جامعة سعيدة، الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

حفظ أمن المعلومات في ظل الذكاء الاصطناعي

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص: إدارة إلكترونية

مــن إعداد الطالبين:

- بن جلول لطيفة
- عمراني عائشة الفارحة

تحت إشراف الأستاذة:

الدكتورة- قادري أمال

أعضاء لجنة المناقشة

الدكتور شيخاوي أحمد	**أستاذ التعليم العالي**	**جامعة –سعيدة– الدكتور مولاي الطاهر**	**رئـــيـــســا**
الدكتورة قادري أمــال	**أستاذ محاضر –ب–**	**جامعة –سعيدة– الدكتور مولاي الطاهر**	**مـشـرفا ومقررا**
الدكتورة مـــراح نعيمة	**أستاذ التعليم العالي**	**جامعة –سعيدة– الدكتور مولاي الطاهر**	**عـــضـــوا**

السنة الجامعية: 2025_2026

جامعة سعيدة، الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

حفظ أمن المعلومات في ظل الذكاء الاصطناعي

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص: إدارة إلكترونية

مــن إعداد الطالبين:

- بن جلول لطيفة
- عمراني عائشة الفارحة

تحت إشراف الأستاذة:

الدكتورة- قادري أمال

أعضاء لجنة المناقشة

الدكتور شيخاوي أحمد	**أستاذ التعليم العالي**	**جامعة –سعيدة– الدكتور مولاي الطاهر**	**رئـــيـــســا**
الدكتورة قادري أمــال	**أستاذ محاضر –ب–**	**جامعة –سعيدة– الدكتور مولاي الطاهر**	**مـشـرفا ومقررا**
الدكتورة مـــراح نعيمة	**أستاذ التعليم العالي**	**جامعة –سعيدة– الدكتور مولاي الطاهر**	**عـــضـــوا**

السنة الجامعية: 2025_2026

بسم الله الرحمن الرحيم

﴿...يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ...﴾

صدق الله العظيم

(سورة المجادلة، الآية 11)

شكر و عرفان

الحمد لله الذي بنعمته تتم الصالحات، وبفضله تتحقق الغايات.

نتوجه بجزيل الشكر والامتنان إلى أستاذتنا المشرفة الأستاذة الدكتورة قادري أمال، التي أشرفت على هذا العمل المتواضع، وقدمت لنا الدعم العلمي و النفسي، وأرشدتنا بتوجيهاتها السديدة وملاحظاتها البنّاءة، فكانت نعم الموجه والمساند في كل مراحل إعداد هذه المذكرة.

كما نتقدم بأسمى عبارات الشكر والتقدير إلى كافة الأساتذة الأفاضل الذين كان لهم دور فاعل في مسيرتنا العلمية، والذين لم يبخلوا علينا بعلمهم وتوجيهاتهم القيمة طيلة سنوات الدراسة، فلهم منا كل الاحترام والعرفان.

ولا يفوتنا أيضًا أن نشكر كل من ساهم من قريب أو بعيد في إنجاز هذا العمل، وخصّنا بكلمة طيبة، أو مشورة، أو مساعدة، فلهم جميعًا منا فائق الاحترام والتقدير.

"بن جلول لطيفة" " عمراني عائشة الفارحة"

إهـــــداء

إلى من كان لهم الفضل بعد الله في وصولنا إلى هذه المرحلة، إلى روح أمي الغالية رحمة الله عليها و والدي أطال الله في عمره ، رمز العطاء و التضحية، الذين لم يبخلوا علينا بالدعم والدعاء والمساندة، نهدي هذه المذكرة تقديرًا وامتنانًا لما بذلتموه من أجلنا.

إلى أخواتي العزيزات و أخصص الشكر إلى الأستاذة إكرام ، و الأستاذة الدكتورة بن جلول مريم ، اللتان ساهمتا بالنصيحة و الدعم لي طوال المسار الجامعي ، نشارككم هذا الإنجاز الذي لا يكتمل إلا بذكراكم.

إلى زملائنا في العمل ، الذين قدموا لنا يد العون و المساندة ، فكان لتعاونهم الأثر الكبير في تجاوز التحديات و تحقيق النجاح أخص بالذكر الدكتور رملي مخلوف ، الدكتور مخلوف أحمد ، و الأستاذ المهندس سويلم عبد الكريم.

إلى كل من ساهم من قريب أو بعيد في إنجاز هذا العمل، نهديكم ثمرة جهدنا، عرفانًا وتقديرًا.

"بن جلول لطيفة"

إهـــداء

إلى من كان لهم الفضل بعد الله في وصولنا إلى هذه المرحلة، إلى الوالدين الكريمين، رمز العطاء والتضحية، الذين لم يبخلوا علينا بالدعم والدعاء والمساندة، نهدي هذه المذكرة تقديرًا وامتنانًا لما بذلتموه من أجلنا.

إلى أخواتي العزيزات و أخص الشكر إلى حبيبتي " أسيل مروة " ، اللواتي ساهمتا بالتضحية و الدعم لي طوال المسار الجامعي ،

و إلى صديقي العزيز و حبيبي محمد نشارككم هذا الإنجاز الذي لا يكتمل إلا بذكراكم.

إلى زملائنا في العمل ، الذين قدموا لنا يد العون و المساندة ، فكان لتعاونهم الأثر الكبير في تجاوز التحديات و تحقيق النجاح أخص بالذكر الدكتور مخلوف أحمد ، الدكتور رملي مخلوف ، و الأستاذ المهندس سويلم عبد الكريم.

إلى كل من ساهم من قريب أو بعيد في إنجاز هذا العمل، نهديكم ثمرة جهدنا، عرفانًا وتقديرًا.

" عمراني عائشة الفارحة"

قائمة المختصرات

المختصرات	الـدلالـة
ج.ر.ج.ج:	الجريدة الرسمية للجمهورية الجزائرية
ع:	العدد
ص ص :	صفحات متعددة
مج:	المجلد
د.ط:	دون طبعة
ط:	طبعة
ج:	جزء
ص:	الصفحة

مقدمة

شهد العالم خلال العقود الأخيرة تحولا جذريا بفعل الثورة الرقمية والتطور المتسارع لتكنولوجيات الإعلام والاتصال، الأمر الذي أدى إلى بروز مجتمع معلوماتي أصبحت فيه المعلومة موردا استراتيجيا لا يقل أهمية عن الموارد الاقتصادية والطبيعية والبشرية. فلم تعد المعلومات مجرد وسيلة مساعدة في التسيير الإداري
أو الاقتصادي، بل أصبحت أساسا لاتخاذ القرار، وضمان استمرارية المرافق العمومية، وتحقيق الأمن الوطني، وحماية المصالح الحيوية للدولة والمؤسسات.

غير أن هذا التطور التقني المتسارع لم يخل من آثار قانونية معقدة، ونتيجة لهذا التحول برز مفهوم أمن المعلومات باعتباره أحد أهم التحديات القانونية والتقنية المعاصرة، بالنظر إلى تزايد الاعتماد على الأنظمة الرقمية وقواعد البيانات والشبكات الإلكترونية في مختلف القطاعات، و برز الى جانب ذلك تقنية الذكاء الاصطناعي إذ أثار إشكالات دقيقة تتعلق بحماية الخصوصية والبيانات الشخصية، وحدود المعالجة الآلية للمعلومات، ومشروعية المراقبة الرقمية، وصعوبة تحديد المسؤولية القانونية عن أفعال الأنظمة الذكية، إضافة إلى التحديات المرتبطة بالإثبات في الجرائم المعلوماتية العابرة للحدود. كما أدى تضخم استعمال الخوارزميات والأنظمة الذكية إلى ظهور مخاطر جديدة تمس الحقوق والحريات الأساسية، خاصة الحق في الخصوصية، وحرية الأفراد في التحكم في بياناتهم الشخصية، والحماية من القرارات الآلية غير الشفافة.

وقد ازدادت أهمية هذا المجال مع الانتشار الواسع للذكاء الاصطناعي، الذي أصبح يشكل ثورة تكنولوجية حقيقية بفضل قدرته على تحليل البيانات الضخمة، والتعلم الذاتي، واتخاذ القرارات، والكشف المبكر عن التهديدات السيبرانية، والتنبؤ بالمخاطر، والاستجابة السريعة للهجمات الإلكترونية.وعلى المستوى الدولي، تشكل اتفاقية بودابست حول الجريمة المعلوماتية، واتفاقية مجلس أوروبا رقم 108+ المتعلقة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات الشخصية، واللائحة الأوروبية العامة لحماية البياناتGDPR ، إضافة إلى اللائحة الأوروبية للذكاء الاصطناعي لسنة 2024، ومبادئ منظمة التعاون والتنمية الاقتصادية بشأن الذكاء الاصطناعي، أهم المرجعيات القانونية الدولية التي تسعى إلى تنظيم استعمال التكنولوجيا الحديثة وضبط آثارها القانونية والأمنية.

وأولى المشرع الجزائري أهمية بالغة لحماية أمن المعلومات والمعطيات الشخصية، وذلك مع تزايد الاعتماد على الرقمة في الإدارة والخدمات العمومية. وقد كرس ذلك من خلال التعديل الدستوري لسنة 2020

في المادة 47 التي نصت على حماية الحياة الخاصة وسرية المراسلات والاتصالات، وحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مع تجريم كل مساس غير مشروع بهذه الحقوق[1].

كما صدر القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الذي يعد الإطار التشريعي الأساسي لحماية البيانات الشخصية في الجزائر،[2] و الذي عدل لاحقا بموجب القانون رقم 25-11 المعدل والمتمم له،[3] إضافة إلى القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ليضع قواعد خاصة لمواجهة الجرائم المعلوماتية والاعتداءات الواقعة على الأنظمة المعلوماتية[4].

وتكمن أهمية دراسة هذا الموضوع في كونه يجمع بين البعدين القانوني والتقني، خاصة في تخصص دولة ومؤسسات، لأن حماية أمن المعلومات لم تعد مرتبطة فقط بحماية البيانات الرقمية، بل أصبحت مرتبطة بحماية الثقة في الإدارة والمؤسسات، وضمان استمرارية الخدمات العمومية، والحفاظ على الأمن الوطني والسيادة الرقمية للدولة، مع ضرورة تحقيق التوازن بين متطلبات الأمن المعلوماتي واحترام الحقوق والحريات الفردية.

تهدف هذه الدراسة إلى الإحاطة بمختلف الجوانب المرتبطة بحفظ أمن المعلومات في ظل الذكاء الاصطناعي، من خلال تحليل الإطارين القانوني والتقني المنظمين لهذا المجال، والكشف عن أوجه القصور التي قد تعيق تحقيق حماية فعالة للمعلومات، مع استشراف الآليات الكفيلة بتطوير منظومة أمن المعلومات بما ينسجم مع التطورات المتسارعة التي فرضتها تطبيقات الذكاء الاصطناعي.

تتمثل الأسباب الذاتية لاختيار هذا الموضوع في الرغبة الشخصية في دراسة أحد المواضيع الحديثة التي أصبحت تفرض نفسها بقوة في الواقع القانوني والتقني المعاصر، خاصة أن أمن المعلومات والذكاء الاصطناعي

---

[1] – المادة 47 من المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق ل30 ديسمبر سنة2020 المتعلق بالتعديل الدستوري 2020 ، ، ج.ر.ج.ج، عدد 82 الصادرة في 15 جمادي الاولى 1442هـ الموافق ل30 ديسمبر 2020 و المعدل و المتمم بموجب القانون رقم 26/04 المؤرخ في 26 مارس 2026، المتعلق بالتعديل الدستوري 2026 ج ر، العدد 22 بتاريخ 26 مارس 2026

[2] – القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، 2018

[3] – القانون رقم 25-11 المؤرخ في 28 محرم عام 1447 الموافق 24 جويلية 2025، المعدل والمتمم للقانون رقم 18-07، الجريدة الرسمية، العدد 48، 2025.

[4] – القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، 2009.

من المسائل التي ترتبط مباشرة بحياة الأفراد والمؤسسات والدولة. كما أن الاهتمام بهذا الموضوع نابع من الرغبة في فهم كيفية تأثير التقنيات الذكية على حماية البيانات والمعلومات، ومدى قدرة القانون على مواكبة هذه التطورات المتسارعة، لاسيما في ظل تزايد الاعتماد على الرقمنة في مختلف القطاعات.

أما الأسباب الموضوعية، فتعود إلى الأهمية الكبيرة التي يكتسيها موضوع أمن المعلومات في ظل الثورة الرقمية، باعتباره من أهم التحديات التي تواجه الدول والمؤسسات في الوقت الراهن. كما أن الانتشار الواسع لتقنيات الذكاء الاصطناعي أفرز إشكالات قانونية وتقنية جديدة تتعلق بحماية البيانات الشخصية، والخصوصية، والمسؤولية القانونية، والإثبات في الجرائم المعلوماتية. ويضاف إلى ذلك حداثة الموضوع وارتباطه بالتشريعات الوطنية والدولية، خاصة القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والقانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إضافة إلى المرجعيات الدولية الحديثة ذات الصلة بالذكاء الاصطناعي وحماية البيانات.

وعليه الإشكالية التي يمكن طرحها هي:

إلى أي مدى يسهم الذكاء الاصطناعي في ضمان وتعزيز حماية البيانات و حفظ أمن المعلومات في ظل كفاية أو قصور الآليات القانونية والتقنية المعتمدة؟

وتتفرع عن هذه الإشكالية مجموعة من التساؤلات الفرعية، أهمها:

- **ما المقصود بأمن المعلومات، وما علاقته بالذكاء الاصطناعي؟**
- **كيف يساهم الذكاء الاصطناعي في الكشف عن التهديدات المعلوماتية ومواجهتها؟**
- **ما هي أهم النصوص القانونية الدولية والوطنية التي تحمي أمن المعلومات والبيانات الشخصية؟**
- **ما هي التحديات القانونية التي يطرحها الذكاء الاصطناعي في مجال المسؤولية والإثبات والخصوصية؟**
- **ما هي الآليات القانونية المقترحة لتطوير الحماية القانونية لأمن المعلومات في ظل الذكاء الاصطناعي؟**

بناءًا على الأسئلة الفرعية، يمكن صياغة الفرضيات على النحو التالي :

- أن أمن المعلومات يمثل مجموعة من التدابير القانونية والتقنية الرامية إلى حماية المعلومات من مختلف المخاطر، وأن الذكاء الاصطناعي يرتبط به ارتباطًا وثيقًا باعتباره وسيلة لتعزيز أمن المعلومات، مع إمكانية أن يشكل في الوقت ذاته مصدرًا لتهديدات جديدة تستوجب مواكبتها.
- أن الذكاء الاصطناعي يساهم بفعالية في الكشف المبكر عن التهديدات المعلوماتية والتصدي لها من خلال تحليل البيانات الضخمة، والتنبؤ بالهجمات السيبرانية، والاستجابة السريعة لها، بما يعزز

مستوى أمن المعلومات.

- أن المنظومة القانونية الجزائرية تتضمن نصوصًا تشريعية تنظم المسؤولية القانونية والإثبات الرقمي وحماية الخصوصية، إلا أنها لا تزال بحاجة إلى تطوير وتحيين لمواكبة التحديات التي أفرزها الذكاء الاصطناعي.
- أن تطوير الحماية القانونية لأمن المعلومات في ظل الذكاء الاصطناعي يقتضي تحديث التشريعات، وتعزيز المسؤولية القانونية، وتنظيم استخدام تطبيقات الذكاء الاصطناعي، ودعم التعاون بين الجوانب القانونية والتقنية لمواجهة المخاطر المعلوماتية المستحدثة.

هذا و قد حظي موضوع أمن المعلومات والذكاء الاصطناعي باهتمام متزايد في الدراسات القانونية والتقنية، حيث تناولته العديد من البحوث إما من الجوانب التقنية لأمن المعلومات، أو الأطر القانونية المنظمة للذكاء الاصطناعي، أو حماية البيانات الشخصية والأمن السيبراني. وقد ركزت بعض الدراسات على التحديات التي يفرضها الذكاء الاصطناعي على سرية المعلومات وسلامتها، في حين اهتمت دراسات أخرى بالضمانات القانونية والتشريعية الكفيلة بحماية المعلومات الرقمية. إلا أن أغلب هذه الدراسات عالجت الموضوع من زاوية جزئية، الأمر الذي يبرز أهمية هذه الدراسة التي تسعى إلى تناول موضوع حفظ أمن المعلومات في ظل الذكاء الاصطناعي من منظور قانوني متكامل، مع التركيز على التشريع الجزائري وإجراء اسقاط ببعض التشريعات الدولية كلما اقتضت الحاجة.

ومن بين أهم الدراسات التي اعتمدنا عليها :

1-دراسة عبد الباسط عيساوي، سفيان زيتون، بعنوان آثار الذكاء الاصطناعي على الأمن السيبراني: دراسة حالة الجزائر، حيث تناولت الدراسة واقع الأمن السيبراني في الجزائر، وأهم التهديدات التي تستهدف البيانات الرقمية، كما استعرضت الآليات والتدابير المتخذة لمواجهة الجرائم السيبرانية، وأكدت ضرورة تحديث التشريعات وتعزيز الوسائل التقنية لمواكبة التطور الرقمي.

2- دراسة سهيلة بضياف وآمنة حمراني، بعنوان «أمن المعلومات في الجزائر – الإجراءات والتحديات»، حيث هدفت الدراسة إلى تقييم مستوى أمن المعلومات في الجزائر، وتوصلت إلى أن فعالية أمن المعلومات ترتبط بدرجة كبيرة بمستوى الحماية المطبقة وكفاءة العنصر البشري، مما يستلزم اعتماد سياسات أمنية أكثر تطورا.

و من خلال اللاضطلاع على هذه الدراسات لاحظنا أنها تتشابه مع الدراسة الحالية في تناولها موضوع أمن المعلومات والذكاء الاصطناعي، إلا أن معظمها ركز على الجانب التقني أو على حماية البيانات بوجه عام، بينما تتميز الدراسة الحالية بتركيزها على تحليل مدى كفاية الآليات القانونية، إلى جانب الآليات التقنية،

لضمان حفظ وأمن المعلومات في ظل الاعتماد المتزايد على تقنيات الذكاء الاصطناعي، مع التركيز على التشريع الجزائري

و يقتصر نطاق و حدود هذه الدراسة على بحث الجوانب القانونية المتعلقة بحفظ أمن المعلومات في ظل استخدام تقنيات الذكاء الاصطناعي، حيث يقتصر نطاق الدراسة من حيث الزمان في الفترة التي شهدت التطور المتسارع لتقنيات الذكاء الاصطناعي وتزايد استخدامها في مختلف المجالات، مع التركيز على المستجدات التشريعية والقانونية ذات الصلة حتى تاريخ إنجاز هذه الدراسة.

أما نطاق الدراسة من حيث المكان تنصب أساسا على التشريع الجزائري المنظم لحماية وأمن المعلومات، مع الاستئناس ببعض التشريعات والاتفاقيات الدولية ذات الصلة كلما اقتضت المقارنة أو دعم التحليل

و للإجابة على الاشكالية اعتمدنا على المنهج الوصفي لشرح مفاهيم أمن المعلومات والذكاء الاصطناعي، والمنهج التحليلي لتحليل النصوص القانونية الوطنية والدولية ذات الصلة، والمنهج المقارن لمقارنة التوجه الجزائري ببعض التجارب والمعايير الدولية الحديثة، إضافة إلى المنهج الاستشرافي من خلال اقتراح آليات مستقبلية لتطوير الحماية القانونية لأمن المعلومات في ظل الذكاء الاصطناعي.

و خلال إعداد هذه الدراسة واجهتنا بعض الصعوبات لاسما كون أن هذا الموضوع هو حديث من حيث تشعبه بين الجوانب القانونية والتقنية، مما جعل الإحاطة به تتطلب الرجوع إلى مراجع متعددة ومتنوعة. كما واجهتنا صعوبة في قلة المراجع القانونية المتخصصة التي تجمع بين أمن المعلومات والذكاء الاصطناعي في التشريع الجزائري، إضافة إلى التطور السريع لهذا المجال، الأمر الذي يجعل النصوص القانونية في حاجة دائمة إلى التحديث والمواكبة. كما أن الطابع التقني لبعض المفاهيم المرتبطة بأمن المعلومات والذكاء الاصطناعي شكل صعوبة إضافية في تبسيطها وربطها بالجانب القانوني.

و من أجل تقديم مضمون هذا البحث تم تقسيم هذه الدراسة إلى فصلين ، سنتناول في **الفصل الأول الى الإطار النظري لأمن المعلومات في مجال الذكاء الاصطناعي**، الذي قسمناه بدوره الى مبحثين سنتطرق **في المبحث الأول** الى الإطار المفاهيمي لأمن المعلومات في مجال الذكاء الاصطناعي، **والمبحث الثاني** دور الذكاء الاصطناعي في تعزيز امن المعلومات.

أما **الفصل الثاني، فقد خصص لدراسة الإطار القانوني لحماية أمن المعلومات في ظل الذكاء الاصطناعي**، الذي قسمناه بدوره الى مبحثين سنتطرق في **المبحث الأول** الى للتنظيم القانوني لحماية أمن المعلومات من خلال تحليل التنظيم القانوني الوطني والدولي لحماية البيانات والخصوصية ومكافحة الجرائم المعلوماتية، **و المبحث الثاني** الى المخاطر والآفاق المستقبلية لحماية أمن المعلومات في ظل الذكاء الاصطناعي ثم دراسة التحديات القانونية المرتبطة بالذكاء الاصطناعي وآفاق تطوير الحماية القانونية مستقبلا ، و في الأخير خاتمة تحتوي على مجموعة من النتائج و الإقتراحات .

الفصل الأول:

الإطار النظري لأمن المعلومات في مجال الذكاء الاصطناعي

يعد أمن المعلومات من الموضوعات الأساسية التي فرضت نفسها في ظل التطور التكنولوجي المتسارع، خاصة مع التوسع الكبير في استعمال الأنظمة الرقمية والشبكات الإلكترونية، وما ترتب عن ذلك من مخاطر وتهديدات تمس سرية المعلومات وسلامتها وتوافرها. وفي المقابل، برز الذكاء الاصطناعي كأحد أهم التقنيات الحديثة القادرة على تطوير وسائل الحماية، من خلال تحليل البيانات، والكشف عن التهديدات، والتنبؤ بالمخاطر، والمساهمة في الاستجابة السريعة للحوادث الأمنية.

وانطلاقا من ذلك، يتناول هذا الفصل الإطار النظري لأمن المعلومات في مجال الذكاء الاصطناعي، من خلال مبحثين أساسيين؛ حيث خصص المبحث الأول لدراسة الإطار المفاهيمي لأمن المعلومات والذكاء الاصطناعي، وذلك بالتطرق إلى مفهوم أمن المعلومات وأهميته وخصائصه ومخاطره، ثم بيان مفهوم الذكاء الاصطناعي من حيث مراحل تطوره، وخصائصه، وأنواعه، وتطبيقاته في المجال الأمني.

أما المبحث الثاني، فيتناول دور الذكاء الاصطناعي في تعزيز أمن المعلومات، من خلال بيان آلياته في الكشف عن التهديدات المعلوماتية، كالكشف المبكر عن الهجمات، وتحليل السلوكيات غير الطبيعية، والاستجابة الذكية للحوادث الأمنية، ثم إبراز مساهمته في تطوير وسائل الحماية، ولا سيما أنظمة المصادقة والتحكم في الولوج، وحماية الشبكات والبيانات بواسطة تقنيات التعلم الآلي، مع التطرق إلى مزايا وحدود اعتماد الذكاء الاصطناعي في مجال أمن المعلومات.

المبحث الأول: الإطار المفاهيمي لأمن المعلومات في مجال الذكاء الاصطناعي

أدى التطور التكنولوجي المتسارع والتحول نحو الرقمنة إلى بروز المعلومات كأحد أهم الأصول التي تعتمد عليها الدول والمؤسسات في تسيير شؤونها وتحقيق أهدافها. ومع هذا التطور، تزايدت المخاطر والتهديدات التي تستهدف المعلومات بمختلف أشكالها، سواء كانت مخزنة أو متداولة عبر الأنظمة والشبكات، الأمر الذي جعل مسألة حمايتها ضرورة حتمية لا يمكن الاستغناء عنها، ويعد أمن المعلومات كأحد المفاهيم الحديثة التي تهدف إلى حماية البيانات من مختلف أشكال الاعتداء أو الضياع أو التلاعب، وضمان استخدامها بشكل آمن وموثوق. ولا يقتصر هذا المفهوم على الجانب التقني فقط، بل يشمل كذلك أبعادا قانونية وتنظيمية تهدف إلى وضع إطار شامل لحماية المعلومات.

وعليه، يهدف المبحث الأول إلى بيان مفهوم أمن المعلومات من خلال التطرق إلى تعريفه وأهميته، وكذا إبراز مختلف التهديدات والمخاطر المرتبطة به، ثانيا التطرق إلى مفهوم الذكاء الاصطناعي من حيث تطوره، أنواعه، وتطبيقاته المختلفة في مجال أمن المعلمات.

المطلب الأول: مفهوم أمن المعلومات

مع الانتشار الواسع للتقنيات الحديثة ودخولها في مختلف جوانب الحياة اليومية، أصبحت المعلومات عنصرا أساسيا في نجاح الأفراد و المؤسسات. وفي هذا السياق، يبرز مفهوم أمن المعلومات كضرورة ملحة لحماية البيانات من المخاطر التي قد تهددها، سواء كانت اختراقات إلكترونية أو استخدام غير مشروع. وتكمن أهميته في ضمان حماية البيانات والحفاظ على سريتها وسلامتها، إضافة إلى تأمين الوصول إليها عند الحاجة، مما يعزز الثقة في البيئة الرقمية ويساهم في استقرار الأنظمة وتطورها.

الفرع الأول: تعريف أمن المعلومات

أولا : المقصود بأمن المعلومات

قبل التطرق إلى تعريف أمن المعلومات، علينا أولا تحديد مفهوم كل من الأمن والمعلومة، باعتبار أن مصطلح أمن المعلومات يتكون من هذين العنصرين الأساسيين.

أ- الأمن: بصفة عامة يقصد به حالة الطمأنينة والحماية من المخاطر والتهديدات، سواء كانت مادية أو معنوية. كما يعني اتخاذ مجموعة من الإجراءات والوسائل التي تهدف إلى الوقاية من الأخطار وضمان الاستقرار والسلامة.

