتصادية، التي تستغلها لتحقيق أرباح وجذب شرائح جديدة من المستهلكين، من خلال تحليل هذه البيانات التي يخلفها أفراد اثناء استخدامهم للأجهزة أو المواقع الالكترونية[3]

ومن جهة أخرى، تمتلك الهيئات العامة كميات كبيرة من البيانات. الخاصة بالمواطنين، وتستخدمها غالبا في تنظيم شؤون النظام والأمن، ورغم أن ذلك يبدو منطقيا في الظاهر إلا أن خطورة هذه البيانات تبرز عند وقوعها في أيد غير أمينة، فقد تستغل في الابتزاز أو التشهير أو التهديد. [4]

[1] – خالد سويلم، محمد سويلم، المرجع السابق ص 1889.

[2] – المرجع نفسه، ص ص1890،1889

[3] – المرجع نفسه، ص1889،

[4] – المرجع نفسه، ص1889.

وبالتالي، معالجة البيانات الشخصية قد تمثل انتهاك للحق في الحياة الخاصة، وهو من أبرز حقوق الإنسان المتفق عليها عالميا، ويمنح هذا الحق كل فرد إمكانية منع التدخل أو الفضول غير المشروع فى حياته الخاصة أو حياته أسرية، واتخاذ ما يراه مناسبا لحماية خصوصيته. كما يعترف الفرد بحقه القانوني في اللجوء إلى القضاء لمنع أي اعتداء على خصوصيته، حتى قبل وقوع الضرر وهو ما يترتب التزاما عاما على الجميع باحترام هذا الحق[1]

ثانيا– أهمية حمايتها

في الوقت الراهن، أصبحت معظم الأنشطة الاقتصادية، التجارية الاجتماعية، وحتى السياسية تمارس في الفضاء الالكتروني ورغم ما جلبته هذه التحولات من فوائد كبيرة وتسهيلات لحياة الناس، فإن انتقال هذه الأنشطة من البيئة التقليدية إلى العالم الرقمي صاحبته ممارسات ضارة مثل السرقة والتخريب، والتي تسهدف أساسا البيانات المتوفرة سواء كانت شخصية كالأسماء، الصور، التسجيلات الصوتية أو غير الشخصية.

لقد أثرت الثورة التكنولوجية بشكل مباشر على خصوصية الافراد من خلال ثلاثة أبعاد رئيسية:

1-**سهولة دمج المعلومات**: حيث أصبح بالإمكان تجميع كميات هائلة من البيانات، حتى على المستوى الشخصي، مما أدى إلى تراكم معلومات قد لا يعرفها أقرب الأقربين إلى الفرد.

2-**ازدهار سوق المعلومات**: وأصبح بإمكان كل من يملك مصلحة أن يحصل على ما يحتاجه من بيانات بسهولة[2]

3-**غياب وسائل الحماية الكافية**: إذ لم تكن هناك، ولاتزال وسائل كافية ومتكاملة لحماية هذه المعلومات في العصر الرقمي.

[1] – خالد سويلم، محمد سويلم، المرجع السابق ص1890.

[2] – الشيخ الحسن محمد يحي، سيد محمد سيد احمد، الحماية القانونية للبيانات الشخصية "مجلة القضاء والقانون، كلية العلوم القانونية والاقتصادية جامعة نواقشط، العدد4 العددي أبريل 2018، ص6. المتوفر على الموقع: https://www.academia.edu اطلع عليه بتاريخ 2025/01/12 ، على الساعة 10.00.

ونظرا لتزايد أهمية المعلومات، وخاصة الشخصية منها، ظهرت الحاجة إلى توفير حماية قانونية خاصة لها، فبدأت التشريعات تتجه نحو سن قوانين تنظم تحميل البيانات ومعالجتها وحمايتها.[1]

أما في حال غياب الحماية القانونية، فان الأفراد معرّضون للعديد من المخاطر، مثل: السرقة، انتحال الهوية، الاحتيال، التزوير والجرائم الالكترونية المختلفة. فعلى سبيل المثال، شهدت الولايات المتحدة في عام 2012 أكثر من 12 مليون ضحية لجرائم نفذت باستخدام البيانات الشخصية، بينما سجل في بريطانيا نحو89000 جريمة احتيال باستخدام البيانات الشخصية في النصف الأول من عام 2017 وحده، بحسب منظمة "Cifas". مما دفع رئيس خدمة مكافحة الاحتيال هناك لوصف الوضع بأنه بلغ "مستوى وبائي"، بوقوع نحو 500 حالة يوميا.

ومع كل موجة تكنولوجية جديدة، تصبح حماية الخصوصية الشخصية أكثر تعقيدا، فعلى سبيل المثال، مع ظهور "انترنت أشياء" (2008-2009)، بات من السهل تحديد مواقع الأشخاص والأعمال التي يمارسونها لحظيا وأصبح من الممكن تقنيا ربط البيانات المجهولة بأشخاص محددين لمن يملك معلومات إضافية عنهم.

وتتنوع الجهات التي قد تنتهك الخصوصية؛ من شركات ومؤسسات خاصة، إلى أفراد عاديين وكل بدوافع مختلفة. وللتصدي لهذه التحديات، سعت اغلب دول العالم إلى سن قوانين الحماية البيانات الشخصية، بهدف تحقيق التوازن بين الاستفادة من البيانات الرقمية، وضمان أمن وخصوصية أصحابها من المخاطر التي قد تنجم عن إساءة استخدامها. [2]

[1] الشيخ الحسن محمد يحي، سيد محمد سيد احمد، المرجع السابق، ص6.

[2] – المرجع نفسه، ص ص 06،07.

المطلب الثاني: ماهية الإدارة الالكترونية وتطبيقها في الجزائر

نتيجة التطور الذي شهدته السنوات الأخيرة من تطور المعلومات والاتصالات والتقدم ما أدى إلى ظهور مفهوم الإدارة الالكترونية الذي يعتبر حديث النشأة وذلك نتيجة الاستخدام المتزايد لجهاز الكمبيوتر إذ أنها تعتمد على الوسائل الإلكترونية والتقنية الحديثة كالبريد الالكتروني والهاتف والفاكس ما يساعد على إنجاز الأعمال وتقديم الخدمات للمستفيدين بسهولة وبسرعة وهذا ما سيتم التطرق إليه من خلال فروع هذا المطلب.

الفرع الأول: مفهوم الإدارة الالكترونية وخصائصها:

لقد اختلف الفقهاء والباحثون وأهل اللغة في وضع تعريف محدد لمصطلح الإدارة الالكترونية وذلك وفقا لتخصصاتهم ونظرتهم المختلفة للمعني، وعليه يمكن تصنيف هذه التعريفات من خلال تقسيمها إلى معنى لغوي للإدارة الالكترونية وتعريف اصطلاحي مع التطرق إلى أهم خصائصها:

أولا– تعريف الإدارة الالكترونية:

1- **التعريف اللغوي:** يتكون مصطلح الإدارة الالكترونية من كلمتين إدارة والكترونية

أ– إدارة: من مصدر أدَارَ [1]، ويقصد بها إدارة الموجودات والمطلوبات بشكل يحقق التوازن الأمثل، والإدارة مصدر الرياسة والتصرف، وقيل هي علم وقت تدبيرالأعمال وتوجيهها والسيطرة عليها وضبطها واستعمال الحكمة في اتخاذ قرارات مناسبة بشأنها. والإدارة وظيفة تحقيق الأهداف عن طريق الآخرين[2].

ب– إلكترون: اسم مفرد، جمعه الكترونيات والمنسوب إلى الإكترون، بدأ ينتشر العقل الالكتروني

[1] معجم المعاني الجامع على الرابط https://www.almaany.com تاريخ أخر زيارة10 /2025/02، ساعة13:30

[2] – المصدر نفسه.

في كل المكاتب، آلة الحاسوب تعتمد على مادة إلكترون لإجراء أدت العمليات الحسابية وبأسرع وقت ممكن يسمى أيضا كمبيوتر.[1]

2_التعريف الاصطلاحي:

نظرا الحداثة موضوع الإدارة الالكترونية الذي تم طرحه مؤخرا والذي يعد من المصطلحات العلمية الجديدة، فإنه لم يتم التوصل إلى تعريف دقيق يمكن أن يتفق عليه الخبراء والباحثون على مستوى العالم، بما في ذالك الولايات المتحدة الأمريكية، التي تعتبر مركز ظهور وانتشار الأعمال الالكترونية[2].

ولقد حاولنا جمع أهم التعاريف للإدارة الالكترونية فيمايلي:

عرفها يوسف كافي على أنها تحويل كافة الأعمال والخدمات الإدارية التقليدية (الإجراءات الطويلة باستخدام الأوراق إلى أعمال وخدمات إدارية والكترونية تنفذ بسرعة عالية ودقة متناهية، باستخدام تقنيات الإدارة وهو ما يطلق عليه إدارة بلا أوراقPaperless Management[3] وعليه فالإدارة الكترونية تعني تحويل الأعمال والخدمات العادية التي تتم عن طريق الأوراق إلى خدمات رقمية تتم باستخدام أساليب إدارية على مستوى الإدارة بدون الحاجة إلى استخدام الأوراق.

وفي تعريف آخر؛ هي منهجية جديدة تقوم على الاستيعاب الشامل والاستخدام الواعي والاستثمار الايجابي لتقنيات المعلومات والاتصالات في ممارسة الوظائف الأساسية في الإدارة على مختلف المستويات في المؤسسات المعاصرة، وتسهم الإدارة الالكترونية في تحقيق الغاية الأساسية

[1] – معجم المعاني الجامع، المصدر السابق.

[2] محمد باب حسن واشرف محمود احمد، إمكانية تطبيق الإدارة الالكترونية بجامعة جنوب الواحي، مجلة كلية التربية، جامعة عين شمس العدد34، الجزء الأول، 2010، ص54،55 www.reseavchgate.net بتاريخ 2025/02/22 على الساعة 14.00.

[3] مولاي خليل عمار طهرات، الإدارة الالكترونية المفهوم ومتطلبات التطبيق، ملتقى وطني حول جودة الخدمات في ظل التحول الرقمي للإدارة الالكترونية في المؤسسات الجزائرية (رهانات وتحديات تقييم الواقع واستشراف الواقع، شلف ومستغانم، ص6Univ-ghardaia.dz. بتاريخ 2025/03/14 على الساعة 14.00.

للمنظمات المعاصرة الساعية إلى التميز وذلك بتمكينها من بناء قدرات تنافسية فعالة تجعلها قادرة على الوصول السريع المجي للأسواق واستقطاب معاملات الشرائح المستهدفة من الزبائن معها وولائهم لها."[1]

كما تعرف أيضا بأنها منظومة الأعمال الإلكترونية وأنها إدارة توجيه وتنفيذ الأعمال الالكترونية[2]، والأنشطة التي يتم تنفيذها الكترونيا عبر الشبكات[3]، وذلك أن الإدارة الالكترونية هي وظيفة إنجاز الأعمال من طرف الآخرين باستعمال النظم والوسائل الالكترونية إذ أنها تقدم وظيفة ديناميكية مستمرة من أجل تحسين وتسريع إنجاز الأعمال من خلال استخدام شبكات الاتصال وعلى رأسها الانترنت، أي أنها العملية الإدارية القائمة على الإمكانيات المتميزة للانترنيت والشبكات في التخطيط والتوجيه من اجل تحقيق الأهداف المنظمة.

ومن خلال التعريفات السابقة نستنتج أن الإدارة الالكترونية تعني قدرة المؤسسة أو الإدارة على تقديم كافة الخدمات والمعاملات للأفراد والمؤسسات الكترونيات عن طريق وسائل الكترونية لتصبح أكثر كفاءة وسرعة إذا أنها تمثل عملية إدارية تعتمد على الإمكانيات الالكترونية الحديثة مثل: شبكة الإنترنت وغيرها إذ أنها تهدف إلى زيادة كفاءة وفعالية الأداء بالمؤسسة أو الإدارة.

تمثل الإدارة الالكترونية نوعا من الاستجابة القوية لتحديات القرن الواحد والعشرين حيث تتمثل أهميتها في:

[1] – سعد غالب ياسين، الادارة الالكترونية، دار اليازوري العلمية للنشر والتوزيع 27 جوان 2020، ص08.

[2] – كمال فار، معوقات تطبيق الادارة الالكترونية في (المرفق العام مرفق الحالة المدنية ببلدية برج بوعريريج نموذجًا)، مجلة الحكمة لدراسات الاعلامية والاتصالية، المجلد8 العدد4 جامعة الجزائر 3، 2021/02/10، ص82، https://asjp.cerist.dz

[3] – فريحة، رمزي بهاء الدين، الادارة الالكترونية واسلوب الادارة بالاهداف المجلة الجزائر للعلوم القانونية والسياسية المجلد 56، العدد1، جامعة بن خلدون، تيارت، الجزائر، 2019، ص156. https://asjp.cerist.dz بتاريخ 2025/02/18 على الساعة 15سا

– تحسين وتطوير مهارات العاملين على لاستخدام تكنولوجيا المعلومات[1]. المساعدة على توفير المعلومات بشكل مستمر وبسرعة من اجل اتخاذ القرار وهو ما يطلق عليه انبثاق ثروة المعلومات والمعرفة وذالك انه نتيجة تراكم وانفجار المعلومات والمعرفة ما جعل القدرات الإنسانية عاجزة على الإلهام بها إلى انبثاق العالم الرقمي والتطورالسريع لتقنيات المعلومات وشبكات الاتصال وهو ما جعل الاتصال يتم آنيا وفورا لإن الأقمار الصناعية بشبكاتها المجهزة بالحاسوب استطاعت نقل الصوت والصورة معا.

إضافة إلى فرص وتحديات تكنولوجيا المعلومات إن تمثل تكنولوجيا المعلومات إطلالة على مستقبل العلم والثقافة والحضارة الإنسانية ولقد تجسدت في أفكار من الإبداع والابتكار وتطوير قدرات الحاسوب ومساحة تخزينه وذكائه[2] وربطه بمنظومات شبكات الاتصال وقواعد البيانات والأقمار الصناعية ونظم التخطيط والسيطرة المعلوماتية بمستوى من التكامل والاندماج ليس له مثيل ويستخدم الذكاء الصناعي في نظم المتعامل التجاري بصورة أفضل ما جعل المؤسسات صناعية عالية التقنية تقوم بتجهيز أموال وقصاصات ورق[3].

إضافة إلى ثورة الأعمال الانترنت حيث إن الانترنت تعتبر أكبر تقدم تكنولوجي نتيجة اختراع آلة الطباعة قبل 500 عام ما أدى إلى زيادة عدد مستخدمي شبكة الانترنت من 3 ملايين إلى أكثر من 100 مليون.

كما تظهر أهميتها بالنسبة للإدارة الدولية حيث إن قيمة ما ينفقه قطاع الأعمال هو 470 مليون ولا تخصص لشراء المنتوجات والخدمات من خلال شبكة المعلومات العالمية كما انه نتيجة

[1] – قاتة حسين، شني تالية، "الادارة الالكترونية مفهوم جديد ومنهج معاصرفي مجال الادارة مجلة التنمية والاقتصاد التطبيقي"، جامعة الجزائر03، المجلد 05، العدد02، 3ديسمبر2021، 65. https://asjp.cerist.dz بتاريخ 2025/02/26 على الساعة 14.00.

[2] – سعد غالب ياسين، مرجع السابق، ص20.

[3] – المرجع نفسه، ص ص 20.21.

للنمو الهائل في استخدام شبكة الانترنت ما ادى الى ظهور نماذج جديدة للأعمال لم تكن معروفة في السابق مثل نماذج أعمال شركة Google Yahoo! Cam Hmazon حيث إن الشركات الصناعية الكبرى مثل GM Ford أصبحت تعتمد خطط من أجل إنشاء أسواق افتراضية لها على شبكة الويب إضافة إلى إن العالم لم يشهد اقتصاد كوني معولم[1] بفضل تكنولوجيا المعلومات والاتصالات ذات التقنية العالية والمرنة الفائقة في التشبيك والحوسبة ما أدى إلى نشوء السوق الالكتروني العالمي الذي نتبادل فيه المنتجات المعلومات بسرعة وبصورة تلقائية إضافة إلى أن مساهمة الإدارة الإلكترونية في تحقيق عبء إيجاد فرص جديدة للعمل عن كامل الدولة بفتح الباب أمام فرص العمل الحرفي الخارج بتشجيع المشروعات الصغيرة وتسويق منتجاتها.

ثانيا– خصائص وأهداف الإدارة الإلكترونية

يتركز مفهوم الإدارة الإلكترونية على العديد من الخصائص والأهداف والتي سيتم تناولها كالأتي:

1– خصائص الإدارة الإلكترونية:

تمتلك الأداة الإلكترونية مجموعة من الخصائص والتي تميزها عن الإدارة التقليدية وهي الميزة الأساسية والجوهرية التي تجعل الدول تسعى إلى تطبيق الإدارة الإلكترونية في منظماتها وفيما يأتي سيتم بيان هذه الخصائص.

- **إنها إدارة بلا ورق:** تعتمد على الوسائل الرقمية مثل البريد الالكتروني الأرشيف الالكتروني الرسائل الصوتية الأدلة والمفكرات الإلكترونية بالإضافة إلى أنظمة المتابعة الرقمية مما يقلل الحاجة إلى المستندات الورقية؛

[1] – سعد غالب ياسين، المرجع السابق، ص 23.

- **إدارة بلا مكان:** تتيح عقد الاجتماعات والمؤتمرات الكترونيا واستخدام الهواتف المحمولة والعمل عن بعد إضافة إلى التعامل مع المؤسسات الافتراضية مما يوفر مرونة في بيئة العمل؛
- **إدارة بلا زمان:** تعمل على مدار الساعة طوال أيام الأسبوع دون التقيد بحدود زمنية مما يعزز الإنتاجية والاستجابة السريعة للمهام.؛
- التمييز من خلال الابتكار والعالمية مع الاعتماد على المعرفة كأساس لتنفيذ الأعمال؛
- الحاجة إلى أنظمة الكترونية متطورة مثل أنظمة التحصيل المجمع والخدمات عن بعد والشراء الالكتروني وأنظمة المتابعة الفورية وتخطيط الموارد ونقاط البيع الالكترونية والتجارة الإلكترونية؛
- التركيز على الاكتشافات والابتكارات بدلا من معالجة المشكلات فقط؛
- إعطاء الأولوية للإجراءات التنفيذية وتحقيق الانجازات؛[1]
- **الإتقان:** تتميز الأعمال الالكترونية في مجال الخدمة العمومية غالبا بالدقة والاتقان متفوقة في ذلك على الأعمال اليدوية كما إن الرقابة عليها تكون أكثر سهولة وفعالية مقارنة بالإدارة التقليدية ؛[2]
- تتميز الإدارة الإلكترونية بقدرتها على تعزيز الغالية التشغيلية من خلال الاستفادة المثلى من أحد التقنيات المتاحة؛[3]
- **تحقيق الشفافية:** فالشفافية الكاملة داخل المنظمة الإلكترونية هو نتيجة مباشرة لوجود الرقابة

[1] – محمود عبد الفتاح رضوان، الادراة الالكترونية وتطبيقاتها الوظيفية"، ط1، دار النشر الكجموعة العربية للتدريب والنشر، القاهرة، مصر، 2012، ص ص 20.21.

[2] – حمزة بن خليفية، دور الادراة الالكترونية في تحسين جودة الخدمات العمومية في الجزائر، أبحاث الملتقى الوطني حول جودة الخدمات في ظل التحول الرقمي والادارة الالكترونية في المؤسسات الجزائرية التحديات تقييم الواقع واستشراف الواقع، مركز الجامعي نور البشير، البيض، الجزائر، ص05. http://dspase.univ.ghrdaia.dz.8080 اطلع عليه بتاريخ: 2025/02/30 على الساعة 15.00.

[3] – لبخور صبرين، الإدارة الالكترونية في المؤسسات الجزائرية ما بين المتطلبات والمعوقات التطبيق، أبحاث الملتقى الوطني حول جودة الخدمات في ظل التحول الرقمي والإدارة الالكترونية في المؤسسات الجزائرية، رهانات وتحديات تقييم الواقع، واستشراف الواقع تلمسان، ص5، http://dspase.univ.ghrdaia.dz.8080 اطلع عليه 2025/03/02 على الساعة 11.00.

الإلكترونية التي تضمن المحاسبة الدورية على جميع الخدمات المقدمة وتعود الشفافية الجسر الذي يربط بين المواطن ومؤسسات المجتمع المدني من جهة والسلطات المسؤولة عن الشأن العام من جهة أخرى مما يتيح مشاركة المجتمع بأكمله في صناعة الرؤية واتخاذ القرارات؛

مثلت خصائص تطبيق الإدارة الإلكترونية دافعا أساسيا للقائمين على مبادرات التحول الالكتروني في العديد من الدول والحكومات مما أدى إلى وضع استراتيجيات إلكترونية مقسمة إلى مراحل وفقا للظروف والإمكانات المتاحة وهذا يؤكد إن التحول إلى الإدارة الإلكترونية يجب إن يتم بصورة مرحلية لضمان نجاحه.[1]

ثانيا: أهداف الإدارة الالكترونية

إن الإدارة الإلكترونية مرتبطة بالعديد من الأهداف التي تسعى المنظمات للوصول إليها او تحقيقها من خلال تبينها الإدارة الإلكترونية نوجزها فيما يلي:

1- **التقرب من المواطنين:** يتطلب توفير تامين موحد وسهل الوصول إلى جانب إجراءات بسيطة وغير معقدة مما يعزز ثقتهم بالإدارة العامة التي وجدت أساسا لخدمتهم ومساعدتهم .

2- **زيادة عمل كفاءة الإدارة:** تحسن كفاءة الإدارة يتم من خلال تعاملها مع المواطنين والشركات والمؤسسات وذلك عبر تبسيط الإجراءات وتسريع الاحجاز والارتقاء بمستوى أداء الخدمات.

3- **توفير البيانات والمعلومات للمستفيدين بصورة فورية:** القدرة على استيعاب أكبر عدد ممكن من المواطنين في إن واحد وذلك لان الإدارة التقليدية تظل محدودة في انجاز معاملات المواطنين مما يضطرهم غالبا في الانتظار طوابير الطويلة.

[1] – أحمد درويش، الشفافية والنزاهة حلمنا القادم، نشرية تكنولوجيا الإدارة، العدد8، مارس 2007، وزارة الدولة للتنمية الإدارية، مصر، ص3.

4- إلغاء نظام الأرشيف الوطني الورقي التقليدي: استبداله بنظام الأرشيف الالكتروني لما يوفره من كفاءة ومرونة في إدارة الوثائق بالإضافة إلى قدرته على تصحيح الأخطاء المحتملة بسهولة[1].

_تعزيز الشفافية في الإدارة والقضاء على البيروقراطية للحد من فرص الفساد الإداري وتقليل التعقيدات الإدارية؛

_تحقيق مبدأ العدالة في تقديم الخدمة بدقة وتكلفة وجودة ووقت متساوي مع ضمان المساواة في المعاملة والتقدير والاحترام؛

_تكامل القطاع العام والقطاع الخاص تحت مظلة موحدة من خلال البنية الإلكترونية التي تربط بينهما حيث يعتمد القطاع العام على القطاع الخاص لتوفير السلع والخدمات ويتم هذا التواصل بشكل الكتروني فعال؛

_تحسين أداء المؤسسات الحكومية من خلال مجموعة من الإجراءات التي تهدف إلى خفض الإنفاق الحكومي وتكاليف المباشرة وتعزيز التنسيق بين المؤسسات وتقليل دوره الوقت وتسهيل الوصول والتواصل عبر الخدمات الإلكترونية ويتم ذلك من خلال نشر الطول الرقمية مما يسهم في تحقيق مبادئ الشفافية والعدالة لجميع شرائح المجتمع وتعزيز الديمقراطية.[2]

_تجميع البيانات من مصادرها الأصلية

_توظيف تكنولوجيا المعلومات لدعم وترسيخ ثقافة مؤسسة إيجابية بين جميع العاملين.[3]

---

[1] – قادة دليلة، الإدارة الكترونية ودورها في تحسين الخدمة العمومية، دراسة حالة وزارة الداخلية والجماعات المحلية في الجزائر، رسالة دكتوراه في التسيير العمومي، جامعة الجزائر3، 2017 – 2018. ص ص 81.82 http://dspase.univ.alger3.dz بتاريخ 2025/03/03 على الساعة 10.00.

[2] – الشكير أيوب" الادارة الالكترونية في الجزائر تطبيقات وتحديات"، مجلة الادرة الالكترونية والتنمية للبحوث والدراسات، جامعة لونيسي علي، بليدة2، الجزائر، المجلد8، العدد1، 2019، ص ص 281 http://asjp.cerist.dz بتاريخ 2025/03/04 على الساعة 15.00.

[3] – فريحة رمزي بهاء الدين، المرجع السابق، ص156.

الفرع الثاني: الإستراتيجية الجزائرية الرقمية ومظاهر التحول الإلكتروني

التحول الرقمي يعد من أبرز القضايا الحيوية في عصرنا الحالي ذلك بسبب الانتشار الواسع لشبكة الانترنت وتقنيات المعلومات والاتصالات إذ يمثل التحول الرقمي أحد الأسس الرئيسية لتحقيق الكفاءات والفعالية على المستوى المنظمات بشكل عام بناء على ذلك، سنستعرض من خلال هذا الجزء مفهوم التحول الرقمي، أهميته، والمتطلبات اللازمة لتحقيقه

أولا: تعريف التحول الرقمي

يعرف على أنه عملية تحويل نماذج أعمال المؤسسات الحكومية أو الشركات القطاع الخاص إلى نموذج يعتمد على تكنولوجيات الرقمية في تقديم الخدمات وتصنيع المنتجات وتسيير الموارد البشرية.

كما أنه هناك من يرى أنه يتضمن استخدام التكنولوجيا الرقمية كجزء من آليات العمل بهدف تقديم خدمات أكثر سرعة وفعالية للمستخدمين.

بالإضافة إلى أنها تعرف أيضا على أنها عملية تحويل المؤسسات من نموذج العمل التقليدي إلى نموذج جديد يعتمد على دمج التكنولوجيا الرقمية في عالم الأعمال وتتجسد هذه العملية لتحويل الخدمات

الحيوية والأساسية المرتبطة بخدمة الأفراد والمؤسسات والاستثمارات المختلفة من شكلها التعليمي إلى الشكل الإلكتروني[1].

ثانيا: أهمية التحول الرقمي

تقليل التكاليف والجهود وتحسين كفاءة العمليات التشغيلية وتنظيمها تبسيط الإجراءات للحصول على الخدمات المقدمة للجمهور ما يعزز من فرص تقديم خدمات مبتكرة وإبداعية بعيدا عن الأساليب التقليدية في تقديم الخدمة تعزيز كفاءة سير العمل اليومي وتحسين جودة الخدمات المقدمة للمستفيدين، سهولة وسرعة تطبيق الخدمات الجديدة وزيادة مستويات الشفافية وكذا تحسين الحوكمة يسهمان في تقليص الأخطاء وخفض النفقات بشكل متزامن، زيادة الإنتاجية وتحسين جودة الإنتاج مما يحقق استمرارية الأعمال والخدمات.[2]

ثالثا– متطلبات التحول الرقمي: يتم تطبيقه عن طريق

1– التقنيات: يشمل التحول الرقمي نظاما من الأجهزة البيانات التخزين والبرمجيات التي تعمل ضمن بيئات تقنية ومراكز المعلومات ما يتيح استخدام كل الموارد بكفاءة تشغيلية مستمرة بالإضافة إلى ذلك ينبغي ضمان مستوى خدمة ملائم لأفراد المنظمة عملائها ومورديها، ويتم تحقيق ذلك عبر فرق عمل مسؤولة عن الادارة، النظام التقني والبنية التحتية للشبكة.[3]

[1] – بلقاسمي خالد، دهيمي عمر، "مظاهر التحول الرقمي في الجزائر" ملتقى وطني حول جودة الخدمات في ظل التحول الرقمي والإدارة والالكترونية في المؤسسات الجزائرية رهانات وتحديات تقييم الواقع واستشراف الواقع، بويرة، الجزائر، ص3. http://univ.ghardia.dz بتاريخ 2025/03/04 الساعة 11.00.

[2] – عبد االه شوتري، مريم بوينهي، " دور الاستراتيجية الوطنية للتحول الرقمي في تحقيق أبعاد التنمية المستدامة في الجزائر، رؤية 2030، مجلة المعارف، المجلد18، العدد1، جامعة تيبازة، الجزائر، ص410. http://asjp.cevist.dzبتاريخ 2025/03/06 على الساعة 14.00.