إن مفهوم الأمن هو مفهوم واسع يشمل عدة مجالات لها علاقة بالأنشطة الحياتية للإنسان فكل واحد يعرفه وفقا لاختصاصه وفي مفهومه الواسع هو " مجموعة الجهود المبذولة والمشتركة من قبل الدولة وأفراد المجتمع

من خلال مجموعة من النشاطات والفعاليات في شتى مجالات الحياة للحفاظ على حالة التوازن الاجتماعي في ذلك المجتمع "[1]

كما عرفه البعض أنه "مجموعة من الإجراءات الوقائية لتفادي وقوع ضرر كالسرقة أو التعديل أو التخريب، وكذا خرق لأمن المعلومات حين حدوث أي تهديد ينجم عنه فقدان ممتلكات ومعلومات سواء شخصية أو مؤسساتية، وتشمل جميع مجالات الحياة"[2].

ب– المعلومة : هناك العديد من التعاريف للمعلومة، حيث عرفها كل باحث وفقا لاهتماماته فقد عرفت بشكل واسع و عام على أنها : " الهيئة أو الحالة الخاصة للمادة أو الطاقة التي يمكن نقلها أو إبلاغها للغير " ، و لقد اهتمت مختلف التعاريف السابقة لتطور تكنولوجيات الاتصال بطريقة انتقال المعلومة و لم تهتم بمحتوى المعلومة التي تحملها الرسالة أو قيمتها المالية ، أو مدى الاستفادة منها بقدر اهتمامهم بإمكانية نقلها

أو تداولها بين مختلف الوسائل ، فليس كل رسالة تنقل إلى الغير تمثل معلومة ، تستوجب الحماية و إنما الحماية تشمل بعض المعلومات ، التي لها ميزة أو قيمة معينة و ليس كل المعلومات .

فالمعلومة هي كل بيان أو معطى تمت معالجته وتنظيمه بطريقة تجعله ذا معنى وقيمة بالنسبة لمن يستخدمه. فالمعلومة قد تكون في شكل أرقام أو نصوص أو صور أو وثائق أو ملفات إلكترونية، وتستعمل في اتخاذ القرارات وتسيير مختلف الأنشطة.

وتعرف المعلومات أيضا بأنها مجموعة من الرموز والحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلا للتبادل أو الاتصال أو التفسير أو التأويل أو المعالجة، سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تعبئتها وتخزينها وجمعها ونقلها بوسائل وأشكال مختلفة. ونلاحظ من خلال هذا التعريف أنه اهتم بالمعلومة في علاقتها بتكنولوجيا الاتصال: حيث أضاف مصطلح الأنظمة الإلكترونية ومختلف العمليات التي قد تطرأ على المعلومة إلكترونيا[3].

وعليه، فإن الجمع بين مفهومي الأمن والمعلومة يؤدي بنا إلى مفهوم أمن المعلومات، الذي يهدف إلى حماية المعلومات من كل خطر قد يؤدي إلى كشفها أو تعديلها أو إتلافها أو منع الوصول إليها.

ج – أمن المعلومات: هناك عدة تعاريف تناولت مفهوم أمن المعلومات، نذكر منها ما يلي: " يعبر عن أمن المعلومات بأنه: " الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية ".

---

[1]– سهيلة بضياف وآمنة حمراني، " أمن المعلومات في الجزائر – الإجراءات والتحديات "، المجلة الجزائرية للأمن والتنمية، جامعة باتنة، مج 09، ع 16، جانفي 2020، الجزائر، ص 178.

[2]– خالد ياسين الشيخ، أمن نظم المعلومات والرقابة –التحكم، مذكرة ماجستير، جامعة دمشق، المعهد العالي للتنمية الإدارية 2010، ص 2.

[3] – خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، الدار الجامعية للطباعة والنشر، القاهرة، د.ط، 2008، ص 26.

كذلك أمن المعلومات هو: " مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي، للحفاظ على المعلومات والأجهزة والبرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال "[1].

كما عرف كل من Whitman[2] و Mathod[3] أمن المعلومات في كتابهما " مبادئ أمن المعلومات " بأنه (الحفاظ على سرية وتوفر وسلامة المعلومات كأصل في مراحل المعالجة والحفظ والنقل، وبتحقيق ذلك عبر التطبيق الفعلي للسياسات الأمنية ومن خلال تعزيز الوعي والتعليم والتدريب، ويرى كلاهما أن تحقيق إدارة أمن نظم المعلومات يشمل المكونات التالية:

- الأمن المادي: بما يشمله من مصادر وممتلكات ومبادئ لمنع الوصول غير المشروع.
- أمن الأفراد: لحماية الأفراد والمجموعات الذين لهم حق الوصول للمعلومات.
- أمن العمليات: لحماية الأنشطة والعمليات التي يقوم بها المخولون.
- أمن الاتصالات: لحماية الوسائط والتكنولوجيا المستخدمة والمحتوى.
- أمن الشبكات: لحماية مكونات الشبكة والتراسل والمحتويات.
- أمن البيانات: لحماية سرية وسلامة وتوافر المعلومات [4].

من خلال التعاريف السابقة يتضح أن أمن المعلومات مصطلح يضم في طياته عمليات وإجراءات شاملة لحماية الوسائل والأجهزة والكيانات الرقمية المتوفرة عن طرق وضع خطة ومنهجية محكمة وضرورة الإلتزام بتطبيقها [5].

---

[1] – قدافيه أمينة، "استراتيجية أمن المعلومات، مجلة أبعاد اقتصادية"، جامعة أحمد بوقرة بومرداس ، مج 06، ع 01، ص 165.

[2]: Michael E. Whitman أكاديمي وباحث متخصص في أمن المعلومات وإدارة المخاطر، له العديد من المؤلفات العلمية في مجال الأمن السيبراني، ويُعد من أبرز المساهمين في تطوير مناهج تدريس أمن المعلومات في الجامعات.

[3] Herbert J. Mattord أستاذ جامعي ومتخصص في أمن المعلومات وإدارة النظم، تركز أبحاثه على حوكمة أمن المعلومات وإدارة المخاطر والسياسات الأمنية، وشارك في تأليف عدد من المراجع الأكاديمية المعتمدة في هذا المجال.

[4] – فيلالي أسماء، شليل عبد اللطيف، "تهديدات أمن المعلومات وسبل التصدي لها"، مجلة البشائر الاقتصادية، جامعة تلمسان، مج 04، ع 03 ،2017، ص 164-165.

[5] – بليان مسعود، عكنوش نبيل، "أمن الوثائق والمعلومات الإلكترونية واستراتيجيات حفظها في الأرضية الرقمية لقطاع التربية"، مجلة المعيار، مج 25، عدد 59، 2021، ص 10.

يمكن القول أن **أمن المعلومات**: هو مجموعة من الممارسات والتقنيات المصممة لحماية البيانات من الوصول غير المصرح به، الإستخدام غير القانوني، التعديل أو التدمير، يهدف إلى ضمان سرية البيانات، تكاملها، وتوافرها عند الحاجة.

أي من وجهة نظرية: هو العلم الذي يبحث في نظريات وسبل توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الإعتداء عليها.

ومن وجهة تقنية: هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية[1].

يمكن استنتاج أن أمن المعلومات يشمل الأمن السيبراني كأحد مكوناته، و تجدر الإشارة **لتعريف الأمن السيبراني** وفقا لما ورد في وفقا لقاموس (Merriam-Webster) فهو :"التدابير المتخذة لحماية جهاز كمبيوتر أو نظام كمبيوتر (كما هو الحال على الإنترنت) من الوصول غير المصرح به أو الهجوم"[2].

كما يعرفه باحثين من شركة IBM على أنه :" ممارسة حماية الأفراد والأنظمة و البيانات من الهجمات السيبرانية باستخدام تقنيات وعمليات وسياسات متنوعة"[3].

عموما لقد وضع مصطلحي أمن المعلومات والأمن السيبراني لمعالجة القضايا المتعلقة بأمن المعلومات في البيئات الإلكترونية وغير الإلكترونية. و على الرغم من الترابط الوثيق بين الأمن السيبراني وأمن المعلومات، وتداخلهما في بعض الجوانب، فإن الاختلاف الرئيسي بينهما يكمن في المعلومات. بحيث يركز أمن المعلومات على حماية المعلومات في كل مكان، بينما يركز الأمن السيبراني تحديدا على المعلومات في الفضاء الإلكتروني. فكلاهما يهدف إلى حماية الأصول الرقمية و ضمان سريتها و سلامتها و توفرها ، و العلاقة بينهما تكمن في

[1] – د.أحمد الحصيني، مقدمة أمن المعلومات، منتدى الرياض الاجتماعي الثالث – المجتمع والتقنية – تحديات وآفاق، تاريخ النشر جانفي 2020 https://hemaya.org.sa

[2] -Cybersecurity noun, At :https://www.merriam-webster.com/dictionary/cybersecurity. Consulted : 2026/04/18 17:15

[3] -Gregg Lindemulder , Matt Kosinski , Alexandra Jonker, What is cybersecurity?

At : https://www.ibm.com/think/topics/cybersecurity?mhsrc=ibmsearch_a&mhq=cyber%20security. Consulted: 2026/04/18 16:02

أن أمن المعلومات مفهوم أوسع يشمل السياسات و الإجراءات لحماية جميع المعلومات ، أما الأمن السبيراني هو جزء من أمن المعلومات يركز على حماية البيانات و الأنظمة في البيئة الرقمية من الهجمات الإلكترونية[1] .

ثانيا :خصائص أمن المعلومات

تتمثل أهم خصائص أمن المعلومات في ثلاث خصائص رئيسية، وهي: السرية، والسلامة، والتوافر. وتعرف هذه الخصائص في مجال أمن المعلومات بأنها الركائز الأساسية التي تقوم عليها حماية الأنظمة والبيانات[2]، وهي كالتالي:

أ – السرية: و يقصد بها حماية المعلومات من الاطلاع أو الكشف أو الوصول إليها من طرف أشخاص غير مرخص لهم. فالمعلومة قد تكون ذات طبيعة شخصية أو مالية أو إدارية أو أمنية، ولذلك فإن كشفها لغير أصحاب الصلاحية قد يؤدي إلى أضرار خطيرة، سواء بالنسبة للفرد أو المؤسسة. وتتحقق السرية من خلال عدة وسائل، مثل كلمات المرور، والتشفير، وتحديد صلاحيات المستخدمين، وعدم السماح بالوصول إلى البيانات إلا لمن يملك حق استعمالها[3].

ب – السلامة أو التكاملية: تعني المحافظة على صحة المعلومات ودقتها، ومنع تعديلها أو حذفها أو إتلافها بطريقة غير مشروعة. فالمعلومة لا تكون ذات قيمة إذا تعرضت للتغيير أو التلاعب، لأن القرارات التي تبنى عليها تصبح غير صحيحة. ولهذا تهدف هذه الخاصية إلى ضمان بقاء البيانات كما أنشئت أو خزنت أو أرسلت، دون تحريف أو تزوير أو عبث[4].

ج – التوافر: يقصد به ضمان إمكانية الوصول إلى المعلومات والأنظمة عند الحاجة إليها من قبل الأشخاص المخول لهم ذلك. فحتى لو كانت المعلومات سرية وسليمة، فإنها تفقد قيمتها العملية إذا تعذر الوصول إليها وقت الحاجة، خاصة في المؤسسات التي تعتمد على الأنظمة الرقمية في تقديم خدماتها أو إدارة

[1] - Smys, S., & Haoxiang, W. (2021). Data elimination on repetition using a blockchain based cyber threat intelligence. IRO Journal on Sustainable Wireless Systems, 2(4), 149-154. Quoted from : Hamed Taherdoost,Cybersecurity vs. Information Security,Procedia Computer Science,Volume 215,2022, p 485. At : https://www.sciencedirect.com/science/article/pii/S1877050922021214, consulted : 21/05/2026.

[2] – خالد ممدوح إبراهيم، أمن المعلومات، الدار الجامعية، الإسكندرية، ط1، 2008، ص 21.

[3] – محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، د.ط، 2004، ص 37.

[4] – عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، ط1، 2006، ص 45.

نشاطها. ويتحقق التوافر من خلال النسخ الاحتياطي، وخطط استمرارية العمل، وحماية الأنظمة من الأعطال والهجمات التي تؤدي إلى تعطيل الخدمة[1].

وإلى جانب هذه الخصائص الثلاث، يضيف بعض الباحثين خصائص أخرى مكملة، مثل الموثوقية وعدم الإنكار والمساءلة .فالموثوقية تعني التأكد من هوية المستخدم أو مصدر المعلومة، وعدم الإنكار يعني عدم قدرة الشخص على إنكار قيامه بتصرف إلكتروني معين بعد ثبوته، أما المساءلة فتعني إمكانية تتبع الأفعال داخل النظام لمعرفة المسؤول عن كل عملية تمت عليه[2].

الفرع الثاني: أهمية وأهداف أمن المعلومات

يعد أمن المعلومات من الموضوعات الأساسية في البيئة الرقمية الحديثة، لأنه يرتبط بحماية البيانات والمعلومات من مختلف صور الاعتداء أو الاستخدام غير المشروع. ولا يتحقق أمن المعلومات بمجرد امتلاك أجهزة أو برامج حماية، بل يقوم على مجموعة من الخصائص والأهداف التي تضمن سلامة المعلومات واستمرار استخدامها بطريقة آمنة ومنظمة[3].

أولا: أهمية أمن المعلومات

تتمثل أهمية أمن المعلومات في كونه أصبح ضرورة أساسية في العصر الحديث، خاصة مع التطور الكبير في استعمال التكنولوجيا والأنظمة الرقمية داخل المؤسسات والإدارات ومختلف القطاعات. فلم تعد المعلومات مجرد بيانات عادية، بل أصبحت موردا مهما تعتمد عليه المؤسسات في اتخاذ القرارات، وتنظيم العمل، وتقديم الخدمات، وحماية مصالحها[4].

وتبرز أهمية أمن المعلومات في حماية البيانات من السرقة أو الضياع أو التعديل غير المشروع، خصوصا عندما يتعلق الأمر بالمعلومات الحساسة مثل البيانات الشخصية، الحسابات المالية، الأسرار المهنية، والوثائق الإدارية. فأي اختراق لهذه المعلومات قد يؤدي إلى أضرار كبيرة، سواء من الناحية المالية أو القانونية أو حتى من حيث سمعة المؤسسة وثقة المتعاملين معها[5].

---

[1] – خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2009، ص 52.

[2] – يونس عرب، جرائم الكمبيوتر والإنترنت، اتحاد المصارف العربية، بيروت، ط1، 2001، ص 28.

[3] – خالد ممدوح إبراهيم، أمن المعلومات، المرجع السابق، ص 21.

[4] – يونس عرب، موسوعة القانون وتقنية المعلومات: قانون الكمبيوتر، اتحاد المصارف العربية، بيروت، ط 1، 2002، ص 41.

[5] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 45.

كما يساعد أمن المعلومات على ضمان استمرارية العمل، لأن تعرض الأنظمة المعلوماتية لهجمات إلكترونية أو أعطال تقنية قد يؤدي إلى توقف الخدمات وتعطيل نشاط المؤسسة. لذلك فإن توفير الحماية اللازمة للمعلومات يساهم في تقليل المخاطر وضمان استمرار الخدمات بشكل عادي ومنتظم.

وتكمن أهميته أيضا في تعزيز الثقة بين المؤسسة ومستخدميها أو عملائها، فكلما كانت المعلومات محمية ومؤمنة، زادت ثقة الأفراد في التعامل مع المؤسسة أو النظام الرقمي. كما أن أمن المعلومات يساهم في احترام القوانين والتشريعات المتعلقة بحماية البيانات والخصوصية.

وعليه، يمكن القول إن أمن المعلومات لم يعد اختيارا، بل أصبح ضرورة حتمية لحماية الأفراد والمؤسسات والدول من المخاطر الإلكترونية، وضمان سلامة المعلومات وسريتها وتوافرها عند الحاجة إليها.

ثانيا :أهداف أمن المعلومات

يهدف أمن المعلومات أساسا إلى حماية المعلومات من كل تهديد قد يمس سريتها أو سلامتها أو توافرها. فالغاية الأولى منه هي منع الوصول غير المشروع إلى البيانات، وذلك بحصر استعمالها في الأشخاص المصرح لهم فقط. وهذا الهدف يكتسي أهمية خاصة في ظل انتشار قواعد البيانات الإلكترونية والمعاملات الرقمية التي تحتوي على معلومات شخصية وحساسة[1].

ويهدف أمن المعلومات إلى حماية البيانات من التعديل أو الإتلاف أو الفقدان، لأن أي تغيير غير مشروع في المعلومات قد يؤدي إلى نتائج خطيرة، مثل تزوير الوثائق، أو إفساد السجلات، أو اتخاذ قرارات خاطئة بناء على بيانات غير صحيحة. ولذلك تسعى المؤسسات إلى وضع ضوابط تقنية وتنظيمية تضمن بقاء المعلومات دقيقة وكاملة[2].

ومن أهداف أمن المعلومات كذلك ضمان استمرارية عمل الأنظمة والخدمات المعلوماتية، وذلك من خلال الوقاية من الأعطال والهجمات الإلكترونية والكوارث التقنية. فتعطل النظام المعلوماتي قد يؤدي إلى توقف نشاط المؤسسة، وخسائر مالية، واضطراب في تقديم الخدمات، خاصة في القطاعات الحساسة مثل البنوك، والصحة، والإدارة العمومية[3].

[1] – محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 39.

[2] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، ط1، 2003، ص 66.

[3] – خالد ممدوح إبراهيم، أمن المعلومات، المرجع السابق، ص 24 .

كما يهدف أمن المعلومات إلى تعزيز الثقة في البيئة الرقمية، لأن الأفراد والمؤسسات لا يمكنهم الاعتماد على المعاملات الإلكترونية إذا لم تكن محمية وآمنة. فكلما توفرت آليات الحماية والرقابة، زادت ثقة المستخدمين في تبادل المعلومات واستعمال الخدمات الإلكترونية[1].

يمكن القول إن أمن المعلومات لا يقتصر على الجانب التقني فقط، بل هو نظام متكامل يجمع بين الوسائل الفنية، والإجراءات الإدارية، والتوعية البشرية، والقواعد القانونية، بهدف حماية المعلومات وضمان استخدامها بطريقة آمنة ومشروعة.

الفرع الثالث: مخاطر أمن المعلومات

تعد مخاطر أمن المعلومات من أخطر الإشكالات التي تواجه الأفراد والمؤسسات في العصر الرقمي، وذلك بسبب الارتباط الكبير بين مختلف الأنشطة الإدارية والاقتصادية والاجتماعية بالأنظمة المعلوماتية. فكلما زاد الاعتماد على الحاسوب والإنترنت وقواعد البيانات، زادت احتمالات التعرض للاعتداءات الإلكترونية التي قد تمس سرية المعلومات أو سلامتها أو توافرها.

وتتمثل أولى هذه المخاطر في الدخول غير المشروع إلى الأنظمة المعلوماتية، حيث يقوم شخص غير مرخص له باختراق نظام معلوماتي أو قاعدة بيانات بهدف الاطلاع على المعلومات أو نسخها أو تغييرها أو استغلالها. ويعد هذا النوع من المخاطر من أكثر صور الاعتداء انتشارا، لأنه يمس مباشرة خصوصية المعلومات ويهدد سرية البيانات المخزنة داخل الأنظمة[2].

ومن المخاطر المهمة كذلك سرقة المعلومات والبيانات، وهي تتحقق عندما يتم الاستيلاء على معلومات شخصية أو مالية أو إدارية أو تجارية دون إذن صاحبها. وتزداد خطورة هذا الفعل عندما تكون المعلومات المسروقة مرتبطة بالحسابات البنكية أو الملفات الطبية أو الأسرار المهنية أو البيانات الخاصة بالمؤسسات، لأن استعمالها غير المشروع قد يؤدي إلى أضرار مالية وقانونية جسيمة[3].

كما تشكل الفيروسات والبرمجيات الخبيثة خطرا كبيرا على أمن المعلومات، لأنها قد تؤدي إلى إتلاف الملفات، أو تعطيل الأجهزة، أو التجسس على المستخدمين، أو التحكم في الأنظمة عن بعد. وتنتقل هذه البرمجيات غالبا عبر البريد الإلكتروني، أو الروابط المشبوهة، أو البرامج غير الموثوقة، مما يجعل الوقاية منها أمرا ضروريا من خلال التحديث المستمر واستعمال برامج الحماية[4].

---

[1] – يونس عرب، موسوعة القانون وتقنية المعلومات: قانون الكمبيوتر، اتحاد المصارف العربية، بيروت، ط1، 2002، ص 41.

[2] – محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 131.

[3] – عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي: دراسة قانونية متعمقة في القانون المعلوماتي، دار الفكر الجامعي، الإسكندرية، 2006، ص 18 .

[4] – خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، مرجع سابق، ص 66.

ومن بين المخاطر أيضا تغيير البيانات أو إتلافها، حيث قد يتعرض النظام المعلوماتي إلى تعديل غير مشروع للمعلومات، سواء بالحذف أو الإضافة أو التحريف. وتكمن خطورة هذا النوع من المخاطر في أنه يمس سلامة المعلومات ودقتها، وقد يؤدي إلى اتخاذ قرارات خاطئة بناء على بيانات غير صحيحة، خاصة في القطاعات الحساسة مثل البنوك، والصحة، والإدارة العامة[1].

وتظهر كذلك مخاطر أمن المعلومات في تعطيل الخدمات والأنظمة، وذلك من خلال الهجمات التي تستهدف منع المستخدمين الشرعيين من الوصول إلى المعلومات أو الخدمات الإلكترونية. ويؤدي هذا التعطيل إلى توقف العمل داخل المؤسسة، وفقدان الثقة في خدماتها، وقد ينتج عنه ضرر مالي أو إداري كبير، خصوصا إذا كان النظام المستهدف يقدم خدمات حيوية للجمهور.

ولا تقتصر مخاطر أمن المعلومات على الاعتداءات التقنية فقط، بل تشمل أيضا الأخطاء البشرية، مثل ضعف كلمات المرور، أو مشاركة البيانات مع الغير، أو فتح روابط مجهولة، أو عدم احترام قواعد الحماية داخل المؤسسة. فالإنسان يبقى من أضعف حلقات أمن المعلومات، لأن الإهمال أو نقص التكوين قد يسمح بوقوع اختراقات حتى مع وجود وسائل تقنية متطورة[2].

كما أن غياب السياسات الأمنية الواضحة داخل المؤسسات يزيد من احتمالية وقوع المخاطر، لأن حماية المعلومات لا تعتمد فقط على البرامج والأجهزة، بل تحتاج إلى تنظيم إداري، وتحديد للصلاحيات، وتكوين مستمر للموظفين، ووضع خطط للاستجابة للحوادث الأمنية عند وقوعها.

وبناء على ذلك، يمكن القول إن مخاطر أمن المعلومات متعددة ومتداخلة، منها ما هو تقني، ومنها ما هو بشري أو تنظيمي. لذلك فإن مواجهتها تتطلب اعتماد مقاربة شاملة تجمع بين الحماية التقنية، والتوعية، والرقابة القانونية، والإدارة الجيدة للمخاطر.

المطلب الثاني: الذكاء الاصطناعي

تتقدم التكنولوجيا بسرعة كبيرة هذه الأيام وتجعل حياة الإنسان مليئة بالراحة، وتوفر الأشياء المطلوبة وغير المطلوبة بنقرة واحدة فقط، تساعد التكنولوجيا بشكل كبير في مجال الأعمال أيضا، هناك العديد من الوسائل والتقنيات المتوفرة في السوق التي تعمل على تحسين الإنتاج، والذكاء الاصطناعي هو أحد هذه الوسائل التي تساعد في زيادة كفاءة العمل.

يتحرك الذكاء الاصطناعي بسرعة مع ظهور الاكتشافات والمعالم الجديدة طوال الوقت، ومن ناحية الذكاء البشري فإن الذكاء الاصطناعي يبشر بالقدرة على القيام بالمهام المتعددة، واستدعاء المعلومات وحفظها

[1] – نهال عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمّان، ط1، 2008، ص 77.

[2] – عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص 18.

بشكل مثالي، والعمل بشكل مستمر دون فترات راحة، وإجراء العمليات الحسابية بسرعة قياسية والتدقيق في السجلات والوثائق الطويلة واتخاذ قرارات منحازة[1].

الفرع الأول: تطور الذكاء الاصطناعي

يُعد الذكاء الاصطناعي من أبرز التقنيات التي أحدثت تحولًا جوهريًا في مختلف المجالات، نتيجة التطور المتسارع الذي شهده على المستويين العلمي والتقني. ولما كان فهم تطبيقاته وآثاره يقتضي الإحاطة بأسسه النظرية، فإنه يستوجب الوقوف على مراحل تطوره التاريخية، وتحديد مفهومه، وبيان أهم خصائصه، باعتبارها الأساس الذي تقوم عليه مختلف تطبيقاته المعاصرة.

أولا: مراحل تطور الذكاء الاصطناعي

أ – مرحلة البدايات الفكرية

إن الذكاء الاصطناعي من المواضيع التي اهتم بها الإنسان منذ القدم ففكرة محاكاة الذكاء البشري لطالما جذبت إنتباه العديد من الفلاسفة ، وقد وردت في كثير من القصص الخرافية اليونانية وإن لم ترق لمستوى يسمح بتطبيقها وتجسيدها ، ويرى البعض أن المقدمة الأولى لعلم الذكاء الاصطناعي قد مهد لها الفيلسوف الإنجليزي Hobbes Tomas سنوات 1950عندما إعتبر أن الفكر يتكون من عملية رمزية وأن كل شيء في الحياة يمكن تمثيله رياضيا، ما قاد مباشرة لمفهوم أن الآلة بمقدورها محاكاة التفكير البشري بالإستعانة بعمليات رياضية و رموز خارجية ، لهذا السبب يعتبر Hobbes أب الذكاء الإصطناعي.

ب – مرحلة التأسيس العلمي للذكاء الاصطناعي (1950–1956)

في عام 1950 نشر آلان تورينغ (Turing Alan) ورقة مهمة بعنوان " آلية الحوسبة والذكاء" مع الأخذ في الإعتبار السؤال الأساسي "هل يمكن للآلات أن تفكر؟ «، إقترح Turing لعبة محاكاة عرفت بإسم إختبار تورينغ بعد ذلك، حيث إذا كان بإمكان الآلة إجراء محادثة لا يمكن تمييزها عن محادثة مع إنسان، فمن المنطقي القول إن الآلة ذكية، وبذلك كان اختبار تورينغ هو أول تجربة مقترحة لقياس ذكاء الآلة.