[3] – خيرة شاوشي وزهرة خلوف، "التحول الرقمي في الجزائر مجلة المحاسبة، التدقيق والمالية، جامعة الجيلالي بونعامة خميس مليانة الجزائر، المجلد9 العدد 1، 25/اوت 2023، ص19 . http://asjp.cevist.dzبتاريخ 2025/03/07 على الساعة 14.00.

2- **البيانات:** إذ انه ينبغي على منظمات الأعمال إن تبذل مجهودا منتظمة وفعالة في إدارة وتحليل البيانات وذلك لضمان توفير بيانات الإحصائي والبحث عن البيانات الخاصة بالتنبؤات المستقبلية إضافة إلى ذلك من المهم متابعة البيانات بشكل مستمر لضمان استمراريتها.

3- **الموارد البشرية:** تعتبر الموارد البشرية عنصرا أساسيا لا يمكن الاستغناء عنه في تطبيق التحول الرقمي داخل المنظمات حيث يجب توفير كوادر مؤهلة لديهما القدرة على استخدام البيانات وتحليلها لاتخاذ قرارات فعالة.

4- **العمليات:** تحتاج المؤسسات إلى إنشاء بنية تقنية قوية وفعاله لتعزيز الأداء على المستويات الداخلية والخارجية هذا الإجراء هو المفتاح لضمان نجاح التحول الرقمي الأمثل تشمل هذه البنية وضع سياسات وإجراءات شاملة تغطي جميع نشاطات المؤسسة وعملياتها بحيث تتكامل مع التقنيات اللازمة والتطبيقات المطورة والبيانات المعالجة بطريقة منسقة ومترابطة[1].

رابعا: نماذج التحول الرقمي في الجزائر

لقد حاولت الجزائر مواكبة التحولات الرقمية السريعة التي يعيشها العالم من جهة ورغبتها في إرساء مجتمع المعرفة من خلال استخدام الوسائل التكنولوجية في أداء أعمالها في مختلف القطاعات من جهة أخرى ومن بين نماذج تبنيها مشروع الجزائر الإلكترونية نجد منها:

1- **قطاع وزارة العدالة:** استفاد قطاع العدالة مثل العديد من القطاعات الأخرى من إستراتيجية التحول الرقمي من خلال دمج التكنولوجيا الورقية بأخرى الكترونية باستخدام التصديق الالكتروني لما يتيح للمواطن إدارة ومتابعة قضاياه عبر الانترنت بسهولة كباقي ذلك استخراج شهادة الجنسية وصحيفة السوابق العدلية رقم 3 بالإضافة إلى ذلك يتم إرسال الوثائق الالكترونية بصورة آلية وتستخدم تقنية التواصل المرئي عن بعد[2]

[1] – خيرة شاوشي وزهرة خلوف، المرجع السابق ص20.

[2] – بلقاسمس خالد، دهيمي مراد، المرجع السابق، ص6.

2- قطاع وزارة البريد والمواصلات السلكية واللاسلكية: أطلقت الجزائر مجموعة من الخدمات الرقمية حيث شاهد بريد الجزائر تقدما ملحوظا في تقديم خدمات رقمية حديثة يتضمن ذلك توافر الخدمات عبر أجهزة الصرف الآلي والخدمات عن بعد فضل عن التعاملات عبر المكاتب البريدية كما تم استحداث مكاتب بريد المتنقلة على شكل حافلات والتي باتت تقدم خدمات واسعة للمواطنين وتشمل هذه الخدمات الرقمية ما يلي:

أ_البطاقة الذهبية: إذ يقدم بريد الجزائر لعملائه نوعين من البطاقات الذهبية البطاقة العادية والبطاقة الذهبية المدفوعة

ب_ تعبئة رصيد الانترنت والهاتف المحمول: إذ يتم ذلك بسهولة وبسرعة باستخدام البطاقة الذهبية إن تتم عملية الدفع بأمان تام بدون مخاطر.

ج_ تطبيق بريد موب: حيث انه عن طريق تطبيق بريد موب الذي يعد تطبيقا للهاتف المحمول يمكن التسجيل والدخول بسهولة لإدارة حسابات البريد والعمليات المالية من أي مكان وفي أي وقت براحة وسير.

د_ دفع الفواتير عبر الانترنت: اذ يوفر بريد الجزائر للعملاء إمكانية سداد الفواتير عبر الانترنت بالإضافة إلى مختلف المدفوعات مثل فاتورة المياه فواتير الكهرباء باستخدام الهاتف المحمول وتتطلب ذلك إدخال معلومات البطاقة الذهبية والمبلغ المراد دفعه ثم تأكيد العملية.[1]

3- قطاع التعليم العالي والبحث العلمي: تعتزم الوزارة إطلاق 36 منصة رقمية جديدة في إطار جهودها المستمرة لرقمنة القطاع تشمل هذه المنصات منصة الشباك الموحد الالكتروني ومنصة التوثيق والتصديق على الشهادات الجامعية للخريجين بالإضافة إلى منصة الحافظة الإلكترونية التي تدعم

[1] – بلقاسمي خالد ودهيمي عمر، المرجع السابق ، ص8

التصديق الالكتروني وهناك أيضا منصة مخصصة لنشر الأبحاث العلمية في مجال الطب ومنصة خاصة بشهادات تبرئة الخدمة.[1]

4_قطاع وزارة العمل و التشغيل و الضمان الاجتماعي: لقد بادرت الحكومة الجزائرية بتفعيل تكنولوجيا المعلومات والاتصال وشبكة الانترنت لتعزيز خدماتها الرقمية ودفع عجلة التطور في إطار ذلك أطلقت مشروع البطاقة الإلكترونية للضمان الاجتماعي المعروفة ببطاقة الشفاء في عام 2005 بهدف تحديث نظام الضمان الاجتماعي الوطني توفر هذه البطاقة لحاملها سرعة الحصول على التعويضات دون الحاجة لتقديم مستندات مكتوبة أو ملا استمارة وإرفاق ورقة العلاج وذلك بعد التحقق من هوية المستفيدين لضمان تقديم الخدمات المتاحة عبر الضمان الاجتماعي.[2]

5–قطاع وزارة الموارد المالية: يعد قطاع الموارد المالية من بين القطاعات التي سارعت في اعتماد الرقمنة في الجزائر حيث أطلقت في واحد ديسمبر 2020 تطبيقا الكترونيا يسمى خدمتي موجها لمستخدمي ومهني قطاع المياه يأتي هذا في إطار القطاع وتبسيط الإجراءات الإلكترونية مما يساهم في تحسين الخدمة العامة والقضاء على البيروقراطية.

كما يساعد التطبيق أيضا المواطنين في الدفع الالكتروني للفواتير بالإضافة إلى انه يتيح لجميع الزبائن والمتعاملين في قطاع الموارد المائية الوصول إلى البوابة الالكترونية لعرض انشغالاتهم ومتطلباتهم وإرسال ملفاتهم عبر هذه المنصة ومن خلال ما تم ذكره يظهر إن الجزائر حاولت رقما كل القطاعات لمواكبة التحولات السريعة التي يشهدها العالم وعصرنة القطاع العام من جهة وتسهيل العمل الإداري وترقية الخدمة والتقريب بها المواطنين من جهة أخرى[3]

الفرع الثالث: متطلبات الإدارة الالكترونية في الجزائر

[1] – المرجع نفسه، ص9

[2] – بلقاسمي خالد دهيمي عمر، المرجع سابق، ص8

[3] – المرجع نفسه، ص6.

تمثل الإدارة الإلكترونية عملية معقدة والنظام متكامل للتضمن مكونات تقنية ومعلوماتية ومالية وتشريعية وبيئية وبشرية وغيرها لذا من الضروري توفر مجموعة من المتطلبات المتكاملة لتطبيق الإدارة الالكترونية وتحويلها إلى واقع عملي.

أولا– المتطلبات الإدارية: وتتمثل في

1– **وضع الاستراتيجيات وخطط التأسيس:** ويتطلب الأمر إنشاء إدارة أو هيئة متخصصة في التخطيط والمتابعة والتنفيذ لوضع خطط المشروع الإدارة الإلكترونية كما ينبغي الاستعانة بالجهات الاستشارية والبحثية لإجراء الدراسات اللازمة وتحديد المواصفات العامة والمعايير الخاصة بالإدارة الإلكترونية بالإضافة إلى ضمان التكامل والتوافق بين المعلومات والمرتبطة بأكثر من جهة.[1]

2– **القيادة والدعم الإداري:** ان تغيير القيادة من ابرز العوامل المؤثرة في نجاح أو فشل إي مشروع حيث تعد المفتاح الأساسي لتحقيق النتائج الموجودة أين يلعب دعم الإدارة وقدرتها على خلق بيئة عمل ملائمة دورا حيويا في نجاح الإعمال كما أن التزام القيادة يعتبر أمرا ضروريا بالدعم جميع جوانب الاستراتيجيات المؤسسة بالإضافة إلى ذلك فان متابعة القيادة للمشروع وتقديم المعلومات المرتدة تساهم في ضمان نجاحه وتطويله علاوة على ذلك فان قناعة واهتمام الإدارة العليا بتطبيق تكنولوجيا المعلومات في المؤسسات تعتبر من العوامل المساعدة في تحقيق نجاح تطبيق الإدارة الإلكترونية[2].

3– **وضع الأطراف التشريعية الضرورية أو تعديل التشريعات الحالية وتحديثها وفق المستجدات:**

[1] – موسى عبد الناصر، محمد قريشي، مساهمة الادارة الالكترونية في تطوير العمل الادراي بمؤسسة التعليم العالي (دراسة حالة كلية العلوم والتكنولوجيا) مجلة الباحث جامعة بسكرة الجزائر، العدد9، 2011، ص90.

[2] – موسى عبد الناصر، محمد قريشي، المرجع نفسه ص90.

يعد ذلك من خلال إصدار القوانين والأنظمة والإجراءات التي تسهم في تسهيل التحول نحو الإدارة الإلكترونية تماشياً مع المتطلبات الجديدة، إذ إن معظم التشريعات والقوانين الحالية وُضعت في سياق تقليدي، وبالتالي فقد أُسست لأداء العمل وفق معايير تتطلب التفاعل المباشر بين الموظف وطالب الخدمة، بالإضافة إلى الاعتماد على الشهادات الموثوقة. لذا، فإن الانتقال إلى الإدارة الإلكترونية يستلزم وجود بيئة قانونية وتشريعية جديدة. كما أن وجود التشريعات والنصوص القانونية يسهم في تعزيز فعالية الإدارة الإلكترونية، ويمنحها المشروعية والمصداقية اللازمة لكافة النتائج القانونية المترتبة عليها.[1]

4- **تعليم وتدريب العاملين وتوعية والتثقيف العامين:** تتطلب الإدارة الإلكترونية إجراء تغيرات جذرية في نوعية الموارد البشرية المناسبة لها وهذا يستدعي إعادة تقييم نظم التعليم والتدريب الحالية لتلبية متطلبات التحول الجديد ويشمل ذلك إعداد الخطط والبرامج التعليمية والتدريبية على جميع المستويات بالإضافة إلى نوعية أفراد المجتمع بثقافة والطبيعة الإدارة الالكترونية هو سائل استخدامها للمواطنين وتوجيهها بواسطة معا ومراكز تدريب متخصصة وتابعة للحكومة كما يجب تهيئة الاستعداد النفسي والسلوكي والتقني والمادي وغيرها من المتطلبات اللازمة للتكيف مع متطلبات الإدارة الالكترونية.[2]

5- **الهيكل التنظيمي:** نتيجة لعدم ملاءمة النموذج الهرمي التقليدي للمؤسسات، الذي كـــــان سائداً في عصر الصناعة، لنماذج الأعمال الجديدة في عصر تكنولوجيا المعلومات والأعمال التكنولوجية، نجد أن الهياكل التنظيمية المناسبة للأعمال الإلكترونية تتمثل في المصفوفات والشبكات

[1] – محمد جد حسين وأشرف محمود أحمد، المرجع السابق ص63

[2] – حبيبة ذهبية "الادراة الالكترونية ودورها في تحسين الخدمة العمومية، دراسة حالة بلدية خنشلة، مذكرة ماستر، جامعة 8 ماي 1945، قالمة 2015-2016 ص 55. http://dspace.univ.galma.dz بتاريخ: 2025/03/11 على الساعة 10.00.

وتنظيمات الخلايا الحية، التي تتسم بسرعة الاتصالات. وتتطلب تطبيق هذه التغيرات إجراء تعديلات في الجوانب الهيكلية والتنظيمية والإجراءات والأساليب، بحيث تتماشى مع مبادئ الإدارة الإلكترونية.

ويمكن تحقيق ذلك من خلال إنشاء إدارات جديدة، أو إلغاء أو دمج بعض الإدارات القائمة، بالإضافة إلى إعادة تصميم الإجراءات والعمليات الداخلية بشكل ملائم لتطبيق الإدارة الإلكترونية بصورة أسرع وأكثر كفاءة وفعالية، مع مراعاة أن يتم هذا التحول ضمن إطار زمني تدريجي يتماشى مع المراحل التطورية.

ثانيا: المتطلبات البشرية: يعد العنصر البشري الركيزة الأساسية في أي منظمة، إذ لا يمكن للمنظمات تحقيق أهدافها، حتى وإن امتلكت أحدث المعدات والتقنيات، ما لم تتوفر لديها كوادر بشرية مؤهلة بشكل جيد وذات كفاءة عالية. ومن هذا المنطلق، تبرز أهمية تأهيل الكوادر البشرية المتخصصة التي ترتبط بالبيئة المعلوماتية ونظم العمل عبر شبكات الاتصال الإلكترونية.

ويمكن تحقيق ذلك من خلال تنفيذ برامج تدريبية مخصصة، تسهم في إعداد الكفاءات الفنية المطلوبة لضمان تحقيق الأداء المطلوب في تطبيقات الإدارة الإلكترونية، وبهدف التدريب على الشبكة، الذي يمثل أهم ركيزة لتحقيق مشروع الإدارة الإلكترونية.

كما توجد مجموعة من المتطلبات البشرية، والتي يمكن تحديدها على النحو الآتي:

–تحديد وتحليل الاحتياجات الحالية والمستقبلية للكفاءات المؤهلة في مجالات المعلومات، وتطوير البرمجيات، والعمل عبر الإنترنت، مع جذب الكفاءات المتميزة والمتخصصة في مجالات نظم المعلومات وتطوير البرمجيات.

–وضع آليات فعالة تهدف إلى الحفاظ على الأفراد، وتعزيز قدراتهم، وتقديم الحوافز التي تدعم تطويرهم المستمر، والتمكين الإداري، الذي يعد من أهم الركائز الرئيسية للإدارة الإلكترونية، حيث يتطلب تعزيز وتطوير المورد البشري لتأهيل كوادر متخصصة تمتلك مستوى عالياً من المهارات المتنوعة.

وتُعد هذه المهارات مرتبطة بشكل أساسي ببيئة نظم المعلومات، وتشمل قواعد البيانات وآليات العمل في إطار شبكة الإنترنت.[1].

ثالثا: المتطلبات المالية

يعد مشروع الإدارة الإلكترونية من المشاريع الكبرى التي تتطلب استثمارات مالية ضخمة ودعما ماليا مكلفا لتصميم وتطوير البرمجيات الإلكترونية اللازمة بالإضافة إلى الموارد المالية المطلوبة لصيانة الأجهزة وضمان الاستعانة بالمدرب المؤهلين لتدريب الكوادر البشرية على استحداث احدث التقنيات والأنظمة ويهدف المشروع إلى تحقيق استمرارية ونجاح مستدام مع التركيز على تحسين البنية التحتية وتوفير الأجهزة والأدوات المطلوبة بالإضافة إلى تحديث البرمجيات بشكل دوري وتدريب الموارد البشرية بصورة مستمرة ومشروع الإدارة الالكترونية يعد من المشاريع الكبيرة والضخمة التي تتطلب تمويلا ضخما وكافيا لضمان نجاحها لذلك من الضروري توفير الموارد المالية الكافية مع تخصيص ميزانية مستقلة لهذا المشروع، وينبغي أن تكون هذه الميزانية خاضعة للمراجعة الدورية لضمان استمرارية التموين بشكل مستدام.[2]

رابعا: المتطلبات الأمنية

تعتبر ضرورة تحقيق الأمن الالكتروني والحفاظ على السرية الالكترونية امرأ بالغا الأهمية لضمان حماية المعلومات الوطنية والشخصية بالإضافة إلى صيانة الأرشيف الالكتروني من أي تلاعب أو اختراق ويجب أن يتم التركيز على امن الدولة والأفراد سواء من خلال تضمين الأمن في برمجيات بروتوكولات الشبكة أو باستخدام تقنيات مثل التوقيع الالكتروني وكلمة المرور حيث إن المعلومات والوثائق التي يتم حفظها ومعالجتها أو نقلها الكترونيا التنقي متطلبات العمل ونقلها إلكترونين لتنفيذ متطلبات العمل يجب إن تكون محمية بشكل جيد والحفاظ على أمنها من اجل تحقيق امن المعلومات

[1] – كمال فار، المرجع السابق، ص89.

[2] – فراخة رمزي بهاء الدين، المرجع السابق، ص 154.

والحد من التأثيرات السلبية المحتملة لاستخدام شبكة الانترنت وتتصلب الالكترونية اتخاذ بعض الإجراءات اللازمة للضمان حماية البيانات وسلامتها وهي:

-صيانة السياسات الأمنية المتعلقة بتقنيات المعلومات، بما في ذلك استخدام خدمة الانترنت؛[1]

-وضع إستراتيجية وطنية لأمن المعلومات تهدف إلى تعزيز التعاون بين مؤسسات القطاعين العام والخاص لضمان حماية فعالية البيانات وتامين البنية التحتية الرقمية؛

-صياغة القوانين واللوائح التنظيمية التي تسهم في الحد من جرائم السطول الالكتروني وانتهاك خصوصية البيانات ضمن نطاق الإدارة الالكترونية؛

- إضافة الى مجموعة من المتطلبات الأخرى لضمان حماية أمل نظم المعلومات وضع آليات فعالة للمراقبة والتنفيذ على نظم المعلومات نحو الشبكات الحاسوبية الذي يتطلب تحديد مجموعة من الإجراءات والضوابط التي تتضمن حماية البيانات وسلامة العمليات الرقمية؛

- الاحتفاظ بنسخ احتياطية لأنظمة المعلومات بطريقة امن يعتبر من أحد العناصر الأساسية لضمان استمرارية العمل وحماية البيانات من الفقدان ومن المهم تطبيق إجراء اتصال لتامين نسخ احتياطية مثل استخدمت تقنية التشفير وتخزين النسخ في مواقع متعددة إلى جانب الاعتماد على أنظمة حماية متطورة للكشف عن أي محاولات اختراق بالإضافة إلى ذلك يجب التحقق دوريا من صلاحية النسخ الاحتياطية واختيار استعادة البيانات للتأكد من جاهزيتها في حالات الطوارئ.[2]

المبحث الثاني: الإطار القانوني لحماية البيانات الشخصية في التشريع الجزائري

إن حماية البيانات ذات الطابع الشخصي تمثل أحد مرتكزات حماية الخصوصية في العصر الرقمي، نظراً لما تشهده المجتمعات الحديثة من توسع في استخدام تكنولوجيا المعلومات والاتصالات.

[1] – مولاي خليل وعمار طهرات، المرجع السابق، ص16.

[2] – موسى عبد الناصر ومحمد قريشي، المرجع السابق، ص92.

وقد عمل المشرع الجزائري على سن جملة من النصوص المتعلقة بجمع ومعالجة المعطيات الشخصية، من أجل تحقيق التوازن بين حماية حقوق الأفراد من جهة، وتسهيل المعاملات الإلكترونية من جهة أخرى.

وقد جاءت هذه النصوص في شكل قوانين متخصصة وأخرى عامة، تعكس سعي الدولة لتعزيز الإطار القانوني المنظم لهذا المجال. ويتجلى هذا الإطار في محورين أساسيين، نتناولهما من خلال مطلبين.

المطلب الأول: الأسس الدستورية والتشريعية لحماية البيانات الشخصية

لقد كرس المشرع الجزائري من خلال المنظومة الدستورية والتشريعية مبدأ حماية الحياة الخاصة وحرمة المعطيات ذات الطبع الشخصي باعتبارها من الحقوق الأساسية التي يتمتع بها الفرد وقد أتى هذا التكريس من خلال نصوص دستورية واضحة ومن هذا المنطلق جاء الإطار التشريعي ليجسد هذه الحماية من خلال سن قوانين تنظيمية تؤثر عملية جمع ومعالجة البيانات وتضع ضوابط صارمة لحماية حقوق الأفراد ويعتبر القانون رقم 18-07 أهم نص تشريعي في هذا المجال إلى جانب جملة من النصوص القانونية الأخرى التي تدعم هذا التوجه وتكمل الإطار القانوني العام.

الفرع الأول: الحماية الدستورية للبيانات الشخصية

تعد حماية المعطيات الشخصية للإفراد الطبيعيين حقا دستوريا حيث نص عليها دستور 2020 في المادة 47 منه التي جاء فيها حماية الأشخاص عند معالجه المعطيات ذات الطبع الشخصي حق أساسي وفي هذا الإطار كرس القانون رقم 04-15 المعدل والمتمم للأمر 66-156 المتضمن وقانون العقوبات حماية المعطيات عند معالجتها فقط خصص لها القسم السابع المكرر الثالث

بعنوان المساس بأنظمة المعالجة الآلية المعطيات وقد تناول المشرع الجزائري من خلال المواد من 394 مكرر إلى 394 مكرر 7 مختلف الأفعال المجرمة التي تعد مساسا بأنظمة المعالجة مثل التخريب التصميم البحث التجميع التعديل النشر والاتجار بالمعلومات.

كما تم تحديد العقوبات المناسبة لهذه الأفعال حيث تنص القوانين على الغرامات تتراوح ما بين 50.000دج و تصل إلى 100.000دج بحسب جسامات الفعل المرتكب عقوبة الحبس تبدأ من ثلاث أشهر حد أدنى وتصل إلى ثلاث سنوات حسب طبيعة الجريمة وتطبق هذه العقوبات سواء كان مرتكب الجريمة فاعلا أصليا أو شريكا وذلك وفق على المادة 394 مكرر خمسه كما لم تقتصر العقوبات على أشخاص الطبيعيين فقط بل شملت أيضا الأشخاص المعنويين حيث نصت المادة 394 مكرره 4 على أن يعاقب الشخص المعنوي الذي يرتكب لأحدى هذه الجرائم بغرامة تعادل 5 أضعاف الحد الأقصى للغرامة المقررة للشخص الطبيعي.[1]

أما المادة 394 مكرر ستة فقط أكدت على أمكانية مصادره الأجهزة والبرمجيات والوسائل المستخدمة في ارتكاب الجريمة بالإضافة إلى إغلاق المواقع الالكترونية التي كانت وسيله لارتكاب شريطه إن يكون مالك الموقع على علم بارتكاب الفعل الإجرامي في محله أو مكان استغلاله وفي السياق نفسه[2] أولى المشرع الجزائري اهتماما خاصا بحماية الأطفال من الاستغلال عبر الانترنت من خلال المادتين 141 و 142 ومن قانون حماية الطفل رقم 12-15 حيث جرم كل من يقوم بانتهاك خصوصية الطفل واستغلاله عن طريق نشر أو بث بصوره أو بياناته عبر أي وسيله كانت ومهما كان شكلها[3].

---

[1] – القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر رقم 66- 156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية العدد 71، الصادرة بتاريخ 15/نوفمبر 2004، ص113. http://www.joradp.dz التاريخ 2025/03/15 على الساعة 15.00.

[2] – المادة 394 المكرر 6 المصدر السابق، ص113.

[3] – القانون رقم 12/15 المؤرخ في 15 جويلية 2015 المتعلق بحماية الطفل الجريدة الرسمية للجمهورية، العدد39، الصادر بتاريخ 19 جويلية 2015. http:/wipolex-res.wipo.in بتاريخ 2025/03/16 على الساعة 15.00.

كما اصدر المشرع الجزائري القانون رقم 18-07 المتعلقة بحماية الأشخاص الطبيعيين في مجال معالجه المعطيات ذات الطابع الشخصي بهدف تنظيم هذا المجال وضمان حماية الحياة الخاصة للأفراد وبين هذا القانون نطاق معالجه المعطيات الشخصية واليات حمايتها كما أنشأت بموجب سلطه وطنيه مستقلة على تنفيذ أحكامه وتناول الباب الثاني من القانون المبادئ الأساسية لحماية المعطيات الشخصية حيث نصت المادة 7 على ضرورة الحصول على الموافقة صريحة من الشخص المعني قبل الشروع في معالجته بياناته الشخصية مع منحه الحق في سحب موافقته في أي وقت غير إن هذه الموافقة ليست مطلوبة عندما تكون المعالجة ضرورية للامتثال لالتزام قانوني يخص الشخص المعني.[1]

أما فيما يتعلق بمعالجة معطيات الاطفال فقد أوجبت المادة 8 الحصول على موافقة ممثليهم الشرعيين أو الترخيص من القاضي المختص عند الضرورة ويمكن لهذا الاخير منح التراخيص دون موافقة الممثلين الشرعيين إذا اقتضت مصلحة الطفل ذلك.[2]

وفيما يخص طرق المعالجة فيجب أن تكون الأغراض واضحة محددة مشروعه وتحترم طوال مده الاستخدام المعطيات والاحتفاظ بها كما ألزم القانون بإيداع تصريح مسبق يتضمن تفاصيل المعالجة لدى السلطة الوطنية المستقلة ويمكن تقديمه الكترونيا فورا أو خلال مهله أقصاها يومان ويسمح للمسؤول عن المعالجة بالشروع في المعالجة مباشره بعد استلام وصل إيداع.[3]

نصت المادة 17 من نفس القانون على إن أي معالجة للمعطيات التي قد تشكل خطرا على احترام وحماية الحياة الخاصة يجب إن تخضع لترخيص مسبق يصدر بقرار معلل يبلغ إلى المسؤول عن المعالجة في اجل يتعدى 10 أيام من تاريخ إيداع تصريح كما يمنح الترخيص بمعالجه المعطيات الحساسة في الحالات التي تكون فيها المعالجة ضرورية لحماية المصالح الحيوية للشخص المعني أو

[1] – المادة7 من القانون 07/18 المصدر السابق.

[2] – المادة 8 من القانون12/15، المصدر الساق.

[3] – جندلي ووريدة، " حماية المعطيات الشخصية في ضوء التشريع الجزائري والمواثيق الدولية بين الضمانات والتحديات، مجلة البحوث القانونية والسياسية، جتمعة20 أوت 1955 سكيكدة، العدد1، مارس 2022، ص1419. https://asjp.cerist.dz بتاريخ 2025/03/15 على الساعة 14.00.

للشخص أخر[1] من جهة أخرى منحت المادة 35 من القانون 18-07 الحق في طلب تصحيح أو تحسين أو حذف أو حجب المعطيات الشخصية متى تبين أن هذه المعطيات غير كاملة أو غير صحيحة أو انأ معالجتها تخالف أحكام القانون[2] أما المادة 36 من نفس القانون فقد منحت للشخص المعني الحق في الاعتراض على معالجة معطياته الشخصية خاصة إذا كانت الغاية منها أغراضا دعائية أو تجارية[3]

كما ألزمت المادة 40 من هذا القانون المسؤول عن المعالجة باتخاذ جميع التدابير التقنية والاحترازية اللازمة لتامين وحماية المعطيات من الفرضية التلف أو أي استخدام غير مشروع بالإضافة الى التزامه بواجب السر المهني وعدم إفشاء المعطيات التي اطلع عليها أثناء ممارسة مهامه.[4]

بالنظر إلى ما سبق يتضح أن المشرع الجزائري قد خطا خطوة ايجابية في مجال تنظيم معالجة المعطيات ذات الطابع الشخصي حيث أدرج القسم السابع مكرر من قانون العقوبات لتحديد الأفعال التي تمس بأنظمة معالجة المعطيات مع بيان العقوبات المناسبة لكل فعل ومن جهة أخرى اصدر القانون المتعلق بحماية الأشخاص المطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والذي انشأ من خلاله آليات لحماية هذه المعطيات، من بينها السلطة الوطنية ذات الطابع الشخصي ورغم أن هذه الخطوة التشريعية جاءت متأخرة نسبيا مقارنة بالتطور السريع في تكنولوجيا الإعلام والاتصال، الا انها تظل خطوة محمودة نحو تعزيز حماية المعطيات الشخصية في الجزائر [5]

الفرع الثاني: القانون رقم 18 07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة البيانات ذات الطابع الشخصي

[1] – المادة17 من القانون 07/18 المصدر السابق.