وبعد سنتين من تشييد شركة جنرال إلكتريك لأول حاسب لإستخدامه في مجال الأعمال وكان ذلك سنة 1956 ظهرت بوادر الذكاء الاصطناعي، وارتبط هذا المصطلح بـ جون مكارثي McCarthy (John) كموضوع لمؤتمر عقد في كلية دارتموث Dartmouth، وفي نفس السنة أعلن عن أول برنامج

[1] – حيدر فالح سلمان، الخلود الرقمي – الذكاء الإصطناعي ومستقبل البشر، دار جامعة حمد بن خليفة للنشر، د.ط ، ص 16.

ذكاء اصطناعي للحاسب والمسمى " المنظر المنطقي"، وشجعت المقدرة المحدودة للمنظر المنطقي على التفكير الباحثين على تطوير برنامج آخر إسمه "حلال المشاكل العام " (Solver Problem General)[1].

ج – مرحلة الأنظمة الخبيرة والذكاء الرمزي

ففي الثمانينات تحول نموذج الذكاء الإصطناعي إلى الذكاء الإصطناعي الرمزي وما يسمى بـ" الأنظمة الخبيرة " أو " الأنظمة القائمة على المعرفة " بحيث كانت الفكرة الأساسية هي الحصول على معرفة الخبراء البشريين في شكل كمبيوتر ونشرها كبرنامج للعديد من أجهزة الكمبيوتر الشخصية.

د – مرحلة التوسع في التطبيقات العملية

في تسعينات القرن الماضي وحتى عام 2010 عالج الذكاء الإصطناعي المشاكل المعقدة، حيث قدم حلول وجدت مفيدة في مجالات التطبيق المختلفة بما في ذلك إستخراج البيانات، والروبوتات الصناعية واللوجستيات وذكاء الأعمال والبرمجيات المصرفية، والتشخيص الطبي، وأنظمة التوصية ومحركات البحث[2]، وبدأ الباحثون في إستخدام وتطوير أدوات رياضية أكثر تعقيدا، كان هناك إدراك واسع النطاق بأن العديد من مشكلات الذكاء الإصطناعي قد تم العمل عليها بالفعل من قبل باحثين في مجالات مثل الرياضيات أو الإقتصاد أو بحوث العمليات، وسمحت اللغة الرياضية المشتركة بمستوى أعلى من التعاون مع المجالات الراسخة وجعلت الذكاء الإصطناعي تخصصا علميا أكثر صرامة .

ذ – مرحلة التعلم العميق والذكاء الاصطناعي التوليدي

لقد تطور تطورا متسارعا من سنة 2010 حتى سنة 2026 ، إذ انتقل من مرحلة الخوارزميات التقليدية إلى مرحلة **التعلم العميق**، خاصة بعد النجاح الكبير لنموذج **AlexNet** سنة 2012 في تصنيف الصور، وهو ما اعتبر نقطة تحول في استعمال الشبكات العصبية العميقة[3]، ثم تعزز هذا التطور سنة 2016 مع نظام **AlphaGo** الذي تفوق على اللاعب العالمي **Lee Sedol** في لعبة Go ، مما أبرز قدرة الذكاء الاصطناعي على التعلم واتخاذ القرار في مسائل معقدة، وبعد ظهور بنية **Transformer**سنة 2017، تطورت نماذج معالجة اللغة الطبيعية بشكل كبير، فظهرت نماذج مثل **BERT**سنة 2018 و **GPT-3**سنة 2020، ثم دخل الذكاء الاصطناعي مرحلة الانتشار الواسع بعد إطلاق

[1] – محمد طول، أمل بكار، أساسيات حول الذكاء الإصطناعي – إطار مفاهيمي – مداخلة في ملتقى وطني إفتراضي حول استخدامات الذكاء الإصطناعي كضمان لجودة التعليم العالي والبحث العلمي 07 نوفمبر 2022، ص 03

[2] – محمد طول، أمل بكار نفس المرجع ، ص 04 .

[3] Alex Krizhevsky, Ilya Sutskever, Geoffrey E. Hinton, *ImageNet Classification with Deep Convolutional Neural Networks*, NeurIPS, 2012.

ChatGPT سنة 2022. ومع ظهور النماذج متعددة الوسائط مثل **GPT-4o** سنة 2024، أصبح الذكاء الاصطناعي قادرا على التعامل مع النص والصورة والصوت في الوقت الحقيقي، وبحلول سنة 2026، صار الذكاء الاصطناعي التوليدي من أكثر التقنيات ارتباطا بالتحول الرقمي، بعد أن توسع استعماله في التعليم، الصحة، الإدارة، البحث العلمي والأعمال[1].

ثانيا: تعريف الذكاء الاصطناعي

قبل التطرق لتعريف الذكاء الإصطناعي علينا معرفة معنى الذكاء بصورة عامة.

فالذكاء هو الجزء الحساس من القدرة على تحقيقه الأهداف أو الوصول إليها وتختلف درجاته وأنواعه بين البشر والحيوانات والآلات، في البداية كان الهدف من برامج الذكاء أن تحل محل الخبير في تخصص البرامج ولكن ثبت استحالة ذلك وأصبح الهدف من برامج الذكاء هو مساعدة الخبير في أداء علمه بسرعة وكفاءة متميزة.

أما الذكاء الإصطناعي هو العلم والهندسة اللذان يجعلان الحاسب الآلي آلة ذكية وهو اصطناعي لأنه عبارة عم برامج وأجهزة تتعاون لتؤدي عملية فهم معقدة يمكن أن تضاهي ذكاء البشر من فهم وسمع ورؤية وشم وكلام وتفكير أي أنه برامج ذكية + أجهزة = ذكاء إصطناعي[2].

لقد عرف عالم الكمبيوتر الأمريكي جون ماكرثي الذكاء الإصطناعي بأنه: " علم وهندسة صناعة الآلات الذكية وخاصة برامج الكمبيوتر الذكية "، ويعرف الذكاء الإصطناعي أيضا على أنه: " مجموعة متنوعة من الأساليب والتقنيات والأدوات لإنشاء النماذج وحل المشكلات عن طريق محاكاة سلوك الأشخاص المدركين[3].

ثالثا: خصائص الذكاء الاصطناعي

يتمتع الذكاء الإصطناعي بالعديد من الخصائص والمميزات، نذكر منها:

- إستخدام الذكاء في حل المشاكل المعروضة مع غياب المعلومة الكاملة .
- القدرة على إكتساب المعرفة وتطبيقها.
- القدرة على التعلم والفهم من التجارب والخبرات السابقة .
- القدرة على استخدام الخبرات القديمة وتوظيفها في مواقع جديدة.

---

[1] -Stanford Institute for Human-Centered Artificial Intelligence, *The 2026 AI Index Report*, 2026.

[2] – خالد ناصر السيد، أصول الذكاء الإصطناعي، الرياض، مكتبة الرشد، 2004، ص 14.

[3] – وافي حاجة، استخدامات الذكاء الإصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني، الجزائر، منشورات دار لايمة، 2025، ص 20.

- القدرة على الإستجابة السريعة للمواقع والظروف الجديدة.
- القدرة على التعامل مع المواقف الغامضة مع غياب المعلومة.
- القدرة على تقديم المعلومة لإسناد القرارات الإدارية.
- إمكانية تمثيل المعرفة بواسطة الرموز.
- قابلية التعامل مع المعلومات الناقصة، والتعامل مع الفرضيات بشكل متزامن بدقة وسرعة عالية.
- القدرة على معالجة الكم الهائل من المعلومات التي يتعرض لها.
- القدرة على التعرف على الأصوات والكلام، بإضافة إلى حل المشاكل بإستخدام المنطق[1].

الفرع الثاني: أنواع الذكاء الاصطناعي

تقسم أنواع الذكاء الإصطناعي إلى ذكاء إصطناعي الضيق أي المحدود، وذكاء إصطناعي عام وذكاء إصطناعي فائق الذكاء على إعتبار أن أنظمة الذكاء الإصطناعي لا تعمل بشكل مستقل عن المتدخلين أو المبرمجين لها، وسيتم معالجة كل نوع على حدي.

أولا: الذكاء الإصطناعي الضيق " المحدود " Artificial Narrow Intelligence

يقوم هذا النوع من الذكاء الإصطناعي بمهام يمكن أن تكون مدفوعة بخوارزميات معقدة للغاية وشبكات عصبية، فهي مهام موجهة نحو الهدف، مثل التعرف على الوجوه، والبحث عن معلومات محددة، والتحكم في السيارات ذاتية القيادة، وهو النوع الأكثر شيوعا الآن[2].

ثانيا : الذكاء الإصطناعي العام Artificial Generel Intelligence

يعمل الذكاء الإصطناعي العام بقدرة تشابه تفكير الإنسان؛ إذ يجعل الآلة تفكر وتخطط من تلقاء نفسها بشكل مشابه للسلوك الإنساني، ومن تطبيقات هذا النوع ما قدم من دراسات علمية في مجال إنتاج الشبكة العصبية الإصطناعية؛ إذ تعنى بإنتاج نظام شبكات عصبية لروبوتات صناعية مشابهة لتلك التي يحتويها الجسم البشري[3].

كما أن الذكاء الإصطناعي لديه القدرة على التنبؤ بإستقراء المعرفة من خلال مجموعة واسعة من المهام والمواقف التي لا تتناولها البيانات المدخلة مسبقا، ولا الخوارزميات الموجودة.

---

[1] – منال بومعراف، الذكاء الاصطناعي رؤية متعددة التخصصات، كتاب جماعي دولي محكم، ألمانيا، المركز الديمقراطي العربي للدراسات الاستراتيجية، الاقتصادية والسياسية، برلين، ط1، أفريل 2024، ص 73.

[2] – عبد الملك الدناني، خالد درار، عمر بن عمر، تقنيات الذكاء الاصطناعي وتطبيقاته في المجال الإعلامي بالدول العربية، دار شهر زاد للنشر والتوزيع، عمان، ط1 ،2025، ص 10.

[3] – قندوز فتيحة، "الجوانب القانونية لإستخدام الذكاء الإصطناعي"، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة جيجل، الجزائر، مج 09، ع1، 2024، ص 1184 .

ثالثا : الذكاء الإصطناعي الفائق Artificial Super Intelligence

عبارة عن أجهزة أعقد من مجرد محاكاة أو فهم السلوك البشري، فهي مدعومة بقوة المعالجة والتحليل التي تتجاوز القدرات البشرية، ومن غير المرجح أن أي شخص يعيش اليوم سيرى مثل هذا العالم، حيث يتجاوز هذا النوع من الذكاء الإصطناعي القابلية للقياس تقريبا، وكما قال " ستيفن هوكينج ": من المهم البحث في كيفية جني مزايا الذكاء الإصطناعي الفائق مع تجنب المآزق المحتملة.[1]

الفرع الثالث: تطبيقات الذكاء الاصطناعي في مجال أمن المعلومات

يشهد مجال أمن المعلومات تطورا كبيرا بفضل تطبيقات الذكاء الاصطناعي، حيث أصبحت الأنظمة قادرة على تحليل كميات هائلة من البيانات واكتشاف التهديدات بسرعة ودقة عالية. يساهم الذكاء الاصطناعي في التعرف على الأنماط غير الطبيعية، والتنبؤ بالهجمات قبل وقوعها، والاستجابة لها بشكل تلقائي، مما يعزز من حماية الأنظمة والشبكات. كما يستخدم في تحسين أنظمة كشف ومنع التسلل، وتقليل الأخطاء البشرية، وتوفير حلول أمنية أكثر كفاءة ومرونة في مواجهة التهديدات المتزايدة.

و قد أصبح الذكاء الاصطناعي من الوسائل الحديثة التي تعتمد عليها المؤسسات الأمنية لمواجهة التهديدات المتطورة، خاصة مع اتساع استعمال التكنولوجيا وانتشار الجرائم الإلكترونية. فلم تعد الأساليب التقليدية كافية وحدها لرصد المخاطر وتحليلها، بل أصبح من الضروري الاستعانة بأنظمة ذكية قادرة على معالجة كميات ضخمة من البيانات، واكتشاف الأنماط غير العادية، والمساعدة في اتخاذ القرار الأمني المناسب.

وتعد المراقبة الذكية من أبرز تطبيقات الذكاء الاصطناعي في المجال الأمني، حيث تستعمل الكاميرات المزودة بخوارزميات التعرف على الصور والوجوه في مراقبة الأماكن العامة والمنشآت الحساسة. وتساعد هذه الأنظمة على اكتشاف السلوكيات المشبوهة، والتعرف على الأشخاص المطلوبين، وتنبيه الجهات المختصة في الوقت المناسب، مما يساهم في الوقاية من الجرائم قبل وقوعها[2].

كما يستخدم الذكاء الاصطناعي في تحليل البيانات الأمنية، وذلك من خلال جمع المعلومات من مصادر مختلفة، مثل قواعد البيانات، والكاميرات، ووسائل الاتصال، والبلاغات الأمنية، ثم تحليلها لاستخراج مؤشرات تساعد على فهم طبيعة المخاطر. وتكمن أهمية هذا التطبيق في قدرته على الربط بين معطيات كثيرة قد يصعب على الإنسان تحليلها بالسرعة والدقة نفسهما[3].

ومن التطبيقات المهمة كذلك التنبؤ بالجرائم، حيث تعتمد بعض الأنظمة الأمنية على تحليل البيانات السابقة المتعلقة بمكان الجريمة وزمانها وطبيعتها من أجل توقع المناطق أو الفترات التي يمكن أن تشهد ارتفاعا في

---

[1] – عبد الملك الدناني ، خالد درار ، عمر بن عمر ، المرجع السابق ، ص 11 .

[2] – علي بن خلفان بن علي الهنائي، تطبيقات الذكاء الاصطناعي في المجال الأمني: دراسة مطبقة على دول مجلس التعاون لدول الخليج العربية، مجلة الدراسات القانونية والاقتصادية، مج 10، ع 4، 2024، ص 2558 – 2559.

[3] – علي بن خلفان بن علي الهنائي، المرجع نفسه، ص 2570 -2571.

معدلات الجريمة. ولا يعني ذلك الجزم بوقوع الجريمة، وإنما تقديم مؤشرات احتمالية تساعد أجهزة الأمن على توجيه جهودها ومواردها بطريقة أكثر فعالية

ويظهر دور الذكاء الاصطناعي أيضا في الأمن السيبراني، إذ يمكن استعماله في كشف الهجمات الإلكترونية مبكرا، وتحليل السلوك غير الطبيعي داخل الشبكات، والتعرف على محاولات الاختراق والبرمجيات الخبيثة. فالأنظمة الذكية قادرة على مراقبة حركة البيانات باستمرار، واكتشاف الأنماط الشاذة التي قد تدل على وجود تهديد أمني.

كما تستفيد أجهزة الأمن من الذكاء الاصطناعي في التحقيقات الجنائية الرقمية، من خلال تحليل الأدلة الإلكترونية، واسترجاع البيانات، وفحص الأجهزة، وتتبع الأنشطة المشبوهة على الشبكات. ويساعد ذلك المحققين على الوصول إلى أدلة رقمية دقيقة، خاصة في الجرائم التي تتم عبر الإنترنت أو باستعمال الوسائل الإلكترونية[1].

ومن جهة أخرى، يمكن استعمال الذكاء الاصطناعي في إدارة الأزمات والطوارئ، حيث تساعد الأنظمة الذكية على تحليل المعلومات أثناء الكوارث أو الحوادث الكبرى، وتحديد الأولويات، وتوجيه فرق التدخل، وتوقع تطور الوضع الأمني. وهذا يجعل الذكاء الاصطناعي أداة مساعدة في تحسين سرعة الاستجابة وتقليل الخسائر.

ورغم أهمية هذه التطبيقات، فإن استعمال الذكاء الاصطناعي في المجال الأمني يثير عدة تحديات، خاصة ما يتعلق بحماية الخصوصية، وضمان عدم التعسف في استعمال البيانات، وتفادي الأخطاء الناتجة عن الخوارزميات. لذلك فإن نجاح هذه التطبيقات يتطلب وجود إطار قانوني وأخلاقي واضح يوازن بين متطلبات الأمن وحماية الحقوق والحريات.

وبناء على ذلك، يمكن القول إن الذكاء الاصطناعي أصبح أداة فعالة في تطوير العمل الأمني، سواء في الوقاية من الجريمة، أو كشف التهديدات، أو تحليل البيانات، أو تعزيز الأمن السيبراني غير أن استعماله يجب أن يكون مضبوطا بقواعد قانونية ورقابية تضمن توظيفه لخدمة الأمن دون المساس بحقوق الأفراد[2].

[1] – مبسوطة حمد الحاسي، استراتيجية التكامل بين الذكاء الاصطناعي والأمن السيبراني في رصد ومواجهة الهجمات السيبرانية المبكرة، المؤتمر الدولي الأول للتعليم الإلكتروني وتكنولوجيا المعلومات، جامعة الزاوية، ليبيا، 2025،ص8 .

[2] – عبد الباسط عيساوي، سفيان زيتون، آثار الذكاء الاصطناعي على الأمن السيبراني: دراسة حالة الجزائر، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، 2024،ص120 .

المبحث الثاني: دور الذكاء الاصطناعي في تعزيز أمن المعلومات

مع ظل تسارع التطور للتكنولوجيا الرقمية وتزايد الاعتماد على الأنظمة المعلوماتية في مختلف مجالات الحياة، أصبحت مسألة أمن المعلومات من أهم التحديات التي تواجه الدول والمؤسسات على حد سواء وقد أدى هذا التحول الرقمي إلى ظهور تهديدات سيبرانية متطورة تتسم بالتعقيد والسرعة، مما جعل الوسائل التقليدية للحماية غير كافية لمواجهتها بفعالية.

كما برز الذكاء الاصطناعي كأداة حديثة وفعالة في تعزيز أمن المعلومات، من خلال قدرته على تحليل كميات ضخمة من البيانات، واكتشاف الأنماط غير الطبيعية، والتنبؤ بالهجمات قبل وقوعها كما يساهم في تحسين مستوى الاستجابة للحوادث الأمنية وتقليل المخاطر المرتبطة بها.

وعليه، يهدف هذا المبحث إلى إبراز الدور الذي يلعبه الذكاء الاصطناعي في تعزيز أمن المعلومات، وذلك من خلال التطرق إلى آلياته في الكشف عن التهديدات، ثم دراسة مساهمته في الوقاية منها والتصدي لها.

المطلب الأول: آليات الذكاء الاصطناعي في الكشف عن التهديدات المعلوماتية

تعد عملية الكشف المبكر عن التهديدات المعلوماتية من الركائز الأساسية في حماية الأنظمة الرقمية، إذ تسمح بالتدخل السريع قبل تفاقم الأضرار ومع تزايد تعقيد الهجمات السيبرانية وتنوع أساليبها، أصبح من الضروري الاعتماد على تقنيات متطورة قادرة على مواكبة هذا التطور.

وفي هذا الإطار، يوفر الذكاء الاصطناعي مجموعة من الآليات الذكية التي تعتمد على التعلم الآلي وتحليل البيانات الضخمة، مما يمكنها من التعرف على السلوكيات المشبوهة واكتشاف الاختراقات بدقة عالية وفي وقت قياسي كما تساهم هذه الآليات في التنبؤ بالهجمات المستقبلية من خلال تحليل البيانات السابقة واستخلاص الأنماط المتكررة.

ومن هذا المنطلق، سيتم في هذا المطلب دراسة أهم آليات الذكاء الاصطناعي المعتمدة في الكشف عن التهديدات المعلوماتية، مع بيان دورها في تعزيز فعالية أنظمة الأمن السيبراني

الفرع الأول: الكشف المبكر عن الهجمات والاختراقات السيبرانية

يعد الكشف المبكر عن الهجمات السيبرانية من أهم تطبيقات الذكاء الاصطناعي في مجال أمن المعلومات، لأن خطورة الهجوم الإلكتروني لا تكمن فقط في وقوعه، بل في تأخر اكتشافه فكلما تم رصد محاولة الاختراق في بدايتها، أمكن تقليل آثارها ومنع انتقالها إلى باقي مكونات النظام المعلوماتي[1].

ويعتمد الذكاء الاصطناعي في هذا المجال على تحليل حركة البيانات داخل الشبكات، ومراقبة محاولات الدخول، وتتبع الأنشطة غير المعتادة التي قد تدل على وجود تهديد أمني فعوضا عن انتظار وقوع الضرر، تعمل

[1] – محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، د.ط ، 2003، ص 131 .

الأنظمة الذكية على البحث عن المؤشرات الأولى للهجوم، مثل تكرار محاولات تسجيل الدخول، أو استعمال عناوين مجهولة، أو نقل بيانات بكميات غير مألوفة[1].

وتظهر أهمية الكشف المبكر في حماية سرية المعلومات وسلامتها، لأنه يسمح للمؤسسة باتخاذ إجراءات وقائية قبل تمكن المهاجم من الوصول إلى البيانات الحساسة أو تعطيل النظام ولهذا أصبح الذكاء الاصطناعي وسيلة فعالة في أنظمة كشف التسلل، وبرامج مكافحة البرمجيات الخبيثة، وأنظمة مراقبة الشبكات[2].

ومن الناحية القانونية، يتماشى هذا الدور الوقائي مع توجه المشرع الجزائري في القانون رقم 09-04، الذي وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بما يدل على أن الحماية لا تقتصر على العقاب بعد وقوع الجريمة، بل تشمل كذلك آليات الوقاية والرصد المبكر وفقا لما نصت عليه المادة الثانية و ما يليها من هذا القانون[3]، كما صدر المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، وهو ما يعكس اهتمام الدولة بحماية الأنظمة المعلوماتية من المخاطر السيبرانية[4].

وعليه، فإن الكشف المبكر يمثل مرحلة أساسية في أمن المعلومات، لأنه يحول الذكاء الاصطناعي من مجرد أداة تحليل إلى وسيلة وقائية قادرة على حماية النظام قبل وقوع الضرر.

الفرع الثاني: تحليل السلوكيات غير الطبيعية والتنبؤ بالمخاطر

لا يقتصر دور الذكاء الاصطناعي في المجال الأمني على كشف الهجمات بعد بدايتها، بل يمتد إلى تحليل السلوكيات غير الطبيعية والتنبؤ بالمخاطر المحتملة ويقصد بالسلوك غير الطبيعي كل نشاط يخرج عن النمط المعتاد لاستعمال النظام، مثل دخول المستخدم في وقت غير مألوف، أو تحميل ملفات كثيرة دفعة واحدة، أو محاولة الوصول إلى بيانات لا تدخل ضمن صلاحياته[5].

---

[1] – خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، مرجع سابق، ص 66 .

[2] – نهال عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمّان، ط 1، 2008، ص 77 .

[3] – القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[4] – المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج.ر.ج.ج، ع 04 الصادرة في 26جانفي 2020.

[5] – علي بن خلفان بن علي الهنائي، تطبيقات الذكاء الاصطناعي في المجال الأمني: دراسة مطبقة على دول مجلس التعاون لدول الخليج العربية، مجلة الدراسات القانونية والاقتصادية، مج 10، ع 4، 2024، ص 2570 .

وتعتمد الأنظمة الذكية في هذا المجال على بناء نماذج للسلوك العادي للمستخدمين والأنظمة، ثم مقارنة النشاط الجديد بذلك النموذج فإذا ظهر اختلاف واضح، تقوم هذه الأنظمة بإصدار تنبيه أمني قد يدل على وجود محاولة اختراق أو إساءة استعمال للصلاحيات. وتظهر أهمية هذه التقنية خاصة في المؤسسات التي تتعامل مع معلومات حساسة، لأن بعض الهجمات لا تأتي دائما من خارج النظام، بل قد تنتج عن مستخدم داخلي أو حساب تم اختراقه[1].

كما يساعد الذكاء الاصطناعي على التنبؤ بالمخاطر من خلال تحليل البيانات السابقة المتعلقة بالحوادث الأمنية، واستخلاص الأنماط المتكررة التي قد تشير إلى احتمال وقوع تهديد جديد وبذلك تصبح المؤسسة قادرة على توزيع موارد الحماية بطريقة أفضل، وتركيز الرقابة على النقاط الأكثر عرضة للهجوم.

ويرتبط هذا الجانب كذلك بحماية المعطيات ذات الطابع الشخصي، لأن تحليل السلوكيات الأمنية قد يتضمن معالجة بيانات مرتبطة بالأشخاص ولهذا يجب أن يتم استعمال الذكاء الاصطناعي في هذا المجال في إطار احترام القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الذي يشكل الإطار القانوني الأساسي لحماية البيانات الشخصية في الجزائر المعدل و المتمم بموجب القانون رقم 25-11[2]، كما أن التعديل الدستوري لسنة 2020 كرس حماية الأشخاص عند معالجة معطياتهم ذات الطابع الشخصي باعتبارها من الضمانات الأساسية المرتبطة بالحقوق والحريات وفقا لنص المادة 47 التي نصت على : " لكل شخص الحق في حماية حياته الخاصة و شرفه .لكل شخص الحق في سرية مراسلاته و اتصالاته الخاصة في أي شكل كانت .لا مساس بالحقوق المذكورة في الفقرتين الأولى و الثانية إلا بأمر معلل من السلطة القضائية .حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي"[3].

ومن ثم، فإن تحليل السلوكيات غير الطبيعية والتنبؤ بالمخاطر يحقق فائدة أمنية كبيرة، لكنه يجب أن يمارس في حدود الضوابط القانونية، حتى لا يتحول إلى وسيلة للمساس بالخصوصية أو المراقبة غير المشروعة.

---

[1] – علي بن خلفان بن علي الهنائي، المرجع نفسه، ص 2572 .

[2] – القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المعدل و المتمم بموجب القانون رقم 25-11 المؤرخ في 24 يوليو 2025 ،ج .ر.ج.ج العدد 48 الصادرة بتاريخ 24 يوليو 2025 .

[3] – أنظر المادة 47 من التعديل الدستوري لسنة 2020.

الفرع الثالث: الاستجابة الذكية للحوادث الأمنية واحتواؤها

تعد الاستجابة للحوادث الأمنية مرحلة حاسمة في إدارة أمن المعلومات، لأنها تبدأ بعد اكتشاف التهديد أو وقوعه، وتهدف إلى الحد من آثاره ومنع انتشاره داخل النظام. وقد ساهم الذكاء الاصطناعي في تطوير هذه المرحلة من خلال تمكين الأنظمة الأمنية من اتخاذ إجراءات سريعة وآلية، مثل عزل الجهاز المصاب، أو إيقاف حساب مشبوه، أو منع اتصال ضار، أو تنبيه المسؤولين الأمنيين[1].