[2] – المادة 35 ، المصدر نفسه.

[3] – المادة36، المصدر نفسه.

[4] – المادة 40 من القانون 07/18 المصدر السابق

[5] – جندلي وريدة، المرجع السابق ص 140.

يهدف القانون رقم 18-07 إلى حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي من خلال تنظيم جمعها مستخدميها وضمان سريتها يعكس هذا القانون التزام الدولة لحماية الحقوق والحريات الفردية في العصر الرقمي.

أولا/حقوق الشخص المعني والتزامات المسؤول عن المعالجة

عالج المشرع الجزائري حقوق الشخص المعني بالمعالجة في الباب الرابع حيث قصرها على جملة من الحقوق الأساسية تشمل حق الأعلام وحق الولوج وحق التصحيح وحق الاعتراض ومنع الاستكشاف المباشر أما في الباب الخامس فقد بين المشرع الالتزامات الملقاة على عاتق المسؤول عن المعالجة، وذلك من خلال:

1- الحق في الإعلام

اوجب المشرع على المسؤول عن معالجة المعطيات الشخصية إعلام كل شخص يتم جمع معطيات بهوية المسؤول عن معالجة أو ممثله والغرض من هذه المعالجة وكل معلومة أخرى مفيدة ويشمل هذا الالتزام حتى الحالات التي يتم فيها جمع المعطيات بطريقة غير مباشرة أو دون اتصال مباشر بالشخص المعني بما في ذلك جمع المعطيات عبر الشبكات المفتوحة.[1]

وفي حال كان الشخص المعني غير على علم مسبق بوجود معطياته على هذه الشبكات يتعين تنبيه وإعلامه بمكانيه استغلال معطيات الشخصية دون ترخيص منه غير إن المشرع استثنى من هذا الالتزام بعض الحالات حيث تسقط التزاميه الإعلام إذا تعذر إبلاغ الشخص المعني على ان يتم إشعار السلطة الوطنية بذلك مع تقديم مبررات واضحة توضح أسباب التعذر.[2]

2- الحق في الولوج والحق في التصحيح

يتمتع الشخص المعني بحق الاطلاع على ما إذا كانت بياناته الشخصية قد خضعت للمعالجة ومعرفة أهداف تلك المعالجة والجهات التي يتم تزويدها بهذه البيانات كما يحق له الحصول على نسخة

[1] - العيداني محمد ويوسف زروق، المرجع السابق ص124.

[2] - المرجع نفسه، ص124.

من البيانات التي تم جمعها ومعرفة مصادرها يحق للمسؤول عن المعالجة المعطيات الاعتراض إمام السلطة الوطنية على طلبات الولوج إذا كانت تعسفية أو مكررة كما يمكنه طلب تحديد مهلة للرد إذا لم يكن بإمكانه الاستجابة الفورية.[1]

أما فيما يتعلق بحق التصحيح فقد نصت المادة 35 على أحقية الشخص في الحصول دون أي مقابل على تحديث، أو تصحيح أو مسح أو إغلاق بياناته الشخصية من قبل المسؤول عن المعالجة وذلك في حالات محدده من خلال اجل أقصى عشر أيام من تاريخ الإخطار كما يحق للشخص المعني اللجوء إلى السلطة الوطنية في حالة وجود خلاف بشأن معالجة معطياتها الشخصية علاوة على ذلك يحق له إعلام الجهات التي سبق ان تلقت بياناته بأي عملية تصحيح أو مسح أو إغلاق تمت عليه وفي حال وفاة الشخص المعني تنتقل هذه الحقوق إلى ورثته.[2]

3- الحق في الاعتراض ومنع الاستكشاف المباشر

من أبرز الحقوق التي كلفها القانون للإفراد هو الحق في الاعتراض على معالجة بياناتهم الشخصية لاسيما إذا كان الهدف منها تجاريا أو دعائيا ويشمل هذا الحق أيضا منع استخدام البيانات في الاستهداف المباشر عبر إي وسيلة دون الحصول على موافقة مسبقة من الشخص المعني ويعد هذا الحق وسيلة حماية مهمة خاصة لزبائن خدمات الهاتف النقال الذي يلقون يوميا رسائل دعائية ومسابقات وهمية دون إن يعرفوا كيف حصل المرسلون على أرقامهم أو من هم هؤلاء المرسلون مما يصعب عليهم إيقاف هذه الرسائل أو تقديم شكوى بحقهم.[3]

ثانيا: التزامات المسؤول عن المعالجة

1- سرية وسلامة المعالجة

[1] – المرجع نفسه، ص125.

[2] – المادة 35 من القانون 07/18 المصدر السابق.

[3] – العيداني محمد ويوسف زروق، المرجع السابق ص126

يلتزم المسؤول عن المعالجة وفقا لإحكام هذا القانون باتخاذ كافة التدابير التقنية والإجراءات الوقائية اللازمة لحماية وتامين المعطيات ذات الطابع الشخصي من أي اختراق أو تلف أو استخدام غير مشروع لاسيما عند نقلها عبر شبكة معينة وتزداد درجة هذه التدابير تبعا لأهمية المعطيات المعالجة وفي حال استعان المسؤول عن المعالجة بمسؤول أخر يعرف بالمعالجة من الباطن لتنفيذ بعض المهام النيابة عنه يتعين على هذا الأخير تقديم الضمانات الكافية التي تضمن سلامة وامن المعطيات الشخصية.

ويجب إن يتم هذا التعويض بموجب عقد أو سند قانوني مكتوب أو بأي وسيلة يمكن حفظها لاستخدامها كدليل عند الحاجة ويمضي هذا العقد بشكل واضح على ان المعالج من الباطن لا يجوز له التصرف إلا بناء على تعليمات وتوجيهات صريحة من المسؤول الأصلي عن المعالجة وذلك بهدف تحديد المسؤوليات القانونية بشكل دقيق وضمان عدم ضياع حقوق الأفراد بين طرفين كما يلتزم كل من المسؤول عن معالجة والمعالج من الباطن باحترام مبدأ السر المهني حتى بعد انتهاء مهامهم وذلك وفق لإحكام القانون العام وما ينص عليه هذا القانون.[1]

2- معالجة المعطيات الشخصية في مجال التصديق الالكترونين وفي مجال الاتصالات الالكترونية

يلزم مؤدو خدمات التصديق الالكتروني بمعالجة المعطيات الشخصية اللازمة لإصدار الشهادات الالكترونية وحفظها دون استخدامها لأي أغراض أخرى إلا بعد الحصول على موافقة صريحة من أصحابها كما يلزم مقدم خدمات الاتصالات الالكترونية بعد اتخاذ كافة الضمانات اللازمة لحماية هذه المعطيات بإبلاغ السلطة الوطنية المعينة والشخص المعني في حال حدوث أي مساس بالحياة الخاصة مثل الإتلاف أو الضياع أو الإفشاء أو الولوج غير مصرح به ويتعين عليهم أيضا توثيق جميع الانتهاكات التي تمس المعطيات الشخصية والإجراءات المتخذة بشأنها.[2]

[1] – العيداني محمد ويوسف زروق، المرجع السابق، ص126.

[2] – المرجع نفسه ، ص126.

3- نقل المعطيات نحو دولة أجنبية

منح القانون 18 07 السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي الحق في التلخيص بنقل هذه المعطيات إلى دولة أجنبية بشرط أن يتضمن هذه الدولة مستوى كاف من حماية الحياة الخاصة والحريات والحقوق الأساسية للأفراد بالإضافة التي توفرها على الإجراءات الأمنية الملائمة وإلا بشكل هذا النقل تهديدا للأمن العمومي أو المصالح الحيوية للدولة وبهذا يوفر القانون حماية قانونية الوطنية التي كانت سابقا في متناول الشركات الأجنبية العاملة في الجزائر خاصة شركة الاتصال ومزودي خدمة الانترنت والسفارات التي تتلقى يوميا ألاف طلبات التأشيرة ما عرفتها من معطيات شخصية قابلة للتحويل بسهولة إلى خارج في ظل غياب إطار قانوني يمنع ذلك.[1]

كما نصت المادة 45 على استثناءات تتيح نقل المعطيات الشخصية إلى الخارج حتى في حال عدم توفر دوله الأجنبية المستقلة على الشروط المشار إليها وذلك في حالات محددة من بينها الحصول على الموافقة الصريحة للشخص المعني إذا كان النقل ضروريا الحماية حياة هذا الشخص أو المحافظة على مصلحة عامة إذا اقتضى الأمر احترام التزام قانوني أو ضمان اثبات حق أو الممارسة أو الدفاع عنهم إمام القضاء وغيرها من الحالات الاستثنائية التي حددها القانون على سبيل الحصر.[2]

ثانيا : آليات الحماية الإدارية والجزائية للمعطيات ذات الطبع الشخصي

1/ الإجراءات الإدارية

منح المشرع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي صلاحية اتخاذ إجراءات إدارية ضد المسؤول عن معالجة في حال الإخلال بالشكليات المنصوص عليها في أحكام القانون رقم 18-07 وتشمل هذه الإجراءات توجيه إنذار أو اعذرا او فرض غرامة أو السحب المؤقت للترخيص أو التصريح لمدة لا تتجاوز سنة او السحب النهائي لهما إضافة الى معاينة المجلات والأماكن المعينة.

[1] – المرجع نفسه، ص127.

[2] – المادة 45 من القانون 18-07 المصدر السابق.

كما يحق للمسؤول المعني الطعن في هذه القرارات أمام مجلس الدولة ومن جهة أخرى دخول المشرع للسلطة الوطنية فرض غرامة ماليه تصل الى500.000دج على كل مسؤول عن المخالفة يمتنع دون مبرر قانوني عن احترام حقوق الأفراد في الإعلام أو الولوج أو التصحيح أو الاعتراض أو في حال عدم التبليغ للسلطة الوطنية.[1]

وفي سياق أخر أجازه المشرع السلطة الوطنية حسب الحالة ودون حاجة لوصول التصريح أو الترخيص إن تتخذ قراراتها إذا تبين بعد إجراء المعالجة إن التصريح أو الترخيص من شانه المساس بالأمل الوطني أو مخالف للأخلاق أو الآداب العامة.[2]

2/الأحكام الجزائية

يتضمن القانون رقم 18-07 عدة مخالفات تعد جرائم تمس معالجة البيانات ذات الطبع الشخصي وذلك عند مخالفة القواعد القانونية الخاصة بالمعالجة أو في حال جمع البيانات أو استخدامها أو التصرف فيها بطريقة غير قانونية أو نتيجة إهمال عن المعالجة لواجباته وعرقلة عمل السلطة الوطنية ومن بين هذه المخالفات ما يلي:

1- معالجة البيانات دون احترام الكرامة الإنسانية وحرمة الحياة الخاصة والحريات العامة

تنص المادة 54 من القانون 18 07 على معاقبة من يعالج البيانات دون احترام القيام المذكورة بعقوبات مشددة وفقا للتشريع الساري ويمكن إن نصل العقوبة إلى الحبس من سنتين إلى خمس سنوات وغرامة من200.000دج إلى 500.000دج[3]

2-معالجة البيانات دون موافقة الشخصي المعني

[1] – المادة 48 المصدر نفسه.

[2] – يزيد بوجليط؛ عبد الرحمان فطناسي،" الحماية الادارية في مجال المعطيات ذات طابع شخصي على ضوء القانون 18-07، مجلة أبحاث القانونية والسياسية، جامعة 8 ماي قالمة، الجزائر، مجلد6، العدد2، 31ديسمبر2021، ص70. https://asjp.cerist.dzبتاريخ 2025/03/15 على الساعة، 14.00.

[3] – المادة 54 من القانون 18-07 المصدر السابق.

بحسب المادة 55 من القانون 18 07 يعاقب من يعالج البيانات دون موافقة الشخص المعني بالحبس من سنة إلى ثلاث سنوات وغرامة من100.000دج إلى 300.000دج في حال كانت المعالجة تخالف أحكام المادة الثانية من القانون[1]

3 _معالجة البيانات دون تصريح مسبق من السلطة الوطنية

تنص المدرسة 56 من القانون 18 07 على أن من يعالج البيانات دون الحصول على ترخيص مسبق من السلطة الوطنية يعاقب بالحبس من سنتين إلى خمس سنوات وغرامة من200.000دج إلى 500.000دج ما لم تتوفر الشروط التي تعني من التصريح حسب المادة 12 من القانون.[2]

4 –السماح الأشخاص غير مؤهلين بمعالجة بيانات ذات طابع شخصي

وفقا للمادة 58 من القانون 18 07 يعاقب بالحبس من سنتين إلى خمس سنوات وغرامة من200.000دج إلى 500.000دج كل من يمنح الإذن لأشخاص غير مؤهلين بمعالجة البيانات[3]

5– رفض المسؤول عن المعالجة دون مبرر قانوني حقوق المعني بالمعالجة:

حسب المادة 64 من القانون 18-07، فإن أي شخص يرفض، دون سبب مقبول، أن يمنحك حقك في معرفة أو تصحيح معلوماتك الشخصية، يمكن أن يُعاقب بالسجن من شهرين إلى عامين، أو بغرامة مالية تتراوح بين 20.000 و200.000 دينار، أو بالعقوبتين معاً.

وهذا ما ينطبق على الشخص المسؤول عن التعامل مع هذه المعلومات، إذا لم يلتزم بحقوقك المذكورة في المواد 32، 34، 35، و36 من نفس القانون.[4]

6 –خرق المسؤول عن المعالجة الالتزامات المنصوص عليها في المادتين 38 و 39:

[1] – المادة 55 المصدر نفسه.

[2] – المادة 56 المصدر نفسه.

[3] – المادة 58 المصدر نفسه.

[4] – المادة 64 من القانون 18-07 المصدر السابق.

وفقا لأحكام المادة 65 من القانون رقم 18 07 يعاقب كل من يخالف الالتزامات المنصوص عليها بغرامة تتراوح ما بين 200,000 دج إلى 500,000دج وتشمل العقوبة كل من يقوم بمعالجة البيانات ذات طابع الشخصي دون احترام الشروط المنصوص عليها في التشريع الجاري به العمل سواء تعلق الأمر بترخيص غير قانوني أو استغلال بيانات دون تصريح.[1]

7-الاستخدام غير المشروع او الاحتيالي للبيانات المعالجة :

تنص المادة 69 من القانون رقم 18 07 على إن كل من يسيء استخدام البيانات المعالجة أو يستخدمها بشكل احتيالي سوى إن كان من مسؤولين عن المعالجة أو من غير يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 100,000دج إلى 500,000دج[2]

ويعتبر كل شخص له دور في المعالجة مسؤولا عن حماية البيانات سواء كان طبيبا أو مكلفا بمعالجة الملفات أو غيرهم من الموظفين كما يعاقب كل من يستعمل البيانات المعالجة لإغراض غير تلك التي جمعت من اجلها أو يقدمها لإطرافها غير مخولين بذلك ويعد ذلك خرقا صريحا للتشريعات المعمول بها.[3]

من جهة أخرى تطبق العقوبات ذات الصلة على أي شخص يرتكب الجرائم المذكورة وذلك بموجب القانون 18 07 بالإضافة إلى العقوبات التأديبية والإدارية بما في ذلك مصادر المعدات المستخدمة أو إعادة تخصيصها وفقا لإحكام التشريع الساري لاسيما المادة .75

[1] – المادة 65 المصدر نفسه.

[2] – المادة 69 المصدر نفسه.

[3] – يزيد بوحليط عبد الرحمان فطناسي، المرجع السابق ص،71.

وأخيرا يجب الإشارة إلى إن هذه العقوبات لا تحول دون اتخاذ الإجراءات الإدارية أو الجزائية الأخرى، خاصة في حالة وجود سلطة وطنية لحماية البيانات الشخصية، و التي يمكنها مباشرة المتابعة قضائيا.[1]

الفرع الثالث: آليات الحماية في قانون العقوبات الجزائري

يتضمن القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطبع الشخصي جملة من قواعد التي تهدف إلى صون وحماية البيانات ذات الطابع الشخصي خاصة في حالات ارتكاب الجرائم أو المخالفات أو انتهاك الحياة الخاصة للأفراد كما يحدد هذا القانون العقوبات المقررة في حق المخالفين ويمنح سلطة الرقابة للهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي باعتبارها آلية أساسية لضمان حماية حقوق الأشخاص الطبيعيين في هذا المجال.

أولا: السلطة الوطنية حماية المعطيات ذات طابع شخصي

نصت التوصيات الأوروبية الصادرة 1995 على انأ استقلالية هيئات حماية البيانات الشخصية تعد عنصرا أساسيا لا يمكن التنازل عنه وقد أكدت المادة 28 من الاتفاقية على أن الهيئة والهيئات التي تعينها الدولة الإشراف على تنفيذ قوانين حماية البيانات يجب ان تمارس مهامها باستقلالية تامة وفي السياق نفسه تبنت الجزائر هذا التوجه من خلال إقرار إنشاء سلطة وطنية لحماية البيانات تلتزم بالمعايير ذاتها التي حددتها التوصيات الأوروبية.[2]

1- الطبيعة القانونية:

تعرف الهيئة الإدارية المستقلة بأنها هيئات وطنية لا تخضع للسلطة الرئاسية أو الوصايا الإدارية مما يجعلها مختلفة عن الإدارة التقليدية فهي تتمتع باستقلالية عضوية ووظيفة عن السلطتين التنفيذية

[1] – يزيد بوحليط عبد الرحمان فطناسي، المرجع السابق ص،71.

[2] – غزالي نسرين، " حماية الاشخاص الطبيعين في مجال المعطيات ذات طابع شخصي" المجلة الجزائرية للعلوم القانونية والسياسية، كلية الحقوق، جامعة الجزائر، العدد 1، 2019، ص،125 https://asjp.cerist.dz بتاريخ 2025/03/17 على الساعة، 14.00.

والتشريعية مع بقائها خاضعة للرقابة القضائية وتتميز هذه الهيئات بامتلاكها السلطات واسعة تفوق ما تتمتع به الهيئات الاستشارية وتتمثل مهامها الأساسية في تنظيم ضبط القطاع الاقتصادي ويعد استقلالها ضمانا لإستمراريتها إذ لا يعقل أن تكون الدولة هي طرف فاعل في النشاط الاقتصادي في موقع الخصم والحكم في آن واحد.[1]

2- تشكيلتها

تتألف هذه الهيئة من 16 ويعينون بموجب مرسوم رئاسي وتدوم مدة ولايتهم خمس سنوات يعين رئيس الجمهورية ثلاثة من أعضائها فيما يعين المجلس الأعلى للقضاء ثلاثة قضاة ينتمون إلى المحكمة العليا ومجلس الدولة كما تضم الهيئة عضوا عن كل من غرفتي البرلمان بالإضافة إلى ممثل واحد عن كل من وزارات الدفاع الشؤون الخارجية الداخلية العدل الصحة العمل والمواصلات السلكية واللاسلكية وكذا التكنولوجيا والرق منة يختار أعضاء السلطة الوطنية بناء على كفاءاتهم القانونية والتقنية في مجال معالجه المعطيات ذات الطبع الشخصي.[2]

وتزويد السلطة الوطنية بأمانه تنفيذيه يسيرها أمين تنفيذي ويساعده في مهامه المستخدمون[3]

[1] – غزالي نسرين المرجع السابق، ص125.

[2] – المرجع نفسه، ص126.

[3] – المادة 27 الفقرة1، القانون 18-07 المصدر السابق.

3- المهام:

يؤدي أعضاء السلطة الوطنية قبل التنصيب في وظائفهم اليمين أمام مجلس قضاء الجزائر ويؤدي الأمين التنفيذي ومستخدم الأمانة التنفيذية اليمين أمام الجهة نفسها[1]

تكلّف السلطة الوطنية بالسهر على مطابقة معالجه المعطيات ذات الطابع الشخصي لإحكام هذا القانون وضمان عدم انطواء استعمال تكنولوجيا الإعلام والاتصال على أي إخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة.[2]

تتولى هذه السلطة مهام متعددة تتعلق بحماية المعطيات ذات الطبع الشخصي من بينها إعلام الأشخاص العينيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم وتقديم الاستشارات للأفراد والجهات التي تقوم بمعالجة هذه المعطيات كما تستقبل الاحتجاجات والطعون والشكاوي المرتبطة بعمليات المعالجة وتعلم أصحاب المعطيات الشخصية بحال قضياهم وتشمل مهامها أيضا الترخيص بنقل معطياتهم الشخصية الى الخارج ومنح التراخيص المعالجة وتلقي التصريحات المتعلقة بها بالإضافة الى ذلك تملك السلطة صلاحية اصدار الاوامر بإجراء تعديلات اللازمة لحماية المعطيات، أو اغلاقها أو سحبها أو اتلافها عند الضرورة، فضلا عن وضع القواعد السلوك والاخلاقيات التي يجب الالتزام بها أثناء معالجة المعطيات ذات شخصي.[3]

يجب على رئيس وأعضاء السلطة الوطنية الالتزام بالحفاظ على سرية المحليات ذات الطابع الشخصي والمعلومات التي اطلعوا عليها مالم ينص القانون على خلاف ذلك[4]

كما لا يجوز لرئيس السلطة وأعضاؤها أن يمتلكو، بصفة مباشرة أو غير مباشرة، مصالح في أي مؤسسة ممارسة نشاطاتها في مجال معالجة المعطيات ذات طابع شخصي ويستفيد أعضاء السلطة

[1] – المادة 24 من القانون 18-07، المصدر السابق.

[2] – المادة 27، المصدر نفسه.

[3] – غزالي نسرين، المرجع السابق، ص127.

[4] – المادة 26 من القانون 18-07، المصدر السابق

الوطنية من حماية الدولة ضد التهديدات أو الاهانات أو الاعتداءات من أي طبيعة كانت التي يتعرضون لها بسبب أو خلال تأدية مهامهم أو بمناسباتها.[1]

تتولى السلطة الوطنية مهمة مسك السجل الوطن الحماية المعطيات ذات الطابع الشخصي، حيث تقوم بتقيد التصريحات المقدمة إليها –إضافة إلى التراخيص المتعلقة بها ويشمل هذا السجل جميع الملفات التي تعالجها السلطات العمومية، وكذا تلك التي يعالجها الاشخاص الخواص كما تستند السلطة الوطنية في عملها إلى مراجعة القوانين أو النصوص التنظيمية المنشورة التي تتضمن إحداث ملفات عمومية او معطيات ضرورية تتيح لأشخاص معينين ممارسة حقوقهم و يستثنى من التقيد في هذا السجل الوطني كل ملف يكون الغرض الوحيد من معالجته هو مسك السجل وفقا لمقتضيات تشريعية أو التنظيمية.[2]

ثانيا: الإجراءات الإدارية في حاله مخالفه أحكام القانون 18–07

منح المشرع الجزائري للسلطة الوطنية مجموعه من الإجراءات الإدارية التي يمكن اتخاذها ضد المسؤول عن المعالجة في حال مخالفته لأحكام هذا القانون وقد أدرج المشرح هذه الإجراءات تحت عنوان الإجراءات الإدارية في المادة 46 حتى المادة 48 من القانون 18 07 وتتمثل هذه الإجراءات في الإنذار والأعذار السحب المؤقت أو النهائي لوصل التصريح أو الترخيص بالإضافة إلى الغرامة وفيما يلي توضيح لهذه الإجراءات

الإنذار لا يعد الإنذار بحد ذاته عقوبة تفرضها السلطة الوطنية بل غالبا ما يأتي في شكل تحذير يهدف إلى تذكير المسؤول عن المعالجة بضرورة الامتثال إحكام القانونية واتخذ تدابير اللازمة لتصحيح الوضع وضمان تطابق نشطه مع أحكام القانون المتعلق بحماية المعطيات الشخصية.[3]

[1] – المادة 26 من القانون 18–07، المصدر السابق.

[2] – غزالي نسرين، المرجع السابق، ص128.

[3] – عائشة بن قارة مصطفى، " آليات حماية المعطيات ذات طابع شخصي في التشريع الجزائري، مجلة أحكام القانون 18–07 جامعة عبد الحميد بن باديس، مستغانم، الجزائر، أفريل2019، ص751. https://asjp.cerist.dz بتاريخ 2025/03/18 على الساعة، 12.00.

الأعذار يشبه الأعذار الإنذار من حيث الهدف لكنه يعد وسيله قانونيه تكمن السلطة من اختار المسؤول عن المعالجة بضرورة التزامه بأحكام القانون رقم 18 07 خلال مده زمنيه محدده وذلك قبل اللجوء القضاء.[1]

او السحب المؤقت أو النهائي لوصل التصريح الخامسة من المادة 46 من القانون رقم 18 07 المتعلق بحماية المعطيات ذات الطابع الشخصي في الجزائر إلى فرض غرامة ماليه على كل مسؤول عن المعالجة يخالف أحكام القانون[2] كما حددت المادة 47 من نفس القانون حالتين تفرض فيهما غرامه ماليه قدرها 500,000دج وفي حاله رفض المسؤول عن المعالجة دون مبرر قانوني تمكن المعني من حقوقه في الإعلام الولوج التصحيح أو الاعتراض وهي الحقوق المنصوص عليها في المواد 32 34 35 36 من القانون ويعتبر هذا الرفض مخالفه تعرض المسؤول لعقوبة العزل والحبس كما ورد في المادة 64 من نفس القانون وفي حاله عدم قيام المسؤول عن المعالجة بالتبليغ الإجباري في المنصوص عليها في المواد 4 14 16 من القانون[3].

1- الأحكام الإجرائية

تضمن الدولة عدم انتهاك حرمه السكن فلا يجوز لأحد أن يفتشه إلا إذا كان هناك قانون يسمح بذلك ويجب أن يتم التفتيش بأمر رسمي مكتوب من جهة قضائية مختصة وبطريقه تحترم خصوصية البيت وساكنيه وهذا ما نص عليه الدستور في المادة 47 منه.[4]

كما صرح المشرع بان لا يعتد إمام السلطة الوطنية بالسر المهني في المادة 49 الفقرة 02 من القانون رقم 18-07 مما أعطاها الحق بالولوج إلى المعطيات المعالجة وجميع المعلومات والوثائق.[5]

---

[1] – عائشة قارة، المرجع السابق ص751.

[2] – المادة 46 القانون 18-07 المصدر السابق.

[3] – المادة 47 المصدر نفسه.

[4] – المادة 47 من القانون رقم 16-01 المؤرخ في 06 مارس2016، يعدل ويتمم الامر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات الجريدة الرسمية العدد 14 الصادر في 2016/03/09. https://www.jorap.dzبتاريخ 2025/03/19 على الساعة 11.00.

[5] – المادة 49 من القانون 18-07- المرجع السابق.

بالإضافة الى ضباط وأعوان الشرطة القضائية، يخول لأعوان الرقابة الآخرين الذين تعود إليهم السلطة الوطنية للقيام بمهام البحث ومعاينة الجرائم المنصوص عليها في أحكام هذا القانون وذلك تحت اشراف وكيل الجمهورية وتثبت عن طريق محاضر وتوجه فورا الى وكيل الجمهورية المختص إقليميا.[1]

وتختص الجهات القضائية الجزائرية بالنظر في الجرائم المنصوص عليها في هذا القانون المرتب خارج إقليم الجمهورية إذا كان مرتكبها جزائري أو أجنبيا مقيما في الجزائر أو شخصا معنويا خاضع للقانون الجزائري[2] لكل من يدعي أن احدى حقوقه المنصوص عليها في هذا القانون قد تم التعدي عليها ان يتقدم إلى الجهة القضائية المختصة بطلب اتخاذ الإجراءات التحفظية اللازمة لوقف هذا التعدي أو المطالبة بالتعويض عنه[3].

الأحكام الجزائية: يسأل جنائيا الشخص المسؤول عن معالجه المعطيات ذات الطابع الشخصي في الحالات التي نص عليها القانون رقم 18 07 وذلك في عدد مواده من بينها المادة 54 التي تجرم عدم احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة كذا المساس بحقوق الأشخاص وشرفهم وسمعتهم أثناء معالجه المعطيات ذات الطبع الشخصي وتعاقب هذه الأفعال بالحبس من سنتين إلى خمس سنوات وبغرامه ماليه تتراوح بين 200,000 و500,000 [4]

كما تنص المادة 56 على نفس العقوبة في حال انجاز او الأمر بالإنجاز معالجه المعطيات ذات الطبع الشخصي دون الحصول على التصريح او الترخيص لا سيما عندما تتعلق هذه المعطيات بمعطيات حساسة، وتشمل العقوبة أيضا كل من أدلى بتصريحات كاذبة، أو استمر في معالجة المعطيات الشخصية رغم سحب التصريح أو الترخيص أ أخل بواجب السرية، أو سمح لأشخاص غير مؤهلين بالولوج الى هذه المعطيات.

[1] – المادة 50-51 من القانون 18-07- المصدر السابق.

[2] – المادة 53 المصدر نفسه.

[3] – المادة 52 المصدر نفسه .

[4] – المادة 54 المصدر نفسه.

ويعاقب بالعقوبة ذاتها كل من يعالج المعطيات ذات طابع شخصي رغم إعتراض الشخص المعني خصوصا اذا كانت هذه المعالجة تهدف الى الإشهار التجاري أو اذا كان الاعتراض قائم على أسباب مشروعة ويعاقب بالحبس من سنة الى ثلاثة سنوات وبغرامة من 100.000 الى 300.000 أو بإحدى هاتين العقوبتين فقط مقدم الخدمات الذي لا يقوم بإعلام السلطة الوطنية والشخص المعني عن كل انتهاك للمعطيات الشخصية ويعاقب بالحبس من شهرين الى سنتين وبغرامة من 20.000 د.ج الى 200.000د.ج أو بإجدى هاتين العقوبتين فقط كل مسؤول عن المعالجة يرفض دون سبب مشرع حقوق الاعلام او الولوج او التصحيح او الاعتراض ويعد اخلال بالتشريعات المسؤول عن المعالجة التدابير التقنية والتنظيمية المناسبة لحماية المعطيات من المخاطر المحتملة او في حال قيام المعالج بالمعالجة دون تنظيمها بموجب سند او عقد قانوني فان ذلك يشكل خرقا للضوابط المنظمة لمعالجة المعطيات الشخصية.

ويعاقب بغرامة من 200.000 دج الى 500.000 دج المسؤول عن المعالجة ومن قام بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع او تلك الواردة في التصريح او الترخيص ضف الى ذلك يصادر محل الجريمة بغرض اعادة تخصيصه أو تدميره وتضاعف العقوبات في حالة العود أي ارتكاب جريمة أخرى .

المطلب الثاني: حماية البيانات الشخصية في التشريعات الخاصة.

نظراً لتداخل البيانات الشخصية مع العديد من المجالات الأخرى وارتباطها الوثيق بخصوصية الأفراد، لم يتضمن قانون حماية المعطيات الشخصية جميع الجزاءات المترتبة على انتهاك هذه البيانات. وهذا ما دفع المشرع الجزائري إلى إدراج عقوبات ضمن قوانين أخرى، مثل قانون الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، وقانون التوقيع والتصديق الإلكتروني، بالإضافة إلى القواعد المتعلقة بالبريد والاتصال الإلكتروني. وسيتم توضيح ذلك بالتفصيل.

الفرع الأول: القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

تتميز العديد من الجرائم المرتبطة بتكنولوجيا الإعلام و الاتصال أنها تمس بالمعطيات الشخصية وهذا ما يجعل من القانون09-04 أداة فعالة لحماية هذه المعطيات لاسيما حفظ المعطيات المتعلقة بحركة السير[1] وهي " المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا من حلقة الاتصال، توضح مصدر الاتصال، و الوجهة المرسل إليها، و الطريق الذي يسلكه، ووقت وتاريخ و حجم و مدة الاتصال ونوع الخدمة"، على إلزام مقدمي الخدمات الحائزين على معطيات معلوماتية للقيام بحفظ هذه المعطيات لمدة سنة ابتداء من تاريخ تسجيلها و تشمل:

- الخصائص التقنية، وكذا تاريخ ووقت ومدة كل اتصال.
- المعطيات المتعلقة بالتجهيزات الظرفية المستعملة للاتصال.
- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم، وكذا عناوين المواقع التي تم الاطلاع عليها.

كما تم أيضاً اعتماد تجريم عدم الامتثال لهذه الالتزامات، وتحميل المسؤولية الجزائية للأفراد الطبيعيين والاعتباريين عند التسبب في عرقلة سير التحقيقات القضائية، حيث يُعاقب الفرد الطبيعي بالسجن لمدة تتراوح من ستة أشهر إلى خمس سنوات، بالإضافة إلى غرامة مالية تتراوح بين

[1] المادة رقم02من القانون09-04، المؤرخ في05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكانتها ج.ر.ج.ج.ع47،المؤرخة في 16 أوت 2009.
www.joradp.dz

50.000 دج و500.000 دج. أما الشخص المعنوي، فتُطبق عليه العقوبات وفقاً لما هو منصوص عليه في مواد قانون العقوبات.

بالإضافة إلى ذلك، وحسب نص المادة 29 من المرسوم الرئاسي 21-439 المتعلق بإعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها، فإنه يتوجب على أعضاء الهيئة ومستخدميها، تحت طائلة العقوبات الجزائية، الالتزام باستخدام البيانات التي يتم الحصول عليها بشكل مشروع، بغض النظر عن طبيعتها. ويشمل ذلك البيانات المستمدة من الاتصالات الإلكترونية أو أي معلومات أخرى تتلقاها أو تجمعها الهيئة بهدف الوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال.[1]

الفرع الثاني: القانون 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين:

نظر الارتباط الوثيق بين التوقيع الالكتروني والبيانات الشخصية خصوصا تلك المعالجة التي يتم بشكل آلي، فقد أدرج المشرع الجزائري مجموعة من العقوبات ضمن القانون15-04 سيتم تناول تفاصيل كل منها بالشكل التالي:

1- جريمة حيازة، إنشاء أو استعمال بيانات إنشاء توقيع الكتروني خاص بالغير:

تؤكد المادة 68 من القانون15-04 على تجريم استخدام أو حيازة أو إفشاء بيانات استخدام أو حيازة أو إنشاء بيانات تتعلق بإنشاء توقيع الكتروني خاص شخص، ويفرض القانون عقوبة بالحبس تراوح بين ثلاثة (3) أشهر وثلاث (3) سنوات بالإضافة إلى غرامة مالية تراوح بين مليون دينار (دج1000.000)إلى خمسة(5000.000دج)ملايين دينارکما يحق للقاضي اختيار تنفيذ إحدى العقوبتين فقط ، كما تبين هذه المادة أن الجريمة تحدث فور حيازة بيانات لإنشاء توقيع

[1] -المادة29 من المرسوم الرئاسي21-439 المؤرخ في 07نوفمبر2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها،ج.ر.ج ج،ع40، المؤرخة في 11نوفمبر2021.www.mpt.gov.dz

الكتروني خاص بالآخرين، و يعكس ذلك حرص المشرع على حماية التوقيع الالكتروني لصوت البيانات الشخصية و حماية أثارها و انعكاساتها على التجارة الالكترونية و التعاملات عبر الانترنيت بشكل عام.

2- جريمة إخلال مقدمي الخدمات بالحفاظ على سرية البيانات والمعلومات:

ألزم المشرع مقدمي خدمات التصديق الالكتروني، سواء كانوا أشخاص طبيعيين أو اعتباريين، بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكتروني التي يصدرونها،[1] وان احدث إخلال بهذا الالتزام، تفرض عقوبة بالحبس تتراوح من ثلاثة(03) أشهر إلى سنتين(02)،مع غرامة مالية تتراوح بين200.000دج إلى 1000.000دج أو بإحدى هاتين العقوبتين فقط.

كما نص ذات القانون على منع المدققين من إفشاء أي معلومات سرية اطلعوا عليها خلال عمليات التدقيق،[2] وفي حالة المخالفة، يعاقب المدقق بالحبس لمدة تتراوح من ثلاثة أشهر إلى سنتين وغرامة مالية تتراوح بين 200000دج، أو بإحدى هاتين العقوبتين فقط.[3]

3- جريمة جمع البيانات الشخصية للمعني موافقته الصريحة:

حيث نص القانون19-04 على ضرورة منع مؤدي خدمات التطبيقات الالكترونية من الوصول إلى البيانات الشخصية للمستخدم إلا بعد الحصول على موافقته الصريحة[4] كما يشدد القانون عدم جمع أي بيانات أخرى غير ضرورية لمنح وحفظ شهادة التصديق الالكتروني وفي حالة مخالفة أحكام هذه المادة يعاقب مقدم الخدمات بالحبس لمدة تتراوح بين ستة أشهر وثلاث سنوات، وبغرامة مالية تتراوح بين مائتي 200000الف دج ومليون 1000000دج، أو بإحدى هاتين العقوبتين

---

[1] المادة02 من القانون15-04مؤرخ في11ربيع الثاني عام1436 الموافق لأول فبراير2015،يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين.ج.ر.ج ج.عدد6. www.joradp.dz بتاريخ 2025/03/14 على الساعة 14.00

[2] المادة 73 من القانون 19 04 المصدر السابق.

[3] -المادة 70 المصدر نفسه.

[4] - المادة 71 المصدر السابق.

الفرع الثالث: المرسوم التنفيذي رقم16-142 المحدد لكيفيات حفظ الوثيقة الممضاة الكترونيا

لقد حدد هذا المرسوم كيفيات حفظ الوثيقة الموقعة الكترونيا والتي تتمثل في:

1-كيفية حفظ الوثيقة الموقعة الكترونيا:

حسب ما جاء في المرسوم التنفيذ رقم16-142، فان حفظ الوثيقة الموقعة الكترونيا التي هي عبارة عن وثيقة الكترونية مرفقة أو متصلة منطقيا بتوقيع الكتروني[1]، يضمن استرجاع هذه الوثيقة في شكلها الأصلي لاحقا، بالإضافة إلى التحقق من توقيعها الالكتروني.

كما يجب أن يتضمن فقط الوثيقة الموقعة الكترونيا مجموعة من العناصر تتمثل في:

- الوثيقة الالكترونية وتوقيعها الالكتروني، أيا كان مرفقا أو متصلات بشكل منطقي؛
- شهادة التصديق الالكتروني للموقع؛
- قائمة الشهادات الالكترونية الوسيطة إلى غاية الوصول إلى السلطة الوطنية للتصديق الالكتروني عندما يتعلق الأمر بشهادة الكترونية موصوفة؛
- قوائم الشهادات الملغاة أو نتائج التحقيق في حالة الشهادات الالكترونية البسيطة إلى غاية الوصول للسلطة الوطنية للتصديق الالكتروني؛
- تاريخ وتوقيع الوثيقة من الاقتضاء؛[2]

كما انه ورد في نفس المرسوم انه يجب أن يتم حفظ الوثيقة الموقعة الكترونيا بواسطة دعامة والتي تشمل أي وسيلة مادية أينا كان شكلها أو خصائصها المادية تسمح باستلامها وحفظ استرجاعها بواسطة الوسائل التقنية الملائمة على أن تشمل الوثيقة الموقعة الكترونيا نفس العناصر عند نقلهما من

[1]- المادة02 من المرسوم التنفيذي رقم 16-142 مؤرخ في 27 رجب عام 1437 الموافق ل05 مايو 2016، يحدد كيفيات هذه الوثيقة الموفقة الكترونيا، ج،ر،ج،ج عدد28، مؤرخة في 8مايو 2016.

[2] -المادة 04 المصدر نفسه

دعامة حفظا إلى دعامة حفظ أخرى مع التحقق من التوقيع، بالإضافة إلى أن الأشخاص سواء كانوا طبيعيين أو معنويين موقعين مستلمين للوثيقة ضمان حفظهما بأنفسهم أو بواسطة لمرف ثالث على أن يتم حفظ الوثيقة خلال مدة منفعتها.

خلاصة الفصل الأول:

تناول هذا الفصل الإطار المفاهيمي والقانوني لحماية البيانات الشخصية في ظل التحول نحو الإدارة الإلكترونية، حيث تم التطرق في المبحث الأول إلى تحديد ماهية البيانات الشخصية، من خلال بيان مفهومها، وخصائصها، وأهمية حمايتها باعتبارها من الحقوق الأساسية المتصلة بحرمة الحياة الخاصة. كما تم تسليط الضوء على مفهوم الإدارة الإلكترونية وخصائصها، مع التركيز على تجربتها في الجزائر.

أما في المبحث الثاني، فقد تم تناول الإطار القانوني الناظم لحماية البيانات الشخصية في التشريع الجزائري، من خلال استعراض الأسس الدستورية والتشريعية التي تضمن حماية هذه البيانات، لاسيما القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، بالإضافة إلى الآليات الجنائية المقررة في قانون العقوبات.

كما تم التطرق إلى حماية البيانات الشخصية في ظل بعض التشريعات الخاصة، لاسيما القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والقانون 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، إلى جانب المرسوم التنفيذي 16-142 المتعلق بكيفية حفظ الوثيقة الرقمية المعالجة إلكترونياً، بما يعكس الجهود المبذولة من قبل المشرّع الجزائري في توفير بيئة قانونية تواكب متطلبات الإدارة الإلكترونية وتحمي خصوصية الأفراد في الفضاء الرقمي.

الفصل الثاني

الآليات العملية لحماية البيانات الشخصية في ظل الادارة الالكترونية

تمهيد:

مع تزايد الاعتماد على البيانات الشخصية في مختلف التعاملات الرقمية والإدارية، أصبحت الحاجة إلى آليات فعالة لحمايتها أمرًا لا غنى عنه، ويعود ذلك إلى ما تشكله هذه البيانات من أهمية بالغة في تحديد هوية الأفراد وتنظيم علاقاتهم القانونية والاجتماعية، فضلًا عن كونها هدفًا رئيسًا للهجمات الإلكترونية والانتهاكات غير المشروعة. وبالنظر إلى تعدد الجهات المتداخلة في حماية البيانات الشخصية وتنوع الوسائل المعتمدة، جاء هذا الفصل ليسلط الضوء على أبرز الآليات المعتمدة لحماية البيانات الشخصية، سواء من خلال الجهة المكلفة بالحماية أو الوسائل التقنية والوقائية المتبعة.

ففي المبحث الأول، يتم تناول دور الجهات المكلفة بحماية البيانات الشخصية من خلال تحليل مساهمة السلطة الوطنية الإدارية المستقلة، وما تملكه من مهام وصلاحيات في هذا المجال، وكذلك سلطات الضبط القضائية والقضاء والمؤسسات العامة والخاصة باعتبارهم أطرافًا فاعلة في ضمان تطبيق القوانين وتحقيق الحماية الفعلية للبيانات.

أما المبحث الثاني، فيسلط الضوء على الآليات التقنية والتدابير الوقائية من خلال عرض الوسائل الفنية كالتشفير والجدران النارية وتقنيات التحقق من الهوية، إلى جانب التدابير الوقائية والتوعية، والتي تشمل السياسة الأمنية والهيئات المختصة بالحماية ونشر الوعي بأهمية حماية البيانات بين أفراد المجتمع. ويهدف هذا الفصل إلى إبراز التكامل بين الدور المؤسسي والتقني في مجال حماية البيانات الشخصية بما يساهم في إقامة بيئة قانونية وأمنية متوازنة تحفظ الحقوق وتمنع التجاوزات.

المبحث الأول: الآليات المؤسساتية لحماية البيانات الشخصية

نص المشرع الجزائري في القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين، على إنشاء سلطة وطنية تتمتع بالاستقلال المالي والإداري، إلى جانب هيئات قطاعية أخرى تلعب دورًا تنفيذيًا ومتكاملًا في مجال اختصاصها. سنتطرق في المطلب الأول من هذا البحث لدراسة السلطة الوطنية لحماية البيانات ذات الطابع الشخصي من حيث تنظيمها وتشكيلها، بالإضافة إلى صلاحياتها في مجال حماية البيانات، والرقابة والتحقيق المخولة لها. وفي المطلب الثاني سنركز على دور الهيئات الضبط القطاعية والقضائية، ودور المؤسسة العامة في حماية البيانات الشخصية.

المطلب الأول: السلطة الوطنية لحماية البيانات ذات الطابع الشخصي.

عمل المشرع الجزائري على وضع سلطة إدارية مستقلة تتكفل بحماية البيانات الشخصية بصورة مباشرة أو غير مباشرة، وهي سلطة مكرسة في إطار معالجة معطيات الطابع الشخصي للأشخاص الطبيعيين بموجب أحكام القانون 18-07 بالسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، حيث يقوم أعضاؤها جاهدين بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي.

الفرع الأول: تنظيم السلطة الوطنية وتشكيلها.

نص المشرع الجزائري في القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، على إنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كهيئة مستقلة إداريًا وماليًا، تسند لها مهام الرقابة والتوجيه في مجال حماية الخصوصية والمعطيات الشخصية.

1- الطبيعة القانونية للسلطة الوطنية:

تُعرف الهيئة الإدارية المستقلة بأنها هيئة وطنية لا تخضع للسلطة الرئاسية ولا للوصاية الإدارية، وتمتاز بصلاحيات واسعة تجعلها مختلفة عن الهيئات الاستشارية، وتكمن مهامها في تنظيم القطاع الاقتصادي. ويُعد استقلالها شرطًا أساسيًا لضمان الحياة الخاصة، إذا كانت الدولة تسعى لإضفاء الطابع الاقتصادي دون التدخل فيه مباشرة، الأمر الذي يفرض أن تكون هذه الهيئات مستقلة من حيث التكوين والقرارات. وقد ظهرت أولى هذه الهيئات في الجزائر سنة 1990، وكانت الهيئة الأولى في مجال الإعلام، وهي المجلس الأعلى للإعلام.

وقد أقر المشرع صراحة بأنها هيئة إدارية مستقلة. وفيما يخص الهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي، فقد منحها المشرع سلطة إصدار الأوامر ومراقبة الدخول إلى السوق القضائية وسلطة التحقيق، كما منحها استقلالًا شبه تام إداريًا وماليًا، إذ نشأت بمرسوم رئاسي صدر عن رئيس الجمهورية، ويقع مقرها في الجزائر العاصمة، وتخضع لمراقبة الدولة، وتتمتع بالشخصية المعنوية والاستقلال المالي، كما تضع نظامها الداخلي الذي يحدد مهامها وسيرها وتنظيمها بعد المصادقة عليها[1].

2- الطابع الجماعي للتشكيلة:

تتشكل السلطات الوطنية لحماية المعطيات الشخصية، وفقًا للمادة 23 من القانون رقم 18-07، بهيكلة جماعية تضم رئيسًا يعينه رئيس الجمهورية، وثلاثة قضاة يقترحهم المجلس الأعلى للقضاء من بين أعضاء المحكمة العليا والمجلس الدستوري، وعضوين اثنين يمثلان غرفتي البرلمان يختارهما كل

[1]- فيصل بوخلفة: حماية المعطيات ذات الطابع الشخصي "بين النصوص التقليدية ومتطلبات التقنية"، مجلة الدراسات والبحوث القانونية، جامعة سطيف 2، المجلد 8، العدد 1، جانفي 2023، ص 72، المتوفر على الموقع https://asjp.cerist.dz ، اطلع عليه بتاريخ 24، الساعة 12:30.

غرفة عقب التشاور مع رؤساء المجموعات البرلمانية، بالإضافة إلى ممثل عن المجلس الوطني لحقوق الإنسان، ووزارات الدفاع الوطني، الشؤون الخارجية، الداخلية، العدل، البريد والمواصلات السلكية واللاسلكية، التكنولوجيات والرقمنة، الصحة، والعمل والتشغيل والضمان الاجتماعي[1].

3- الطابع المختلط للتشكيلة:

استنادًا إلى ما سبق نصه في المادة 23، فإن تشكيلة السلطات الوطنية لحماية المعطيات الشخصية تتسم بطبيعة مختلطة، ويتجلى ذلك من خلال تمثيل السلطات الثلاث: التنفيذية، التشريعية، والقضائية، وذلك على النحو التالي[2].

- **ممثلوا السلطة التنفيذية:**

تتمثل السلطة التنفيذية في تشكيلة الهيئة بثلاثة أشخاص من بينهم رئيس الحكومة الذي يختاره رئيس الجمهورية، بالإضافة إلى ممثل واحد عن المجلس الوطني لحقوق الإنسان. وتشمل التشكيلة الوزارية وزير الدفاع الوطني، ووزير الشؤون الخارجية، والوزير المكلف بالشؤون الداخلية، وحافظ الأختام، والوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة، إضافة إلى وزير الصحة، ووزير العمل والتشغيل والضمان الاجتماعي[3].

- **ممثلوا السلطة التشريعية:**

[1]- المادة 23 من القانون 18-07، المصدر السابق.

[2]- قرانة عادل، بوحديد فارس: "مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري:، مجلة العلوم القانونية والاجتماعية، كلية الحقوق والعلوم السياسية، الجزائر، جامعة باجي مختار عنابة، المجلد 6، العدد 2، جوان 2021، ص 1061، متوفر على الموقع https://asjp.cerist.dz، اطلع بتاريخ 2025/4/2، الساعة 15:30 .

[3]- قرانة عادل، بوحديد فارس: المرجع سابق، ص 1061

يقوم رئيس كل غرفة من غرف البرلمان، بعد التشاور مع رؤساء المجموعات البرلمانية، باختيار أحد الأعضاء عنها[1].

- **ممثلوا السلطة القضائية:**

يقترح ثلاثة قضاة من قبل المجلس الأعلى للقضاء، ويُختارون من بين قضاة المحكمة العليا ومجلس الدولة للتمثيل في الهيئة[2].

4- جهة التعيين ووسيلته:

يعين رئيس السلطة الوطنية وأعضاؤها بمرسوم رئاسي يصدر عن رئيس الجمهورية بصفته ممثلاً للسلطة التنفيذية، ما يطرح تساؤلاً حول استقلالية العضوية ومدى تأثرها بهذه الصفة في ظل غياب أي آلية انتخابية لاكتساب العضوية في السلطة الوطنية[3].

5- مدة العضوية:

حدد المشرع الجزائري مدة العضوية في السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، سواء بالنسبة لرئيسها أو أعضائها، بخمس سنوات قابلة للتجديد. غير أن قابلية التجديد هذه تثير تساؤلات حول مدى ضمان استقلالية هذه السلطة[4].

6- سير عمل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

[1]- المرجع نفسه، ص 1061

[2]- قرانة عادل، بوحديد فارس المرجع السابق، ص 1061

[3]- المرجع نفسه، ص 1061

[4]- المرجع نفسه، ص 1061

يقوم أعضاء الهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي بأداء مهامهم، بما في ذلك الأمين التنفيذي والمستخدمون التنفيذيون. ويستفيد رئيس الهيئة وأعضاؤها من حماية الدولة ضد أي تهديدات أو اعتداءات قد يتعرضون لها أثناء تأدية مهامهم[1].

تتمتع الهيئة الوطنية باستقلالية تامة من الناحية الإدارية والوظيفية، ولا تخضع لأي سلطة أو وصاية من أي جهة كانت، ولا يحق لأي جهة التدخل في قراراتها أو التأثير على سير عملها. كما لا يجوز لأعضائها أو لأي موظف فيها أن تكون لهم مصالح شخصية أو مالية مع الجهات العاملة في مجال معالجة المعطيات، ولا يمكن أن يكون لهم أي ارتباط بمؤسسات تمارس أنشطة مشابهة بشكل مباشر أو غير مباشر.

ويُطلب من أعضاء الهيئة الالتزام بالحفاظ على سرية المعطيات والمعلومات التي يطلعون عليها خلال ممارسة مهامهم، ويستمر هذا الالتزام حتى بعد انتهاء مهامهم ما لم يوجد استثناء محدد. ويشمل هذا الالتزام جميع المعلومات والوثائق التي يتم الوصول إليها أثناء العمل. كما تُعد الهيئة الوطنية تقريراً سنوياً عن نشاطاتها يُرفع إلى رئيس الجمهورية[2].

الفرع الثاني: صلاحية السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

تضطلع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بدور محوري في ضمان احترام المبادئ القانونية المتعلقة بالجماعة ومعالجة واستعمال المعطيات الشخصية، وتمنح في هذا الإطار جملة من الصلاحيات التي يحددها القانون رقم 18-07 لسنة 2018، وتتوزع هذه الصلاحيات كما يلي:

1- الصلاحيات التوجيهية والاستشارية:

[1]- خالدي فتيحة، المرجع السابق، ص 49.

[2]- خالدي فتيحة، المرجع السابق، ص 49

- توعية الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم والتزاماتهم القانونية.
- تقديم آراء ومقترحات تسهم في تبسيط وتوحيد الإطار القانوني والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.
- العمل على تطوير علاقات التعاون مع السلطات الأجنبية المختصة بمراقبة المعالجة المتماثلة[1].

2- الصلاحيات التنظيمية والاقتراحية:

- إصدار الأوامر باتخاذ التدابير الضرورية لحماية المعطيات ذات الطابع الشخصي محل المعالجة.
- اعتماد عقوبات السلوك التي يقدمها المسؤولون عن المعالجة وفقًا لاحكام القانون.
- تقديم مقترحات تهدف إلى تعزيز حماية المعطيات ذات الطابع الشخصي[2].

3- الصلاحيات المتعلقة بالتراخيص المسبق لبعض المعالجات:

- منع التراخيص والتأشيرات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.
- إصدار الترخيص لنقل المعطيات ذات الطابع الشخصي إلى الخارج وفق الشروط المنصوص عليها قانونا[3].

4- الصلاحيات التقنية والمطابقة:

- تقديم الاستشارات للأفراد والهيئات التي تعزم إجراء معالجات أو أبحاث قد يترتب عنها معالجة معطيات ذات طابع شخصي.
- إجراء التحقيقات وتلقي الطعون والاعتراضات المتعلقة بتنفيذ عملية المعالجة وإبلاغ المعنيين بنتائجها.
- إصدار أوامر بإتلاف أو حذف أو تجميد المعطيات التي يتم معالجتها بطريقة مخالفة.

[1]- المادة25 من القانون 18-07- المصدر السابق

[2]- المادة25 من القانون 18-07- المصدر السابق.

[3]- المادة25 المصدر نفسه.

- إخطار السلطات العمومية في حال تسجيل خروقات لأحكام القانون المتعلقة بحماية المعطيات الشخصية[1].

5- الصلاحيات التأديبية والجزاءات الإدارية:

- توقيع جزاءات غير قضائية في حال مخالفة الأحكام القانونية مثل التنبيه الرسمي، التوبيخ، المنع المؤقت أو النهائي للمعالجة.
- نشر التراخيص المسحوبة والآراء الصادرة في التسجيل الوطني لحماية المعطيات ذات الطابع الشخصي[2].

كما أن المسؤول عن معالجة المعطيات ملزم بالتعاون مع السلطة الوطنية، وفي حال الامتناع أو عرقلة عملها كرفض إجراء عملية التحقيق مثلا، يعد ذلك مخالفة تستوجب المساءلة، وهذا ما نصت عليه المادة 61 من خلال إجراء عملية التحقيق في عين المكان ورفض ذات الوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية، أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة، أو إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب، أو عدم تقديمها بشكل مباشر وواضح[3].

يتم إنشاء سجل وطني خاص بحماية المعطيات الشخصية تحت إشراف السلطة الوطنية، يُدرج في هذا السجل مختلف الملفات التي تخضع للمعالجة سواء من قبل الجهات العمومية أو الخواص، بالإضافة إلى مراجع القوانين والنصوص التنظيمية المنشورة المتعلقة بإنشاء ملفات عمومية، كما يُسجل

[1]- المادة25 المصدر نفسه.

[2]- المادة25 من القانون 18-07- المصدر السابق.

[3]- المادة 61 المصدر نفسه

فيها جميع التصريحات المقدمة للسلطة الوطنية والتراخيص الصادرة عنها، وغيرها من البيانات الضرورية التي يحق للأشخاص المعنيين الاطلاع عليها وفق الإجراءات القانونية والتنظيمية المحددة[1].

الفرع الثالث: آليات الرقابة والتحقيق المخولة للسلطة الوطنية.

هذا الفرع لا يتناول صلاحيات السلطة بشكل عام بل يركز على كيف تمارس تلك الصلاحيات عمليًا أو من خلال الوسائل الرقمية، إجراءات تحقيق وأدوات المعاينة.

1- وسائل الرقابة الميدانية:

تشير النصوص إلى ضرورة إنشاء جهة رقابية رسمية تكون مسؤولة عن متابعة تطبيق قواعد حماية البيانات الشخصية، بما في ذلك إصدار التصاريح المتعلقة بمعالجة هذه البيانات ومنح التراخيص للجهات التي تتعامل معها، لضمان تنفيذ العمليات وفق الأطر القانونية والتنظيمية المحددة، وتنفيذ الزيارات التفتيشية الفجائية أو المبرمجة لمقر المؤسسات المعالجة، فحص البنية التحتية الرقمية، وقواعد البيانات وأنظمة الحماية، والاعتماد على فرق رقابية متخصصة قانونيًا وتقنيًا[2].