وتتميز الاستجابة الذكية بأنها لا تعتمد فقط على التدخل البشري، بل تستند إلى تحليل فوري للبيانات وتحديد طبيعة الحادث ودرجة خطورته. فإذا اكتشف النظام مثلا برمجية خبيثة أو محاولة تسريب بيانات، يمكنه أن يتخذ إجراءات أولية لاحتواء الخطر قبل تدخل الفريق المختص. وهذا يساعد على تقليل زمن الاستجابة، وهو عامل مهم جدا في الحوادث السيبرانية[2].

كما يساعد الذكاء الاصطناعي في ترتيب الأولويات أثناء الحوادث الأمنية، لأن المؤسسات قد تتلقى عددا كبيرا من التنبيهات يوميا، وليس كل تنبيه يدل على خطر حقيقي وهنا تقوم الأنظمة الذكية بفرز التنبيهات وتصنيفها حسب درجة الخطورة، مما يسمح للفرق الأمنية بالتركيز على الحوادث الأكثر تهديدا للنظام[3].

وتكتسي هذه الاستجابة أهمية قانونية وتنظيمية، لأن المرسوم الرئاسي رقم 20-05 وضع منظومة وطنية لأمن الأنظمة المعلوماتية، كما تشير الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية إلى إحداث وكالة أمن الأنظمة المعلوماتية في إطار هذه المنظومة وهذا يدل على أن التعامل مع الحوادث السيبرانية أصبح جزءا من السياسة العامة لحماية البنية الرقمية للدولة[4].

غير أن الاستجابة الذكية يجب أن تكون مضبوطة بقواعد واضحة، لأن بعض الإجراءات الآلية قد تمس حقوق المستخدمين، مثل تعليق الحسابات أو مراقبة النشاط أو معالجة البيانات الشخصية. لذلك ينبغي أن تخضع هذه الآليات لمبدأ المشروعية، والضرورة، والتناسب، مع احترام قواعد حماية المعطيات الشخصية[5].

وبناء على ذلك، يمكن القول إن الاستجابة الذكية للحوادث الأمنية تمثل مرحلة متقدمة في أمن المعلومات، لأنها لا تكتفي بكشف الخطر، بل تعمل على احتوائه وتقليل آثاره، مع ضرورة إخضاعها للرقابة القانونية والتنظيمية.

---

[1] – مبسوطة حمد الحاسي، استراتيجية التكامل بين الذكاء الاصطناعي والأمن السيبراني في رصد ومواجهة الهجمات السيبرانية المبكرة، المؤتمر الدولي الأول للتعليم الإلكتروني وتكنولوجيا المعلومات، جامعة الزاوية، ليبيا، د.ط ،2025، ص 6 .

[2] – مبسوطة حمد الحاسي، المرجع نفسه، ص 8 .

[3] – علي بن خلفان بن علي الهنائي، المرجع السابق، ص 2590 .

[4] – المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

[5] – القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

المطلب الثاني: مساهمة الذكاء الاصطناعي في تطوير وسائل حماية أمن المعلومات

يظهر دور الذكاء الاصطناعي كأداة فعالة في تطوير حماية أمن المعلومات، ليس فقط من خلال كشف المخاطر، بل أيضا من خلال التنبؤ بها والاستجابة لها بطريقة أكثر سرعة ودقة. وعلى هذا الأساس، سيتم تناول هذا المطلب من خلال الفروع الآتية: استخدام الذكاء الاصطناعي في أنظمة المصادقة والتحكم في الولوج، حماية الشبكات والبيانات بواسطة تقنيات التعلم الآلي، ثم مزايا وحدود اعتماد الذكاء الاصطناعي في مجال أمن المعلومات.

الفرع الأول: استخدام الذكاء الاصطناعي في أنظمة المصادقة والتحكم في الولوج

تعد المصادقة والتحكم في الولوج من أهم وسائل حماية أمن المعلومات، لأن أول خطوة لحماية النظام المعلوماتي هي التأكد من هوية المستخدم، ثم تحديد حدود الصلاحيات الممنوحة له فليس كل من يدخل إلى النظام يملك الحق في الاطلاع على جميع البيانات أو تعديلها أو نقلها، لذلك تعتمد المؤسسات على آليات تقنية وتنظيمية لضبط الدخول إلى المعلومات الحساسة[1].

وقد ساهم الذكاء الاصطناعي في تطوير هذه الوسائل من خلال الانتقال من المصادقة التقليدية، القائمة غالبا على كلمة المرور، إلى مصادقة أكثر ذكاء تعتمد على تحليل عدة مؤشرات، مثل سلوك المستخدم، ومكان الاتصال، ونوع الجهاز، وطريقة الكتابة، وسجل الدخول السابق فإذا لاحظ النظام سلوكا غير مألوف، كالدخول من مكان غريب أو محاولة الوصول إلى بيانات غير معتادة، يمكنه طلب تحقق إضافي أو منع العملية مؤقتا[2].

كما يمكن للذكاء الاصطناعي أن يساعد في تحسين أنظمة التحكم في الولوج، من خلال تحليل الصلاحيات الممنوحة للمستخدمين واكتشاف الأخطاء أو التعارضات داخل سياسات الوصول. فبعض المستخدمين قد يحتفظون بصلاحيات قديمة لم تعد ضرورية، مما يشكل خطرا على أمن المعلومات، وهنا يمكن للأنظمة الذكية اقتراح تقليص الصلاحيات أو تعديلها وفقا لمبدأ "أقل امتياز"[3].

ومن الناحية القانونية، يرتبط هذا الموضوع بالتوقيع والتصديق الإلكترونيين، لأنهما يمثلان وسيلة لإثبات الهوية والثقة في التعاملات الإلكترونية. وقد نظم المشرع الجزائري ذلك بموجب القانون رقم 15-04،

---

[1] – المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية، ISO/IEC 27002:2022"، أمن المعلومات والأمن السيبراني وحماية الخصوصية — عناصر التحكم في أمن المعلومات"، المنظمة الدولية للتوحيد القياسي، جنيف، 2022.

[2] – كارين سكار فون وموروجياه سوباير، "دليل إدارة كلمات المرور للمؤسسات"، منشور NIST الخاص رقم 118-800، المعهد الوطني للمعايير والتكنولوجيا، 2009، الصفحات 7-8.

[3] – فينسنت سي. هو، ديفيد فيريولو، ريك كون، آدم شنيتزر، كينيث ساندلين، روبرت ميلر، كارين سكار فون، "دليل تعريف واعتبارات التحكم في الوصول المستند إلى السمات"(ABAC) ، منشور NIST الخاص رقم 162-800، المعهد الوطني للمعايير والتكنولوجيا، 2014، الصفحات 1-2.

الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، كما صدر المرسوم التنفيذي رقم 16-134[1] المتعلق بتنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها[2].

وعليه، فإن الذكاء الاصطناعي لا يلغي الوسائل التقليدية للمصادقة والتحكم في الولوج، بل يطورها ويجعلها أكثر قدرة على التكيف مع المخاطر الحديثة، خاصة في ظل تزايد سرقة كلمات المرور وانتحال الهوية الرقمية.

الفرع الثاني: حماية الشبكات والبيانات بواسطة تقنيات التعلم الآلي

يعد التعلم الآلي من أبرز فروع الذكاء الاصطناعي المستعملة في حماية الشبكات والبيانات، لأنه يسمح للأنظمة الأمنية بالتعلم من البيانات السابقة واكتشاف الأنماط المتكررة التي قد تدل على وجود تهديد. فبدل الاعتماد فقط على قواعد ثابتة، تستطيع أنظمة التعلم الآلي تحليل حركة الشبكة والتعرف على السلوك العادي، ثم اكتشاف أي نشاط غير مألوف قد يشير إلى محاولة اختراق أو تسريب بيانات[3].

وتظهر أهمية التعلم الآلي في حماية الشبكات من خلال مراقبة تدفق البيانات، وتصنيف الأنشطة المشبوهة، واكتشاف البرمجيات الخبيثة، وتحليل الرسائل والروابط الضارة. كما يمكنه المساهمة في كشف الهجمات التي تتطور بسرعة، والتي قد لا تستطيع برامج الحماية التقليدية التعرف عليها إذا لم تكن مسجلة مسبقا في قواعد بياناتها[4].

أما في مجال حماية البيانات، فيساعد التعلم الآلي على اكتشاف محاولات الوصول غير المشروع، ومراقبة حركة الملفات الحساسة، والتنبيه عند وجود نقل غير عادي للبيانات. وتزداد أهمية هذه التقنية في المؤسسات التي تتعامل مع كميات ضخمة من المعلومات، مثل البنوك، والمؤسسات الصحية، والإدارات العمومية، لأن المراقبة اليدوية تصبح صعبة وغير كافية[5].

---

[1] – المرسوم التنفيذي رقم 16-134 المؤرخ في 25 أفريل 2016، المحدد لتنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها، ج.ر.ج.ج، ع 26، الصادرة بتاريخ 28 أبريل2016

[2] – القانون رقم 15-04 المؤرخ في 01 فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر.ج.ج، ع 06، الصادرة في 10 فبراير 2015.

[3] – Murat Kantarcioglu and Bhavani Thuraisingham, Data Mining for Security Applications, IOS Press, Amsterdam, 2008, pp. 3-12.

[4] Clarence Chio and David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms, O'Reilly Media, 1st Edition, 2018, pp. 1-15.

[5] Soma Halder and Sinan Ozdemir, Hands-On Machine Learning for Cybersecurity, Packt Publishing, 1st Edition, 2018, pp. 9-20.

وقد أشار المعهد الوطني الأمريكي للمعايير والتكنولوجيا NIST إلى أهمية توظيف التعلم الآلي في التحقق من سياسات التحكم في الولوج، لأن هذه السياسات قد تحتوي على أخطاء تؤدي إما إلى منح صلاحيات زائدة أو منع صلاحيات مشروعة. وهذا يبين أن التعلم الآلي لا يقتصر على كشف الهجمات، بل يمتد إلى تحسين البنية الأمنية للنظام ذاته[1].

ومن الناحية التنظيمية، فإن حماية الشبكات والبيانات تتصل كذلك بالقواعد القانونية الخاصة بالتجارة الإلكترونية، خاصة القانون الجزائري رقم 18-05 المتعلق بالتجارة الإلكترونية، لأن المعاملات الإلكترونية لا يمكن أن تتم في بيئة موثوقة إلا إذا كانت البيانات المتبادلة محمية، وكانت هوية الأطراف قابلة للتحقق[2].

وبناء على ذلك، فإن تقنيات التعلم الآلي أصبحت أداة مهمة في تطوير حماية الشبكات والبيانات، لأنها تمنح أنظمة أمن المعلومات قدرة أكبر على التحليل، والاكتشاف، والتنبؤ، والتكيف مع التهديدات الجديدة.

الفرع الثالث: مزايا اعتماد الذكاء الاصطناعي في مجال أمن المعلومات

يتميز اعتماد الذكاء الاصطناعي في مجال أمن المعلومات بعدة مزايا، أهمها السرعة في تحليل البيانات، والقدرة على التعامل مع كميات ضخمة من المعلومات، واكتشاف الأنماط الخفية التي قد يصعب على الإنسان ملاحظتها. كما يساعد الذكاء الاصطناعي على تقليل زمن الاستجابة للحوادث الأمنية، من خلال إصدار تنبيهات فورية أو اقتراح إجراءات وقائية عند ظهور مؤشرات الخطر[3].

ومن مزاياه أيضا أنه يساهم في الانتقال من الحماية التقليدية القائمة على رد الفعل إلى الحماية الاستباقية، حيث لا ينتظر النظام وقوع الهجوم، بل يحاول التنبؤ به من خلال تحليل السلوكيات والمؤشرات السابقة. وهذا يسمح للمؤسسات بتقوية دفاعاتها قبل حدوث الضرر، خاصة في مواجهة الهجمات المعقدة والمتغيرة[4].

---

[1] فينسنت سي. هو، د. ريتشارد كون، ديفيد ف. فيريولو، جيفري فواس، "التعلم الآلي للتحقق من سياسة التحكم في الوصول"، تقرير NIST الداخلي رقم 8360(NISTIR) ، المعهد الوطني للمعايير والتكنولوجيا، 2021، ص 3 .

[2] – القانون رقم 18-05 المؤرخ في 10 مايو 2018، يتعلق بالتجارة الإلكترونية، ج.ر.ج.ج ، ع 28، الصادرة في 16 مايو2018 .

[3] Ethem Alpaydin, Introduction to Machine Learning, MIT Press, 4th Edition, 2020, pp. 1-6.

[4] Sumeet Dua and Xian Du, Data Mining and Machine Learning in Cybersecurity, CRC Press, 1st Edition, 2011, pp. 15-25.

غير أن الاعتماد على الذكاء الاصطناعي في أمن المعلومات لا يخلو من حدود ومخاطر فقد تصدر الأنظمة الذكية إنذارات خاطئة، أو تفشل في كشف هجوم جديد إذا كانت البيانات التي تدربت عليها غير كافية أو غير ممثلة للواقع. كما أن المهاجمين قد يستعملون بدورهم تقنيات الذكاء الاصطناعي لتطوير هجمات أكثر تعقيدا، مثل الهجمات الموجهة ضد نماذج التعلم الآلي أو محاولات خداع الخوارزميات[1].

غير أن الذكاء الاصطناعي يحتاج إلى بينات كثيفة حتى يعمل بكفاءة، وهذا قد يثير إشكالات قانونية وأخلاقية تتعلق بحماية الخصوصية والمعطيات الشخصية لذلك لا يجوز استعماله في مراقبة المستخدمين أو تحليل بياناتهم إلا في إطار مشروع وواضح، يراعي مبدأ الضرورة والتناسب وحماية الحقوق الأساسية[2].

كما أن الذكاء الاصطناعي لا يمكن أن يكون بديلا كاملا عن العنصر البشري، لأن القرار الأمني يحتاج أحيانا إلى تقدير قانوني وتنظيمي لا تستطيع الخوارزميات القيام به وحدها فالأنظمة الذكية يمكنها تقديم مؤشرات وتحليلات، لكنها تحتاج إلى رقابة بشرية للتأكد من صحة النتائج وتفادي التعسف أو الخطأ في استعمالها.

وعليه، فإن الذكاء الاصطناعي يمثل إضافة قوية لوسائل حماية أمن المعلومات، لكنه لا يشكل حلا مطلقا. فنجاحه يتوقف على جودة البيانات، وحسن تصميم الخوارزميات، ووجود رقابة بشرية وقانونية تضمن استعماله بطريقة مشروعة وآمنة.

[1]- أبوستول فاسيليف وآخرون، "التعلم الآلي العدائي: تصنيف ومصطلحات الهجمات وتخفيف حدتها"، منشور الذكاء الاصطناعيNIST AI 100-2e2025 ، المعهد الوطني للمعايير والتكنولوجيا، 2025، الصفحات 4 .

[2]- المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية، ISO/IEC 27701:2019"، التقنيات الأمنية — امتداد لمعياري ISO/IEC 27001 و ISO/IEC 27002 لإدارة معلومات الخصوصية"، المنظمة الدولية للتوحيد القياسي، جنيف، 2019.

خلاصة الفصل الأول:

من خلال هذا الفصل، خلصنا إلى أن أمن المعلومات والذكاء الاصطناعي عنصران مترابطان في ظل التحول الرقمي. ويقوم أمن المعلومات على حماية سرية البيانات وسلامتها وتوافرها بالوسائل التقنية والقانونية لمواجهة مخاطر الاختراقات والأخطاء البشرية.

وقد تبين أن الذكاء الاصطناعي، عبر تقنيات التعلم الآلي والعميق، أصبح أداة فعالة لتعزيز الأمن من خلال الكشف المبكر عن الهجمات، والتنبؤ بالمخاطر، وحماية الشبكات.

وفي الأخير، فإن اعتماد هذه التقنيات يثير تحديات قانونية وأخلاقية تتعلق بالخصوصية والأخطاء الخوارزمية، مما يتطلب إطاراً تنظيمياً واضحاً ورقابة بشرية مستمرة لضمان التوازن بين الأمن السيبراني واحترام الحقوق والحريات.

الفصل الثاني:

الإطار القانوني لحماية أمن المعلومات في ظل الذكاء الاصطناعي

يتمحور هذا الفصل حول المعالجة القانونية لهذا الموضوع، باعتبار أن حماية أمن المعلومات لا يمكن أن تتحقق بالوسائل التقنية وحدها، بل لا بد لها من أساس قانوني يحدد نطاق الحماية، والحقوق محل الحماية، والالتزامات الواقعة على عاتق الدولة والمؤسسات، والجزاءات المترتبة عن الإخلال بهذه الالتزامات.

فأمن المعلومات في ظل الذكاء الاصطناعي لم يعد مجرد مسألة مرتبطة بحماية الأنظمة من الاختراق، بل أصبح موضوعا يمس الحقوق والحريات الأساسية، وعلى رأسها الحق في الخصوصية، وسرية المراسلات، وحماية المعطيات ذات الطابع الشخصي. كما أصبح يرتبط بسيادة الدولة الرقمية، وبحماية البنى التحتية الحساسة، وبضمان استمرارية المرافق العمومية، خاصة في ظل اعتماد المؤسسات على قواعد بيانات وأنظمة معالجة آلية وخوارزميات ذكية قادرة على جمع البيانات وتحليلها والتنبؤ بالسلوكيات واتخاذ قرارات قد تؤثر مباشرة في مراكز الأفراد القانونية.

ومن هنا، فإن الإطار القانوني لحماية أمن المعلومات في ظل الذكاء الاصطناعي يقوم على مستويين متكاملين: مستوى دولي يتجسد في الاتفاقيات والمعايير الدولية المتعلقة بمكافحة الجريمة المعلوماتية، وحماية البيانات، وتنظيم الذكاء الاصطناعي؛ ومستوى وطني يتمثل في النصوص الدستورية والتشريعية والتنظيمية التي تحمي الخصوصية والمعطيات الشخصية وتجرم الاعتداءات الواقعة على الأنظمة المعلوماتية. ويبرز التحدي الأساسي في مدى قدرة هذه القواعد على مواكبة التطور السريع للذكاء الاصطناعي، خصوصا في مسائل المسؤولية، والإثبات، والرقابة، والتوازن بين الأمن والحرية.

سنتطرق في هذا الفصل إلى معالجة التنظيم القانوني لحماية أمن المعلومات في المبحث الأول والمخاطر والآفاق المستقبلية لحماية أمن المعلومات في ظل الذكاء الإصطناعي في المبحث الثاني.

المبحث الأول: التنظيم القانوني لحماية أمن المعلومات

يقصد بالتنظيم القانوني لحماية أمن المعلومات مجموع القواعد القانونية ذات الطبيعة الدستورية والتشريعية والتنظيمية، إضافة إلى الاتفاقيات والمعايير الدولية، التي تهدف إلى حماية المعلومات والأنظمة المعلوماتية من الاعتداءات غير المشروعة، وضمان سلامة المعالجة الرقمية للبيانات، ومنع استعمال التكنولوجيا، بما في ذلك الذكاء الاصطناعي، في المساس بالحقوق والحريات الأساسية.

المطلب الأول: الأساس القانوني الدولي والوطني لحماية أمن المعلومات

يقوم الأساس القانوني لحماية أمن المعلومات على منظومة متعددة المصادر، تجمع بين القانون الدولي، والمعايير التقنية، والقانون الوطني. فالعالم الرقمي بطبيعته لا يعترف بالحدود التقليدية للدولة، إذ يمكن أن تقع الجريمة المعلوماتية في دولة، وتستعمل خوادم موجودة في دولة ثانية.

الفرع الأول: الاتفاقيات والمعايير الدولية في مجال الأمن السيبراني وحماية البيانات

تحتل الاتفاقيات والمعايير الدولية مكانة أساسية في بناء النظام القانوني لحماية أمن المعلومات، لأنها توفر إطارا مرجعيا مشتركا للدول في مواجهة المخاطر السيبرانية التي تتجاوز الحدود الوطنية، "تعد اتفاقية بودابست المتعلقة بالجريمة المعلوماتية لعام 2001 أول صك دولي تناول مكافحة الجرائم التي تمس أمن المعلومات، حيث ألزمت الدول الأطراف بوضع تدابير تشريعية لمواجهة الدخول غير المشروع للأنظمة المعلوماتية[1] ".

فالجريمة المعلوماتية، بخلاف الجريمة التقليدية، تتميز بسرعة التنفيذ، وصعوبة تحديد مكان ارتكابها، وتعدد الفاعلين والضحايا، واعتمادها على أنظمة وشبكات عابرة للدول. لذلك لم يعد ممكنا معالجة أمن المعلومات بمنطق داخلي صرف، بل أصبح التعاون الدولي ضرورة قانونية وعملية لحماية الأنظمة والبيانات والأفراد.

ويجد هذا التوجه أساسه الأول في قواعد القانون الدولي لحقوق الإنسان، خاصة في الحق في الخصوصية. فقد نص الإعلان العالمي لحقوق الإنسان لسنة 1948 في المادة 12 على عدم جواز تعريض أي شخص لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته، كما قرر حق كل شخص في حماية القانون من مثل هذا التدخل. كما كرس العهد الدولي الخاص بالحقوق المدنية والسياسية في المادة 17 الحماية ذاتها ضد التدخل التعسفي أو غير القانوني في الخصوصية والمراسلات والشرف والسمعة. وبذلك فإن حماية أمن

[1] – خالد ممدوح، أمن المعلومات والخصوصية في ظل التحديات السيبرانية، دار الفكر الجامعي، الإسكندرية، ط1، 2021، ص 44.

المعلومات لا تعد مجرد حماية تقنية للبيانات، بل هي امتداد قانوني لحماية الخصوصية والكرامة الإنسانية في البيئة الرقمية[1].

وتعد اتفاقية بودابست بشأن الجريمة المعلوماتية لسنة 2001 من أهم الاتفاقيات الدولية في مجال مكافحة الاعتداءات الواقعة على الأنظمة المعلوماتية. وقد جاءت هذه الاتفاقية لتوحيد التجريم في مجال الجريمة السيبرانية، فنصت على جرائم أساسية مثل الدخول غير المشروع إلى الأنظمة، والاعتراض غير المشروع للبيانات، والاعتداء على سلامة المعطيات، والاعتداء على سلامة النظام، وإساءة استعمال الأجهزة والبرامج، والتزوير والاحتيال المرتبطين بالحاسوب. وتكمن أهمية هذه الاتفاقية في أنها لم تكتف بالجانب الموضوعي للتجريم، بل نظمت أيضا الجوانب الإجرائية، مثل الحفظ العاجل للبيانات المخزنة، والتفتيش والحجز المعلوماتي، وجمع بيانات المرور، كما أقرت آليات التعاون الدولي والمساعدة القضائية وتسليم المجرمين[2].

وتبرز أهمية اتفاقية بودابست في موضوع حفظ أمن المعلومات في ظل الذكاء الاصطناعي من زاويتين: الأولى أنها تشكل أساسا لتجريم الأفعال التي تمس سرية البيانات وسلامتها وتوافرها، وهي العناصر الجوهرية لأمن المعلومات؛ والثانية أنها تضع قواعد للتعاون الدولي في ملاحقة الجريمة السيبرانية، وهو أمر بالغ الأهمية عندما تستعمل تقنيات الذكاء الاصطناعي في تنفيذ الهجمات، أو إخفاء هوية الجاني، أو توليد محتوى احتيالي، أو أتمتة عمليات الاختراق. ومن ثم، فإن هذه الاتفاقية تمثل نموذجا قانونيا مهما، حتى بالنسبة للدول غير الأطراف فيها، لأنها أسهمت في تشكيل المعايير الدولية العامة لمكافحة الجريمة المعلوماتية.

غير أن التطور السريع للجريمة السيبرانية أدى إلى ظهور حاجة دولية أوسع من الإطار الإقليمي لاتفاقية بودابست، وهو ما تجسد في اعتماد الأمم المتحدة لاتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، التي اعتمدتها الجمعية العامة بموجب القرار رقم 243/79 بتاريخ 24 ديسمبر 2024[3]، وفتحت للتوقيع في هانوي يوم 25 أكتوبر 2025، على أن تبقى مفتوحة للتوقيع في مقر الأمم المتحدة بنيويورك إلى غاية 31

[1] – المادة 12 من الإعلان العالمي لحقوق الإنسان، المعتمد من الجمعية العامة للأمم المتحدة بتاريخ 10 ديسمبر 1948؛ والمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية، المعتمد بتاريخ 16 ديسمبر 1966، دخل حيز النفاذ في 23 مارس 1976.

[2] – مجلس أوروبا، "اتفاقية الجرائم السيبرانية"، بودابست، 23 نوفمبر 2001، مجموعة معاهدات أوروبا (ETS) رقم 185، المواد 2، 3، 4، 5، 6، 7، 8، 16، 19، 20، 23.

[3] – الأمم المتحدة، "اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية؛ تعزيز التعاون الدولي لمكافحة جرائم معينة تُرتكب بواسطة نظم تكنولوجيا المعلومات والاتصالات وتبادل الأدلة ذات الشكل الإلكتروني المتعلقة بالجرائم الخطيرة"، اعتُمدت بموجب قرار الجمعية العامة رقم 243/79 في 24 ديسمبر 2024؛ فُتح باب التوقيع عليها في هانوي في 25 أكتوبر 2025؛ وتدخل حيز التنفيذ بعد إيداع الصك الأربعين للتصديق أو القبول أو الموافقة أو الانضمام.

ديسمبر 2026، ولا تدخل حيز النفاذ إلا بعد إيداع الصك الأربعين للتصديق أو القبول أو الموافقة أو الانضمام. وتعد هذه الاتفاقية أول معاهدة عالمية شاملة في هذا المجال، وتهدف إلى تعزيز التعاون الدولي في مكافحة الجرائم المرتكبة بواسطة أنظمة تكنولوجيا المعلومات والاتصال، وتبادل الأدلة الإلكترونية في الجرائم الخطيرة.

وتتجلى قيمة هذه الاتفاقية الأممية في أنها تنقل التعاون الدولي في مجال أمن المعلومات من مستوى المعايير الإقليمية إلى مستوى عالمي أشمل، لأن الجرائم السيبرانية أصبحت تمس جميع الدول بغض النظر عن درجة تطورها التقني. كما أنها تربط بين مكافحة الجريمة المعلوماتية وحفظ الأدلة الإلكترونية، وهو جانب جوهري في ظل الذكاء الاصطناعي، لأن الجريمة قد تترك آثارا رقمية متناثرة ومعقدة، وقد يتم ارتكابها بواسطة أنظمة آلية أو حسابات مزيفة أو أدوات توليد ذكية. غير أن فعالية هذه الاتفاقية ستظل مرتبطة بمدى تصديق الدول عليها، ومدى قدرة التشريعات الوطنية على تكييف أحكامها مع الضمانات الدستورية المتعلقة بالخصوصية وحرية التعبير وحقوق الدفاع.

أما في مجال حماية البيانات الشخصية، فتعد اتفاقية مجلس أوروبا رقم 108 لسنة 1981 أول صك دولي ملزم قانونا في مجال حماية الأفراد تجاه المعالجة الآلية للمعطيات الشخصية. وقد أوجبت هذه الاتفاقية على الدول الأطراف اتخاذ التدابير التشريعية اللازمة لضمان احترام الحقوق والحريات الأساسية للأفراد عند معالجة بياناتهم الشخصية. ثم جرى تحديثها بموجب اتفاقية 108+ لمواجهة التحديات الناتجة عن تطور تكنولوجيات الإعلام والاتصال، وتعزيز فعالية آليات الحماية والتنفيذ.[1]

وتكتسي اتفاقية 108+ أهمية خاصة في مجال الذكاء الاصطناعي، لأن الأنظمة الذكية تعتمد أساسا على جمع البيانات وتحليلها وربطها واستنتاج أنماط منها. ومن ثم، فإن حماية أمن المعلومات في ظل الذكاء الاصطناعي لا تعني فقط حماية النظام من الاختراق، بل تعني كذلك حماية الشخص من المعالجة غير المشروعة لبياناته. فالمبادئ التي تقوم عليها حماية البيانات، مثل المشروعية، والشفافية، وتحديد الغرض، وتقليل البيانات، ودقة المعطيات، وتحديد مدة الحفظ، وأمن المعالجة، تشكل في حقيقتها ضمانات قانونية ضد الانحراف في استعمال الذكاء الاصطناعي.

وفي الإطار الأوروبي، يشكل النظام العام لحماية البيانات المعروف بـGDPR ، الصادر بموجب اللائحة الأوروبية رقم 679/2016، أحد أهم النماذج التشريعية المقارنة في مجال حماية البيانات الشخصية.

[1] – مجلس أوروبا، "اتفاقية حماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي"، مجموعة معاهدات أوروبا (ETS)رقم 108، ستراسبورغ، 28 يناير 1981؛ مجلس أوروبا، "البروتوكول المعدِّل لاتفاقية حماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي"، مجموعة معاهدات أوروبا المحدثة (CETS) رقم 223، عام 2018.

فهو يؤكد على مبادئ جوهرية مثل مشروعية المعالجة، والإنصاف، والشفافية، وتحديد الغرض، وتقليل البيانات، والدقة، وتحديد مدة الاحتفاظ، وسلامة وسرية المعطيات. كما يفرض في المادة 32 اتخاذ تدابير تقنية وتنظيمية مناسبة لضمان مستوى أمني ملائم للمخاطر. ورغم أن هذا النظام أوروبي النطاق، إلا أنه أصبح مرجعا دوليا مهما تستلهم منه العديد من التشريعات الوطنية مبادئ حماية البيانات[1].

وفي مجال الذكاء الاصطناعي تحديدا، برزت مبادئ منظمة التعاون والتنمية الاقتصادية بشأن الذكاء الاصطناعي، التي اعتمدت سنة 2019 وتم تحديثها سنة 2024، باعتبارها أول معيار حكومي دولي للذكاء الاصطناعي الموثوق. وتقوم هذه المبادئ على احترام حقوق الإنسان والقيم الديمقراطية وسيادة القانون، وتعزيز الشفافية، والمتانة، والسلامة، والأمن، والمساءلة. وتكمن أهميتها في أنها تنقل النقاش حول الذكاء الاصطناعي من البعد التقني إلى البعد القانوني والأخلاقي، بحيث لا يكون الذكاء الاصطناعي مقبولا لمجرد فعاليته التقنية، بل يجب أن يكون آمنا، قابلا للمساءلة، ومحترما للحقوق الأساسية[2].

كما اعتمد الاتحاد الأوروبي اللائحة رقم 1689/2024، المعروفة بقانون الذكاء الاصطناعي، وهي أول إطار قانوني شامل لتنظيم الذكاء الاصطناعي وفق مقاربة قائمة على المخاطر. وتقوم هذه المقاربة على التمييز بين أنظمة محظورة بسبب خطورتها غير المقبولة، وأنظمة عالية الخطورة تخضع لالتزامات مشددة، مثل إدارة المخاطر، وجودة البيانات، والتوثيق، والشفافية، والرقابة البشرية، والدقة، والصلابة السيبرانية. وتظهر أهمية هذا القانون في موضوع أمن المعلومات لأنه يجعل الأمن السيبراني جزءا من شروط مشروعية استعمال الأنظمة الذكية، لا مجرد خيار تقني تابع لإرادة المؤسسة[3].

وإلى جانب الاتفاقيات والقواعد القانونية، توجد معايير تقنية دولية تؤدي دورا مهما في حماية أمن المعلومات، خاصة معيار ISO/IEC 27001:2022 المتعلق بنظام إدارة أمن المعلومات، ومعيار ISO/IEC 27002:2022 المتعلق بضوابط أمن المعلومات والأمن السيبراني وحماية الخصوصية. وتكمن أهمية هذه المعايير في أنها لا تنشئ التزامات جزائية أو مدنية مباشرة مثل القوانين، لكنها توفر نموذجا عمليا لإدارة المخاطر، وتحديد الأصول المعلوماتية، ووضع سياسات الحماية، ومراقبة الامتثال، وتحسين نظام الأمن

[1] – اللائحة (الاتحاد الأوروبي) رقم 679/2016 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016، "اللائحة العامة لحماية البيانات"، الجريدة الرسمية للاتحاد الأوروبي، L 119، 4 مايو 2016، المادتان 5 و32.

[2] – منظمة التعاون الاقتصادي والتنمية، "توصية المجلس بشأن الذكاء الاصطناعي"، الوثيقة القانونية رقم OECD/LEGAL/0449، اعتُمدت في عام 2019، وحُدثت في عام 2024.

[3] – اللائحة (الاتحاد الأوروبي) رقم 1689/2024 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 13 يونيو 2024، بشأن وضع قواعد موحدة للذكاء الاصطناعي، وخاصة الأحكام المتعلقة بالتصنيف القائم على المخاطر، وأنظمة الذكاء الاصطناعي عالية المخاطر، والإشراف البشري، والدقة، والمتانة، والأمن السيبراني.

بصورة مستمرة. ولذلك فإنها تعد مرجعا مهما للمؤسسات العامة والخاصة عند بناء نظام قانوني وتنظيمي فعال لحماية أمن المعلومات[1].

كما يعد إطار الأمن السيبراني الصادر عن المعهد الوطني الأمريكي للمعايير والتكنولوجياNIST Cybersecurity Framework 2.0 لسنة 2024 من أهم الأطر المرجعية في إدارة مخاطر الأمن السيبراني. وقد أصبح هذا الإطار يقوم على ست وظائف أساسية هي: الحوكمة، والتحديد، والحماية، والكشف، والاستجابة، والاسترداد. وتظهر قيمة هذا الإطار في أنه يربط أمن المعلومات بالحوكمة وإدارة المخاطر، وهو ما ينسجم مع متطلبات الذكاء الاصطناعي، لأن الخطر لا ينشأ فقط من الهجوم الخارجي، بل قد ينشأ أيضا من طريقة تصميم النظام الذكي، أو نوعية البيانات المستعملة، أو غياب الرقابة البشرية، أو ضعف المساءلة داخل المؤسسة[2].

وعليه، يمكن القول إن الاتفاقيات والمعايير الدولية في مجال الأمن السيبراني وحماية البيانات تؤسس لفكرة جوهرية مفادها أن أمن المعلومات في ظل الذكاء الاصطناعي لا يقوم على الحماية التقنية فقط، بل يقوم على ثلاثية مترابطة: التجريم والتعاون الدولي لمواجهة الاعتداءات السيبرانية، وحماية الخصوصية والبيانات الشخصية عند المعالجة، وإخضاع الأنظمة الذكية لمبادئ الشفافية والمساءلة والرقابة وإدارة المخاطر.

الفرع الثاني: التشريعات الوطنية الخاصة بحماية المعطيات والبيانات الشخصية

تحتل التشريعات الوطنية الخاصة بحماية المعطيات ذات الطابع الشخصي مكانة مركزية في بناء الحماية القانونية لأمن المعلومات، لأنها تمثل الإطار الداخلي الذي يحدد شروط جمع البيانات، ومعالجتها، وتخزينها، واستعمالها، ونقلها، والجزاءات المترتبة عن مخالفة قواعد حمايتها.

وإذا كانت الاتفاقيات والمعايير الدولية ترسم المبادئ العامة، فإن القانون الوطني هو الذي يمنح هذه المبادئ قوة الإلزام داخل الدولة، ويحدد الجهة المختصة بالرقابة، والمسؤول عن المعالجة، وحقوق الشخص المعني، والضمانات الواجب احترامها عند استعمال الوسائل الرقمية أو الذكاء الاصطناعي في معالجة البيانات.

وقد انتقل المشرع الجزائري في مجال حماية المعطيات الشخصية من منطق الحماية التقليدية للحياة الخاصة إلى منطق الحماية الرقمية للمعطيات، وهو ما يظهر من خلال دسترة هذا الحق في المادة 47 من تعديل دستور لسنة 2020، حيث نص المؤسس الدستوري على أن لكل شخص الحق في حماية حياته الخاصة وشرفه، على سرية مراسلاته واتصالاته الخاصة، كما قرر صراحة أن حماية الأشخاص عند معالجة المعطيات ذات الطابع

[1] – مواصفةISO/IEC 27001:2022 ، "أمن المعلومات والأمن السيبراني وحماية الخصوصية — أنظمة إدارة أمن المعلومات — المتطلبات"، المنظمة الدولية للتوحيد القياسي، 2022.

[2] – المعهد الوطني للمعايير والتكنولوجيا، "إطار الأمن السيبراني لـ NIST (الإصدار 2.0)"، وثيقة بيضاء للأمن السيبراني صادرة عنNIST ، بتاريخ 26 فبراير 2024.

الشخصي حق أساسي، وأن القانون يعاقب على كل انتهاك لهذه الحقوق. وبذلك، لم تعد حماية البيانات الشخصية مجرد مسألة تقنية أو إدارية، بل أصبحت حقا دستوريا يرتبط مباشرة بالحقوق والحريات الأساسية[1].

وتكريسا لهذا الأساس الدستوري، صدر القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وهو النص الوطني الأساسي في هذا المجال. ويهدف هذا القانون إلى تحديد قواعد حماية الأشخاص الطبيعيين عند معالجة معطياتهم الشخصية، سواء تمت المعالجة بطريقة آلية كلية أو جزئية، أو بطريقة غير آلية متى كانت المعطيات واردة في ملفات أو قابلة للورود فيها. وبذلك وسع المشرع نطاق الحماية ليشمل كل معالجة منظمة للبيانات، سواء قامت بها هيئة عمومية أو شخص من أشخاص القانون الخاص[2].

و قد أقر المشرع الجزائري من خلال القانون رقم 18-07 في المادتين 17 و 18 من [3]حماية قانونية صارمة للمعطيات ذات الطابع الشخصي، حيث نص على وجوب إخضاع أي عملية معالجة لإذن مسبق من السلطة الوطنية لحماية المعطيات[4]".

وتكمن أهمية القانون رقم 18-07 في أنه وضع تعريفا واسعا للمعطيات ذات الطابع الشخصي، معتبرا إياها كل معلومة بغض النظر عن دعامتها، متعلقة بشخص معرف أو قابل للتعرف عليه، بصورة 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 أو الاقتصادية أو الثقافية أو الاجتماعية. وهذا التعريف الواسع يسمح بإدخال البيانات التي تعتمد عليها أنظمة الذكاء الاصطناعي ضمن دائرة الحماية القانونية، خاصة أن هذه الأنظمة لا تعالج الاسم واللقب فقط، بل قد تعالج الصورة، الصوت، البصمة، الموقع الجغرافي، السلوك الرقمي، والخصائص البيومترية وفقا لما نصت عليه المادة 03 من القانون أعلاه[5].

كما ميز المشرع بين المعطيات الشخصية العادية والمعطيات الحساسة، إذ اعتبر من قبيل المعطيات الحساسة تلك التي تكشف الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي، أو تلك المتعلقة بالصحة أو الحياة الجنسية. وتظهر أهمية هذا التمييز في ظل الذكاء

---

[1] – المادة 47 من التعديل الدستوري لسنة 2020.

[2] – القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – أنظر المادتين 17 و 18 من القانون 18 -07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

[4] – ليلى بن شيخ، "الآليات القانونية لحماية البيانات الشخصية في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، جامعة الوادي، مج 5، ع 2، 2019، ص 112.

[5] – المادة 3 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الاصطناعي لأن بعض الخوارزميات قد تكون قادرة على استنتاج معطيات حساسة من بيانات تبدو في ظاهرها عادية، وهو ما يفرض تشديد الرقابة القانونية على هذا النوع من المعالجة، وعدم السماح به إلا في الحالات التي يجيزها القانون صراحة وفقا لما نصت عليه المواد من 12 إلى 21 من هذا القانون [1].

ومن أهم المبادئ التي يقوم عليها القانون رقم 18-07 مبدأ الموافقة المسبقة، حيث نصت المادة 7 على أنه لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني. وتعد الموافقة هنا ضمانة جوهرية لأنها تعبر عن إرادة الشخص في قبول معالجة بياناته، غير أن هذه الموافقة يجب أن تكون صريحة وحرة ومستنيرة، فلا يكفي مجرد سكوت الشخص أو استعماله لخدمة رقمية للقول بوجود موافقة قانونية. وتزداد أهمية هذا الشرط في ظل الذكاء الاصطناعي، لأن الشخص قد لا يدرك دائما أن بياناته ستستعمل في التدريب الخوارزمي، أو التنبؤ بالسلوك، أو التصنيف الآلي وفقا لما نصت عليه المواد من 22 إلى 30 من هذا القانون[2].

وإلى جانب الموافقة، أقر القانون مبدأ نوعية المعطيات في المادة 9، إذ اشترط أن تكون المعطيات معالجة بطريقة مشروعة ونزيهة، ومجمعة لغايات محددة وواضحة ومشروعة، وألا تعالج لاحقا بطريقة تتنافى مع هذه الغايات، وأن تكون ملائمة ومناسبة وغير مبالغ فيها بالنظر إلى الغايات التي جمعت من أجلها، وأن تكون صحيحة وكاملة ومحينة عند الاقتضاء. وهذه المبادئ تمثل جوهر الحماية القانونية للبيانات، لأنها تمنع المؤسسات من جمع بيانات واسعة دون مبرر، أو استعمالها في أغراض جديدة دون سند قانوني، وهو ما يكتسي أهمية خاصة عند استعمال الذكاء الاصطناعي القائم على تحليل كميات ضخمة من المعلومات وفقا لنص المادة 32 من القانون 18-07 [3].

كما أخضع المشرع بعض عمليات المعالجة لنظام التصريح أو الترخيص المسبق لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي. فالأصل أن المعالجة تخضع لتصريح مسبق، بينما تخضع بعض المعالجات الحساسة أو عالية الخطورة إلى الترخيص. ويظهر من هذا التنظيم أن المشرع لم يكتف بإقرار حقوق لاحقة للشخص المعني، بل وضع رقابة قبلية تهدف إلى منع المعالجة غير المشروعة قبل وقوعها، وهو توجه

[1] – المواد 12 إلى 21 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المواد 22 إلى 30 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

[3] – المادة 32 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

وقائي ينسجم مع طبيعة المخاطر الرقمية التي يصعب إصلاح آثارها بعد تسريب البيانات أو إساءة استعماله وفقا لنصوص المواد 34 و 35 و 36 من القانون 18-07 [1].

وتعد السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي حجر الزاوية في النظام الوطني لحماية البيانات. فقد أنشأ القانون رقم 18-07 هذه السلطة لدى رئيس الجمهورية باعتبارها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والإداري. وتكلف هذه السلطة بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة، كما تتلقى التصريحات، وتمنح التراخيص، وتفصل في الشكاوى، وتأمر بالتغييرات اللازمة، وتطور التعاون مع السلطات الأجنبية المماثلة وذلك لنص المادين 40 و 41 من نفس القانون [2].

وتعزز الطابع المؤسساتي لهذه الحماية بصدور المرسوم الرئاسي رقم 22-187 المؤرخ في 18 ماي 2022، المتضمن تعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، مما سمح بتفعيل هذه الهيئة وإخراجها من مستوى النص القانوني إلى مستوى الممارسة المؤسساتية. ويعد تنصيب هذه السلطة خطوة مهمة في حماية أمن المعلومات، لأن وجود سلطة رقابة مستقلة يسمح بمراقبة الإدارات والمؤسسات والمتعاملين الذين يقومون بمعالجة البيانات، خاصة عندما يتعلق الأمر ببيانات واسعة أو حساسة أو مرتبطة بخدمات رقمية موجهة للجمهور [3].

أما من حيث حقوق الشخص المعني، فقد كرس القانون مجموعة من الضمانات الأساسية، أهمها الحق في الإعلام، والحق في الولوج، والحق في التصحيح، والحق في الاعتراض. فالحق في الإعلام يلزم المسؤول عن المعالجة بإعلام الشخص، مسبقا وبصفة صريحة ودون لبس، بهوية المسؤول عن المعالجة، وأغراض المعالجة، والمرسل إليهم، ومدى إلزامية الرد، وحقوقه، وإمكانية نقل المعطيات إلى بلد أجنبي. وهذا الحق يمثل أساس

[1] – المواد 34 و35 و36 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المادتان 40 و41 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – المرسوم الرئاسي رقم 22-187 المؤرخ في 17 شوال عام 1443 الموافق 18 ماي سنة 2022، المتضمن تعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 35 لسنة 2022.يبين هذا المرسوم الانتقال من النص القانوني إلى التفعيل المؤسساتي للسلطة الوطنية، باعتبارها الجهة المكلفة بالرقابة على احترام قانون حماية المعطيات.

الشفافية، لأن الشخص لا يستطيع حماية بياناته أو الاعتراض على معالجتها إذا لم يكن يعلم أصلا بوجود هذه المعالجة و ذلك وفقا لما جاء في نص المادة 32 من القانون 18-07 [1].

أما الحق في الولوج، فيمنح الشخص المعني إمكانية معرفة ما إذا كانت معطياته الشخصية محل معالجة أم لا، ومعرفة أغراض المعالجة وفئات البيانات والمرسل إليهم، والحصول على معلومات مفهومة حول البيانات الخاصة به ومصدرها. كما يمنحه الحق في التصحيح أو التحيين أو المسح أو الإغلاق عندما تكون البيانات غير صحيحة أو غير كاملة أو معالجتها غير مطابقة للقانون. وهذه الحقوق تكتسي أهمية خاصة في ظل الذكاء الاصطناعي، لأن الخطأ في البيانات قد يؤدي إلى قرارات آلية خاطئة تمس المركز القانوني أو الاجتماعي أو المهني للشخص و ذلك وفقا لما جاء في نصوص المواد 34،35،36 من القانون 18-07 [2].

ومن جهة أخرى، فرض القانون التزامات صارمة من خلال المادتين 40 و41 من القانون 18-07 على المسؤول عن المعالجة والمعالج من الباطن، منها الالتزام بالسر المهني، وعدم معالجة البيانات إلا بناء على تعليمات المسؤول عن المعالجة، واتخاذ تدابير أمنية تقنية وتنظيمية مناسبة لحماية البيانات من الإتلاف أو الضياع أو النشر أو الولوج غير المرخص. وهذه الالتزامات تعكس انتقال التشريع من حماية شكلية للبيانات إلى حماية أمنية فعلية، لأن أمن المعطيات لا يتحقق بمجرد الاعتراف بالحق، بل يتطلب إجراءات عملية تضمن سلامة البيانات وسريتها واستمرارية حمايتها[3].

وقد تعزز هذا الإطار القانوني بصدور القانون **رقم 25-11** المؤرخ في 24 يوليو 2025، المعدل والمتمم للقانون رقم 18-07، حيث أضاف أحكاما أكثر ملاءمة للتحولات الرقمية الحديثة، خاصة ما يتعلق بحقوق الشخص المعني، وانتهاك المعطيات ذات الطابع الشخصي، ومعالجة البيانات لأغراض الوقاية من الجرائم والكشف عنها والتحريات والمتابعات الجزائية، ونقل المعطيات إلى دولة أجنبية أو منظمة دولية. وهذا التعديل يكشف أن المشرع الجزائري بدأ يتجه نحو تحيين قانون حماية البيانات لمواجهة المخاطر الجديدة التي فرضتها الرقمنة والذكاء الاصطناعي[4].

---

[1] – المادة 32 من القانون رقم 18-07، تقر هذه المادة حق الشخص المعني في الإعلام المسبق والصريح بشأن هوية المسؤول عن المعالجة، وأغراضها، والمرسل إليهم، وحقوقه، وهو ما يمثل أساس الشفافية في معالجة البيانات.

[2] – المواد 34 و35 و36 من القانون رقم 18-07، تنظم هذه المواد حق الولوج، وحق التصحيح، وحق الاعتراض، وهي حقوق تسمح للشخص بمراقبة بياناته والتدخل لتصحيحها أو منع استعمالها غير المشروع.

[3] – المواد 40 و41 من القانون رقم 18-07، تقرر هذه المواد التزام السر المهني، وعدم معالجة البيانات إلا وفق تعليمات المسؤول عن المعالجة، وهو ما يعزز حماية البيانات من سوء الاستعمال الداخلي.

[4] – القانون رقم 25-11 المؤرخ في 28 محرم عام 1447 الموافق 24 يوليو 2025، المعدل والمتمم للقانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ومن أهم المستجدات التي جاء بها تعديل 2025 استحداث منصب مندوب حماية المعطيات ذات الطابع الشخصي، حيث يلتزم المسؤول عن المعالجة والسلطة المختصة، كل فيما يخصه، بتعيين مندوب لحماية المعطيات، يختار على أساس كفاءته المهنية ومعرفته المتخصصة بالقانون والممارسات المتعلقة بحماية البيانات. وتظهر أهمية هذا المندوب في كونه آلية داخلية للامتثال القانوني، إذ يسمح بمراقبة مدى احترام المؤسسة لقواعد حماية المعطيات، وتقديم المشورة القانونية والتقنية، وتقليل مخاطر المعالجة غير المشروعة وفقا لنص المادة 41 مكرر من القانون 25-11 [1].

كما أدخل تعديل 2025 من خلال نص المادة 41 مكرر 3 التزاما بمسك دفتر آلي لعمليات المعالجة، يتضمن عمليات الجمع، والتسجيل، والتنظيم، والحفظ، والتغيير، والاستخراج، والاطلاع، والاستعمال، والإرسال، والنشر، والإتاحة، والربط البيني، والتشفير، والمسح، والإتلاف. وتكمن أهمية هذا الدفتر في أنه يخلق أثرا قانونيا وتقنيا للمعالجة، يسمح بتحديد تاريخ العملية ومبرراتها وهوية من قام بها أو اطلع على البيانات أو كشف عنها، وهو ما يشكل ضمانة مهمة في الإثبات والمراقبة والمساءلة عند حدوث خرق أو نزاع[2].

ومن أهم الأحكام الحديثة أيضا إلزام المسؤول عن المعالجة بإجراء دراسة أثر عندما يكون من المحتمل أن يؤدي نوع من المعالجة، خاصة باستعمال تكنولوجيات جديدة، إلى مخاطر عالية على حقوق وحريات الأشخاص الطبيعيين. ويعد هذا الحكم من أكثر الأحكام ارتباطا بالذكاء الاصطناعي، لأن أنظمة الذكاء الاصطناعي غالبا ما تقوم على معالجة واسعة ومعقدة للبيانات، وقد تنتج عنها مخاطر على الخصوصية، أو تمييز خوارزمي، أو تصنيف آلي للأفراد، أو قرارات يصعب تفسيرها. ولذلك فإن دراسة الأثر تسمح بتقدير المخاطر قبل البدء في المعالجة، ووضع الضمانات والتدابير الأمنية المناسبة وفقا للمادة 45 مكرر 6 [3].

كما نظم القانون المعدل في المواد 45 مكرر 8 و مكرر 9 و مكرر 10 مسألة خرق المعطيات ذات الطابع الشخصي، فألزم المسؤول عن المعالجة بإخطار السلطة الوطنية في أجل لا يتجاوز خمسة أيام من علمه بحدوث الخرق، مع بيان طبيعة الخرق، والعواقب المحتملة، والتدابير المتخذة أو المقترح اتخاذها للتخفيف من آثاره. كما يلتزم بتوثيق أي خروقات وآثارها والإجراءات التصحيحية المتخذة، وقد يلزم بإخطار الشخص

[1] – المادة 41 مكرر من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المادة 41 مكرر 3 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

[3] – المادة 45 مكرر 6 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

المعني إذا كان الخرق يحتمل أن يؤدي إلى مخاطر عالية على حقوقه وحرياته. وهذه الأحكام تجعل خرق البيانات واقعة قانونية منتجة لآثار، وليست مجرد حادث تقني داخلي يمكن إخفاؤه [1].

وفيما يتعلق بنقل المعطيات إلى الخارج، وضع المشرع قيودا تهدف إلى منع تحويل البيانات الشخصية إلى دول أو منظمات لا توفر مستوى كافيا من الحماية وذلك وفقا لنص المادة 45 مكرر 13 . وتظهر أهمية هذه القاعدة في ظل الذكاء الاصطناعي، لأن البيانات قد تعالج عبر منصات وخوادم خارج الإقليم الوطني، وقد تستعمل في التدريب أو التحليل أو التخزين السحابي. لذلك فإن نقل البيانات لا يجب أن يخضع فقط لمتطلبات تقنية، بل يجب أن يراعي مستوى الحماية القانونية في الدولة أو المنظمة المتلقية، ومدى وجود ضمانات فعلية لاحترام الحقوق والحريات الأساسية[2].