واستنادًا للمادة 38 يجب على المسؤول عن المعالجة اتخاذ التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف أو الضياع أو التلف أو النشر أو الولوج غير المشروع، خاصة عند معالجة المعطيات عبر شبكة معينة. كما يجب أن تضمن هذه التدابير مستوى مناسبًا من الحماية يتوافق مع طبيعة المخاطر المرتبطة بها[3]. ومن جهة أخرى، تنص المادة 39 على أنه عندما

[1]- كحلاوي عبد الهادي: الحماية القانونية للبيانات الشخصية في التشريع الجزائري، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية – أدرار، 2021-2022، المتوفر على الموقع https://dspace.univ-adar.edu.dz، اطلع عليه بتاريخ 5 أبريل 2025، الساعة 15: 21 .

[2]- معالجة وحماية البيانات ذات الطابع الشخصي: ص 4، المتوفر على الموقع https://archive.unescwa.org، اطلع عليه بتاريخ 8 أبريل 2025، الساعة 22:00.

[3]- المادة 38 من القانون 18-07- المصدر السابق.

تجرى المعالجة لحساب المسؤول عن المعالجة، يجب اختيار معالج من الباطن يلتزم بتوفير جميع الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية اللازمة للمعالجة، مع التأكيد على أن هذه الضمانات يجب اختيار معالج من الباطن يلتزم بتوفير جميع الضمانات الكافية المتعلقة بحماية المعطيات[1] كما يجب أن تتضمن الالتزام المنصوص عليه في الفقرة الأولى من المادة 38، وذلك لضمان التطبيق السليم للتدابير الوقائية والتقليل من المخاطر المحتملة على حقوق وحريات الأفراد[2].

2- صلاحيات جمع الأدلة والتحقيق:

تتمتع السلطة الرقابية المختصة بصلاحيات واسعة تشمل جميع المعلومات والوصول إلى البيانات الضرورية للتحقيق، إضافة إلى إمكانية فرض عقوبات إدارية مثل الغرامات أو منع الوصول إلى البيانات أو حذفها كليًا أو مؤقتًا، بل وقد تصل إلى وقف عملية المعالجة. كما تمتلك هذه السلطة حق اللجوء إلى القضاء لإصدار تدابير أكثر فاعلية عند الحاجة، ومن ذلك الاطلاع على جميع الوثائق والسجلات الورقية المتعلقة بالمعالجة، الولوج إلى الأنظمة المعلوماتية للتحقيق في طرق المعالجة وتخزين البيانات، إمكانية الاستماع إلى مسؤولي المؤسسات أو المعالجين على المعالجة[3].

وفي هذا السياق، تنص المادة 40 على أن المسؤول عن المعالجة، وكذلك الأشخاص الذين يطلعون أثناء ممارسة مهامهم على المعطيات ذات الطابع الشخصي، ملزمون بالحفاظ على السر المهني. ويستمر هذا الالتزام بالعقوبات المنصوص عليها في التشريع الساري المفعول، ويعكس هذا المقتضى أهمية حماية سرية البيانات الشخصية خلال إجراءات التحقيق، ويعد ضمانًا قانونيًا يكمل صلاحيات السلطة الرقابية في الوصول إلى المعطيات دون المساس بحقوق الأفراد وكرامتهم[4].

3- إجراءات المحاضر والإحالة:

ضمن صلاحياتها يمكن للسلطة الرقابية تلقي الشكاوى والطلبات من الأفراد ومتابعتها بفعالية، كما تلتزم هذه الجهة بضمان سرية المعلومات والمهنية في التعامل مع القضايا، ويعد ذلك جزءًا من

[1]- المادة 39 المصدر نفسه.

[2]- المادة 38 المصدر نفسه.

[3]- معالجة وحماية البيانات ذات الطابع الشخصي، المرجع السابق، ص 4.

[4]- المادة 40 من القانون 18-07- المصدر السابق

آليات تفعيل القانون وضمان تطبيقه العملي. وتشمل الإجراءات المتخذة في هذا السياق: تحرير محاضر مخالفة قانونية توثق التجاوزات المكتشفة[1]، إمكانية إحالة الملفات إلى الجهات القضائية المختصة، النيابة العامة مثلًا، خاصة إذا تعلق الأمر بانتهاك جسيم، التوصية بوقف النشاط أو فرض العقوبات الإدارية بالتدرج[2].

4- آليات التظلم والطعن.

يحق لأي فرد التقدم بمراجعة قضائية إدارية في حالة تعرضه لانتهاك متعلق ببياناته الشخصية، سواء أمام القضاة أو السلطة الرقابية المختصة، كما يمكنه المطالبة بتعويض عن الأضرار الناتجة عن المعالجة غير القانونية أو الخاطئة للبيانات، وتحديد المسؤوليات بوضوح واتخاذ التدابير المناسبة. أما في حالة نقل البيانات إلى الدول الأجنبية، فيشترط وجود ضمانات لحماية البيانات بشكل يعادل المعايير المحلية، ويشترط موافقة الشخص المعني، بالإضافة إلى اتخاذ تدابير لحماية الحقوق والحريات الأساسية للأفراد. وفي هذا الإطار، تشمل آليات التظلم والطعن تمكين الجهات المعنية، الشركات أو الأفراد، من الطعن في قرارات السلطة أو القضاء الإداري، وتعزيز مبدأ المسؤولية والشفافية من خلال حق الدفاع وحق الطعن[3].

المطلب الثاني: دور هيئات الضبط الاخرى في حماية البينات الشخصية

تشكل حماية البيانات الشخصية أحد أبرز التحديات القانونية في العصر الرقمي، حيث تتداخل عدة جهات في ضمان حماية هذه الحقوق. لا يقتصر هذا الدور على الهيئات المختصة بحماية المعطيات، بل يمتد ليشمل هيئات ضبط أخرى تتدخل ضمن نطاق اختصاصها القطاعي. كما يلعب القضاء دورًا أساسيًا في تأمين حماية فعالة للبيانات من خلال تطبيق القوانين وتفسيرها. إلى جانب ذلك، تبرز أهمية المؤسسات العامة والخاصة في تبني سياسات وإجراءات تحترم خصوصية الأفراد وتعزز ثقافة حماية البيانات.

الفرع الأول: دور الهيئات الضابطة القطاعية في حماية البيانات الشخصية.

[1]- معالجة وحماية البيانات ذات الطابع الشخصي، المرجع السابق، ص 4.

[2]- المرجع نفسه، ص 4.

[3]- معالجة وحماية البيانات ذات الطابع الشخصي، المرجع السابق، ص 4.

تلعب هيئات الضبط القطاعي دورًا مهمًا في حماية البيانات الشخصية، من بينها سلطة الضبط السمعي البصري في الجزائر، والمعروفة رسميًا باسم السلطة الوطنية المستقلة لضبط السمعي البصري .(ARAV) ليست الجهة الرئيسية المختصة بحماية البيانات الشخصية، لكن قد يكون لها دور غير مباشر ومكمل في هذا المجال، خصوصًا في الإعلام الرقمي والإدارة الإلكترونية ذات الصلة بالقطاع السمعي البصري.

1- التأطير القانوني العام:

سلطة ضبط السمعي البصري أنشئت بموجب القانون العضوي رقم 12-05 المؤرخ في 12 جانفي 2012، المتعلق بالإعلام[1]، وتم تنظيمها لاحقًا في إطار القانون رقم 14-04 المؤرخ في 24 فيفري 2014، المتعلق بالنشاط السمعي البصري، الذي يحدد صلاحيات وهيكلة سلطة الضبط السمعي البصري، بما في ذلك مهامها الرقابية والتنظيمية تجاه القنوات الإعلامية[2].

2- دورها في حماية البيانات الشخصية بشكل غير مباشر:

رغم أن سلطة حماية البيانات الشخصية تناط بالسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، فإن سلطة ضبط السمعي البصري تؤدي دورًا تكميليًا في الحالات التالية:

أ- الرقابة على المحتوى الإعلامي والبث الرقمي:

تتولى سلطة الضبط للسمع البصري مسؤولية مراقبة المحتوى السمعي البصري المعروض على القنوات التلفزيونية والإذاعية لضمان عدم انتهاك خصوصية الأفراد أو بث بياناتهم الشخصية، وهذا

[1]- القانون العضوي رقم12-05 المؤرخ في 18 صفر عام 1433 الموافق لـ 12 يناير سنة2012، يتعلق بالاعلام، ج.ر، العدد 2 ، لسنة 2012.

[2]- القانون رقم 14-04 المؤرخ في 21 جمادى الأولى عام 1435 هـ الموافق لـ 23 مارس 2014، المتعلق بالنشاط السمعي البصري، الجريدة الرسمية للجمهورية الجزائرية، العدد 16، لسنة 2014.

منصوص عليه في المادة 93 لضمان احترام أخلاقيات المهنة والخصوصية في وسائل الإعلام، خصوصًا عند تغطية قضايا تتضمن معطيات حساسة[1].

ب- الإشراف على الالتزام بأخلاقيات المعالجة الرقمية:

في إطار الرقمنة والأنظمة الإلكترونية التي تعتمدها ARAV المؤسسات الإعلامية، تراقب مدى احترام قواعد استخدام الأخلاقيات للبيانات التي تُجمع عن المتلقين، مثل البيانات التحليلية للمشاهدين أو مستخدمي المنصات الرقمية. وتُعتبر المادة 93 موجهًا أساسيًا في هذا السياق، إذ تؤكد على منع انتهاك الحياة الخاصة للأشخاص[2].

ج- إصدار التوصيات والتنبيهات:

يمكن للسلطة إصدار توصيات تخص حماية الحياة الخاصة والبيانات الشخصية في البث الرقمي، سواء على القنوات التقليدية أو عبر الإنترنت، وذلك في نفس المادة 93[3].

3- حدود صلاحياتها:

لا تُرخص أو تُعاقب مباشرة ARAV في قضايا انتهاك البيانات الشخصية خارج الإطار الإعلامي، بل تتدخل في الحالات التي يكون انتهاك الخصوصية قد ظهر عبر وسائل الإعلام أو الرقمية تحت سلطتها. وبموجب المادة 55، تتمتع سلطة الضبط السمعي البصري بعدة صلاحيات تتوزع على مجالات مختلفة تشمل الضبط والمراقبة والاستشراف وتسوية النزاعات. ففي مجال الضبط

[1]- المادة 93 من القانون 12-05 المصدر السابق.

[2]- المادة 93 المصدر نفسه.

[3]- المادة 93 من القانون 12-05 المصدر السابق.

تتولى السلطة دراسة طلب إنشاء خدمات الاتصال السمعي البصري وتثبيتها وتخصيص الترددات المخصصة للبث الإذاعي والتلفزي العمومي، وكذا تطبيق القواعد المرتبطة بشروط الإنتاج والبرمجة، وبث حصص التعبير المباشر وحصص الحملات الانتخابية، كما تُشرف على كيفية بث البرامج المخصصة للتشكيلات السياسية والنقابات والمنظمات الوطنية المعتمدة، وتحدد الشروط التي تُجيد استخدام الإشهار المفتوح للمحتويات، وتضبط البيانات العامة الصادرة عن السلطة العمومية[1].

أما في مجال المراقبة فتسهر السلطة على احترام مضامين البرامج السمعية البصرية للتشريع والتنظيم الساري المفعول، ومراقبة الترددات وضمان جودة الإشعارات، والامتثال لحصص الإنتاج الوطني. وتراقب أيضًا وسائل الإعلام بخصوص احترام المبادئ والقواعد المتعلقة بالنشاط السمعي البصري، وتمارس الرقابة على أرشيف البث، وتجمع المعلومات الضرورية من مختلف الإدارات والهيئات دون قيود لإعداد تقاريرها وقراراتها[2].

وفي المجال الاستشرافي، تشارك السلطة في إعداد الإستراتيجية الوطنية لتطوير النشاط السمعي البصري، وتقترح التدابير المناسبة لترقية الأداء، وتشارك في المفاوضات الدولية الخاصة بالترددات وأدوات البث، وتبدي رأيها بشأن أدوات استخدام الترددات، وتقدم اقتراحاتها عند الطلب لأي جهة قضائية في حال وجود نزاع مرتبط بممارسة النشاط السمعي البصري[3].

أما في مجال تسوية النزاعات فتتدخل السلطة للتحكيم في النزاعات بين مستغلي خدمات السمع البصري، سواء بينهم أو مع المستعملين، وتحقق في الشكاوى الصادرة عن الأحزاب السياسية، والنقابات، والجمعيات، والأشخاص الطبيعيين أو المعنويين، في حال وجود خروقات تمس باستغلال خدمة الاتصال السمعي البصري أو تمثل انتهاكًا للقانون[4].

---

[1]- المادة 55 من القانون 14-04 المصدر السابق.

[2]- المادة 55 المصدر نفسه.

[3]- المادة 55 من القانون 14-04 المصدر السابق

[4]- المادة 55 المصدر نفسه

الفرع الثاني: دور القضاء في حماية البيانات الشخصية.

للقضاء الإداري في الجزائر علاقة مباشرة بحماية البيانات الشخصية في إطار الإدارة الإلكترونية، حيث يعتبر الضامن لشرعية تصرفات الإدارة وحماية الحقوق والحريات، ومن بينها الحق في حماية البيانات الشخصية.

أولا: الحماية الإجرائية.

تعد المادة 801 من قانون الإجراءات الإدارية المدنية القاعدة العامة التي يُسند إليها في استناد الاختصاص إلى الجهة القضائية الإدارية للنظر في المنازعات الإدارية، التي تنص على أن المحاكم الإدارية تختص بالفصل في:

1- دعاوى إلغاء القرارات الإدارية، والدعاوى التفسيرية، ودعاوى فحص المشروعية للقرارات الصادرة عن الولاية والمصالح غير الممركزة للدولة على مستوى الولاية والبلدية، والمصالح الإدارية الأخرى للبلدية، والمؤسسات العمومية المحلية ذات الصبغة الإدارية.

2- دعاوى القضاء الكامل.

3- القضاء المخول لها بموجب نصوص خاصة[1].

كما حدد المشرع الجزائري اختصاص المحاكم الإدارية من حيث نوعية الدعاوى التي تملك صلاحيات الفصل فيها، وعلى وجه الخصوص دعاوى الإلغاء[2] الرامية إلى إبطال القرارات الإدارية الصادرة عن الهيئات الإدارية غير الممركزة. وتشمل هذه الهيئات مصالح الدولة غير الممركزة على مستوى الولاية مثل مديريات التربية، الجامعات، المعاهد، والمصالح الإدارية المختلفة للبلدية، كالملاحق البلدية ومصالح الحالة المدنية. كما يشمل ذلك المؤسسات العمومية المحلية ذات الطابع الإداري مثل

[1]- القانون رقم 08-09 المؤرخ في 18 صفر عام 1429 هـ الموافق لـ 25 فبراير سنة 2008، يتضمن قانون الإجراءات المدنية والإدارية، الجريدة الرسمية للجمهورية الجزائرية، العدد 21، الصادر بتاريخ 23 مارس 2008.

[2]- زرير الهام بلحاج أحمد: "الدور الضبطي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي"، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة وهران 1 أحمد بن بلة، وجامعة أبي بكر بلقايد تلمسان، المجلد 9، العدد 1، مارس 2025، ص. 624.

المستشفيات والهياكل الصحية القطاعية التي تتمتع بالشخصية المعنوية والاستقلالية المالية. إلى جانب كافة المؤسسات ذات الطابع الإداري التي منحها التنظيم القانوني استقلالية مالية.

وتختص دعاوى القضاء الكامل بالنظر في جميع القضايا ذات الطابع الإداري، باستثناء قضاء المشروعية الذي يختص بدعاوى الإلغاء والتفسير وفحص مدى مطابقة القرارات الإدارية للقانون. وتشمل اختصاصات القضاء الكامل على سبيل المثال لا الحصر: دعاوى المسؤولية الإدارية، منازعات الملكية للمنفعة العامة، قضايا التعدي والاستيلاء، منازعات الضرائب، منازعات أملاك الدولة، بعض منازعات الضمان الاجتماعي، بعض النزاعات المتعلقة بالاستثمارات الفلاحية.

أما القضايا التي تُخول بموجب نصوص خاصة، فتستلزم تدخل المشرع بنص تشريعي صريح يمنح بموجبه الولاية القضائية للقضاء الإداري للنظر في النزاع[1].

ثانيا: الحماية الجزائية

تضمن القانون 18-07 عددا من المخالفات التي تعد جرائم تمس بمعالجة المعطيات ذات الطابع الشخصي، والتي تُرتكب إما بمخالفة الضوابط والشروط المتعلقة بالمعالجة أو بمناسبة جمع هذه المعطيات أو استخدامها أو التصرف فيها. كما تشمل هذه الجرائم كل ما من شأنه المساس بحقوق الشخص المعني بالمعالجة أو إخلال المسؤول عن المعالجة بالتزاماته، أو عرقلة عمل السلطة الوطنية لحماية المعطيات الشخصية. ومن بين هذه المخالفات نذكر على سبيل المثال[2] نص المادة 50 من القانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي، أنه يمكن للسلطة لحماية المعطيات

[1]- المرجع نفسه، ص 624.

[2]- عز الدين عثماني، خذيري عفاف: "الحماية القانونية للمعطيات ذات الطابع الشخصي في التشريع الجزائري: دراسة في ظل القانون رقم 18-07"، المجلة الدولية للبحوث القانونية والسياسية، جامعة العربي التبسي – تبسة، المجلد 4، العدد 1، سنة 2020، ص. 100

ذات الطابع الشخصي التي تنص على أنه " بضباط وأعوان الشرطة القضائية، ويؤهل أعوان الرقابة الآخرون الذين تلجأ إليهم السلطة الوطنية للقيام ببحث ومعاينة الجرائم المنصوص عليها في أحكام هذا القانون تحت إشراف وكيل الجمهورية[1]. وتعد الأجهزة الأمنية مسؤولة عن التحري والبحث في مختلف الجرائم وملاحقة مرتكبيها، وذلك تحت إشراف جهاز النيابة العامة"[2].

1- معالجة المعطيات دون احترام الكرامة الإنسانية وحرمة الحياة الخاصة والحريات العامة:

تعني استخدام أو جمع أو نشر معلومات شخصية عن الأفراد بطرق تنتهك خصوصياتهم أو تسيء لهم، مثل التجسس أو التشهير أو استغلال البيانات لأغراض غير أخلاقية أو دون موافقة أصحابها، مما يعد انتهاكا لحقوق الإنسان. وهذا ما نصت عليه المادة 54 من القانون 18-07: أنه دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يُعاقب على خرق أحكام المادة 2 من هذا القانون بالحبس من سنتين إلى خمس سنوات وبغرامة من 200,000 دج إلى 500,000 دج[3].

2- معالجة المعطيات دون موافقة الشخص المعني:

في هذا الصدد، تنص المادة 55 من القانون 18-07 على أنه يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100,000 دج إلى 300,000 دج كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 7 من هذا القانون.

ويعاقب بنفس العقوبة كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني، عندما تستهدف هذه المعالجة لاسيما الإشهار التجاري أو عندما يكون الاعتراض مبنيا على أسباب شرعية[4].

[1]- المادة 50 من القانون 18-04 المصدر السابق.

[2]- عز الدين عثماني، خذيري عفاف:المرجع السابق، ص 101.

[3]- المادة 54 من القانون 18-04 المصدر السابق

[4]- المادة 55 مصدر نفسه

3- معالجة المعطيات دون تصريح مسبق لدى السلطات الوطنية:

تعني استخدام أو جمع البيانات الشخصية دون إذن من الجهة الرسمية المختصة، وهو أمر مخالف للقانون. حيث تنص المادة 56 من القانون 18-07 على أنه يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 200,000 دج إلى 500,000 دج كل من أنجز أو أمر بإنجاز معالجات لمعطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون[1].

4- السماح لأشخاص غير مؤهلين بالولوج لمعطيات ذات الطابع الشخصي.

هي خرق للخصوصية من خلال إعطاء بيانات شخصية لأشخاص غير مصرح لهم. وفي هذا الشأن تنص المادة 60 من القانون 18-07 على أنه يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 200,000 دج إلى 500,000 دج كل من سمح لأشخاص غير مؤهلين بالولوج إلى المعطيات ذات الطابع الشخصي[2].

5- رفض المسؤول عن المعالجة دون مبرر قانوني حقوق المعني بالمعالجة.

ونجد المادة 64 من القانون 18-07 تنص على أنه يعاقب بالحبس من شهرين إلى سنتين وبغرامة من 20,000 دج إلى 200,000 دج أو بإحدى هاتين العقوبتين فقط، كل مسؤول عن المعالجة يرفض دون سبب مشروع حقوق الإعلام والولوج أو التصريح أو الاعتراض المنصوص عليها في المواد 32، 34، 35، 36 من هذا القانون[3].

6- خرق المسؤول عن المعالجة الالتزامات المنصوص عليها في المادتين 38 و39:

تعني أن الجهة أو الشخص المكلف بتنفيذ الالتزامات أخل أو لم يلتزم بما يجب عليه فعله وفق الاتفاقية أو العقد. وتُسلط عليه جملة من العقوبات التي تنص عليها المادة 65 من القانون 18-07، على أنه يعاقب بغرامة من 200,000 دينار جزائري إلى 500,000 دينار جزائري، كما

[1]- المادة 56 مصدر نفسه

[2]- المادة 60 المصدر نفسه

[3]- المادة 64 من القانون 18-04 المصدر السابق.

يعاقب بنفس العقوبة كل من قام بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص[1].

7- الاستعمال التعسفي أو التدليس لمعطيات المعالجة.

وفي هذا الشأن نجد المادة 69 من القانون 07/18 تنص على أنه يعاقب الحبس من سنة إلى خمس سنوات بغرامة من 100,000 دج إلى 500,000 دج كل مسؤول عن معالجة، وكل معالج من الباطن، وكل شخص مكلف بالنظر إلى مهامه بمعالجة معطيات ذات طابع شخصي يتسبب أو يسهل ولو عن إهمال الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك[2].

الفرع الثالث: دور المؤسسات العامة والخاصة في حماية البيانات الشخصية.

تلعب المؤسسات العامة والخاصة دورًا محوريًا في حماية البيانات الشخصية للمواطنين والمستخدمين، فما تزايد الاعتماد على التكنولوجيا أصبحت البيانات عرضة لانتهاكات متعددة تتطلب استجابة مسؤولة تسهم القوانين والسياسات المعتمدة في تنظيم طرق جمع البيانات ومعالجتها وحمايتها، ومن خلال تبني أنظمة أمنية متقدمة وتوعية الأفراد تضمن هذه المؤسسات الحفاظ على الخصوصية وبناء الثقة الرقمية.

أولا- الدور المؤسسات العامة في حماية البيانات الشخصية:

[1]- المادة 65 المصدر نفسه.

[2]- المادة 69 المصدر نفسه

تلعب المؤسسات العامة دورًا محوريًا في حماية البيانات الشخصية من خلال وضع الأطر القانونية والرقابية لضمان سرية المعلومات ومنع إساءة استخدامها، ويعد هذا الدور أساسيًا لتحقيق التوازن بين الحق في الخصوصية ومتطلبات المصلحة العامة.

1- تأمين وحماية المعطيات والهياكل:

- وضع آليات فعالة لتعزيز حماية البيانات والمعطيات ذات الطابع الشخصي الخاصة بالمواطنين والمتعاملين الاقتصاديين على المستوى المحلي بما يضمن احترام الخصوصية والسرية المعلوماتية.
- تأمين المرافق العمومية المحلية من خلال تعزيز البنية التحتية الرقمية بالاعتماد على أنظمة حماية موثوقة متوافقة مع الإطار الوطني المعتمد لأمن المعلومات[1].
- تنظيم حملات توعوية دورية لتعزيز الثقافة الأمنية لدى موظفي ومستخدمي الإدارة المحلية من خلال التوعية بأهمية حماية البيانات وطرق التصرف في حالة تعرضهم لمحاولات اختراق، إضافة إلى تنظيم ورشات حول التصيد والهجمات الرقمية.
- رفع وعي المواطنين المنتفعين من خدمات المرافق العمومية المحلية من خلال إطلاق حملات تحسيسية مشتركة تهدف إلى شرح كيفية حماية معلوماتهم الشخصية وضمان الاستخدام الآمن للوسائل الرقمية[2].

2- التزامات الوزارة فيما يخص حماية البيانات الشخصية:

تلتزم الوزارة بحماية البيانات الشخصية من خلال إنشاء وحدة لحمايتها وتكليفها بمسؤوليات تطوير السياسات وتنفيذ الإجراءات المناسبة[3]، كما يتم تعيين مسؤول أول للبيانات يتولى مهام الرقابة،

[1]- رقمنة وعصرنة المرافق العمومية الجوارية: من اجل تعزيز فعالية الخدمة العمومية في تلبية حاجيات المواطن، ديسمبر 2024 ص ص 08 09، المتوفر على الموقع، https://www.interieur.gov اطلع عليه بتاريخ 21 ماي 2025 ساعة 17:00

[2]- رقمنة وعصرنة المرافق العمومية الجوارية: المرجع السابق ، ص 8

وتقوم المكاتب المعنية بإعداد وتنفيذ السياسات المختلفة ذات الصلة، وتحدد الأدوار والمسؤوليات بوضوح لضمان معالجة البيانات بشكل دوري وآمن مع اعتماد نتائج التقييم والمخاطر. كما تتضمن الإجراءات مراجعة العقود والاتفاقيات لتتوافق مع السياسات المعتمدة، وتحرس الوزارة على معالجة الشكاوى والانتهاكات ووضع آليات فعالة للإبلاغ والتحقيق مع التأكد من إشراك جميع الأجهزة ذات العلاقة في تنفيذ السياسات.

وتتخذ خطوات لتوعية المعنيين بجمع البيانات وتعريفهم بحقوقهم وطرق الوصول إليها، بما في ذلك الحصول على موافقة صاحب البيانات عند المعالجة واحترام تفضيلاته فيما يتعلق بآليات الاستخدام مثل الموافقة المسبقة والانسحاب. تراعي الوزارة مبدأ تقليل البيانات المجمعة واستخدامها لأغراض محددة فقط مع الالتزام بعدم المعالجة خارج حدود المملكة إلا بموافقة الجهة المختصة. وتنفيذ إجراءات دقيقة للحفاظ على أمن البيانات وتحديد الصلاحيات بوضوح ومنع الوصول غير المصرح به.

كما تتضمن السياسات التخلص الآمن من البيانات عند انتهاء الغرض منها أو عند طلب صاحبها مع اعتماد ضوابط صارمة على الوصول. كما تنفذ المكاتب آليات للتوثيق الكامل لسير المعالجة وتستخدم حلولًا تقنية مناسبة للحفاظ على سرية البيانات وسلامتها. وفي حال حدوث اختراق أو تسريب للبيانات، تلزم الجهات المعنية بالإبلاغ الفوري خلال 72 ساعة ويتم التنسيق مع الجهاز المختص بالتحقيق في المعالجة، والالتزام بالإجراءات المعتمدة. وتورث الوزارة بوضع قواعد واضحة لمعالجة البيانات ذات الطبيعة الحساسة وفقًا للضوابط المعتمدة وضمان عدم تعارض المعالجة مع السياسات المعتمدة، كما يتم التنسيق مع مكتب إدارة البيانات الوطنية لإعداد الإجراءات اللازمة لمعالجة الشكاوى حسب إطار زمني محدد وتدرج مناسب للتسلسل الإداري[1].

[3]- سياسات حكومة البيانات، ص. 27، https://object.moe.gov.sa :اطّلع عليه بتاريخ 23 ماي 2025، الساعة 12:06.

[1]- سياسات حكومة البيانات، المرجع السابق، ص ص 28–29.

3- تعريف امن البيانات في المؤسسات البلدية:

امن البيانات في المؤسسات البلدية أمر بالغ الأهمية نظرا لتعاملها مع معلومات حساسة تتعلق بالمواطنين والخدمات العامة، ويتطلب الأمر تطبيق سياسات وإجراءات فعالة لحماية البيانات من الوصول غير المصرح به أو الفقدان أو التلاعب، إذ أن أي تهديد قد يؤثر بشكل مباشر على سير العمل وجودة الخدمات المقدمة[1].

تعد حماية البيانات الشخصية جزءا أساسيا من امن المعلومات في المؤسسة البلدية نظرا لاحتوائه على بيانات حساسة كالمعلومات الشخصية والمالية، لذا يجب الالتزام بالقوانين المحلية والدولية مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي، واعتماد تقنيات أمان متقدمة كالتشفير وكلمات المرور الفورية. تواجه المؤسسة تحديات متزايدة بسبب تطور الهجمات السيبرانية، ما يستدعي تحديث الأنظمة الأمنية باستمرار واستخدام أدوات كشف التهديدات وتدريب الموظفين على التعامل الأمن مع البيانات[2].