ولا يمكن عزل حماية المعطيات الشخصية عن باقي التشريعات الوطنية المكملة، خاصة القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، الذي يكتسي أهمية خاصة في حماية الثقة الرقمية، لأن خدمات التصديق الإلكتروني تتطلب جمع بيانات شخصية مرتبطة بهوية الموقع وصحة الشهادة الإلكترونية. كما يفرض هذا القانون أن توجد على التراب الوطني البيانات والمعلومات ذات الطابع الشخصي التي يتم جمعها من طرف مؤدي خدمات التصديق الإلكتروني، وهو ما يعزز حماية البيانات في مجال المعاملات الإلكترونية[3].

كما يعد القانون رقم 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية من النصوص المكملة لحماية البيانات، بالنظر إلى أن خدمات الاتصالات الإلكترونية تشكل الوعاء التقني الذي تمر عبره كميات ضخمة من المعطيات الشخصية. ولذلك فإن حماية سرية الاتصالات، وتنظيم نشاط المتعاملين، وضبط شبكات الاتصال، كلها عناصر ترتبط بشكل مباشر بأمن المعلومات وحماية البيانات، خاصة عندما تستعمل هذه الشبكات في نقل أو تخزين أو معالجة البيانات بواسطة أنظمة ذكية[4].

---

[1] – المواد 45 مكرر 8 و45 مكرر 9 و45 مكرر 10 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المادة 45 مكرر 13 وما يليها من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[3] – القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق 1 فبراير سنة 2015، يرتبط هذا القانون بحماية البيانات في مجال المعاملات الإلكترونية، لأنه ينظم خدمات التصديق والتوقيع الإلكترونيين، وما يرتبط بها من بيانات تعريفية وشهادات رقمية.

[4] – القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، يعد هذا القانون مكملا لحماية المعطيات، لأنه ينظم قطاع الاتصالات الإلكترونية الذي يشكل البنية التقنية لنقل وتبادل البيانات الشخصية والرقمية ج.ر.ج.ج ، ع 27 ، الصادرة بتاريخ 13 مايو 2018

الفرع الثالث: القوانين الوطنية المتعلقة بمكافحة الجرائم المعلوماتية

تعد القوانين الوطنية المتعلقة بمكافحة الجرائم المعلوماتية الامتداد الجزائي والوقائي لحماية أمن المعلومات، لأن حماية المعطيات والبيانات الشخصية لا تكتمل بمجرد الاعتراف بحق الشخص في الخصوصية أو تنظيم شروط المعالجة، بل لا بد من تجريم الأفعال التي تمس الأنظمة المعلوماتية والمعطيات الرقمية، ووضع قواعد إجرائية تسمح بالكشف عن مرتكبيها، وجمع الدليل الإلكتروني، ومتابعة الجرائم التي ترتكب داخل الإقليم الوطني أو تستهدف مصالح الدولة من الخارج.

"إن تجريم –المساس بأنظمة المعالجة الآلية للمعطيات يهدف بالدرجة الأولى إلى حماية سرية وسلامة وتوافر البيانات المخزنة رقمياً، وهو ما نص عليه المشرع في تعديل قانون العقوبات ".

"إن تجريم المساس بأنظمة المعالجة الآلية للمعطيات يهدف بالدرجة الأولى إلى حماية سرية وسلامة وتوافر البيانات المخزنة رقمياً، وهو ما نص عليه المشرع في تعديل قانون العقوبات[1] ".

وقد تعامل المشرع الجزائري مع الجريمة المعلوماتية من خلال مسارين متكاملين: مسار موضوعي يتمثل في تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات ضمن قانون العقوبات، ومسار إجرائي ووقائي يتمثل في القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ويضاف إلى ذلك نصوص مكملة تتصل بحماية المعلومات الإدارية المصنفة، وتنظيم الهيئة الوطنية المختصة بالوقاية من هذه الجرائم ومكافحتها[2].

ويعد قانون العقوبات الجزائري النص الأساسي في التجريم، إذ أدخل المشرع بموجب القانون رقم 04-15 قسما خاصا بعنوان ''المساس بأنظمة المعالجة الآلية للمعطيات''، ضمن المواد من 394 مكرر إلى 394 مكرر 7. ويمثل هذا التعديل نقطة تحول مهمة في السياسة الجنائية الجزائرية، لأنه نقل الاعتداء على النظام المعلوماتي من مجرد فعل تقني إلى جريمة قائمة بذاتها، لها أركانها وعقوباتها وظروف تشديدها. وقد أكدت وثيقة منشورة من وزارة العدل أن هذه المواد خصصت لتجريم صور المساس بأنظمة المعالجة الآلية للمعطيات، خاصة الدخول والبقاء غير المشروع، وحذف أو تغيير المعطيات، وإدخال أو إزالة أو تعديل المعطيات بطريق الغش[3].

وتظهر أهمية المادة 394 مكرر من قانون العقوبات في أنها تجرم فعل الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، حتى ولو لم يترتب عن ذلك ضرر مادي مباشر. وهذا

---

[1] – أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، دار هومة للنشر، الجزائر، ط5 عشر، 2016، ص 302.

[2] – – القانون رقم 24-06، المؤرخ في 19 شوال عام 1445 الموافق لـ 28أبريل سنة 2024، المتضمن قانون العقوبات الجزائري جريدة رسمية العدد 30 الصادرة بتاريخ 30 أبريل 2024 والذي تضمن تعديل وتتميم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966

[3] – المادة 394 مكرر من القانون رقم 24-06، قانون العقوبات الجزائري

يعني أن المشرع اعتبر مجرد اختراق النظام أو البقاء فيه دون حق مساسا بأمن المعلومات، لأن الخطر يبدأ من لحظة كسر الحماية أو تجاوز الترخيص القانوني. كما شدد العقوبة إذا ترتب عن هذا الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة، أو إذا أدى الفعل إلى تخريب نظام اشتغالها، وهو ما يعكس إدراك المشرع للعناصر الجوهرية لأمن المعلومات، وهي السرية والسلامة والتوافر[1].

أما المادة 394 مكرر 1، فتتعلق بصورة أكثر خطورة، وهي إدخال معطيات بطريق الغش في نظام المعالجة الآلية، أو إزالة أو تعديل المعطيات التي يتضمنها النظام. وتكمن خطورة هذه الجريمة في أنها لا تقتصر على الدخول إلى النظام، بل تمتد إلى التأثير في محتوى البيانات ذاتها، وهو ما قد يؤدي إلى تزوير النتائج، أو تعطيل الخدمات، أو تغيير القرارات الإدارية أو المالية أو الأمنية المبنية على تلك البيانات. وتزداد أهمية هذا النص في ظل الذكاء الاصطناعي، لأن الأنظمة الذكية تعتمد في نتائجها على جودة وسلامة البيانات؛ فإذا تم تلويث البيانات أو تعديلها أو إدخال بيانات مضللة، فقد تصدر الخوارزمية قرارات خاطئة أو تمييزية أو خطيرة[2].

كما عالجت المادة 394 مكرر 2 جانبا مهما من الجرائم المعلوماتية، يتمثل في تجريم تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، متى كان من شأنها تمكين ارتكاب الجرائم المنصوص عليها في هذا القسم. كما جرمت حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى هذه الجرائم. وتكمن قوة هذا النص في أنه لا ينتظر وقوع الاختراق النهائي، بل يجرم الأعمال التحضيرية والأدوات والبيانات التي تسهل ارتكاب الجريمة، وهو ما ينسجم مع طبيعة الجرائم السيبرانية التي غالبا ما تسبقها مراحل إعداد وتجميع ونشر أدوات الاختراق أو قواعد البيانات المسروقة[3].

ولم يغفل المشرع الجزائري حماية المصالح العليا للدولة، إذ نصت المادة 394 مكرر 3 على مضاعفة العقوبات إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام. ويعد هذا التشديد مبررا من الناحية القانونية، لأن الاعتداء على أنظمة المؤسسات العمومية أو الدفاع الوطني لا يمس مصلحة فردية فقط، بل قد يهدد الأمن الوطني، واستمرارية المرفق العام، وسلامة المعلومات السيادية. وتكتسي

[1] – المادة 394 مكرر من القانون رقم 24-06، قانون العقوبات الجزائري تجرم هذه المادة الدخول أو البقاء غير المشروع في منظومة المعالجة الآلية للمعطيات، وتشدد العقوبة إذا ترتب عن الفعل حذف أو تغيير للمعطيات أو تخريب نظام اشتغال المنظومة.

[2] – المادة 394 مكرر 1 من القانون رقم 24-06، قانون العقوبات الجزائري

[3] – المادة 394 مكرر 2 من القانون رقم 24-06، قانون العقوبات الجزائري

هذه القاعدة أهمية خاصة في ظل الذكاء الاصطناعي، لأن الهجمات السيبرانية الحديثة قد تستهدف قواعد بيانات إدارية، أو أنظمة مراقبة، أو بنيات تحتية حيوية، أو شبكات تسيير خدمات عمومية[1].

كما أقر قانون العقوبات مسؤولية الشخص المعنوي عن الجرائم المعلوماتية، إذ نصت المادة 394 مكرر 4 على معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي. وتظهر أهمية هذه القاعدة في أن الجرائم المعلوماتية قد ترتكب أحيانا باسم شركات أو مؤسسات أو مزودي خدمات أو كيانات رقمية، وليس فقط من طرف أفراد طبيعيين. ومن ثم، فإن إقرار مسؤولية الشخص المعنوي يسمح بتوسيع نطاق المساءلة، خاصة عندما يكون الإخلال ناتجا عن سياسة مؤسساتية أو تقصير تنظيمي في حماية الأنظمة والمعطيات[2].

وإلى جانب النصوص الموضوعية في قانون العقوبات، جاء القانون رقم 09-04 ليضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وتظهر أهميته في أنه لم يكتف بتجريم الأفعال، بل وضع منظومة إجرائية خاصة تراعي طبيعة الجريمة المعلوماتية، من حيث صعوبة اكتشافها، وسرعة ارتكابها، وإمكانية تنفيذها عن بعد، وارتباطها بأدلة رقمية قابلة للإخفاء أو المحو أو التغيير في وقت قصير. وقد عرف هذا القانون المنظومة المعلوماتية بأنها نظام منفصل أو مجموعة أنظمة متصلة أو مرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، كما عرف المعطيات المعلوماتية ومقدمي الخدمات ومعطيات حركة السير والاتصالات الإلكترونية[3].

وتكمن القيمة القانونية للقانون رقم 09-04 في أنه وضع قواعد المراقبة الإلكترونية، مع إحاطتها بضمانات قانونية. فقد أجازت المادة 3، مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية، وذلك لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية. غير أن المادة 4 قيدت هذه المراقبة بحالات محددة، منها الوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو عند احتمال وقوع اعتداء على منظومة معلوماتية يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات التحقيقات القضائية،

[1] – المادة 394 مكرر 3 من القانون رقم 24-06، قانون العقوبات الجزائري

[2] – المادة 394 مكرر 4 من القانون رقم 24-06، قانون العقوبات الجزائري

[3] – المادة 2 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أو في إطار المساعدة القضائية الدولية. والأهم أن المشرع اشترط الإذن المكتوب من السلطة القضائية المختصة، وهو ما يحقق التوازن بين فعالية التحري وحماية الحقوق الدستورية في السرية والخصوصية[1].

كما نظم القانون رقم 09-04 إجراءات تفتيش المنظومات المعلوماتية، حيث أجازت المادة 5 للسلطات القضائية المختصة وضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا إلى المعطيات المخزنة فيها، أو إلى منظومة تخزين معلوماتية. ويعد هذا النص مهما لأنه يعترف بالطبيعة الخاصة للدليل الإلكتروني، الذي قد لا يوجد في مكان مادي واحد، بل قد يكون مخزنا في خادم بعيد أو منظومة مرتبطة بمنظومة أخرى. لذلك أجاز القانون تمديد التفتيش إلى منظومة أخرى متى كانت المعطيات المطلوبة قابلة للدخول إليها انطلاقا من المنظومة الأولى، مع إعلام السلطة القضائية المختصة [2].

وتظهر خصوصية الجريمة المعلوماتية أيضا في قواعد الحجز، إذ نصت المادة 6 على أنه عندما تكتشف السلطة التي تباشر التفتيش معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث والمعطيات اللازمة لفهمها على دعامة تخزين إلكترونية قابلة للحجز والوضع في أحراز. كما أوجب النص على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات، ومنع المساس بمحتواها. وتعد هذه القاعدة جوهرية من زاوية الإثبات، لأن الدليل الإلكتروني لا تكون له قيمة قانونية إذا لم تثبت سلامته، أو إذا أمكن التشكيك في تغييره أو العبث به أثناء الحجز أو النقل أو التخزين وفقا لنص المواد 7 و 8 و 9 من القانون رقم 09-04 [3].

كما أقر القانون رقم 09-04 نظاما خاصا لحفظ معطيات حركة السير، حيث ألزمت المادة 11 مقدمي الخدمات بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، والخصائص التقنية وتاريخ ووقت ومدة كل اتصال، والمعطيات المتعلقة بالخدمات التكميلية، والمعطيات التي تسمح بالتعرف على المرسل إليه أو عناوين المواقع المطلع عليها. وحدد القانون مدة الحفظ بسنة واحدة ابتداء من تاريخ التسجيل. وتكمن أهمية هذا الالتزام في أن معطيات حركة السير قد تكون

[1] – المادتان 3 و4 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] – المادة 5 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] – المواد 6 و7 و8 و9 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أحيانا الوسيلة الوحيدة لتحديد مصدر الهجوم، أو تتبع مسار الاتصال، أو ربط الفعل الإجرامي بشخص أو جهاز أو حساب معين[1].

غير أن إلزام مقدمي الخدمات بحفظ المعطيات لا يعني إطلاق يدهم في جمع البيانات أو استعمالها، بل يبقى مقيدا بالغرض القانوني وبالضمانات القضائية، لأن هذه المعطيات قد تكشف أنماط الاتصال، والمواقع، والأوقات، والعلاقات الرقمية للأشخاص. لذلك فإن استعمالها يجب أن يتم في حدود التحقيق أو التحري، ووفق مبدأ الضرورة والتناسب. وهذا التوازن مهم جدا في ظل الذكاء الاصطناعي، لأن تحليل معطيات حركة السير بواسطة خوارزميات ذكية قد يسمح باستخلاص معلومات دقيقة عن سلوك الأفراد، مما يفرض رقابة قانونية صارمة على طرق المعالجة والاستغلال.

ومن جهة أخرى، فرض القانون رقم 09-04 التزامات خاصة على مقدمي خدمات الإنترنت، إذ ألزمت المادة 12 هؤلاء بالتدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم، بطريقة مباشرة أو غير مباشرة، بمخالفتها للقوانين، أو تخزينها، أو جعل الدخول إليها غير ممكن. كما ألزمتهم بوضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة، وإخبار المشتركين لديهم بوجودها. وتظهر أهمية هذا النص في أنه يجعل مزود الخدمة شريكا في الوقاية من المحتوى غير المشروع، دون أن يعفي الدولة من ضرورة احترام الضمانات القانونية والقضائية[2].

وتعزز الإطار المؤسساتي لمكافحة الجرائم المعلوماتية بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بموجب المادة 13 من القانون رقم 09-04. وقد كلفت المادة 14 هذه الهيئة بتنشيط وتنسيق عمليات الوقاية من هذه الجرائم ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، وتبادل المعلومات مع نظيراتها في الخارج قصد التعرف على مرتكبي الجرائم وتحديد مكان وجودهم. وهذه المهام تجعل الهيئة آلية متخصصة تجمع بين البعد التقني والبعد القضائي والبعد الدولي[3].

[1] – المادة 11 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] – المادة 12 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] – المواد 13 إلى 18 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وقد أعيد تنظيم هذه الهيئة بموجب المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر 2021، الذي اعتبرها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي وتوضع لدى رئيس الجمهورية. كما بين المرسوم أن الهيئة تمارس مهامها تحت رقابة السلطة القضائية، طبقا لقانون الإجراءات الجزائية والقانون رقم 09-04، وتكلف خصوصا بتحديد الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتنشيط وتنسيق عمليات الوقاية، وضمان المراقبة الوقائية للاتصالات الإلكترونية تحت سلطة القاضي المختص، وتجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها لاستعمالها في الإجراءات القضائية[1].

وتتضح علاقة هذه النصوص بموضوع أمن المعلومات في ظل الذكاء الاصطناعي من خلال أن الذكاء الاصطناعي يمكن أن يكون وسيلة للكشف عن الجرائم المعلوماتية، كما يمكن أن يكون أداة لارتكابها. فمن جهة، يمكن استعماله في تحليل سجلات الاتصال، واكتشاف محاولات الاختراق، والتعرف على الأنماط غير العادية. ومن جهة أخرى، يمكن استعماله في توليد هجمات تصيد أكثر إقناعا، أو إنشاء برمجيات خبيثة، أو تحليل ثغرات الأنظمة، أو انتحال الهوية، أو التلاعب بالبيانات. لذلك فإن النصوص الجزائية التقليدية المتعلقة بالدخول غير المشروع وتغيير المعطيات واستعمال أدوات الاختراق تبقى قابلة للتطبيق، لكنها تحتاج إلى قراءة حديثة تراعي طبيعة الأنظمة الذكية وخطورة الجرائم الخوارزمية.

كما يجب الإشارة إلى الأمر رقم 21-09 المتعلق بحماية المعلومات والوثائق الإدارية، لأنه يمثل نصا مكملا في حماية المعلومات داخل المؤسسات العمومية. فإذا كان قانون العقوبات والقانون رقم 09-04 يركزان على الجرائم المعلوماتية والأنظمة الرقمية، فإن الأمر رقم 21-09 يهتم بحماية المعلومات والوثائق الإدارية ذات الطابع الحساس أو المصنف.

[1] – المرسوم الرئاسي رقم 21-439 المؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، ع 86، الصادرة بتاريخ 11 نوفمبر 2021، يعيد هذا المرسوم تنظيم الهيئة الوطنية ويمنحها صفة سلطة إدارية مستقلة، ويحدد مهامها في الاستراتيجية الوطنية، والمراقبة الوقائية تحت سلطة القاضي، وتجميع وحفظ المعطيات الرقمية لأغراض قضائية.

وتظهر أهمية هذا النص في سياق أمن المعلومات لأن الإدارات العمومية أصبحت تعتمد على الوثائق الرقمية والمنصات الإلكترونية، مما يجعل تسريب الوثائق أو نشرها أو تداولها خارج القنوات القانونية خطرا على الأمن الإداري والمؤسساتي للدولة[1].

وعليه، يمكن القول إن القوانين الوطنية المتعلقة بمكافحة الجرائم المعلوماتية في الجزائر تقوم على منظومة متعددة المستويات: قانون العقوبات يحدد الأفعال المجرمة والعقوبات، والقانون رقم 09-04 يضع الآليات الإجرائية والوقائية الخاصة بالتحري والحجز والمراقبة وحفظ المعطيات، والهيئة الوطنية المختصة تضطلع بالتنسيق والخبرة والتعاون، أما النصوص المكملة مثل الأمر رقم 21-09 فتوسع الحماية إلى المعلومات والوثائق الإدارية. غير أن التحدي الحقيقي في ظل الذكاء الاصطناعي لا يكمن فقط في وجود النصوص، بل في مدى قدرتها على استيعاب الجرائم الجديدة التي ترتكب بواسطة أنظمة ذكية، وفي مدى احترامها في الوقت نفسه للضمانات الدستورية، خاصة الخصوصية، وسرية الاتصالات، وحقوق الدفاع، والرقابة القضائية.

المطلب الثاني: الحماية القانونية للخصوصية والبيانات الشخصية

تعد الحماية القانونية للخصوصية والبيانات الشخصية من أهم مظاهر حماية أمن المعلومات في ظل الذكاء الاصطناعي، لأن الاعتداء على أمن المعلومات لا يقتصر على اختراق الأنظمة أو تعطيلها، بل يمتد إلى المساس بالحياة الخاصة للأفراد، وكشف بياناتهم، وتحليل سلوكهم، واستعمال معلوماتهم الشخصية في غير الأغراض التي جمعت من أجلها. فالمعلومة الشخصية في البيئة الرقمية لم تعد مجرد بيان بسيط يدل على هوية الشخص، بل أصبحت قابلة للربط والتحليل والاستنتاج بواسطة تقنيات الذكاء الاصطناعي، بما يسمح بتكوين صورة دقيقة عن الحياة الخاصة، والعادات، والميول، والتنقلات، والخيارات المهنية أو الصحية أو الاجتماعية.

ومن هذا المنطلق، فإن الحماية القانونية للخصوصية والبيانات الشخصية تقوم على ثلاث ركائز أساسية: أولا، الاعتراف بالحق في الخصوصية الرقمية باعتباره حقا دستوريا وأساسيا؛ ثانيا، وضع ضمانات قانونية تنظم جمع البيانات ومعالجتها وحفظها ونقلها؛ وثالثا، ترتيب المسؤولية القانونية عند انتهاك أمن المعلومات أو خرق الخصوصية. وهذا يعني أن حماية البيانات في ظل الذكاء الاصطناعي لا تقوم فقط على الوسائل التقنية، بل تقوم قبل ذلك على مبدأ الشرعية، والشفافية، والتناسب، والمساءلة، والرقابة القضائية والإدارية.

[1] – الأمر رقم 21-09 المؤرخ في 27 شوال عام 1442 الموافق 8 يونيو سنة 2021، المتعلق بحماية المعلومات والوثائق الإدارية، ج.ر.ج.ج، ع 45، الصادرة بتاريخ 9 يونيو 2021، يمثل هذا الأمر نصا مكملا لحماية أمن المعلومات داخل المؤسسات العمومية، لأنه ينظم حماية المعلومات والوثائق الإدارية، خاصة ذات الطابع الحساس أو المصنف، ويقرر لها آليات حماية ومسؤولية.

الفرع الأول: الأساس القانوني للحق في الخصوصية الرقمية

يقصد بالخصوصية الرقمية حق الشخص في السيطرة القانونية على بياناته ومعطياته الشخصية داخل البيئة الإلكترونية، ومنع الغير من جمعها أو معالجتها أو استعمالها أو نقلها إلا وفق الشروط التي يحددها القانون. ويختلف هذا الحق عن الخصوصية التقليدية من حيث موضوع الحماية، ذلك أن الخصوصية التقليدية كانت تتعلق أساسا بحرمة المسكن والمراسلات والحياة الخاصة، أما الخصوصية الرقمية فتتعلق بالبيانات التي يتركها الشخص أثناء استعماله للخدمات الرقمية، مثل بيانات الهوية، والموقع الجغرافي، والصورة، والصوت، والبصمة، وسجلات الاتصال، وسلوك التصفح، والمعاملات الإلكترونية.

الحق في الخصوصية الرقمية هو امتداد للحق في حرمة الحياة الخاصة، ويقصد به حق الفرد في التحكم في تدفق معلوماته الشخصية ومنع الغير من الاطلاع عليها دون وجه حق [1] ".

وقد أصبح الحق في الخصوصية الرقمية في الجزائر ذا أساس دستوري صريح، حيث نصت المادة 47 من التعديل الدستوري 2020 على أن لكل شخص الحق في حماية حياته الخاصة وشرفه، وأن لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة، أيا كان شكلها، كما نصت صراحة على أن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي، وأن القانون يعاقب على كل انتهاك لهذه الحقوق. وبذلك، لم تعد حماية البيانات الشخصية مجرد حماية تشريعية عادية، بل أصبحت حقا دستوريا يرتبط مباشرة بكرامة الإنسان وحرياته الأساسية[2].

وتكمن أهمية هذا الأساس الدستوري في أنه يفرض على كل سلطة عامة أو مؤسسة أو متعامل اقتصادي أو مسؤول عن المعالجة أن يحترم حدود الشرعية عند التعامل مع بيانات الأفراد. فالإدارة، مثلا، لا يجوز لها أن تجمع أو تستعمل بيانات المواطنين لمجرد سهولة الوسائل التقنية أو توفر الأنظمة الذكية، بل يجب أن تستند إلى نص قانوني، وأن تحترم الغرض المحدد من المعالجة، وألا تستعمل البيانات إلا بالقدر الضروري لتحقيق المصلحة المشروعة. ومن ثم، فإن أي استعمال للذكاء الاصطناعي يمس البيانات الشخصية يجب أن يخضع لرقابة قانونية دقيقة، لأنه قد يتحول من وسيلة لتحسين الخدمة أو الأمن إلى أداة مراقبة أو تصنيف أو تتبع للأشخاص.

ويجد الحق في الخصوصية الرقمية امتداده التشريعي القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث عرف المشرع المعطيات الشخصية تعريفا

[1] – محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، ط 2، 2012، ص 88.

[2] – المادة 47 من التعديل الدستوري لسنة 2020 .

واسعا يشمل كل معلومة متعلقة بشخص معرف أو قابل للتعرف عليه، بصورة مباشرة أو غير مباشرة، لا سيما بالرجوع إلى رقم التعريف أو إلى عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية

أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية. وتظهر قوة هذا التعريف في أنه يستوعب المعطيات التي تعتمد عليها أنظمة الذكاء الاصطناعي، بما في ذلك البيانات البيومترية والسلوكية والاستنتاجية[1].

كما يتأكد الأساس القانوني للخصوصية الرقمية من خلال ربط حماية البيانات بفكرة ''المعالجة''، لأن الخطر في البيئة الرقمية لا ينشأ فقط من كشف البيانات، بل ينشأ كذلك من جمعها، وتنظيمها، وحفظها، وتعديلها، وربطها، وتحليلها، ونقلها، واستعمالها في اتخاذ القرار. ولهذا أخضع القانون رقم 25-11 المعالجة الآلية الكلية أو الجزئية للمعطيات الشخصية، وكذلك المعالجة غير الآلية عندما تكون البيانات واردة في ملفات أو قابلة للورود فيها، لأحكامه، سواء قامت بها هيئات عمومية أو خواص. وبذلك وسع المشرع نطاق الحماية ليشمل مختلف صور التعامل مع البيانات، لا مجرد النشر أو الإفشاء[2].

وتزداد أهمية هذا الأساس القانوني في ظل الذكاء الاصطناعي، لأن هذه التقنية لا تكتفي باستعمال البيانات في صورتها الخام، بل قد تستخلص منها نتائج وتوقعات وتصنيفات تؤثر في الشخص المعني. وقد عالج المشرع الجزائري هذه المسألة في التعديل الأخير للقانون رقم 18-07، من خلال القانون 25-11 حيث نص على أنه لا يمكن أن تؤسس الأحكام القضائية التي تقتضي تقييما لسلوك شخص على مجرد المعالجة الآلية للمعطيات الشخصية المتضمنة تقييم بعض جوانب شخصيته، كما لا يمكن لأي قرار آخر ينشئ آثارا قانونية تجاه شخص أن يتخذ فقط بناء على مجرد معالجة آلية يكون الغرض منها تحديد صفات الشخص المعني أو تقييم بعض جوانب شخصيته. وهذا الحكم يعد من أهم الضمانات القانونية ضد مخاطر القرار الخوارزمي المجرد[3].

وعليه، فإن الأساس القانوني للحق في الخصوصية الرقمية يقوم على حماية دستورية من جهة، وحماية تشريعية تفصيلية من جهة أخرى. فهو حق دستوري لأنه يرتبط بالحياة الخاصة وسرية الاتصالات، وهو حق تشريعي لأنه يترجم إلى قواعد عملية تتعلق بالموافقة، والغرض، والتصريح، والترخيص، وحقوق الشخص المعني، والرقابة، والمسؤولية. ومن ثم، فإن أي استعمال للذكاء الاصطناعي في معالجة البيانات يجب أن يقرأ في ضوء هذا الأساس، لا في ضوء الفعالية التقنية فقط.

---

[1] – المادة 3 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[2] – المادة 4 من القانون رقم 25-11المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – المادة 45 مكرر 1 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الفرع الثاني: الضمانات القانونية لمعالجة وحماية البيانات الشخصية

لا تتحقق حماية البيانات الشخصية بمجرد الاعتراف بالحق في الخصوصية، بل لا بد من ضمانات قانونية عملية تقيد المسؤول عن المعالجة وتمنح الشخص المعني وسائل قانونية للدفاع عن بياناته. "تتمثل أهم ضمانات المعالجة في مبدأ 'الشفافية' ومبدأ 'التناسب'، بحيث لا يتم جمع من البيانات إلا ما كان ضرورياً للغرض الذي جمعت من أجله، مع ضمان حق صاحب البيانات في الولوج والتصحيح[1] ".

وتقوم هذه الضمانات في القانون الجزائري على مجموعة من المبادئ، أهمها الموافقة، والمشروعية، والشفافية، وتحديد الغرض، وتقليل البيانات، والتصريح أو الترخيص المسبق، والرقابة من طرف السلطة الوطنية، وحق الشخص في الإعلام والولوج والتصحيح والاعتراض.

وتعد الموافقة الصريحة من أهم الضمانات القانونية، حيث نص القانون رقم 25-11 على أنه لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني، ما لم يوجد استثناء قانوني. وتكتسي الموافقة أهمية خاصة في ظل الذكاء الاصطناعي، لأن الشخص قد يوافق على استعمال خدمة رقمية دون أن يعلم أن بياناته ستستعمل في التدريب الخوارزمي، أو التنبؤ بالسلوك، أو التصنيف الآلي. لذلك يجب أن تكون الموافقة حرة ومستنيرة ومحددة، لا مفترضة ولا غامضة ولا مستخلصة من مجرد السكوت[2].

وإلى جانب الموافقة، يفرض القانون مبدأ نوعية المعطيات، وهو من أقوى الضمانات الموضوعية لحماية البيانات. فالمعطيات يجب أن تعالج بطريقة مشروعة ونزيهة وفقا لنص المادة 09 من القانون 25-11 ، وأن تجمع لغايات محددة وواضحة ومشروعة، وألا تعالج لاحقا بطريقة تتنافى مع تلك الغايات، وأن تكون ملائمة ومناسبة وغير مبالغ فيها بالنظر إلى الغرض من جمعها، وأن تكون صحيحة وكاملة ومحينة عند الاقتضاء. ويعني ذلك أن المؤسسة لا تملك حرية مطلقة في جمع البيانات بحجة تحسين الخدمة أو دعم الأمن المعلوماتي، بل يجب أن تلتزم بالقدر الضروري والمناسب فقط[3].

وتبرز أهمية هذه القاعدة في مجال الذكاء الاصطناعي لأن الخوارزميات تحتاج غالبا إلى كميات كبيرة من البيانات، وهو ما قد يغري المؤسسات بجمع معطيات واسعة دون تحديد دقيق للغرض. غير أن منطق القانون يختلف عن منطق التقنية؛ فالتقنية تبحث عن أكبر قدر من البيانات لتحسين الأداء، أما القانون فيبحث عن

---

[1] – وفاء شويتامي، الحماية القانونية للبيانات الشخصية في المعاملات الإلكترونية، مذكرة ماجستير، كلية الحقوق، جامعة بن يوسف بن خدة (الجزائر 1)، 2015، ص 56.

[2] – لمادة 7 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[3] – المادة 9 من القانون 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

أقل قدر مشروع وضروري لتحقيق الغرض. ومن هنا يظهر مبدأ التناسب باعتباره حاجزا قانونيا ضد الإفراط في جمع البيانات واستعمالها.

ومن الضمانات المهمة كذلك نظام التصريح والترخيص المسبق لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي. فبعض عمليات المعالجة تخضع للتصريح، بينما تخضع عمليات أخرى للترخيص، خاصة إذا تعلقت بمعطيات حساسة، أو بنقل البيانات إلى الخارج، أو بعمليات معالجة ذات أثر خاص على الحقوق والحريات. وهذا النظام الوقائي يسمح بمراقبة المعالجة قبل تنفيذها، وليس بعد وقوع الضرر فقط، وهو أمر ضروري لأن خرق البيانات قد يؤدي إلى أضرار يصعب إصلاحها وفقا لما جاء في نص المواد من 12 إلى 21 من القانون 25-11 [1].

وتضطلع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بدور جوهري في ضمان هذه الحماية، إذ كلفها القانون بالسهر على مطابقة معالجة المعطيات الشخصية لأحكام القانون، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة طبقا للمادة 25 من القانون 25-11. كما تتولى منح التراخيص، وتلقي التصريحات، وإعلام الأشخاص بحقوقهم، وتلقي الشكاوى والطعون، والأمر بالتغييرات اللازمة، وإغلاق المعطيات أو سحبها أو إتلافها، ووضع معايير حماية المعطيات[2].

أما من جهة الشخص المعني، فقد منحه القانون عدة حقوق تشكل ضمانات مباشرة، أهمها الحق في الإعلام، والحق في الولوج، والحق في التصحيح، والحق في الاعتراض. فالحق في الإعلام يفرض على المسؤول عن المعالجة أن يعلم الشخص مسبقا بهوية المسؤول عن المعالجة، وأغراض المعالجة، والمرسل إليهم، ومدى إلزامية الإجابة، وحقوقه، وإمكانية نقل المعطيات إلى الخارج. ويمثل هذا الحق أساس الشفافية، لأن الشخص لا يستطيع ممارسة حقوقه إذا كان يجهل وجود المعالجة أو غرضها أو الجهة التي تقوم بها طبقا للمادة 32 و ما يليها من القانون [3].

كما يكتسي الحق في الولوج والتصحيح والاعتراض أهمية خاصة في ظل الذكاء الاصطناعي، لأن الخطأ في البيانات قد يؤدي إلى نتائج آلية خاطئة، مثل رفض خدمة، أو تصنيف شخص تصنيفا غير عادل،

[1] – المواد 12 إلى 21 من القانون رقم 25 –11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المادة 25 من القانون 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

[3] – المواد 32 و34 و35 و36 من القانون 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

أو ربطه بخطر أمني غير حقيقي. لذلك فإن تمكين الشخص من الاطلاع على بياناته وتصحيحها والاعتراض على معالجتها يشكل ضمانة قانونية ضد الخطأ الخوارزمي وضد الاستعمال غير المشروع للبيانات.

وقد عزز المشرع الجزائري هذه الضمانات بموجب التعديل الأخير للقانون رقم 25-11 ، حيث أوجب تعيين مندوب لحماية المعطيات ذات الطابع الشخصي، يختار على أساس كفاءته المهنية ومعرفته المتخصصة بالقانون والممارسات المتعلقة بحماية البيانات وفقا لنص المادة 41 مكرر . وتظهر أهمية هذا المندوب في كونه آلية داخلية للامتثال، يتولى مراقبة احترام قواعد الحماية، وتقديم المشورة، والتحسيس، والتكوين، والتواصل مع السلطة الوطنية[1].

كما أوجب القانون مسك سجل نشاطات المعالجة ودفتر آلي لعمليات المعالجة طبقا للمادة 41 مكرر من القانون 25-11 ، يتضمن عمليات الجمع، والتسجيل، والتنظيم، والحفظ، والتغيير، والاستخراج، والاطلاع، والاستعمال، والإرسال، والنشر، والربط البيني، والتشفير، والمسح، والإتلاف. وتكمن أهمية هذه السجلات في أنها تحقق مبدأ التتبع والمساءلة، إذ تسمح بمعرفة من عالج البيانات، ومتى تمت المعالجة، وما هو مبررها، ومن اطلع عليها أو كشف عنها. وهذه الضمانة مهمة جدا في مجال أمن المعلومات، لأنها تساعد على كشف الخرق وتحديد المسؤول عنه[2].

ومن أهم الضمانات المستحدثة أيضا إلزام المسؤول عن المعالجة بإجراء دراسة أثر عندما يكون من المحتمل أن يؤدي نوع من المعالجة، لا سيما باستعمال تكنولوجيات جديدة، إلى مخاطر عالية على حقوق وحريات الأشخاص الطبيعيين وفقا للمادة 45 مكرر 6 من القانون . ويعد هذا الحكم من أكثر الأحكام ارتباطا بالذكاء الاصطناعي، لأن الأنظمة الذكية تقوم غالبا على معالجة واسعة ومعقدة وغير شفافة للبيانات. لذلك تسمح دراسة الأثر بتقييم المخاطر قبل بدء المعالجة، وتحديد التدابير الأمنية والتنظيمية الكفيلة بتقليلها[3].

كما ألزم القانون المسؤول عن المعالجة أو المعالج من الباطن بوضع التدابير التقنية والتنظيمية الداخلية الملائمة لحماية المعطيات الشخصية من الإتلاف العرضي أو غير المشروع، أو الضياع، أو التلف، أو النشر، أو الولوج غير المرخص، خاصة عندما يتم إرسال البيانات عبر شبكة معينة. وهذا الحكم يربط بوضوح بين

[1] – المادة 41 مكرر من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المادة 41 مكرر من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – المادة 45 مكرر 6 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

حماية البيانات وأمن المعلومات، لأن حماية الخصوصية لا تتحقق إلا إذا كانت البيانات محمية تقنيا وتنظيميا ضد الاختراق والتسريب وسوء الاستعمال[1].

وعليه، فإن الضمانات القانونية لمعالجة وحماية البيانات الشخصية في القانون الجزائري لم تعد تقتصر على الموافقة والتصريح فقط، بل أصبحت تشمل منظومة متكاملة تقوم على الشفافية، والرقابة، والتوثيق، ودراسة الأثر، والتدابير الأمنية، ومندوب حماية المعطيات، وحقوق الشخص المعني. وهذه الضمانات تمثل الأساس القانوني الذي يجب أن يخضع له استعمال الذكاء الاصطناعي في المؤسسات العامة والخاصة.

الفرع الثالث: المسؤولية القانونية عن انتهاك أمن المعلومات وخرق الخصوصية

تعد المسؤولية القانونية النتيجة الطبيعية لأي انتهاك لأمن المعلومات أو خرق للخصوصية، لأن الحقوق الرقمية لا تكون فعالة إلا إذا ترتب على مخالفتها جزاء قانوني. "تقوم المسؤولية المدنية عن انتهاك الخصوصية الرقمية بمجرد حدوث ضرر ناتج عن تقصير في اتخاذ التدابير الأمنية الكافية لحماية قواعد البيانات من الاختراق[2] ".

والمسؤولية في هذا المجال قد تكون إدارية، أو مدنية، أو جزائية، بحسب طبيعة الفعل المرتكب، والضرر الناتج عنه، وصفة الشخص أو الجهة التي ارتكبت الانتهاك. وتزداد أهمية هذه المسؤولية في ظل الذكاء الاصطناعي، لأن الضرر قد لا ينتج عن فعل مادي مباشر، بل عن معالجة آلية، أو خوارزمية خاطئة، أو نظام ذكي صمم أو استعمل دون احترام قواعد الحماية.

أولا، تقوم المسؤولية الإدارية عندما يخرق المسؤول عن المعالجة أحكام قانون حماية المعطيات الشخصية. فقد منح القانون رقم 25-11 السلطة الوطنية صلاحية اتخاذ إجراءات إدارية ضد المسؤول عن المعالجة، تشمل الإنذار، والإعذار، والسحب المؤقت أو النهائي لوصل التصريح أو الترخيص، والغرامة. كما جعل قرارات السلطة الوطنية قابلة للطعن أمام مجلس الدولة، وهو ما يحقق التوازن بين سلطة الرقابة وحق الدفاع[3].

وتكمن أهمية المسؤولية الإدارية في أنها ذات طبيعة وقائية وتصحيحية، لأنها لا تنتظر دائما وقوع جريمة جزائية، بل تتدخل بمجرد مخالفة قواعد المعالجة أو الإخلال بشروط التصريح أو الترخيص. وهذا مهم في مجال

[1] – المادة 45 مكرر 7 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – مروان محمد عبده، المسؤولية المدنية والنائية في جرائم الحاسب الآلي، دار الكتب القانونية، مصر، ط 1، 2018، ص 145.

[3] – المواد 46 و47 و48 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الذكاء الاصطناعي، لأن بعض المخاطر يجب وقفها قبل تحولها إلى ضرر فعلي، خاصة إذا تعلق الأمر بمعالجة واسعة للبيانات أو باستعمال تقنيات جديدة قد تمس حقوق الأفراد وحرياتهم.

ثانيا، تقوم المسؤولية المدنية عندما يؤدي خرق أمن المعلومات أو انتهاك الخصوصية إلى ضرر يصيب الشخص المعني. وقد قرر القانون رقم 25-11 صراحة أنه يمكن لكل شخص يدعي أنه تم المساس بحق من حقوقه المنصوص عليها في هذا القانون أن يطلب من الجهة القضائية المختصة اتخاذ إجراءات تحفظية لوضع حد لهذا التعدي أو الحصول على تعويض. وهذا النص مهم لأنه يمنح الشخص المتضرر وسيلة قضائية مباشرة، فلا يكتفي بتقديم شكوى إلى السلطة الوطنية، بل يستطيع اللجوء إلى القضاء للمطالبة بوقف التعدي والتعويض[1].

وتستند المسؤولية المدنية كذلك إلى القواعد العامة في القانون المدني، خاصة مبدأ المسؤولية التقصيرية القائم على الخطأ والضرر والعلاقة السببية. فكل من تسبب بخطئه في ضرر للغير يلتزم بالتعويض، ويمكن تطبيق هذا المبدأ على حالات تسريب البيانات، أو إتلافها، أو استعمالها في غير الغرض المرخص، أو اتخاذ قرار آلي خاطئ بسبب بيانات غير صحيحة أو معالجة غير مشروعة. وفي ظل الذكاء الاصطناعي، قد يثور الإشكال حول تحديد المسؤول: هل هو مصمم النظام، أم مالكه، أم المؤسسة المستعملة له، أم المسؤول عن المعالجة؟ لذلك يجب ربط المسؤولية بالجهة التي تحدد غرض المعالجة ووسائلها، وبكل من أخل بالتزام الحماية أو الرقابة أو التحقق.

ثالثا، تقوم المسؤولية الجزائية عندما يشكل الفعل المرتكب جريمة منصوصا عليها في قانون حماية المعطيات الشخصية أو قانون العقوبات أو القوانين الخاصة بمكافحة الجرائم المعلوماتية. فقد رتب القانون رقم 25-11 عقوبات جزائية على عدة أفعال، منها معالجة المعطيات دون الموافقة الصريحة، ومعالجة المعطيات الحساسة خارج الحالات القانونية، وإنجاز أو استعمال معالجة لأغراض غير مصرح بها أو غير مرخص لها، وجمع البيانات بطريقة تدليسية أو غير نزيهة أو غير مشروعة، والسماح لأشخاص غير مؤهلين بالولوج إلى معطيات شخصية[2].

كما يعاقب القانون على رفض المسؤول عن المعالجة، دون سبب مشروع، تمكين الشخص من حقوق الإعلام أو الولوج أو التصحيح أو الاعتراض، وعلى عدم إعلام السلطة الوطنية والشخص المعني عن كل

[1] – المادة 52 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المواد 54 إلى 60 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

انتهاك للمعطيات الشخصية في مجال خدمات الاتصالات الإلكترونية. وتدل هذه الأحكام على أن المشرع لم ينظر إلى حقوق الشخص المعني باعتبارها مجرد حقوق شكلية، بل رتب على عرقلتها أو رفضها جزاءات جزائية، مما يعزز الطابع الإلزامي لحماية البيانات[1].

وتقوم المسؤولية كذلك عند حدوث خرق للمعطيات ذات الطابع الشخصي. وقد عرف القانون المعدل خرق المعطيات بأنه كل خرق للأمن يؤدي، بصفة عرضية أو غير قانونية، إلى الإتلاف أو الضياع أو التغيير أو الكشف أو الوصول غير المرخصين إلى المعطيات المنقولة أو المخزنة أو المعالجة بطريقة أخرى. كما ألزم المسؤول عن المعالجة بإخطار السلطة الوطنية في أجل لا يتجاوز خمسة أيام من علمه بالخرق، وإخطار الشخص المعني إذا كان الخرق يحتمل أن يؤدي إلى مخاطر عالية على حقوقه وحرياته[2].

وتظهر أهمية هذا الالتزام في أن خرق البيانات لم يعد شأنا داخليا للمؤسسة يمكن إخفاؤه، بل أصبح واقعة قانونية منتجة لآثار، يجب التصريح بها وتوثيقها ومعالجة نتائجها. ففي ظل الذكاء الاصطناعي، قد يكون خرق البيانات أكثر خطورة من الخرق التقليدي، لأن البيانات المسربة قد تستعمل في تدريب نماذج أخرى، أو في انتحال الهوية، أو في بناء ملفات شخصية دقيقة، أو في تنفيذ هجمات احتيالية موجهة.

ولا تقتصر المسؤولية الجزائية على قانون حماية المعطيات، بل تمتد أيضا إلى قانون العقوبات والقانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، خاصة عندما يكون انتهاك الخصوصية نتيجة دخول غير مشروع إلى منظومة معلوماتية، أو اعتراض غير مشروع للاتصالات، أو تغيير أو حذف أو إتلاف للمعطيات، أو استعمال وسائل تقنية لاختراق الأنظمة. وقد نظم القانون رقم 09-04 إجراءات المراقبة والتفتيش والحجز داخل المنظومات المعلوماتية، مع اشتراط الإذن المكتوب من السلطة القضائية المختصة في حالات المراقبة الإلكترونية، وهو ما يربط مكافحة الجريمة المعلوماتية بضمانة الرقابة القضائية[3].

[1] – المادتان 64 و66 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المواد 45 مكرر 8 و45 مكرر 9 و45 مكرر 10 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

[3] – المواد 3 و4 و5 و6 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وعليه، فإن المسؤولية القانونية عن انتهاك أمن المعلومات وخرق الخصوصية تقوم على منظومة متكاملة: مسؤولية إدارية تمارسها السلطة الوطنية لضمان الامتثال، ومسؤولية مدنية تتيح للمتضرر طلب وقف التعدي والتعويض، ومسؤولية جزائية تعاقب الأفعال الخطيرة التي تمس البيانات أو الأنظمة أو حقوق الشخص المعني. غير أن التحدي الأكبر في ظل الذكاء الاصطناعي يتمثل في ضرورة تطوير قواعد الإسناد والإثبات، حتى لا يبقى الضرر الخوارزمي دون مسؤول محدد، وحتى لا تتحول التقنية إلى وسيلة للإفلات من المساءلة.

المبحث الثاني: مخاطر و آفاق حماية أمن المعلومات في ظل الذكاء الاصطناعي

إذا كان التنظيم القانوني لحماية أمن المعلومات يقوم على قواعد دستورية وتشريعية وتنظيمية تهدف إلى حماية الخصوصية والمعطيات الشخصية ومكافحة الجرائم المعلوماتية، فإن تطور الذكاء الاصطناعي فرض تحديات قانونية جديدة لم تكن مطروحة بنفس الحدة في ظل الأنظمة المعلوماتية التقليدية. فالذكاء الاصطناعي لا يقتصر على تخزين البيانات أو نقلها، بل يقوم على تحليلها، وتصنيفها، واستنتاج أنماط منها، وقد يصل في بعض الحالات إلى اقتراح قرارات أو اتخاذها بصورة آلية، وهو ما يجعل الخطر القانوني أكثر تعقيدا[1].

وتظهر هذه التحديات أساسا في صعوبة تحديد المسؤولية عن أفعال الأنظمة الذكية، لأن الضرر قد ينتج عن خطأ في التصميم، أو ضعف في البيانات، أو سوء في التدريب، أو غياب الرقابة البشرية، أو سوء استعمال من طرف الجهة المشغلة. كما تظهر في قصور التشريعات الحالية، التي وضعت في أغلبها لتنظيم حماية البيانات أو مكافحة الجريمة المعلوماتية، ولم توضع خصيصا لتنظيم الذكاء الاصطناعي كنظام مستقل قادر على التعلم والتنبؤ والتأثير في الحقوق والحريات[2].

وتزداد الصعوبة أيضا في مجال الإثبات، لأن الجرائم المرتبطة بالذكاء الاصطناعي قد تتم بوسائل آلية، وبأدلة رقمية قابلة للتغيير أو الإخفاء أو التوزع عبر عدة أنظمة ودول. ولذلك فإن حماية أمن المعلومات في ظل الذكاء الاصطناعي لا تقتضي فقط تطوير وسائل الحماية التقنية، بل تفرض كذلك تطوير قواعد المسؤولية، وتحيين النصوص التشريعية، وتعزيز الخبرة القضائية الرقمية، وضمان احترام الحقوق والحريات عند استعمال الوسائل الذكية في التحري أو المعالجة أو الرقابة [3].

---

[1] – المعهد الوطني للمعايير والتكنولوجيا، "إطار إدارة مخاطر الذكاء الاصطناعي (الإصدار 1.0)"، منشور NIST للذكاء الاصطناعي رقم AI100-1 ، وزارة التجارة الأمريكية، يناير 2023.

[2] – المعهد الوطني للمعايير والتكنولوجيا، "إطار إدارة مخاطر الذكاء الاصطناعي (الإصدار 1.0)"،المرجع نفسه.

[3]– منظمة التعاون الاقتصادي والتنمية، "توصية المجلس بشأن الذكاء الاصطناعي"، الوثيقة القانونية رقم OECD/LEGAL/0449، اعتُمدت في 22 مايو 2019، جرى مراجعتها في 8 نوفمبر 2023، وحُدثت في عام 2024.

المطلب الأول: التحديات القانونية في مجال الذكاء الاصطناعي

تتمثل التحديات القانونية في مجال الذكاء الاصطناعي في مجموع الصعوبات التي تواجه القانون عند محاولة إخضاع الأنظمة الذكية لقواعد المسؤولية والرقابة والإثبات. فالقاعدة القانونية التقليدية تقوم غالبا على وجود فاعل بشري، وسلوك محدد، وضرر، وعلاقة سببية بين الفعل والنتيجة. أما في مجال الذكاء الاصطناعي، فإن القرار أو النتيجة قد تصدر عن منظومة تقنية معقدة، تتداخل فيها الخوارزمية، والبيانات، والمطور، والمستخدم، والمؤسسة المشغلة، ومزود الخدمة، مما يجعل تحديد المسؤول أمرا بالغ الصعوبة[1].

وتتجلى خطورة هذه التحديات عندما يتعلق الأمر بأمن المعلومات، لأن النظام الذكي قد يستعمل في كشف الهجمات وحماية البيانات، لكنه قد يتسبب في الوقت نفسه في انتهاك الخصوصية أو تحليل السلوك أو تصنيف الأشخاص أو إحداث ضرر نتيجة قرار آلي خاطئ. ولذلك اتجهت المعايير الحديثة إلى ربط الذكاء الاصطناعي بمبادئ الشفافية، والأمن، والحوكمة، والرقابة البشرية، والمساءلة، وإدارة المخاطر[2].

وبناء على ذلك، يمكن حصر أهم التحديات القانونية في ثلاثة محاور كبرى: صعوبة تحديد المسؤولية القانونية عن أفعال الأنظمة الذكية، وقصور وعدم ملاءمة التشريعات الحالية للتطور التكنولوجي، ثم صعوبات الإثبات في الجرائم المرتبطة بالذكاء الاصطناعي.

الفرع الأول: صعوبة تحديد المسؤولية القانونية عن أفعال الأنظمة الذكية

تعد مسألة المسؤولية القانونية من أخطر الإشكالات التي يطرحها الذكاء الاصطناعي، لأن النظام الذكي لا يعمل دائما وفق أوامر مباشرة وبسيطة من الإنسان، بل قد يعتمد على خوارزميات قادرة على التعلم من البيانات وتطوير نتائجها بناء على المعطيات التي تتلقاها. "إن الاستقلالية التي تتمتع بها أنظمة الذكاء الاصطناعي تثير إشكالية 'الفجوة في المسؤولية'، حيث يصعب إسناد الفعل الضار للمبرمج أو المستخدم في حالة اتخاذ النظام لقرار ذاتي غير متوقع[3] ".

وهذا يطرح سؤالا قانونيا جوهريا: من يتحمل المسؤولية إذا تسبب نظام ذكاء اصطناعي في خرق أمن المعلومات أو انتهاك الخصوصية أو اتخاذ قرار خاطئ؟ هل هو المصمم الذي وضع الخوارزمية؟ أم مزود

[1] NIST, *AI RMF 1.0*,.

[2] – منظمة التعاون الاقتصادي والتنمية(OECD) ، "توصية المجلس بشأن الذكاء الاصطناعي."

[3] رامي متولي القاضي، المسؤولية القانونية عن أخطاء الذكاء الاصطناعي، دار الجامعة الجديدة، الإسكندرية، د.ط ، 2020، ص 210.

البيانات؟ أم المؤسسة التي استعملت النظام؟ أم المستخدم الذي اعتمد على نتائجه؟ أم المسؤول عن المعالجة الذي حدد غرض استعمال البيانات؟ [1].