1- التشفير:

هو التقنية لحماية البيانات أثناء التخزين والنقل، حيث يحول النص الواضح الى شكل غير قابل للقراءة الا من قبل المصرح لهم، مما يقلل من خطر الوصول غير المصرح به، ويُستخدم التشفير لضمان سرية البيانات وسلامتها من التلاعب او الكشف.

2- التحكم في الوصول:

[1]- تاروت، خالد عواد الزعبي: "أمن البيانات وأهميتها في مجال مدخل البيانات في المؤسسات البلدية"، مجلة المجتمع العربي للنشر العلمية، بلدية الصلاة الكبرى، نوفمبر 2024، ص. 489.

[2]- تاروت، خالد عواد الزعبي: المرجع نفسه، ص. 490.

يتضمن تطبيق سياسات صارمة لتحديد صلاحيات الوصول إلى البيانات والملفات بناء على الدور الوظيفي لكل مستخدم، لضمان وصوله فقط إلى المعلومات الضرورية لأداء مهامه، وذلك من خلال إجراءات تحقيق وتوثيق مثل كلمة المرور والبطاقات الذكية، بهدف حماية الأنظمة من الدخول غير المصرح به ورصد الأنشطة المشبوهة.

3- التدريب والتوعية:

تقديم برامج تدريبية ونوعية لموظفي الجهات حوا أهمية حماية البيانات والحفاظ على الخصوصية، وتشمل هذه البرامج تعليمهم كيفية التعامل مع المعلومات الحساسة والتعرف على المخاطر المحتملة وطرق الحماية المناسبة.

4- المراقبة والتدقيق:

تطبيق آليات لرصد وتدقيق أنشطة الوصول للبيانات لضمان عدم وجود وصول أو استخدام غير مصرح به.

5- الامتثال للقوانين واللوائح:

الالتزام بالتشريعات المحلية والدولية لحماية البيانات عبر تنفيذ السياسات والإجراءات لضمان التوافق القانوني والتحقق من مطابقة العمليات للمعايير المعتمدة[1].

ثانيا: دوري المؤسسات الخاصة في حماية البيانات الشخصية:

تلعب المؤسسات الخاصة دورا حيويا في حماية البيانات الشخصية من خلال اعتماد سياسات امن معلومات صارمة، وضمان الامتثال للتشريعات المتعلقة بالخصوصية. وتلتزم هذه المؤسسات بتأمين بيانات العملاء ومنع الوصول غير المصرح به إليها، ويعكس هذا الدور أهمية القطاع الخاص في تعزيز الثقة الرقمية وحماية الأفراد.

[1]- أروى محمود قبلان الدعجة. "استراتيجية حماية البيانات والخصوصية في عمل حفظة الملفات بالبلديات"، مجلة المجتمع العربي للنشر للدراسات العلمية، بلدية الموقر، العدد 63، جويلية 2024، ص. 89_95

1- المساعي القانونية في الأمر رقم 04/10 الرابعة المعدل والمتمم من الأمر 03/11 .

تنص المادة 17 من الفقرة 02 على انه يجوز لبنك الجزائر واللجنة المصرفية تبادل المعلومات مع السلطات المختصة بمراقبة البنوك والمؤسسات المالية في الدول الأخرى، شريطة احترام مبدأ المعاملة بالمثل، وان تكون تلك السلطات ملتزمة بدورها بواجب السر المهني وفقا لنفس الضمانات المعمول بها في الجزائر. كما يحق لمصفّي البنك أو المؤسسة المالية الحصول على المعلومات اللازمة لأداء مهامه[1]. ونجد المادة 139 تنص على انه يعاقب كل مخالفة لأحكام الواردة في الكتاب السادس أعلاه والأنظمة المتخذة لتطبيقه، بالحبس من شهر إلى ستة أشهر وبغرامة يمكن أن تصل إلى 20% من قيمة الاستثمار[2].

وتنص المادة 25 صراحة على ضرورة التزام أعضاء الإدارة بالسرية المهنية، والحفاظ على سرية المعلومات الخاصة بالعملاء التي يطلعون عليها بحكم مهامهم، ولا يجوز لأعضاء مجلس الإدارة أن يفشوا، بصفة مباشرة أو غير مباشرة، وقائع أو معلومات اطلعوا عليها في إطار عهدتهم[3]، وذلك دون المساس بالالتزامات المفروضة عليهم بموجب القانون، ما عدا الحالات التي يُدعون فيها للإدلاء بشهادة في دعوى جزائية[4].

2- المساعي القانونية في قانون العقوبات:

جاءت المادة 301 من قانون العقوبات بحماية أسرار الأشخاص وحياتهم الخاصة من خلال إصدار عقوبة يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من 500 إلى 5000 دج، الأطباء والجراحون والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو

[1]- المادة 17 من الأمر 03-11 المؤرخ في 27 جمادى الثانية عام 1424 الموافق لـ 26 أوت 2003، المتعلق بالنقد والقرض.

[2]- المادة 139، المصدر نفسه

[3]- المادة 25، المصدر نفسه.

[4]- المادة 25 من قانون العقوبات، المصدر السابق.

المؤقتة على أسرار أُدلي بها إليهم وأفشوها، فيما عدا الحالات التي وجب عليهم فيها القانون إنشاؤها ويصرح لهم بذلك[1].

وفي الفقرة 302، كل من يعمل بأي صفة كانت في مؤسسة وأدلى أو شرع في الإدلاء إلى أجانب أو إلى جزائريين يقيمون في بلاد أجنبية بأسرار المؤسسة التي يعمل فيها دون أن يكون مخولا له ذلك، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 500 إلى 10000 دج. وإذا أُدلي بهذه الأسرار إلى جزائريين يقيمون في الجزائر، فتكون العقوبة الحبس من ثلاثة أشهر إلى سنتين وبغرامة من 500 إلى 1500 دج[2].

وتنص الفقرة الرابعة من نفس المادة على أنه في جميع الحالات يجوز الحكم، وعلى ذلك، بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 من هذا القانون لمدة سنة على الأقل وخمس سنوات أو أكثر[3].

توسيعا للحماية الجزائية للسرية البنكية وخصوصية العملاء، لم يُعفِ قانون العقوبات الشخص المعني من المسؤولية الجزائية متى ثبت أن الفعل قد ارتكب باسمه ولحسابه من قبل أجهزته أو ممثليه الشرعيين[4]، حسب نص المادة 303 مكرر 3. يكون الشخص[5] المعنوي مسؤولا جزائيا عن الجرائم المحددة في الأقسام 3 و4 و5 من هذا الفصل، وذلك طبقا للشروط المنصوص عليها في المادة 51 مكرر.

[1]- المادة 301، من قانون العقوبات المصدر السابق

[2]- المادة 302، المصدر نفسه.

[3]- الفقرة 04 من المادة 302، المصدر نفسه.

[4]- خليفية، هدى لتوش. "دليل سرية المعاملات البنكية وضمان خصوصية العملاء في النظام المعلوماتي"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق، جامعة قسنطينة 1، الجزائر، المجلد 7، العدد 2، ديسمبر 2022، ص. 532

[5]- المادة 3، قانون العقوبات، المصدر السابق.

وتُطبق على الشخص المعنوي عقوبة الغرامة حسب الكيفية المنصوص عليها في المادة 18 مكرر، وفي المادة 18 مكرر2، كالحل، الغلق، منع مزاولة النشاط المهني أو عدة أنشطة مهنية، حظر الصادرات، النشر والتعليق، والغرامة[1].

3- المساعي القانونية في القانون رقم 18 07

صدر القانون رقم 18 07 المؤرخ في 2018/6/10 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي متضمنا أحكاما عامة تطبق على جماعة المؤسسات والهيئات سواء كانت عمومية او خاصة التي تدرج المعطيات الشخصية ضمن أنظمتها المعلوماتية الآلية، بما في ذلك المؤسسات البنكية والتي نصت عليها المادة 03 الفقرة 12 بالمسؤول عن المعالجة، حيث تعرفه بأنه شخص طبيعي آو معنوي عمومي أو خاص أو أيا كان أخر يقوم بمفرده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها[2].

ونجد المادة 02 من نفس القانون تنص على انه تتم معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها او شكلها في اطار احترام الكرامة الانسانية والحياة الخاصة والحريات العامة، والا تمس بحقوق الاشخاص وشرفهم وسمعتهم[3].

وتنص المادة 54 من القانون 18 07 على اعتبار الفعل جنحة، وحدد عقوبته بالحبس من سنتين الى خمس سنوات وبغرامة من 200,000 الى 500,000 دج[4].

[1]- المادة 303 مكرر 3، المصدر نفسه.

[2]- المادة 03 من القانون 18-07، المصدر السابق.

[3]- المادة 02، المصدر نفسه.

[4]- المادة 54 من القانون 18-07، المصدر السابق.

وفي المادة 55 تنص على ان الاطلاع غير المشروع على المعطيات الشخصية الخاضعة للمعالجة في نظام آلي يعد جنحة، ويعاقب عليه بالحبس من سنة الى ثلاث سنوات وبغرامة من 200,000 الى 500,000 دج[1].

وهذا ما تؤكده المادة السابعة في الفقرة الرابعة بانه لا يمكن اطلاع الغير على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة الا من اجل انجاز الغايات المرتبطة مباشرة بالمهام المسؤول عن المعالجة او المرسل اليه، وبعد الموافقة المسبقة للشخص المعني[2].

وكنموذجا على ذلك نجد بنك البنكي يقوم بحماية البيانات الشخصية من خلال:

- **خصوصية المعلومات في بنك البينكسي:**

يستخدم بنك البنك في تطبيقاته الرقمية لجمع البيانات عبر الانترنت بهدف تقديم مجموعة متنوعة من الخدمات للعملاء تشمل إدارة الحسابات وتنفيذ المعاملات المالية، وتخضع هذه التطبيقات لسياسة خصوصية تنظم كيفية جمع البيانات واستخدامها ومشاركتها، ويلتزم بنك بنكسي بمعالجة البيانات الشخصية وفقا لأحكام القانون رقم 18 07 المتعلق بحماية الأفراد فيما يخص معالجة البيانات ذات الطابع الشخصي، وهو قانون يتماشى الى حد كبير مع اللائحة العامة لحماية البيانات الأوروبية.GPPR .

- **سياسة الخصوصية لدى بنك بينكسي:**

وفقا لأحكام القانون الجزائري رقم 18 07 المتعلق بحماية الأشخاص الطبيعيين فيما يخص معالجة المعطيات ذات الطابع الشخصي، تم إعداد سياسة خصوصية تهدف إلى توضيح كيفية التعامل مع

[1]- المادة 55 المصدر نفسه.

[2]- المادة 7 المصدر نفسه

المعلومات الشخصية التي يمكن استخدامها بمفردها أو مع غيرها لتحديد هوية شخص ما أو التواصل معه أو تحديد موقعه، سواء بشكل مباشر أو في سياق معين. وفي هذا الإطار، قام بنك "بنكسي" بوضع سياسة خصوصية واضحة تشرح كيفية دمج واستخدام وحماية المعلومات الشخصية للعملاء على مختلف منصاته الالكترونية[1].

بما في ذلك موقعه الإلكتروني وتطبيقه على أجهزة أندرويد، وتهدف هذه السياسة إلى ضمان الشفافية والفهم الواضح من قبل المستخدمين لكيفية التعامل مع بياناتهم الشخصية، بما يشمل جمعها واستخدامها وتخزينها ومعالجتها والتصرف فيها وفقًا للضوابط القانونية المعمول بها.

- **ملفات الارتباط وحماية الخصوصية**

يولي بنك بينكسي أهمية كبيرة لخصوصية عملائه أثناء تصفحهم لموقعه الإلكتروني أو استخدامهم لتطبيقه الرسمي، كما يمنح البنك لعملائه إمكانية التحكم الكامل في كيفية استخدام ملفات تعريف الارتباط على أجهزتهم، سواء كانت أجهزة كمبيوتر، هواتف ذكية، أو أجهزة لوحية، وذلك من خلال إعدادات قابلة للتعديل في أي وقت.

- **حماية المعطيات لدى بنك بنك لتحقيق مفهوم الخصوصية:**

يلتزم بنك البنكسي بحماية خصوصية بيانات عملائه، حيث لا يقوم ببيع أو تبادل أو تحويل المعلومات الشخصية إلى أطراف ثالثة دون موافقة صريحة، باستثناء الشركاء المساعدين في تقديم الخدمات شريطة التزامهم بالسرية. وقد يفصح البنك عن بعض المعلومات في حالة استثنائية امتثالا للقانون أو لحماية الممتلكات. كما يمكن مشاركة بيانات غير حساسة لأغراض تسويقية، ويؤكد البنك التزامه الكامل بالقوانين الجزائرية لحماية البيانات وتحقيق الخصوصية[2].

[1]– زيدان، سمية: عثماني، سفيان: "دراسة تحليلية: خصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية – دراسة حالة بنك بنكسي الجزائر"، مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، جامعة المسيلة، المجلد 17، العدد 2، ديسمبر 2024، ص. 68

[2]– زيدان، سمية: عثماني، سفيان: مرجع سابق، ص. 68–70

ثانيا: آليات حماية البيانات الطبية في البيئة الرقمية.

1- أمن البيانات الطبية من خلال حماية الأنظمة الإلكترونية:

في ظل التدفق الكبير للمعلومات والاستخدام الواسع للتقنية الرقمية في البنية التحتية الحيوية، أصبح من الضروري تعزيز أمن المعلومات والشبكات لحمايتها من الهجمات السيبرانية المتنوعة التي قد تلحق أضرارا بالأفراد وتؤدي إلى تعطيل الخدمات الأساسية، ومن هذا المنطق تبرز أهمية حماية المنشآت الحيوية لضمان استمرارية عملها، ولا سيما المنشآت الصحية التي تعد جزءا أساسيا من حياة الأفراد، ويمكن ترجمة هذه الجهود إلى مجموعة من الإجراءات الوقائية والتقنية لضمان السلامة الرقمية لتلك المنشآت.

أ- التقليل من الأجهزة المتصلة بإنترنت الأشياء:

للحد من مخاطر أجهزة الإنترنت المتصلة بالشبكة مثل الأجهزة، يجب مراقبتها دوريا للكشف عن محاولات الاختراق، مع تطبيق تدابير أمنية مثل تحديث البرامج الثابتة، استخدام جدران حماية متخصصة، تفعيل تشفير قوي للبيانات، وتقييد الوصول لمنع استغلالها من قبل المهاجمين[1] .

ب- تخزين البيانات في نسخ احتياطية:

تعد النسخ الاحتياطية من البيانات إجراء أساسيا لضمان استمرارية العمل وحمايتها من الهجمات السيبرانية أو الأعطال التقنية، ويتم ذلك عبر استراتيجية منظمة تشمل نسخ البيانات دوريا وتخزينها في مواقع آمنة ومتنوعة، مع ضرورة تشفيرها لمنع الوصول غير المصرح به وضمان سرية المعلومات.

ج- تحديث البرامج والأنظمة المعلوماتية لسد الثغرات:

[1]. محفوف، عبد الحكيم: "حماية البيانات الطبية في الفضاء الرقمي: دراسة ميدانية للمؤسسة العمومية للصحة الجوارية برج منايل"، مذكرة تخرج لنيل إجازة، المدرسة الوطنية للمانجمنت وإدارة الصحة، 2023، ص. 33-34.

تعد تحديثات البرامج والأنظمة من الإجراءات الأساسية لحماية النظم المعلوماتية، تسهم في سد الثغرات الأمنية التي قد يستغلها المهاجمون، يشمل ذلك أنظمة التشغيل، التطبيقات، وبرامج الحماية كبرامج مكافحة الفيروسات وجدران الحماية. تأخير وتجاهل هذه التحديثات يزيد من خطر التعرض للهجمات السيبرانية.

د- رصد الأمن لمختلف الأنشطة السيبرانية وضمان الاستجابة السريعة:

لحماية الأنظمة المعلوماتية وضمان استجابتها السريعة للتهديدات، يجب استخدام تقنيات متقدمة لرصد حركة البيانات وتحليلها لاكتشاف الأنشطة المشبوهة مبكرا مثل البرمجيات الخبيثة أو محاولات الاختراق. كما ينبغي دمج آليات استجابة فورية لمعالجة الحوادث كعزل الأنظمة المصابة وتنفيذ خطط الطوارئ، مما يقلل من تأثير الهجمة والأضرار المحتملة.

هـ- الالتزام بالتشفير العالي أثناء نقل البيانات عبر الشبكة:

تشفير البيانات أثناء نقلها عبر الشبكة ضروري لحماية المعلومات الحساسة وضمان سريتها. يعتمد ذلك على استخدام بروتوكولات ssl/tls وتشفير قوي يمنع التنصت أو التلاعب. كما يعد التحقق من هوية الأطراف المتبادلة للبيانات أمرا أساسيا لضمان عدم وصولها إلى جهات غير موثوقة، مما يعزز الأمان العام[1].

ثالثا: حماية أمن البيانات الشخصية والطبية في التشريع الجزائري:

أدرك المشرع الجزائري أهمية مواكبة التحديات الأمنية التي تفرضها البيئة الرقمية، فسعى إلى إدخال تعديلات تشريعية جوهرية على قانون العقوبات، بدءا بالقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، الذي أضيف من خلاله قسم خاص يعالج الجرائم المتعلقة بالأنظمة الآلية لمعالجة المعطيات. وقد تم تعزيز هذا الإطار القانوني لاحقا بالقانون رقم 09-04 المتعلق بالوقاية من جرائم

[1]- محفوف، عبد الحكيم: مرجع سابق، ص. 34.

تكنولوجيا الإعلام والاتصال ومكافحتها، حيث وسع نطاق التجريم ليشمل سلوكيات إجرامية جديدة في الفضاء الرقمي[1].

وفي سياق حماية البيانات الشخصية والطبية، صدر القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطبع الشخصي، والذي يعد من أبرز القوانين في هذا المجال. وتهدف هذه التعديلات إلى توسيع نطاق الحماية الجنائية لتشمل مختلف أشكال الاعتداء على الأنظمة المعلوماتية، مع تحديث الأدوات القانونية لمواجهة الجرائم الإلكترونية المستجدة. واعتبر القانون من الأفعال المجرمة الدخول غير المصرح به أو البقاء غير المشروع داخل المنظومة المعلوماتية كليا أو جزئيا باستخدام وسائل احتيالية، أو إدخال بيانات بطريقة مخادعة، أو حذفها أو تعديلها بشكل غير مشروع. كما شمل التجريم عملية تطوير أو جمع أو توزيع أو بيع أو نشر البيانات المخزنة أو المنقولة عبر الأنظمة المعلوماتية، بالإضافة إلى حيازة أو كشف أو استغلال تلك البيانات بطرق غير قانونية. وقد نص المشرع على عقوبات مشددة في حال العبث بالبيانات عن طريق الحذف أو التغيير أو التسبب في تعطيل نظام تشغيل المنظومة المعلوماتية[2].

المبحث الثاني: الآلية التقنية لحماية البيانات الشخصية

تعد الآليات التقنية جزءًا جوهريًا في حماية البيانات الشخصية في العصر الرقمي، حيث تقدم حلولًا وأدوات لضمان السرية وسلامة المعلومات تعمل هذه الآليات على حماية خصوصية الأفراد من خلال منع الوصول غير المصرح به إلى البيانات أو استخدامها بشكل غير قانوني، مما يسهم في تعزيز الثقة في التعاملات الإلكترونية ويمنح الأفراد شعورًا بالأمان عند الاستفادة من الخدمات الرقمية. وتكمن أهمية هذه الآليات في حماية البيانات من الاختراق والاستغلال غير المشروع، مما يضمن الحفاظ على سلامة وسرية المعاملات والامتثال للقوانين والتشريعات المتعلقة بحماية البيانات

[1]- محفوف، عبد الحكيم: مرجع سابق، ص. 34.

[2]- مرجع نفسه، ص. 38.

الشخصية. بناءً على ذلك، سيتناول هذا المبحث الوسائل الفنية المستخدمة لتأمين البيانات الشخصية في المطلب الأول، بينما يتركز المطلب الثاني على دور الهيئات المختصة في حمايتها، بالإضافة إلى التدابير المرغوبة المتعلقة بأمن تلك البيانات.

المطلب الأول: الوسائل الفنية لتأمين البيانات الشخصية

تلعب الوسائل الفنية دورًا بارزًا في حماية البيانات الشخصية في عصر يتسم بالتكنولوجيا والتواصل الرقمي. تهدف هذه الوسائل إلى توفير الحماية اللازمة للبيانات ومنع أي وصول غير مصرح به أو استغلال غير قانوني. وتكمن أهميتها في ضمان خصوصية الأفراد من خلال استخدامها في أغراض قانونية، وتوفير الإمكانية للأفراد للتحكم الكامل ببياناتهم، مثل الوصول إليها وتعديلها وامتثالها لمتطلبات القوانين ذات الصلة. وفي هذا السياق نستعرض أبرز الوسائل الفنية المستخدمة لحماية البيانات الشخصية، وهي كما يلي:

الفرع الأول: تقنيات تشفير البيانات الشخصية

تعتبر سياسة التشفير أحد أدوات الاساسية في العالم التكنولوجي الحديث اذ تمثل هذه السياسة جملة من المبادئ والقواعد التي تهدف الى تحقيق الامان الرقمي ومنع اساءة استغلاله اذ أصبحت سياسات التشفير مع التطور السريع للتكنولوجيا محط اهتمام والحكومات لضمان تكامل المعلومات التهديدات السيبرانية.

1-تعريف تقنية التشفير:

تعتبر هذه التقنية وسيلة تعتمد على استخدام خوارزميات رياضية ذكية تتيح لحامل المفتاح السري تحويل رسالة أو نص واضح إلى نص أو رسالة[1] غير مفهومة يُدعى بالنص المشفر[2]، ومن ثم إعادتها إلى حالتها الأصلية باستخدام ذات المفتاح لفك التشفير.

أما فيما يخص التشريع الجزائري، فإنه لم يقدم تعريفًا مباشرًا لهذه التقنية، بل اقتصر على توضيح ماهية المفتاح الخاص والعام في قانون 15-04 الذي ينظم قواعد العمل للتوقيع والتصديق الإلكتروني، فالمفتاح السري الخاص هو مجموعة الأعداد التي تكون خاصة فقط بالجهة الموقعة، بينما المفتاح العام أو العمومي فهو يتكون من أعداد يمكن للجميع الوصول إليها للتحقق من صحة التوقيع الإلكتروني.

وبناءً على ما سبق، فإن عملية التشفير هي عملية تحويل النص إلى رموز وإشارات غير مفهومة بحيث تبين بلا معنى، وتهدف إلى منع الآخرين من الاطلاع عليها إلا من يمتلكون التصريح لفك تشفير النص وفهم مضمونه. وتقوم هذه التقنية على ثلاث عناصر مترابطة، وهي:

- المعلومات التي سيتم تحويلها إلى صيغة مشفرة.
- خوارزمية التشفير المستخدمة لتطبيق الحماية على المعلومات، وخوارزمية فك التشفير التي تعيد هذه المعلومات إلى حالتها الأصلية.
- المفاتيح وهي مجموعة أو سلسلة من الرموز التي تعتمد على معادلات رياضية معقدة يتم تقديمها في هيئة خوارزميات[3]

[1]- حزان فتيحة: حماية الأنظمة الرقمية بين الآلات التقنية والأجهزة. الحماية، قراءة في أحكام المرسوم الرئاسي 20-05. مجلة الحقوق والعلوم الإنسانية، المجلد 13، العدد 3، جامعة بومرداس، الجزائر، 30 أكتوبر 2020. ص 175

[2]- أحمد عربيي، حورية قاسمي: دور سياسة التشفير الإلكتروني في حماية نظم معلومات الإدارة الإلكترونية بمؤسسة بريد الجزائر، المدية. مجلة الاقتصاد الجديد، المجلد 12، العدد 1، جامعة المدية، الجزائر، 1 جانفي 2021. ص 313.

[3]- عقوني محمد، مجري يوسف: الآليات القانونية لحماية الخصوصية المعلوماتية في البيئة الافتراضية. مجلة الباحث للعلوم القانونية والسياسية، العدد 5، جامعة بسكرة، جامعة سوق أهراس، 2021. ص 46.

وأما عن كيفية إجراء التشفير، فيتم التأكد من أن المعلومات التي تصل إلى المرسل إليه هي نفس البيانات التي قام المرسل بالتوقيع عليها، حيث يتم تشفير التوقيع الإلكتروني.

استخدام نظامين رئيسيين، الأول هو نظام المتماثل، وهو نوع من البرمجيات التي تعتمد على استخدام رموز هندسية معقدة، أما النظام الثاني فهو نظام البيومتري الذي يعتمد على خصائص شخصية تتعلق بصاحب التوقيع نفسه[1].

2- ضوابط التشفير

أ. مشروعية تشفير المعلومات والبيانات:

تعتبر مشروعية تشفير البيانات والمعلومات موضوعًا هامًا في إطار التعاملات الإلكترونية، خاصة تلك التي تتم عبر الوسائط الرقمية، حيث نجد أن المشرع الجزائري، من خلال القانون 15-04، وضع نصوصًا واضحة تناولت نظام التشفير، حيث عرف التشفير بمختلف أنواعه سواء الخاص أو العام، وسمح باستخدامه في المراسلات الإلكترونية وعمليات التجارة الإلكترونية.

كما أكد القانون الجزائري على حماية البيانات المشفرة والعناصر المستخدمة في عمليات التشفير وفك التشفير من أي تعدٍ، كما يشمل حماية مفاتيح التشفير الشخصية الخاصة بالتوقيع التي تُستخدم خارج نطاق الأطراف المعنية بالعلاقة.

كذلك تطرق إلى استخدام التشفير في تنفيذ الجرائم مثل الاحتيال أو سرقة المفاتيح التي تعيد النص المشفر إلى أصله باستخدام أدوات فك التشفير...

وفي سياق أوسع أشارت معظم التشريعات العربية إلى موضوع التشفير بشكل غير مباشر، خاصة عند الحديث عن التوقيع الإلكتروني في التشريعات المتعلقة بالتجارة الإلكترونية، ومع ذلك يُلاحظ أن

[1]- مرجع نفسه ص 46.

المشرعين التونسي والمصري طرحوا نصوصًا قانونية صريحة تتناول عملية التشفير مباشرة، مما يعكس حرصهم على تجنب أي لبس أو اختلافات تفسيرية متعلقة بالموضوع[1].

ب.الحق في الحفاظ على سرية البيانات والمعلومات المشفرة:

حيث يعبر المشرع الجزائري، من خلال القانون 15-04، أن الاعتداء على البيانات المنقولة بين طرفي العقد عبر الوسائط الإلكترونية يُعد انتهاكًا لخصوصية وسرية تلك البيانات والمعلومات، حيث أقر القانون بأنه لا يجوز لأي طرف ثالث الاطلاع على المعطيات ذات الطابع الشخصي التي تخضع للمعالجة أو المرسلة إليه، كما أنه لا يشترط موافقة الشخص المعني إذا كانت المعالجة ضرورية لتنفيذ عقد يُعتبر الشخص المذكور طرفًا فيه، أو لإنجاز إجراءات سابقة للعقد تمت بناءً على طلبه.

وعليه، يتعين ضمان سرية البيانات المستخدمة لإنشاء التوقيع الإلكتروني بالوسائل التقنية المتاحة وقت الاعتماد، كما يقع على عاتق الجهات المؤدية لخدمات التصديق الإلكتروني مسؤولية الحفاظ على سرية البيانات والمعلومات المرتبطة بشهادات التصديق الإلكتروني الصادرة، نظرًا لأن هذه البيانات تحمل طابعًا خاصًا وسريًا وتعكس إدارة طرف العلاقة القانونية.

حيث إن إفساد مثل هذه البيانات أو المراسلات من شأنه أن يُلحق ضررًا بطرفي العقد ويُعد انتهاكًا لخصوصياتهما، خاصة إذا تم فك تشفيرها، فقد نص المشرع الجزائري على عقوبات تُطبق على كل من ينتهك سرية البيانات المشفرة أو يطّلع عليها ويكشف عنها، سواء كان ذلك من قبل أطراف ثالثة أو مقدمي خدمات التصديق الإلكتروني أو الأشخاص المكلفين بالتدقيق[2].

[1]- عقوني محمد، مجري يوسف: سابق، ص 47.

[2]- مرجع نفسه: ص 48.

ج. **اعتبار النص المشفر محررًا إلكترونيا:**

نتيجة لإقرار المشرع بأهمية النص المشفر وحجيته في إثبات جميع التصرفات القانونية التي تتم عبر الوسائط الإلكترونية، فإنه يُعد من الوثائق الإلكترونية، على الرغم من أنه قد لا يكون مفهومًا للعامة. وبناءً على ذلك، يتم تحويل الإشارات والرموز المستخدمة فيه إلى نصوص واضحة ومقروءة، تكون ملزمة قانونيًا لكل من يُخالف الالتزامات التي تعهد بها طرفا الاتفاق[1].

3- طرق التشفير:

يمكن تصنيفها وفقًا لنوعية المفتاح المستخدم في التشفير:

أ. **تقنية التشفير المتماثل أو الأحادي والمفتاح الواحد:**

نظام الكتابة بالمفتاح الخاص يعتمد على مفتاح واحد، يُطلق عليه المفتاح الواحد، والذي يكون مشتركًا بين مرسل الرسالة ومستلمها. هذا النظام يستخدم نفس المفتاح أو الرمز السري لتشفير الرسائل وكذلك لفك تشفيرها.

حيث إنه في بداية العملية يتفق الطرفان على كلمة مرور يتم استخدامها لإنشاء التشفير وفكه. بمجرد إدخال كلمة المرور، يتم تحويلها إلى صيغة ثنائية يستطيع الحاسوب التعامل معها، وعند ما يتم إرسال الرسالة إلى الطرف الآخر، يتوجب عليه فك التشفير لإزالة الغموض واسترجاع النص إلى صورته الأصلية باستخدام كلمة المرور التي استُخدمت في عملية التشفير[2]. وتُسمى أيضًا بتقنية التشفير[3] الأحادي أو المفتاح الواحد[4].

[1]- عجبوني محمد، مجري يوسف: سابق، ص 49.

[2]- مرجع نفسه: ص 50.

[3]- حزان فتيحة: المرجع السابق، ص 177.

[4]- أحمد عريبي، حورية قاسمي: المرجع السابق، ص 314.

ب.تقنية التشفير غير المتماثل:

يعتمد هذا النوع من التشفير على استخدام مفتاحين مختلفين، أحدهما مفتاح خاص يحتفظ به المستخدم سرًا ولا يُشاركه مع أي شخص، والآخر هو مفتاح عام يتم توزيعه على الأطراف الأخرى التي يرغب المستخدم في تلقي رسالة مشفرة منهم.

ويتم استخدام هذين المفتاحين المرتبطين بطريقة رياضية لإنشاء توقيع إلكتروني لتحويل البيانات والمعلومات، ومن ثم تتبعها مرة أخرى بنظام التشفير غير المتماثل. وبهذا النظام، حتى ولو تمكن الآخرون من معرفة المفتاح العام، فإنهم لن يكونوا قادرين على اكتشاف المفتاح الخاص المرتبط به أو استخدامه لفهم محتوى الرسالة، حيث إن المفتاح الخاص يظل حكرًا على الشخص المرسل ويُستخدم لتشفير الرسائل أو فك تشفيرها، بينما المفتاح العام يكون متاحًا لعدة جهات أو أفراد للتواصل المشفر مع المرسل[1].

الفرع الثاني: أنظمة الحماية والجدران النارية.

تعتبر انظمة الحماية والجدران النارية من ابرز الاساليب االتكنولوجية المستخدمة لضمان امان الشبكات الرقمية اذ تلعب دورا اساسيا في تقليل المخاطر الناجمة عن الاختراقات والهجمات التي قد تستهدف البيانات الشخصية او الشبكات ومع تطور التقنيات اصبحت انظمة الحماية تعتمد على الذكاء الاصطناعي والتحليل المستمر للبيانات ،اذ اصبحت تشكل انظمة الحماية والجدران النارية حجز الاساس في تامين المعلومات وضمان سلامة الانظمة الرقمية

1-تعريف الجدران النارية:

هو برنامج أو جهاز يهدف إلى حماية جهاز الحاسوب أثناء اتصاله بشبكة الإنترنت من المخاطر المحتملة، وتتمثل وظيفته في فحص جميع المعلومات والبيانات القادمة عبر الإنترنت أو أي شبكة أخرى، ثم تحديد ما إذا كانت تتوافق مع إعداداته قبل السماح بمرورها إلى الجهاز، فإذا كانت تحمل تهديدات مثل الفيروسات أو برامج التجسس، يقوم الجدار الناري برفضها ومنعها من الوصول.

[1]- عقوني محمد، مجري يوسف: مرجع سابق، ص 50-51.

حيث إنه يمكن تشبيه الجدار الناري بنقاط التفتيش التي تعمل كحاجز أمني بين جهاز الحاسوب وشبكة الإنترنت، حيث يؤدي دورًا حاسمًا في تقليل احتمالات الاختراق والجهات الإلكترونية.

وتتجلى أهميته في كونه إحدى الأساسيات لضمان حماية الحاسوب من المتسللين أو البرمجيات الضارة، خصوصًا في ظل البيئة غير الآمنة لشبكة الإنترنت التي تكثر فيها المخاطر الأمنية، وعلى المستخدمين الحرص على تأمين أجهزتهم أثناء الاتصال بالإنترنت باستخدام جدار ناري مناسب. يمكن تحميل برامج الجدران النارية بسهولة من الإنترنت عبر مواقع موثوقة مثل www.download.com : لتعزيز أمان الأجهزة وحمايتها بكفاءة[1].

2- أشكال الجدار الناري

أ- **Pascal Filter** :يعمل على المستوى الثالث من الشبكة، حيث لا يسمح بمرور حزمة البيانات إلا إذا كانت متوافقة مع القوانين المعرفة مسبقًا، حيث يقوم مدير الجدار الناري بتحديد هذه القوانين، وفي حالة عدم تحديدها يتم اعتماد القواعد الافتراضية. لا يحتفظ بأي معلومات تتعلق بحالة الاتصال، وبالتالي لا يهتم بمعرفة ما إذا كانت الحزمة قد أُرسلت مباشرة من المصدر أو إذا تم تعديلها والتلاعب بها[2].

ب-**Proxies Filters** : يعمل البروكسي على جهاز مخصص أو كبرنامج مثبت على جهاز لأغراض عامة، ويُعتبر بمثابة بوابة بين الشبكات، حيث يقوم بتسهيل الوصول لتطبيق معين داخل الشبكة، ومن المهم أن ندرك أنه يتم توجيه جميع الطلبات عبر خادم البروكسي. على سبيل المثال، إذا كان هناك خطر من المواقع التي تحتوي على كلمة "تحميل"، فسوف تمر الطلبات أولًا عبر خادم

[1]- حزام فتيحة: المرجع السابق، ص 175.

[2]-. إيناس عدي: الجدار الناري، المحاضرة السادسة، المتوفر على الموقع .www.hama.univ.edu.sg :اطّلع عليه بتاريخ 8 ماي 2025، الساعة 13:45.

البروكسي، حيث يؤدي دوره كمترشح (فلتر)، إذ يقوم البروكسي بفحص محتوى الحزمة وتحديد ما إذا كانت ستمرر أم لا، وذلك بناءً على القواعد المحددة له[1].

ج- **Host Based** : يمكن أن يكون النظام إما على جهاز حاسوب شخصي أو على هيئة خادم، وعادة ما تُنفذ عملية التحكم والتصفية في هذا النوع من خلال منتج برمجي مثل الجدار الناري المدمج في نظام التشغيل ويندوز.

د- **State Filters** : يحافظ على تتبع حالة الاتصال ويُحقق ما إذا كان الاتصال قد تم إنشاؤه بنجاح، ومن ثم انتقال البيانات، وأخيرًا التأكد من إنهاء الاتصال بشكل صحيح.

و- **Hybnd Firewall** : هو دمج بين عدة أنواع مختلفة من الجدران النارية التقليدية[2].

3- سياسات الجدار الناري:(Firewall Policies)

أ- **Drop** .في هذه الحالة، يقوم الجدار الناري بقطع الاتصال سواء كان داخليًا أو خارجيًا، اعتمادًا على القوانين المحددة له مسبقًا.

ب- **Accept**:في هذه الحالة، يقوم الجدار الناري بقبول الاتصالات الصادرة والواردة استنادًا إلى القوانين المحددة له مسبقًا.

ج- **Default Policy** : بشكل افتراضي، يقوم الجدار الناري بحظر جميع الحزم الواردة مع السماح بمرور الحزم الصادرة. وبالنسبة للاتصالات الواردة، فإن قوانين الحظر تأخذ الأولوية على قوانين السماح، بينما في حالة الاتصالات الصادرة تكون قوانين السماح ذات أولوية أعلى من قوانين الحظر[3].

---

[1]- المرجع نفسه.

[2]-. إيناس عدي: مرجع سابق.

[3]- مرجع نفسه.

3- منطقة منزوعة السلاح:(Demilitarized Zone – DMZ)

يعني ذلك أن الشبكات بدون حماية أو جدار ناري معرضة للخطر. وكما هو معروف في مجالات الشبكات، يوجد نوعان رئيسيان هما:

1. **الشبكات الداخلية** :(**LAN**) من أهم المكونات التي تشملها الأجهزة المركزية (السيرفرات) بالإضافة إلى أجهزة المستخدمين، هي أجهزة الرواتر وغيرها. ومن اللازم أن تكون هذه الأجهزة محمية ومؤمنة بشكل كامل لمنع أي اختراق أو تدخل مع أي شبكة خارجية.
2. **الشبكة الخارجية:** بصفتها العامة لا تتمتع بمستوى عالٍ من الحماية، وتُعتبر بالنسبة للشبكة الداخلية مصدرًا رئيسيًا لخطر الاختراق والتهديدات. وعادة ما يتم الفصل بين الشبكتين باستخدام وسيلة حماية، والتي قد تكون بأبسط أشكالها مثل جهاز الراوتر أو جدار ناري[1].
3. DMZ :هذا النوع الثالث من الشبكات يتميز بكونه متوسطًا بين النوعين الآخرين، حيث تُصنف كشبكة محايدة. فهي ليست مؤمنة ومحميّة بالكامل كما هو الحال في الشبكات الداخلية، ولا هي معرضة بشكل كامل ومباشر للمستخدمين كما يحدث مع شبكة الإنترنت.

ويُعتمد إنشاء منطقة منزوعة السلاح (DMZ) كحل عند الحاجة للسماح للمستخدمين الخارجيين بالوصول إلى خدمات محددة داخل الشبكة المحلية مثل خادم الويب و(FTP) ، وذلك دون المساس بأمان الشبكة الداخلية. بدلًا من وضع هذه الخدمات ضمن نطاق الشبكة الداخلية، الذي قد يعرّض النظام بأكمله لمخاطر الاختراق والهجمات، يتم فصل هذه الخدمات في شبكة مستقلة تُعرف بـ.DMZ .

وتُساهم هذه الإستراتيجية (DMZ) في حماية الشبكة الداخلية من أي تهديدات محتملة قادمة من الإنترنت، حيث تُعد بمثابة طبقة أمان إضافية وعازلة تمنع التهديدات من التأثير المباشر على البنية

[1]- إيناس عدي: المرجع السابق.

الأساسية للشبكة المحلية. وفي الوقت نفسه، تتيح تقديم الخدمات اللازمة للمستخدمين الخارجيين بكفاءة وأمان. كما أن DMZ تُعد باختصار حلقة وصل بين الشبكة العامة (WAN) والشبكة المحلية(LAN) ، مُصممة بعناية لتحقيق التوازن بين الأمان وتوفير الخدمات[1].

الفرع الثالث: تقنيات التحقق من الهوية وإدارة الوصول

ينص القانون الجزائري 04/15 المادة الرابعة على أن مقدمي خدمات التصديق الإلكتروني، قبل إصدار شهادة التصديق الإلكتروني، يجب التحقق من تكامل بيانات إنشاء التوقيع مع بيانات التحقق، حيث يتم منح شهادة أو أكثر لكل شخص يتقدم بطلب، وذلك بعد التأكد من هويته، وفي بعض الحالات التحقق من صفاته الخاصة. في حالة الأشخاص المعنويين، يلتزم مقدم خدمات التصديق الإلكتروني بحفظ سجل يتضمن هوية وصفة الممثل القانوني للشخص المعني والمستخدم للتوقيع، مما يستعمل لتصديق هوية الشخص الطبيعي المستخدم للتوقيع الإلكتروني في كل مرة يتم فيها استعماله[2].

حيث يهدف مزود خدمات التصديق الإلكتروني، من خلال إعطاء شهادة التصديق الإلكتروني، إلى تعزيز الثقة بين الأطراف الأخرى في صحة المعلومات الواردة فيها، خاصة ما تعلق بهوية الموقع وربط التوقيع الإلكتروني به، مما يجعل التعامل معها يتم بثقة واطمئنان[3]. كما أن هيئة التوثيق تيسر للأطراف المعتمدة على الشهادة الإلكترونية أدوات تثبت أن الشخص المذكور في الشهادة كان يتحكم بأداة التوقيع، وأنها كانت فعالة وقت التوقيع[4].

[1]- المرجع نفسه.

[2]- المادة 44 من القانون 15-04: المصدر السابق

[3]- هلا الحسن: تصديق التوقيع الإلكتروني. مجلة جامعة دمشق للعلوم القانونية والاقتصادية، مج 46، العدد 1، جامعة دمشق، 2010، ص 531. الموقع www.damascusuniversity.edu.sy :، اطّلع عليه بتاريخ 10 ماي 2025، الساعة 8:30 مساءً.

[4]- عقوني محمد، وماجري يوسف: مرجع سابق، ص 56.

علاوة على ذلك، نص القانون 07/18 على ضرورة أن يقوم كل مزود خدمات بحفظ جرد خاص بالانتهاكات المتعلقة بالبيانات ذات الطابع الشخصي والإجراءات التي تتخذ لمعالجتها[1].

المطلب الثاني: هيئات حماية البيانات الشخصية والتدابير التوعوية لحمايتها:

لقد سعى المشرع الجزائري إلى معالجة القضايا المتعلقة بالأمن السيبراني من خلال توفير آليات متطورة تشرف عليها وزارة الدفاع الوطني، نظرًا للطابع الحيوي لهذه القضايا التي ترتبط بسيادة الدولة بشكل شامل. حيث جاء هذا التوجه استنادًا إلى أحكام المرسوم الرئاسي 05/20، خصوصًا المادة الثالثة منه التي تنص على استناد منظومة وطنية لأمن الأنظمة المعلوماتية. وفي هذا السياق، سنسلط الضوء على مهام وتشكيلة هيئتي المنظومة الوطنية: المجلس الوطني لأمن الأنظمة المعلوماتية، بالإضافة إلى التدابير التوعوية لتعزيز أمن الأنظمة المعلوماتية.

الفرع الأول: المجلس الوطني لأمن الأنظمة المعلوماتية.

وهو كيان مستحدث مشابه لهيئة التصديق الإلكتروني التي يتم إقرارها بموجب القانون 04/15 المتعلق بالتوقيع الإلكتروني.

أ. تشكيلته:

يشكل المجلس برئاسة وزير الدفاع الوطني أو ممثله، ويتضمن في تركيبته ممثلين من رئاسة الجمهورية والوزير الأول، كما يضم المجلس الوزراء المسؤولين عن الشؤون الداخلية، العدل، المالية، الطاقة،

[1]- الفقرة الثانية، المادة 43 من القانون18. 07- المصدر السابق.

الاتصالات، التعليم العالي. كما يمكن للمجلس الاستعانة بأي شخص أو مؤسسة من شأنها تقديم الإرشاد أو المساعدة في أداء مهامه[1].

يلعب المجلس دورًا محوريًا في إعداد وصياغة الإستراتيجية المتعلقة بأمن الأنظمة المعلوماتية، حيث يتولى مجموعة من المهام المهمة، إذ تشمل هذه المهام النظر في مكونات الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية التي تقدمها الوكالة وتحديدها، ودراسة مخطط عمل الوكالة وتقارير أنشطتها والموافقة عليها، بالإضافة إلى التصديق على اتفاقيات التعاون والاعتراف المتبادل مع الجهات الأجنبية المختصة في مجال أمن الأنظمة المعلوماتية. كما يتولى المجلس الموافقة على سياسة التصديق الإلكتروني التي تعتمدها السلطة الوطنية المختصة، وتحديد تصنيف الأنظمة المعلوماتية، واقتراح تعديلات على الهيكل التنظيمي أو التنظيم الخاص بهذا المجال. علاوة على ذلك، يقدم المجلس رأيه الحاسم عند الحاجة بشأن أي مشروع يتصل بأمن الأنظمة المعلوماتية[2].

يصادق المجلس على نظامه الداخلي، وينعقد كلما استدعت الضرورة ذلك، بمشاركة الهيئات العامة والخاصة، من أجل وضع استراتيجية بناءً على دعوة من رئيسه[3]. كما يتولى رئيس المجلس إعداد جدول الأعمال مع الحرص على المتابعة التكنولوجية في مجال أمن الأنظمة، كما ينظم اجتماعات المجلس ويحدد مواعيدها[4].

أما فيما يتعلق بالدعوات وجدول الأعمال، فهي تُرسل إلى الأعضاء قبل خمسة أيام من تاريخ الاجتماع، وفي الحالات الطارئة يمكن تقديم جدول الأعمال خلال الانعقاد، مع تقديم المساندة للجهات المختصة في معالجة الحوادث المرتبطة بأمن الأنظمة المعلوماتية بعد استشارة المجلس. كما

[1]- المادة 5 من المرسوم الرئاسي 20-05: مؤرخ في 24 جمادى الأولى عام 1441 الموافق لـ 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية. الجريدة الرسمية، المؤرخة في 26 جانفي 2020

[2]- المادة 4 من المرسوم الرئاسي 20-05: المصدر السابق.

[3]- المادة 12: المصدر نفسه.

[4]- المادة 13 من المرسوم الرئاسي: المصدر السابق

يطلع باعتماد وتصديق منتجات أمن الأنظمة المعلوماتية، والمصادقة على أنظمة إنشاء وفحص التوقيع الإلكتروني، وتحديد المعايير والإجراءات الخاصة بمنح شهادة الجودة أو التصديق، واعتماد الخدمات في مجال أمن الأنظمة المعلوماتية بما يتماشى مع القوانين والتنظيمات المعمول بها.علاوة على ذلك، تشرف الوكالة على تنفيذ برامج الإرشاد والتوعية لتعزيز أمن الأنظمة المعلوماتية[1].

ب.تنظيم وسير وكالة أمن الأنظمة المعلوماتية:

تدار الوكالة من قبل لجنة توجيه بلجنة علمية، ويتم الإشراف على سيرها من قبل مدير عام. كما تضم الوكالة مركزًا وطنيًا عمليًا لأمن الأنظمة المعلوماتية، إلى جانب المديريات والمصالح التقنية والإدارة التي تعمل تحت سلطته.

1- لجنة التوجيه:

لها طابع مميز بالإضافة إلى معناها، وهو ما سنتناوله بالتفصيل من خلال النقاط التالية:

أ. تشكيلتها:

يُعين رئيس لجنة التوجيه وفقًا للتنظيم المعتمد في وزارة الدفاع الوطني، وتتشكل اللجنة من ممثلين عن الهيئات التالية: وزارة الدفاع الوطني، الوزارة المكلفة بالشؤون الخارجية، الوزارة المكلفة بالداخلية، الوزارة المكلفة بالعدل، الوزارة المكلفة بالمالية، الوزارة المكلفة بالطاقة، الوزارة المكلفة بالتعليم العالي، الوزارة المكلفة بالصناعة، الوزارة المكلفة بالاتصالات، الوزارة المكلفة بالتجارة، مصالح الأمن،

[1]- المادة 19: المصدرنفسه.

سلطة ضبط البريد والاتصالات الإلكترونية، السلطة الوطنية للتصديق الإلكتروني، الهيئة الوطنية لحماية البيانات ذات الطابع الشخصي، والسلطة الحكومية للتصديق الإلكتروني.

ويُضاف إلى ذلك المدير العام للوكالة بصفة استشارية. وتتولى مصالح الوكالة أمانة لجنة التوجيه، حيث يجوز للجنة التوجيه الاستعانة بأي شخص أو مؤسسة تراها مؤهلة لتقديم المشورة الجلسة. تُتخذ قرارات المجلس بالأغلبية، وفي حالة تعادل الأصوات يُرجّح صوت الرئيس[1]. تدون نتائج اجتماعات المجلس في محاضر رسمية[2]، وتصدر أعمال المجلس وفق الحالة على شكل قرارات، توصيات، آراء، أو تقارير. كما تُقدّر وتُسجل الإعتمادات المالية اللازمة لتسيير المجلس في ميزانية وزارة الدفاع الوطني[3].

الفرع الثاني: وكالة أمن الأنظمة المعلوماتية: تعد وكالة امن الانظمة المعلوماتية من الجهات المؤسسية المختصصة في حماية واستدامة الامن السيبراني في العالم الرقمي المتطور.

أ– تعريفها:

تصنف الوكالة وفقا للمادة 17 من المرسوم الرئاسي 05/20 كمؤسسة عامة ذات طابع إداري تتمتع بالشخصية والاستقلال المالي، ويقع مقرها في مدينة الجزائر.

ب– مهامها:

تُحدد وتُصنّف مكونات الوكالة وآليات عملها وصلاحياتها بموجب قرار صادر عن وزير الدفاع الوطني[4]، حيث تتولى الوكالة مجموعة من المهام الرئيسية المنصوص عليها في المادة 18، ومن أبرزها إعداد وتطوير عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وعرضها على المجلس الوطني،

[1]– المادة 20 من المرسوم الرئاسي: مصدر سابق.

[2]– المادتان 21 و22: المصدر نفسه.

[3]– المادة 14 من المرسوم الرئاسي: مصدر سابق.

[4]– المادة 15: مصدر نفسه.

وتنسيق تنفيذ الإستراتيجية الوطنية التي يحددها المجلس في هذا المجال. كما تتضمن المهام اقتراح آليات اعتماد مزودي خدمات التدقيق لأمن الأنظمة المعلوماتية، وإجراء تحقيقات رقمية في حال وقوع هجمات أو حوادث سيبرانية. تستهدف المؤسسة الوطنية، بالإضافة إلى ذلك، إلى جمع وتحليل وتقييم المعطيات المتعلقة بأمن الأنظمة المعلوماتية لاستخلاص المعلومات الضرورية لحماية منشآت المؤسسة الوطنية، والإشراف على عملية التدقيق، وتقديم المشورة والدعم للإدارات والمؤسسات العامة والخاصة لوضع إستراتيجية فعالة. كما تعمل الوكالة على المتابعة التكنولوجية المستمرة لضمان التقدم في مجال أمن الأنظمة المعلوماتية كما تتولى الوكالة مسؤولية إعتماد وتصديق أمانة الانظمة المعلوماتية، بالإضافة الى المصادقة على أنظمة إنشاء وفحص التوقيع الالكتروني كما تعمل على وضع المعايير والاجراءات اللازمة لمنح الشهادات الحودة والتصديق واعتماد المنتجات ومزودي الخدمات في مجال أمن الانظمة المعلوماتية بما يتوافق مع القوانين واللوائح السارية الى جانب ذلك تقوم بتنفيذ أنشطة تهدف الى توجيه وتوعية الجمهور بأهمية الانظمة المعلوماتية[1]

تنظيم سير وكالة أمن الانظمة المعلوماتية

تدار الوكالة من قبل لجنة التوجيه مدعومة بلجنة عمليه ويتم الإشراف على تسييرها من قبل مدير عام كما تضم الوكالة مراكز وطنية عمليات الأمن الأنظمة المعلوماتية إلى جانب المديريات والمصالح التقنية والإدارية التي تعمل تحت سلطته[2]

1- **لجنة التوجيه:** لها طابع مميز بالإضافة إلى معناها وهذا ما سنتناوله بالتفصيل من خلال النقاط التالية:

أ- **تشكيلها:** يعين رئيس لجنة التوجيه وفقا للتنظيم المعتمد في وزارات الدفاع الوطني وتتشكل اللجنة من ممثلي عن الهيئات التالية: وزاره الدفاع الوطني، الوزارة المكلفة بالشؤون الخارجية، الوزارة المكلفة بالداخلية، الوزارة المكلفة بالعدل، الوزارة المكلفة بالمالية، الوزارة المكلفة بالطاقة الوزارة المكلفة بالتعليم العالي، الوزارة المكلفة بالصناعة، الوزارة المكلفة بالاتصالات، الوزارة

[1] - المادة 19 من المرسوم الرئاسي 20-05 المصدر السابق.
[2] - المادة 20 المصدر نفسه

المكلفة بالتجارة، مصالح الأمن سلطة الضبط البريد والاتصالات الالكترونية السلطة الوطنية للتصديق الالكتروني، الهيئة الوطنية لحماية البيانات، ذات طابع شخصي والسلطة الحوكومية للتصديق الالكتروني ويضاف إلى ذلك المدير العام للوكالة بصفة استشاريه وتتولى مصالح الوكالة بصفة استشارية، وتتولى مصالح الوكالة أمانة لجنة التوجيه

يجوز للجنة التوجيه الاستعانة بأي شخص أو مؤسسه تراها مؤهلة لتقديم المشورة[1]

والمساهمة في إنجاز أعمالها، ويتم تحديد القائمة الاسمية لأعضائها بموجب قرار من وزير الدفاع الوطني بناء على اقتراح من الجهات التي ينتمي إليها الأعضاء، ولا يُسمح لأعضاء لجنة التوجيه بتعويض من ينوب عنهم في حال غيابهم[2].

ب. مهامها

تشمل المهام الرئيسية تحليل واقتراح مكونات الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، ودراسة واعتماد البرامج السنوية ومتعددة السنوات المرتبطة بتنفيذ هذه الإستراتيجية، كما تعمل على تقييم نتائج الأعمال التي أنجزتها الوكالة وتحديد الأسباب والوسائل اللازمة لتلبية الاحتياجات الوطنية في مجال أمن الأنظمة المعلوماتية. بالإضافة إلى ذلك، تناقش الوكالة كافة القضايا المتعلقة بتنظيم وسائل العمل داخل الوكالة، بما في ذلك نتائج إدارة الأنظمة، الأوضاع المالية للسنة الماضية، تقديرات الإيرادات والنفقات، وتوظيف وتدريب الموظفين، إلى جانب اعتماد رواتب العاملين فيها. ويتم أيضا التركيز على اعتماد النظام الداخلي للوكالة[3].

[1] - المادة 21-22 المصدر نفسه.

[2] – المادة 16 من المرسوم الرئاسي: المصدر السابق

[3] – المادة 34: مصدر نفسه.

ج- سير لجنة التوجيه:

تعقد اجتماعاتها في دورة عادية أربع مرات سنويا بناء على دعوة من رئيسها، بالإضافة إلى ذلك يمكنها عقد دورة استثنائية عند الحاجة وفقا للإجراءات المحددة في نظامها الداخلي. تعد اللجنة نظامها الداخلي وتقوم بالمصادقة عليه من خلال دورتها الأولى، كما تُوثق نتائج أعمال لجنة التوجيه في محضر يتم إعداده ليكون موضوع تقدير يُرسل إلى وزير الدفاع الوطني[1].

1- المدير العام لوكالة أمن الأنظمة المعلوماتية:

يُعين وفقا للتنظيم الساري في وزارة الدفاع الوطني، وتنتهي مهمته بنفس الآليات المتبعة[2]. كما يتولى المدير العام مسؤولية تنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، إلى جانب تنفيذ المخططات والبرامج التي تضعها لجنة التوجيه[3].

أ. مهامه:

المدير العام يضطلع بمسؤولية إدارة الوكالة في حدود التشريعات والتنظيمات السارية، حيث يقوم بإعداد خطط العمل وبرامج نشاط الوكالة وتقديمها إلى لجنة التوجيه للحصول على الموافقة، كما يقوم بتحضير مشروع الميزانية التقديرية وعرضه على اللجنة للنقاش قبل أن يشرف على تنفيذه. ويتولى أيضا إبرام الصفقات وتوقيع العقود والاتفاقيات المتعلقة بمهام الوكالة وفقا للأنظمة المعمول بها، ويمثل الوكالة قانونيا أمام الجهات القضائية. بالإضافة إلى ذلك، يمارس السلطة الإدارية على جميع موظفي الوكالة،

[1]- المادة 23: مصدر نفسه.

[2]- حزام فتيحة: مرجع سابق، ص 184.

[3]- المادة 26 من المرسوم الرئاسي: مصدر سابق

ويهتم بتأهيلهم لضمان تحقيق أهداف المؤسسة، كما يتحمل مسؤولية إعداد النظام الداخلي للوكالة وصرف ميزانيتها مع تقديم تقرير شامل عن الأنشطة المختلفة للوكالة لرئيس المجلس. كما يتمتع بصلاحيات تعيين المديرين، ورئيس المركز الوطني العملياتي لأمن الأنظمة المعلوماتية، ورؤساء المصالح، مع مراعاة الضوابط المعمول بها في وزارة الدفاع الوطني[1]. علاوة على ذلك، يقوم المدير العام بتحديد النظام الداخلي للوكالة بموجب قرار من وزير الدفاع الوطني بناء على اقتراحه وبعد موافقة اللجنة المختصة[2].

2-اللجنة العلمية للوكالة:

تتألف من عشرة 10 أعضاء يتم اختيارهم لفترة ثلاث 03 سنوات قابلة للتجديد من قبل لجنة التوجيه، وذلك من بين الأساتذة والباحثين والخبراء في مجال أمان الأنظمة المعلوماتية[3].

أ. مهامه

يقوم المدير العام بالتشاور مع اللجنة العلمية في جميع القضايا ذات الطابع العلمي التي تندرج ضمن اختصاصات الوكالة المتعلقة بأنشطة البحث والتطوير في مجالات أمن الأنظمة المعلوماتية، وتبدي اللجنة رأيها وتقدم توصياتها بشأن دراسة البرامج والمشاريع التي يقترحها المدير العام للوكالة وطرق تنفيذ برامج ومشاريع البحث والتطوير، فيما يتعلق باختيار واقتناء المراجع العلمية اللازمة، بالإضافة إلى تنظيم المشاركة في الفعاليات والأنشطة العلمية المرتبطة بأمن الأنظمة المعلوماتية، وتنظيم أنشطة التكوين العلمي، بالإضافة إلى تحسين الكفاءات وإعادة التأهيل لصالح موظفي الوكالة

[1]- المادة 27: مصدر نفسه.

[2]- حزام فتيحة: مرجع سابق، ص 184.

[3]- المادة 29 من المرسوم الرئاسي: مصدر سابق

والمستخدمين المكلّفين بأمان الأنظمة المعلوماتية في الإدارات والمؤسسات والهيئات العامة. علاوة على ذلك، تقوم اللجنة خلال دورتها الأولى بالمصادقة على نظامها الداخلي[1].

وإلى جانب ذلك، يحق للجنة الاستعانة بأي شخصية علمية أو خبير يمكنه تقديم مساهمة فعّالة انطلاقا من خبرته وكفاءته في مجال أمن الأنظمة المعلوماتية[2].

الفرع الثالث: برامج التوعية والتثقيف حول أمن الأنظمة المعلوماتية.

تُعرف برامج التوعية وفقا للمعهد الوطني للمعايير التقنية في الولايات المتحدة الأمريكية بأنها حملة تهدف إلى استخدام مختلف الوسائل المتاحة لجذب انتباه الجمهور المستهدف وتوجيه اهتمامهم نحو أهمية الأمن السيبراني، حيث تهدف هذه البرامج إلى زيادة وعي الأفراد بالمخاطر والتهديدات الأمنية مع التركيز على الوقاية منها والتعامل معها بشكل صحيح. وفي هذا السياق، هناك العديد من الأساليب والسياسات التي يمكن تبنيها لتنفيذ برامج التوعية بالأمن السيبراني[3]، ويعتمد اختيار وتنفيذ هذه الأساليب على عوامل متعددة، منها الوضع الأمني الذي تواجهه المنظمة أو البيئة المحيطة بها. ويمكن تلخيص هذه الأساليب والسياسات في: التوعية بأسلوب التعليم والتدريب، التوعية بأسلوب الترغيب والتشجيع، التوعية بأسلوب الفرض والإجبار، وأخيرا التوعية بأسلوب العقاب، وإذا كانت الأساليب والسياسات السابقة هي الممكنة لتطبيق التوعية بالأمن السيبراني، فإن رؤية البحث العلمي تجمع على أن أفضل برامج التوعية هي تلك التي تقتضي استخدام جميع الأساليب المذكورة بشكل تدريجي ومتسلسل[4].

[1]- المادة 30 مصدر نفسه.

[2]- المادة 31: مصدر نفسه.

[3]- ياسر محمد مساوي: دور التوعية بالأمن السيبراني في الحد من آثار تعقيد وسائل التحقق الرقمي من الهوية على سلوك المستعمل في الطرفين. مجلة جامعة أم القرى للهندسة والعمارة، المجلد 11، العدد 1، معهد الإدارة العامة، 2020، ص 41.

[4]- المرجع نفسه، ص 41.

ملخص الفصل الثاني:

يتناول الفصل الثاني من هذا البحث الآليات العلمية لحماية البيانات الشخصية في ظل الإدارة الإلكترونية، حيث إنه في المبحث الأول ركز على الآليات المؤسسية لحماية البيانات الشخصية، إذ إنه تطرق إلى دور السلطة الوطنية لحماية البيانات الشخصية من خلال استعراض تنظيمها وصلاحياتها في هذا المجال، إلى جانب الآليات التي تمارس من خلالها الرقابة وإجراء التحقيقات بصفتها جهة مسؤولة عن الحماية. أما المطلب الثاني، فقد ناقش دور الجهات الأخرى في حماية البيانات الشخصية، ويشمل ذلك تناول دور هيئات الضبط القطاعية ودور القضاء، إضافة إلى دور المؤسسات العامة والخاصة في هذا الإطار.

وفي المبحث الثاني، تم التركيز على الآليات التقنية لحماية البيانات الشخصية، إذ تناول المطلب الأول أنظمة الحماية الإلكترونية مثل تقنيات التشفير الإلكتروني، والجدران النارية، والتحقق

من الهوية، بينما خُصص المطلب الثاني لتسليط الضوء على الهيئات المعنية بحماية البيانات الشخصية، بالتطرق إلى المجلس الوطني لأمن الأنظمة المعلوماتية ووكالة أمن الأنظمة المعلوماتية. إلى جانب ذلك، نتناول في هذا المبحث أهمية التدابير التوعوية في تعزيز أمن الأنظمة المعلوماتية.

خـــاتمـة

في دراستنا لموضوع حماية البيانات الشخصية ضمن إطار الإدارة الإلكترونية، تبين أن المشرع قد بذل جهودا حثيثة لتحقيق أعلى درجات الحماية للبيانات ذات الطابع الشخصي للأفراد، وهذا يهدف للتصدي لأي اعتداء أو انتهاك يمكن أن يمس هذه البيانات من قبل المؤسسات أو الجهات التي تتعامل معها خلال مهامها.

ولتحقيق ذلك، تم تجريم الأفعال التي تشكل تهديدا لسلامة وسرية المعطيات، مع فرض عقوبات متفاوتة. كما قام المشرع بإنشاء هيئة مستقلة تُعنى بالإشراف على تطبيق هذه الحماية وتقييم فعاليتها عبر السلطات والصلاحيات الممنوحة لها، إضافة إلى إنشاء مؤسسات أخرى مثل المجلس الوطني لأمن الأنظمة المعلوماتية ووكالة أمن الأنظمة المعلوماتية، ودور برامج التوعية في تعزيز أمن البيانات الشخصية. وعليه يمكن اجمال نتائج الدراسة ومقترحاتها فيمايلي:

النتائـــــج:

- وضع المشرع الجزائري حماية قانونية خاصة للأفراد فيما يتعلق بالبيانات الشخصية، بما في ذلك إصدار القانون 18-07 وإنشاء هيئة مستقلة لضمان الحماية.
- سن عقوبات لردع كل من يخالف الأحكام المتعلقة بحماية البيانات ذات الطابع الشخصي.
- تحسين فعالية نقل الوثائق إلكترونيا.
- الإقرار بأن التحول من الإدارة التقليدية إلى الإدارة الإلكترونية يمثل تحديا كبيرا يتطلب تعاملا حذرا مع سلبياته واستغلال إيجابياته.
- الإدارة الإلكترونية تعد نمطا جديدا يتطلب تخطيطات دقيقة ورؤية واعية، مع الحاجة إلى توفير موارد تقنية، معلوماتية، مادية وبشرية.

المقترحـــــتات

- ضرورة التشريع في عملية مأسسة الدولة باستخدام التكنولوجيات الحديثة لمواجهة المخاطر والتهديدات التي قد تصيب أمان البيانات الشخصية.
- العمل على تطوير برامج وتطبيقات إلكترونية دقيقة للكشف عن عمليات التلاعب أو انتهاك البيانات ذات الطابع الشخصي.
- تعزيز إمكانات الشرطة التقنية بهدف رصد الاختراقات والاعتداءات المتعلقة بالبيانات الشخصية.
- نشر الوعي العام حول أهمية الثقافة الإلكترونية وأثرها على الحياة اليومية.

- تأهيل وتدريب الموظفين للتعامل مع التقنيات الحديثة بكفاءة.
- توفير أجهزة الحاسب في جميع الإدارات العامة لاستبدال العمل التقليدي بالأجهزة الإلكترونية.
- التقليل من الإجراءات الروتينية التي تعيق عملية التحول نحو الإدارة الإلكترونية، سعيا لتحقيق هذا الانتقال بسلاسة وفعالية أكبر.

قائمة المصادر والمراجع

- **المصادر:**

– النصوص القانونية

أولا: القوانين العضوية

1. القانون العضوي رقم 12-05 المؤرخ في 18 صفر عام 1433 الموافق لـ 12 يناير سنة 2012، يتعلق بالإعلام، الجريدة الرسمية للجمهورية الجزائرية، العدد 2.

ثانيا: القوانين العادية

2. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية، العدد 71، الصادرة بتاريخ 15 نوفمبر 2004.
3. القانون رقم 08-09 المؤرخ في 18 صفر عام 1429 هـ الموافق لـ 25 فبراير سنة 2008، يتضمن قانون الإجراءات المدنية والإدارية، الجريدة الرسمية للجمهورية الجزائرية، العدد 21، الصادر بتاريخ 23 مارس 2008.
4. القانون رقم 09-04 المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، المؤرخة في 16 أوت 2009.
5. القانون رقم 14-04 المؤرخ في 21 جمادى الأولى عام 1435 هـ الموافق لـ 23 مارس 2014، المتعلق بالنشاط السمعي البصري، الجريدة الرسمية للجمهورية الجزائرية، العدد 16.
6. القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 هـ الموافق لأول فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، العدد 6.
7. القانون رقم 15-12 المؤرخ في 15 جويلية 2015، المتعلق بحماية الطفل، الجريدة الرسمية للجمهورية الجزائرية، العدد 39، الصادر بتاريخ 19 جويلية 2015.

8. القانون رقم 16-01 المؤرخ في 06 مارس 2016، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 14، الصادر في 09 مارس 2016.
9. القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادر في 13 جوان 2018.

ثالثا: الأوامر

10. الأمر رقم 03-11 المؤرخ في 27 جمادى الثانية عام 1424 هـ الموافق لـ 26 أوت 2003، المتعلق بالنقد والقرض.

رابعا: المراسيم الرئاسية

11. المرسوم الرئاسي رقم 20-05 المؤرخ في 24 جمادى الأولى عام 1441 هـ الموافق لـ 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية، المؤرخة في 26 جانفي 2020.
12. المرسوم الرئاسي رقم 21-439 المؤرخ في 07 نوفمبر 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 40، المؤرخة في 11 نوفمبر 2021.

خامسا: المراسيم التنفيذية

13. المرسوم التنفيذي رقم 16-142 المؤرخ في 27 رجب عام 1437 هـ الموافق لـ 05 مايو 2016، يحدد كيفيات إعداد الوثيقة الموفقة إلكترونيا، الجريدة الرسمية للجمهورية الجزائرية، العدد 28، المؤرخة في 08 مايو 2016.

○ المراجع

أولا: الكتب

1. عادل عبد الصادق. "البيانات الشخصية، الصراع على نمط الحادي والعشرين". المركز العربي لأبحاث الفضاء الإلكتروني، 11 ديسمبر 2018.

2. سعد غالب ياسين .*الإدارة الإلكترونية* .دار اليازوري العلمية للنشر والتوزيع، 27 جوان 2020.

3. محمود عبد الفتاح رضوان .*الإدارة الإلكترونية وتطبيقاتها الوظيفية* .ط1، دار المجموعة العربية للتدريب والنشر، القاهرة، 2012.

4. يحي إبراهيم دهشان. "الحماية الجنائية للبيانات في ظل التحول الرقمي". مدرسة القانون الجنائي، كلية الحقوق، جامعة الزقازيق.

ثانيا: المقالات العلمية

1. أحمد عربيي وحورية قاسمي. "دور سياسة التشفير الإلكتروني في حماية نظم معلومات الإدارة الإلكترونية بمؤسسة بريد الجزائر، المدية ."*مجلة الاقتصاد الجديد*، المجلد 12، العدد 1، جامعة المدية، 1 جانفي 2021.

2. أحمد درويش .*الشفافية والنزاهة حلمنا القادم* .نشرية تكنولوجيا الإدارة، العدد 8، وزارة الدولة للتنمية الإدارية، مصر، مارس 2007.

3. أروى محمود قبلان الدعجة. "استراتيجية حماية البيانات والخصوصية في عمل حفظة الملفات بالبلديات ."*مجلة المجتمع العربي للنشر للدراسات العلمية*، العدد 63، جويلية 2024.

4. خالد عواد الزعبي. "أمن البيانات وأهميتها في مجال مدخل البيانات في المؤسسات البلدية ." *مجلة المجتمع العربي للنشر العلمية*، نوفمبر 2024.

5. جندلي وريدة. "حماية المعطيات الشخصية في ضوء التشريع الجزائري والمواثيق الدولية بين الضمانات والتحديات ."*مجلة البحوث القانونية والسياسية*، جامعة 20 أوت 1955 – سكيكدة، العدد 1، مارس 2022.

6. جوهر قوادري صامت. "الضوابط القانونية لمعالجة البيانات الشخصية الإلكترونية ."*مجلة الدراسات القانونية المقارنة*، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي الشلف، المجلد 6، العدد 2، 2020.

7. حزان فتيحة. "حماية الأنظمة الرقمية بين الآلات التقنية والأجهزة: قراءة في أحكام المرسوم الرئاسي 20-05 ."*مجلة الحقوق والعلوم الإنسانية*، المجلد 13، العدد 3، جامعة بومرداس، 30 أكتوبر 2020.

8. حمليل نوارة. "حماية المعطيات الشخصية في مواجهة الإدارة الإلكترونية ."*المجلة النقدية للقانون والعلوم السياسية*، جامعة مولود معمري، تيزي وزو، المجلد 15، العدد 2، 30 ديسمبر 2020.

9. خالد سويلم ومحمد سويلم. "الحماية القانونية للبيانات الشخصية الإلكترونية: دراسة مقارنة ." *مجلة الدراسات والبحوث القانونية*، كلية الحقوق، جامعة الزقازيق.

10. خلايفية هدى. "تداول البيانات الشخصية على مواقع التواصل الاجتماعي: المخاطر والحماية القانونية ."*المجلة الأكاديمية للبحث القانوني*، كلية الحقوق، جامعة الإخوة منتوري – قسنطينة، المجلد 14، العدد 1، 2023.

11. خيرة شاوشي وزهرة خلوف. "التحول الرقمي في الجزائر ."*مجلة المحاسبة، التدقيق والمالية*، جامعة الجيلالي بونعامة – خميس مليانة، المجلد 9، العدد 1، 25 أوت 2023.

12. وليد رمضان وعبد الرزاق محمود. "الحماية الدستورية والقانونية للبيانات الشخصية ." *مجلة مصر المعاصر*، كلية الحقوق، جامعة بني يوسف.

13. رمزي فريخة. "الإدارة الإلكترونية وأسلوب الإدارة بالأهداف ."*المجلة الجزائرية للعلوم القانونية والسياسية*، المجلد 56، العدد 1، جامعة بن خلدون، تيارت، 2019.

14. زرير إلهام بلحاج أحمد. "الدور الضبطي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ."*المجلة الأكاديمية للبحوث القانونية والسياسية*، جامعة وهران 1 وجامعة تلمسان، المجلد 9، العدد 1، مارس 2025.

15. سمية زيدان وسفيان عثماني. "خصوصية وأمن المعلومات المصرفية في بيئة البنوك الرقمية – دراسة حالة بنك بنكسي الجزائر ."*مجلة العلوم الاقتصادية والتسيير والعلوم التجارية*، جامعة المسيلة، المجلد 17، العدد 2، ديسمبر 2024.

16. الشكير أيوب. "الإدارة الإلكترونية في الجزائر: تطبيقات وتحديات ."*مجلة الإدارة الإلكترونية والتنمية للبحوث والدراسات*، جامعة لونيسي علي، بليدة 2.

17. الشيخ الحسن محمد يحي وسيد محمد سيد أحمد. "الحماية القانونية للبيانات الشخصية ."*مجلة القضاء والقانون*، كلية العلوم القانونية والاقتصادية، جامعة نواكشوط، العدد 4، أبريل 2018.

18. عائشة بن قارة مصطفى. "آليات حماية المعطيات ذات طابع شخصي في التشريع الجزائري ."*مجلة أحكام القانون 18-07*، جامعة عبد الحميد بن باديس – مستغانم، أفريل 2019.

19. عبد الله شوتري ومريم بوينهي. "الاستراتيجية الوطنية للتحول الرقمي وأبعاد التنمية المستدامة في الجزائر: رؤية 2030 ."*مجلة المعارف*، المجلد 18، العدد 1، جامعة تيبازة.

20. عبيزة منيرة. "الحماية القانونية للبيانات الشخصية من الجرائم المعلوماتية في ضوء التشريع الجزائري ."*مجلة الاجتهاد القضائي*، جامعة سطيف 2، المجلد 15، العدد 2، 30 نوفمبر 2023.

21. عز الدين عثماني وخذيري عفاف. "الحماية القانونية للمعطيات ذات الطابع الشخصي في التشريع الجزائري: دراسة في ظل القانون رقم 18-07 ."*المجلة الدولية للبحوث القانونية والسياسية*، جامعة العربي التبسي – تبسة، المجلد 4، العدد 1، 2020.

22. عقوني محمد ومجري يوسف. "الآليات القانونية لحماية الخصوصية المعلوماتية في البيئة الافتراضية ."*مجلة الباحث للعلوم القانونية والسياسية*، العدد 5، جامعة بسكرة، 2021.

23. غزالي نسرين. "حماية الأشخاص الطبيعيين في مجال المعطيات ذات طابع شخصي ." *المجلة الجزائرية للعلوم القانونية والسياسية*، كلية الحقوق، جامعة الجزائر، العدد 1، 2019.

24. فيصل بوخلفة. "حماية المعطيات ذات الطابع الشخصي بين النصوص التقليدية ومتطلبات التقنية ."*مجلة الدراسات والبحوث القانونية*، جامعة سطيف 2، المجلد 8، العدد 1، جانفي 2023.

25. قاتة حسين وشني تالية. "الإدارة الإلكترونية: مفهوم جديد ومنهج معاصر في الإدارة ."*مجلة التنمية والاقتصاد التطبيقي*، جامعة الجزائر 3، المجلد 5، العدد 2، 3 ديسمبر 2021.

26. قرانة عادل وبوحيديد فارس. "مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري ."*مجلة العلوم القانونية والاجتماعية*، كلية الحقوق، جامعة عنابة، المجلد 6، العدد 2، جوان 2021.

27. كمال فار. "معوقات تطبيق الإدارة الإلكترونية في المرفق العام: مرفق الحالة المدنية ببلدية برج بوعريريج نموذجًا ."*مجلة الحكمة للدراسات الإعلامية والاتصالية*، المجلد 8، العدد 4، جامعة الجزائر 3.

28. محمد باب حسن وأشرف محمود أحمد. "إمكانية تطبيق الإدارة الإلكترونية بجامعة جنوب الوادي ."*مجلة كلية التربية*، جامعة عين شمس، العدد 34، الجزء الأول، 2010.

29. مريم لوكال. "الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي في ضوء القانون رقم 18-07 ."*مجلة العلوم القانونية والسياسية*، جامعة أمحمد بو قزة – بومرداس، المجلد 10، العدد 1، أفريل 2019.

30. موسى عبد الناصر ومحمد قريشي. "مساهمة الإدارة الإلكترونية في تطوير العمل الإداري بمؤسسات التعليم العالي: دراسة حالة كلية العلوم والتكنولوجيا ."*مجلة الباحث*، جامعة بسكرة، العدد 9، 2011.

31. هلا الحسن. "تصديق التوقيع الإلكتروني ."*مجلة جامعة دمشق للعلوم القانونية والاقتصادية*، المجلد 26، العدد 1، جامعة دمشق، 2010.

32. ياسر محمد مساوي. "دور التوعية بالأمن السيبراني في الحد من آثار تعقيد وسائل التحقق الرقمي من الهوية على سلوك المستعمل ."*مجلة جامعة أم القرى للهندسة والعمارة*، المجلد 11، العدد 1، معهد الإدارة العامة، 2020.

33. يوسف زروق والعيداني محمد. "حماية المعطيات الشخصية في الجزائر في ضوء القانون 18-07 ."*مجلة معالم الدراسات القانونية والسياسية*، جامعة الجلفة، العدد 5، 20 ديسمبر 2018.

ثالثا: الرسائل الجامعية

1. عبد الرزاق رحومة. "دور الإدارة الإلكترونية في تحسين أداء المؤسسات الاقتصادية". رسالة ماجستير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة العربي التبسي – تبسة، 2014.

2. إيمان لطرش. "دور الإدارة الإلكترونية في تحسين الأداء الوظيفي للموارد البشرية في المؤسسات العمومية الجزائرية". مذكرة ماجستير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجزائر 3، 2017.

3. عادل عبد العزيز الرشيد .*البيانات الضخمة :(Big Data) دراسة فقهية* .رسالة مقدمة إلى قسم الفقه، كلية الشريعة، جامعة محمد بن سعود الإسلامية، 2022.

رابعا: المداخلات العلمية

1. سعيدة رحموني. "الإدارة الإلكترونية بين التفعيل القانوني وتحديات الحماية المعلوماتية في الجزائر". مداخلة في ملتقى وطني بعنوان "الحكومة الإلكترونية بين التصور والتطبيق"، جامعة محمد خيضر – بسكرة، الجزائر، 3 مارس 2021.

2. محمد بن ناصر. "واقع حماية البيانات الشخصية في الجزائر في ظل التحول الرقمي". مداخلة في الملتقى الوطني حول "الحوكمة الإلكترونية وحماية الخصوصية"، كلية الحقوق، جامعة قسنطينة، الجزائر، 2022.

خامسا: المواقع الإلكترونية

1. وزارة الرقمنة والإحصائيات، الجزائر. "الاستراتيجية الوطنية للتحول الرقمي في الجزائر ". https://www.mdipi.gov.dz.

2. الهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي. "القانون 18-07 المتعلق بحماية المعطيات الشخصية. https://www.anpdp.dz ".

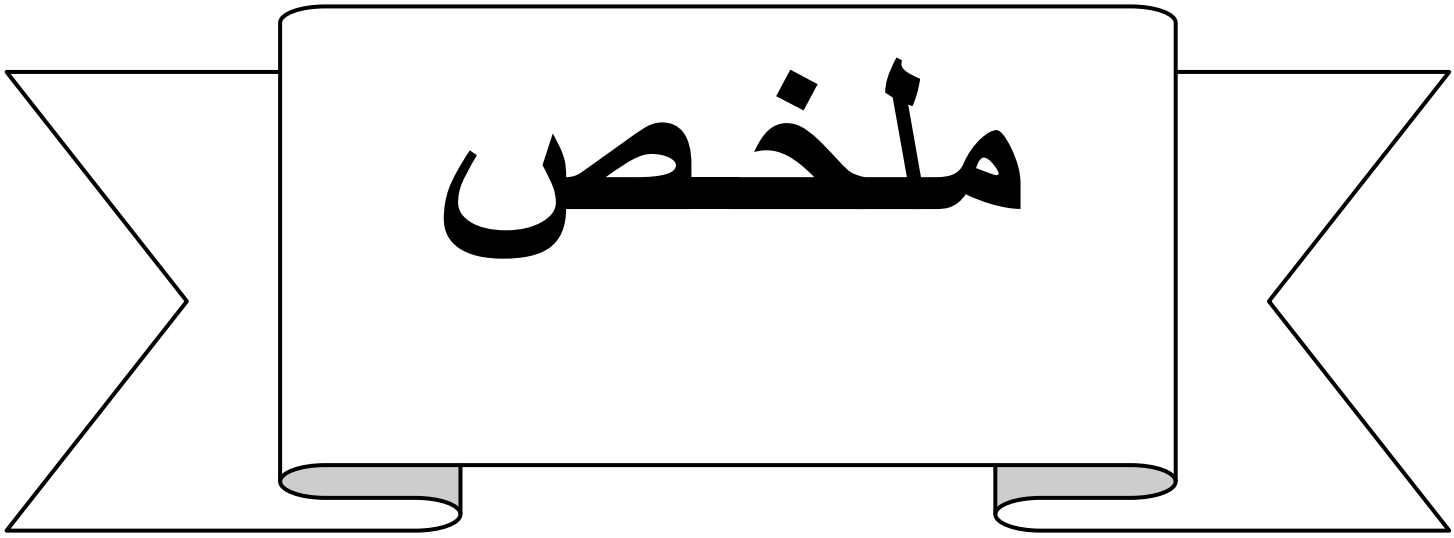
3. الأمانة العامة للحكومة، الجزائر. "النصوص التشريعية والتنظيمية ". https://www.joradp.dz.

4. مفوضية الاتحاد الأوروبي لحماية البيانات. "حول اللائحة العامة لحماية البيانات (GDPR)". https://ec.europa.eu/info/law/law-topic/data-protection_ar.

5. البنك الدولي. "التحول الرقمي في الجزائر: تقييم ومؤشرات ". https://www.worldbank.org.

6. الأمم المتحدة. "التنمية المستدامة والتحول الرقمي ". https://www.un.org/sustainabledevelopment.

الفهـرس


ملخص

ملخص

تهدف هذه الدراسة إلى تبيان الإطار القانوني والعملي لحماية البيانات الشخصية في ظل الإدارة الإلكترونية، بالنظر إلى أن تخزين وتداول المعلومات أصبح يتم بوسائل رقمية، ما يفرض تحديات كبيرة في مجال حماية الخصوصية ومنع الوصول غير المشروع إلى المعلومات الشخصية. وقد تضمنت الدراسة المفاهيم العامة المرتبطة بالبيانات الشخصية والإدارة الإلكترونية، ثم تطرقت إلى الأساس الدستوري والتشريعي لحمايتها، خصوصا في ضوء القانون رقم 18-07 والقوانين ذات الصلة. كما حللت الآليات المؤسساتية والتقنية، بما في ذلك دور السلطة الوطنية لحماية البيانات، والهيئات القضائية والتنظيمية، والوسائل الفنية مثل التشفير والجدران النارية.

وقد خلصت الدراسة إلى أن ضمان حماية فعالة للبيانات الشخصية يقتضي تفعيل دور السلطة الوطنية، والتزام الأفراد والمؤسسات بالتدابير القانونية والتقنية، وتعزيز التعاون بين مختلف الفاعلين، بما يسهم في بناء ثقة حقيقية في التحول نحو إدارة رقمية آمنة وشفافة.

الكلمات المفتاحية: الإدارة الإلكترونية – البيانات الشخصية – السلطة الوطنية – التشريع الجزائري – التشفير – الأمن السيبراني – الخصوصية الرقمية – المجلس الوطني لأمن الأنظمة – وكالة أمن الأنظمة المعلوماتية.

Abstract

This study aims to clarify the legal and practical framework for the protection of personal data in the context of e-governance, considering that the storage and exchange of information now occur through digital means, which poses significant challenges in safeguarding privacy and preventing unauthorized access to personal information. The study covers the general concepts related to personal data and e-governance, and then addresses the constitutional and legislative foundations for data protection, particularly in light of Law No. 18-07 and relevant legal texts. It also analyzes institutional and technical mechanisms, including the role of the National Authority for the Protection of Personal Data, judicial and regulatory bodies, and technical tools such as encryption and firewalls.

The study concludes that ensuring effective protection of personal data requires empowering the role of the national authority, committing individuals and institutions to legal and technical measures, and strengthening cooperation among various stakeholders, all of which contribute to building genuine trust in the transition toward secure and transparent digital governance.

Keywords:E-governance – Personal data – National Authority – Algerian legislation – Encryption – Cybersecurity – Digital privacy – National Council for IT Security – Information Security Agency.