وتزداد هذه الصعوبة لأن المسؤولية القانونية التقليدية تقوم على فكرة الخطأ والضرر والعلاقة السببية. ففي القانون المدني الجزائري، تقوم المسؤولية التقصيرية على قاعدة أن كل فعل يرتكبه الشخص بخطئه ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض. غير أن تطبيق هذا المبدأ على الذكاء الاصطناعي يثير صعوبة عملية، لأن الضرر قد لا ينتج عن خطأ واحد واضح، بل عن سلسلة من العوامل التقنية والتنظيمية، مثل ضعف جودة البيانات، أو غياب الاختبار، أو نقص الرقابة البشرية، أو سوء إعداد النظام، أو استعماله خارج الغرض الذي أنشئ من أجله[2].

ويزداد الأمر تعقيدا عندما يكون النظام الذكي قائما على التعلم الآلي، لأن مخرجاته قد تتغير بمرور الوقت تبعا للبيانات التي يعالجها. فإذا وقع خطأ في نظام كشف التهديدات المعلوماتية، كأن يصنف مستخدما عاديا على أنه مصدر خطر، أو يمنع شخصا من الولوج إلى خدمة رقمية، أو يسمح بمرور هجوم إلكتروني بسبب تحليل خاطئ، فإن تحديد المسؤول يتطلب معرفة دقيقة بسلسلة تصميم النظام وتشغيله ومراقبته. وهنا تظهر مشكلة ''تعدد الفاعلين''، حيث يتداخل دور المطور، والمورد، والمسؤول عن المعالجة، والمعالج من الباطن، والإدارة أو المؤسسة المستعملة للنظام[3].

ولذلك، فإن الاتجاه القانوني الحديث لم يعد يكتفي بالبحث عن الفاعل المباشر، بل يتجه إلى توزيع المسؤولية حسب الدور الذي يلعبه كل طرف في دورة حياة النظام الذكي. فالمطور يسأل عن عيوب التصميم والاختبار، ومزود البيانات يسأل عن جودة البيانات ومشروعيتها، والمؤسسة المستعملة تسأل عن اختيار النظام ومراقبته، والمسؤول عن المعالجة يسأل عن تحديد الغرض ووسائل المعالجة، والمعالج من الباطن يسأل عن احترام تعليمات المسؤول عن المعالجة والتدابير الأمنية. وهذا المنطق قريب مما أقره القانون رقم 25-11 المتعلق بحماية المعطيات الشخصية، عندما ميز بين المسؤول عن المعالجة والمعالج من الباطن، ورتب على كل منهما التزامات تتعلق بالسرية والأمن واحترام شروط المعالجة[4].

---

[1] Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach, 4th ed., Pearson, 2021./

[2] – الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975، المتضمن القانون المدني الجزائري، المعدل والمتمم بموجب القانون رقم 05-10 المؤرخ في 20 يونيو 2005 ، ج.ر.ج.ج رقم 44 ، المادة 124، تقرر هذه المادة القاعدة العامة في المسؤولية التقصيرية، وهي أن كل فعل يرتكبه الشخص بخطئه ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض. وتستعمل كأساس لتحليل المسؤولية المدنية عن أضرار الأنظمة الذكية.

[3] NIST, AI RMF 1.0,

[4] – المادة 3 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

وتظهر أهمية الرقابة البشرية في هذا السياق باعتبارها وسيلة لتخفيف صعوبة المسؤولية. فالأنظمة عالية الخطورة يجب ألا تترك تعمل دون مراقبة بشرية فعالة، لأن غياب هذه الرقابة يجعل القرار الآلي مصدرا مباشرا للخطر، خاصة إذا تعلق الأمر بالبيانات الشخصية أو الأمن أو الخدمات العمومية أو الحقوق الأساسية. وقد أكد قانون الذكاء الاصطناعي الأوروبي أن الرقابة البشرية في الأنظمة عالية الخطورة تهدف إلى منع أو تقليل المخاطر التي قد تمس الصحة أو السلامة أو الحقوق الأساسية[1].

ومن جهة أخرى، يطرح الذكاء الاصطناعي إشكالا خاصا في مجال المسؤولية الجزائية، لأن الجريمة تفترض عادة ركنا ماديا وركنا معنويا. فإذا استعمل شخص نظاما ذكيا لاختراق منظومة معلوماتية أو توليد هجمات تصيد أو تحليل ثغرات أمنية، فإن المسؤولية الجزائية تثبت في حقه متى توافرت النية الإجرامية. أما إذا نتج الضرر عن سلوك غير متوقع للنظام الذكي، أو عن خلل في البيانات، أو عن غياب رقابة كافية، فإن الأمر يصبح أقرب إلى المسؤولية المدنية أو الإدارية أو المهنية، ما لم يثبت أن هناك إهمالا جسيما أو علما بالخطر أو قبولا بنتائجه[2].

وفي مجال حماية البيانات، عالج المشرع الجزائري جزءا من هذه المشكلة عندما اتجه في القانون رقم 25-11، إلى تعزيز الضمانات المرتبطة بالمعالجة الآلية، ودراسة الأثر، وتوثيق عمليات المعالجة، ومندوب حماية المعطيات. وتظهر أهمية هذه الأحكام في أنها تمنع ترك المعالجة الذكية خارج الرقابة، وتجعل المسؤول عن المعالجة مطالبا بتقدير المخاطر وإثبات احترامه لقواعد الحماية[3].

وعليه، فإن صعوبة تحديد المسؤولية القانونية عن أفعال الأنظمة الذكية تفرض ضرورة اعتماد مقاربة قانونية متعددة المستويات، تقوم على تحديد المسؤول عن كل مرحلة من مراحل النظام: التصميم، والتدريب، والتشغيل، والمعالجة، والرقابة، والاستعمال. كما تفرض ضرورة إلزام المؤسسات بتوثيق قراراتها التقنية والقانونية، حتى لا يتحول الذكاء الاصطناعي إلى وسيلة لإخفاء الخطأ أو تفتيت المسؤولية بين عدة أطراف[4].

الفرع الثاني: قصور وعدم ملاءمة التشريعات الحالية للتطور التكنولوجي

يتمثل التحدي الثاني في قصور وعدم ملاءمة التشريعات الحالية للتطور التكنولوجي، ذلك أن كثيرا من النصوص القانونية وضعت في مرحلة كانت فيها الأنظمة المعلوماتية تقوم أساسا على التخزين والمعالجة التقليدية للبيانات، بينما أصبحت الأنظمة الحديثة تعتمد على الذكاء الاصطناعي، والتعلم الآلي، وتحليل البيانات

[1] – اللائحة (الاتحاد الأوروبي) رقم 1689/2024 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 13 يونيو 2024 بشأن وضع قواعد موحدة للذكاء الاصطناعي، المادة 14.

[2] – المواد 394 مكرر إلى 394 مكرر 7 من القانون رقم 24-06 قانون العقوبات الجزائري.

[3] – القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] – منظمة التعاون الاقتصادي والتنمية(OECD) ، "توصية المجلس بشأن الذكاء الاصطناعي."

الضخمة، والحوسبة السحابية، والربط البيني بين المنصات." القواعد التقليدية للمسؤولية التقصيرية القائمة على ركن الخطأ تظل عاجزة عن استيعاب الأضرار السيبرانية المعقدة التي تسببها خوارزميات التعلم العميق[1] ".

وهذا التطور يجعل النصوص القائمة، رغم أهميتها، غير كافية وحدها لضبط جميع المخاطر الجديدة[2].

ففي الجزائر، يتوزع الإطار القانوني ذي الصلة على عدة نصوص، منها التعديل الدستوري في المادة 47 المتعلقة بالخصوصية والمعطيات الشخصية، والقانون رقم 18-07 المعدل و المتمم بموجب القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والقانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقانون العقوبات في المواد المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات. غير أن هذه النصوص، على أهميتها، لا تشكل قانونا خاصا شاملا ينظم الذكاء الاصطناعي من حيث تعريفه، وتصنيف مخاطره، وشروط استعماله، ومسؤولية مطوريه ومشغليه، وحدود توظيفه في المرافق العمومية والقطاعات الحساسة[3].

ويظهر القصور التشريعي بصفة خاصة في أن قانون حماية المعطيات الشخصية يركز أساسا على المعالجة، والموافقة، وحقوق الشخص المعني، والسلطة الوطنية، وهي مسائل جوهرية بلا شك، لكنه لا ينظم بصورة تفصيلية كل ما يتعلق بالشفافية الخوارزمية، وقابلية تفسير القرار الآلي، والتحيز الخوارزمي، وتقييم أنظمة الذكاء الاصطناعي عالية الخطورة، وإلزامية اختبار النماذج قبل استعمالها في الإدارات أو المؤسسات[4].

كما أن قانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يركز على الجريمة المعلوماتية من حيث المراقبة، والتفتيش، والحجز، وحفظ معطيات حركة السير، والتزامات مقدمي الخدمات، غير أنه لا يتناول بصورة خاصة الجرائم التي تنفذ بواسطة أنظمة ذكاء اصطناعي توليدية أو ذاتية التعلم، مثل توليد محتوى

[1] – ياسين بن ورزق، "التحديات القانونية للذكاء الاصطناعي"، مجلة الاجتهاد للدراسات القانونية، المركز الجامعي تمنراست، ع 12، 2022، ص 18.

[2] Ian Goodfellow, Yoshua Bengio, Aaron Courville, *Deep Learning*, MIT Press, 2016،

[3] – المادة 47 من التعديل الدستوري 2020 و القانون رقم 25-11 سالف الذكر؛ القانون رقم 09-04، والمواد 394 مكرر إلى 394 مكرر 7 من القانون رقم 24-06 قانون العقوبات الجزائري

[4] – القانون رقم 25-11المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، في المواد المتعلقة بالموافقة ونوعية المعطيات وحقوق الشخص المعني والسلطة الوطنية.

احتيالي، أو إنشاء هويات رقمية مزيفة، أو أتمتة هجمات التصيد، أو استغلال الذكاء الاصطناعي لاكتشاف الثغرات واستهداف الأنظمة[1].

ومن مظاهر عدم الملاءمة أيضا أن النصوص الجزائية التقليدية تقوم غالبا على تحديد أفعال مادية واضحة، مثل الدخول غير المشروع، أو حذف المعطيات، أو تعديلها، أو اعتراض الاتصالات. غير أن الذكاء الاصطناعي قد يؤدي إلى صور جديدة من الاعتداء، مثل التلاعب بالبيانات التدريبية، أو تلويث قواعد البيانات، أو إنشاء هويات رقمية مزيفة، أو توليد محتوى احتيالي مقنع، أو اتخاذ قرارات آلية تمييزية، أو استنتاج معطيات حساسة من بيانات عادية. وهذه الصور قد لا تكون دائما منصوصا عليها بدقة، مما يفرض إما تأويلا واسعا للنصوص القائمة أو تدخلا تشريعيا صريحا[2].

وتكشف التجارب المقارنة أن الاتجاه الحديث في تنظيم الذكاء الاصطناعي يقوم على مقاربة قائمة على المخاطر. فقانون الذكاء الاصطناعي الأوروبي، الصادر بموجب اللائحة رقم 1689/2024، صنف الأنظمة حسب درجة خطورتها، وميز بين الأنظمة المحظورة، والأنظمة عالية الخطورة، والأنظمة محدودة المخاطر، وفرض على الأنظمة عالية الخطورة التزامات تتعلق بإدارة المخاطر، وجودة البيانات، والتوثيق، والشفافية، والرقابة البشرية، والدقة، والصلابة، والأمن السيبراني. وتفيد هذه المقاربة في أن التنظيم لا يعامل كل تطبيقات الذكاء الاصطناعي بنفس الدرجة، بل يشدد الرقابة كلما زادت مخاطر النظام على الحقوق والحريات[3].

كما أن المعايير غير الملزمة، مثل إطار NIST لإدارة مخاطر الذكاء الاصطناعي، تقدم نموذجا مهما لمعالجة القصور التشريعي، لأنها تربط الذكاء الاصطناعي بالحوكمة، ورسم السياق، والقياس، والإدارة، وهي وظائف تسمح للمؤسسات بتحديد المخاطر قبل وقوعها وإدارتها بشكل مستمر. غير أن هذه المعايير، رغم أهميتها، لا تكفي وحدها إذا لم تتحول إلى التزامات قانونية أو تنظيمية داخلية في القطاعات الحساسة[4].

وعليه، فإن قصور التشريعات الحالية لا يعني غياب الحماية القانونية، بل يعني أن الحماية الموجودة تحتاج إلى تطوير وتحيين وربط مباشر بالذكاء الاصطناعي. فالقانون يجب أن ينتقل من حماية البيانات بعد جمعها إلى

[1] – المواد 3 إلى 12 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] – المواد 394 مكرر إلى 394 مكرر 7 من القانون رقم 24-06، قانون العقوبات الجزائري

[3] – للائحة (الاتحاد الأوروبي) رقم 1689/2024، المواد 6، 9، 10، 13، 14، و15.

[4] – المعهد الوطني للمعايير والتكنولوجيا، "إطار إدارة مخاطر الذكاء الاصطناعي (الإصدار 1.0)"، منشور NIST للذكاء الاصطناعي رقم AI100-1 ، يناير 2023.

تنظيم دورة حياة النظام الذكي بكاملها، من مرحلة التصميم والتدريب، إلى مرحلة التشغيل والرقابة، ثم مرحلة التقييم والمساءلة عند وقوع الضرر[1].

الفرع الثالث: صعوبة الإثبات في الجرائم المرتبطة بالذكاء الاصطناعي

"يواجه القضاء تحدياً كبيراً في إثبات الجرائم المرتبطة بالذكاء الاصطناعي نظراً لخاصية 'الصندوق الأسود' (Black Box)، حيث يصعب تفسير الكيفية التي وصل بها النظام إلى نتيجة إجرامية معينة[2] ".

تعد صعوبات الإثبات من أبرز التحديات القانونية في الجرائم المرتبطة بالذكاء الاصطناعي، لأن الدليل في هذه الجرائم غالبا ما يكون دليلا رقميا غير مادي، قابلا للمحو أو التعديل أو التشفير أو النقل السريع عبر عدة خوادم ومنظومات. وإذا كانت الجريمة التقليدية تترك غالبا آثارا مادية يمكن معاينتها، فإن الجريمة المعلوماتية قد تترك آثارا تقنية دقيقة، مثل سجلات دخول، أو عناوين بروتوكول، أو معطيات حركة سير، أو ملفات مؤقتة، أو بصمات رقمية، وهي آثار تحتاج إلى خبرة تقنية عالية وسلسلة حفظ دقيقة حتى تكون صالحة أمام القضاء وفقا لنصوص المواد 5 و 6 و 7 من القانون رقم 09-04 [3].

وتزداد الصعوبة عندما يرتبط الفعل بالذكاء الاصطناعي، لأن النظام الذكي قد يستعمل في إخفاء مصدر الهجوم، أو توليد رسائل احتيالية متعددة، أو تغيير نمط الهجوم بصورة مستمرة، أو إنشاء هويات رقمية مزيفة، أو إنتاج محتوى مزور يصعب تمييزه عن الحقيقي. كما أن بعض الهجمات قد تستهدف النظام الذكي نفسه، من خلال تلويث بيانات التدريب أو التلاعب بالمدخلات، مما يجعل إثبات العلاقة بين الفعل والنتيجة أكثر تعقيدا من الجرائم المعلوماتية التقليدية[4].

وقد حاول القانون رقم 09-04 مواجهة بعض هذه الصعوبات من خلال وضع قواعد خاصة بالمراقبة والتفتيش والحجز داخل المنظومات المعلوماتية. فقد أجاز، ضمن شروط قانونية، مراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها، كما أجاز التفتيش ولو عن بعد داخل منظومة معلوماتية أو جزء منها، وحجز المعطيات المفيدة في الكشف عن الجرائم أو مرتكبيها، مع السهر على سلامة المعطيات ومنع المساس بمحتواها. وتكمن أهمية هذه القواعد في أنها تعترف بالطبيعة الخاصة للدليل الرقمي، الذي قد يوجد داخل نظام أو خادم

---

[1] – منظمة التعاون الاقتصادي والتنمية، "توصية المجلس بشأن الذكاء الاصطناعي."

[2] – محمد كمال الصاوي، الدليل الرقمي وإجراءات التحقيق في الجرائم التكنولوجية، مطبعة المعارف، القاهرة، د.ط ، 2021، ص 315.

[3] – المواد 5 و6 و7 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[4] – المواد 5 و6 و7 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أو دعامة إلكترونية وليس في مكان مادي تقليدي و ذلك لما نصت عليه المواد من 3 إلى 6 من نفس القانون[1].

كما ألزم القانون رقم 09-04 مقدمي الخدمات بحفظ معطيات حركة السير لمدة سنة واحدة، وهي معطيات قد تكون ضرورية لتحديد مصدر الاتصال، وتاريخ ووقت الدخول، ومدة الاتصال، والتجهيزات المستعملة، والمرسل إليه أو المواقع التي تم الاطلاع عليها. وتظهر أهمية هذه المعطيات في جرائم الذكاء الاصطناعي لأن الجاني قد يستعمل أدوات آلية أو حسابات متعددة أو خوادم وسيطة، مما يجعل تتبع مسار الفعل الإجرامي متوقفا على حفظ هذه البيانات وتحليلها فنيا وقضائيا و ذلك لما نصت عليه المادة 11 من نفس القانون[2].

غير أن وجود هذه القواعد لا يلغي الصعوبات العملية في الإثبات. فالدليل الرقمي يتطلب شروطا دقيقة، منها الحفاظ على سلامة الدليل من لحظة جمعه إلى عرضه أمام القضاء، وتوثيق سلسلة الحيازة، والتأكد من عدم تغييره، وتحديد الجهة التي جمعته، والطريقة التقنية المستعملة في استخراجه، ومدى احترام الضمانات القانونية، خاصة الإذن القضائي عند الاقتضاء. فإذا اختل أحد هذه العناصر، أمكن للمتهم أو الدفاع الطعن في الدليل بحجة عدم سلامته أو عدم مشروعية الحصول عليه و ذلك لنصوص المواد من 6 إلى 9من نفس القانون[3].

وتطرح الأنظمة الذكية صعوبة إضافية تتعلق بإثبات العلاقة السببية. ففي الجريمة التقليدية قد يكون من السهل نسب الفعل إلى شخص محدد، أما في الذكاء الاصطناعي فقد يصعب تحديد ما إذا كان الضرر ناتجا عن خطأ بشري، أو خطأ برمجي، أو خلل في البيانات، أو نتيجة غير متوقعة للنظام، أو سوء استعمال من طرف طرف ثالث. لذلك يصبح الإثبات في هذه الحالة إثباتا مركبا، لا يقتصر على بيان وقوع الضرر، بل يتطلب تحليل بنية النظام، وسجل العمليات، والبيانات المستعملة، وقرارات النموذج، وتدخلات المستخدم، وإجراءات الرقابة[4].

[1] – المواد 3 إلى 6 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] – المادة 11 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] – المواد 6 و7 و8 و9 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[4] – اللائحة (الاتحاد الأوروبي) رقم 1689/2024، المادتان 9 و12.

كما تظهر صعوبة "العلبة السوداء" في الذكاء الاصطناعي، حيث تكون بعض النماذج قادرة على إنتاج نتائج دقيقة دون أن يكون من السهل تفسير كيفية الوصول إليها. وهذه الصعوبة تؤثر مباشرة في الإثبات، لأن القاضي أو الخبير أو جهة التحقيق قد يحتاج إلى معرفة سبب القرار أو التوقع أو التصنيف الذي أنتجه النظام. ولذلك أصبحت الشفافية والتوثيق وقابلية التفسير من الشروط الأساسية للثقة في الأنظمة الذكية، وهي شروط أكدتها المعايير الدولية الحديثة ومقاربة الاتحاد الأوروبي في الأنظمة عالية الخطورة[1].

ومن جهة أخرى، تثير الجرائم المرتبطة بالذكاء الاصطناعي صعوبات في الاختصاص القضائي، لأن الفعل قد يرتكب من خارج الإقليم الوطني، باستعمال خوادم أجنبية، ويستهدف بيانات موجودة في الجزائر أو تخص مواطنين أو مؤسسات جزائرية. وهنا يصبح التعاون الدولي ضروريا، خاصة في حفظ الأدلة الإلكترونية وتبادل المعلومات وتحديد هوية الجناة. وقد تناولت اتفاقية بودابست للجريمة المعلوماتية والاتفاقية الأممية الحديثة لمكافحة الجريمة السيبرانية هذه المسألة من زاوية التعاون الدولي وتبادل الأدلة الإلكترونية، وهو ما يبين أن الإثبات في الجرائم السيبرانية لم يعد مسألة وطنية خالصة، بل أصبح مسألة عابرة للحدود[2].

وعليه، فإن صعوبات الإثبات في الجرائم المرتبطة بالذكاء الاصطناعي تفرض تطوير الخبرة القضائية الرقمية، وتكوين القضاة وضباط الشرطة القضائية، واعتماد سجلات تقنية قابلة للتدقيق، وإلزام المؤسسات بتوثيق أنظمة الذكاء الاصطناعي وقراراتها، وضمان احترام سلسلة حفظ الدليل الإلكتروني. فالحماية القانونية لأمن المعلومات لا تكتمل بمجرد وجود نصوص تجريم، بل تتطلب قدرة عملية على إثبات الجريمة ونسبتها إلى فاعل محدد بطريقة مشروعة ومقنعة أمام القضاء[3].

المطلب الثاني: آليات وآفاق تطوير الحماية القانونية لأمن المعلومات في مجال الذكاء الاصطناعي

إن التحديات القانونية التي يطرحها الذكاء الاصطناعي في مجال أمن المعلومات لا يمكن مواجهتها بمجرد الاكتفاء بالنصوص التقليدية المتعلقة بحماية البيانات أو مكافحة الجرائم المعلوماتية، بل تقتضي تبني مقاربة قانونية مستقبلية تقوم على التحديث، والوقاية، والحوكمة، والتعاون الدولي، والرقابة الحقوقية. فالذكاء

[1] – اللائحة (الاتحاد الأوروبي) رقم 1689/2024، المادتان 13 و14.

[2] – مجلس أوروبا، "اتفاقية مكافحة الجريمة السيبرانية"، بودابست، 23 نوفمبر 2001، المواد 16، 19، 20، 23 وما يليها؛ الأمم المتحدة، "اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية"، المعتمدة بموجب قرار الجمعية العامة رقم 243/79، بتاريخ 24 ديسمبر 2024.

[3] 04-09 ؛ معهدNIST ، "إطار إدارة مخاطر الذكاء الاصطناعي (الإصدار 1.0)"؛ اللائحة (الاتحاد الأوروبي) رقم 1689/2024.

الاصطناعي يتميز بسرعة تطوره، وتعدد مجالات استعماله، وقدرته على تحليل البيانات وربطها واستنتاج نتائج منها، وهو ما يجعل القواعد القانونية الجامدة عرضة للتجاوز إذا لم يتم تطويرها باستمرار[1].

ومن ثم، فإن تطوير الحماية القانونية لأمن المعلومات في مجال الذكاء الاصطناعي يقتضي الانتقال من منطق رد الفعل بعد وقوع الخرق أو الجريمة، إلى منطق الوقاية القانونية المسبقة، وذلك من خلال تحديث التشريعات الوطنية، وتعزيز التعاون الدولي في المجال السيبراني، وضمان التوازن بين حماية الأمن المعلوماتي وحماية الحقوق والحريات الفردية. ولا يكفي في هذا السياق أن تكون الدولة قادرة على حماية أنظمتها وبياناتها، بل يجب أن تكون هذه الحماية منسجمة مع مبادئ الشرعية، والتناسب، والشفافية، والمساءلة، والرقابة القضائية والإدارية[2].

الفرع الاول: تعزيز التعاون الدولي في مجال الأمن المعلوماتي

"نظراً للطابع العابر للحدود لجرائم الذكاء الاصطناعي، أصبح من الضروري صياغة اتفاقيات دولية موحدة تفرض بروتوكولات أمنية مشفرة لحماية الفضاء السيبراني المشترك[3] ".

يمثل التعاون الدولي آلية أساسية لتطوير الحماية القانونية لأمن المعلومات في مجال الذكاء الاصطناعي، لأن التهديدات السيبرانية والجرائم المرتبطة بالذكاء الاصطناعي لا تتوقف عند الحدود الإقليمية للدولة. فقد تنطلق الهجمة من دولة، وتمر عبر خوادم في دولة ثانية، وتستهدف بيانات أو مؤسسات في دولة ثالثة، بينما يكون الجاني الحقيقي مختفيا خلف هويات رقمية أو شبكات افتراضية أو أدوات آلية. ولذلك، فإن الحماية الوطنية وحدها، مهما بلغت قوتها، تبقى غير كافية إذا لم تدعم بتعاون دولي فعال[4].

وقد شكلت اتفاقية بودابست بشأن الجريمة المعلوماتية لسنة 2001 مرجعا دوليا مهما في هذا المجال، لأنها لم تكتف بتوحيد صور التجريم، مثل الدخول غير المشروع والاعتراض غير المشروع والاعتداء على سلامة المعطيات والأنظمة، بل نظمت كذلك قواعد التعاون الدولي، وحفظ البيانات، والتفتيش والحجز، وجمع الأدلة الإلكترونية. وتكمن أهمية هذه الاتفاقية في أنها أرست فكرة أن الجريمة السيبرانية لا يمكن مكافحتها بمنطق وطني مغلق[5].

---

[1] – المعهد الوطني للمعايير والتكنولوجيا، "إطار إدارة مخاطر الذكاء الاصطناعي (الإصدار 1.0)"، منشور NIST للذكاء الاصطناعي رقم AI100-1 ، يناير 2023.

[2] – منظمة التعاون الاقتصادي والتنمية، "توصية المجلس بشأن الذكاء الاصطناعي"، الوثيقة القانونية رقم OECD/LEGAL/0449، اعتُمدت في عام 2019، وحُدّثت في عام 2024.

[3] – عمار بوضياف، المعاهدات الدولية وأثرها في القوانين الداخلية، دار ريحانة، الجزائر، ط 2، 2017، ص 167.

[4] – مجلس أوروبا، "اتفاقية مكافحة الجريمة السيبرانية"، بودابست، 23 نوفمبر .[2001]

[5] – مجلس أوروبا، "اتفاقية مكافحة الجريمة السيبرانية"، المواد 2، 3، 4، 5، 16، 19، 20، و23

وقد تعزز هذا التوجه باعتماد الأمم المتحدة لاتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية بموجب قرار الجمعية العامة رقم 243/79 بتاريخ 24 ديسمبر 2024. وتعد هذه الاتفاقية أول معاهدة عالمية شاملة في مجال الجريمة السيبرانية، وتهدف إلى تعزيز التعاون الدولي في مكافحة الجرائم المرتكبة بواسطة أنظمة تكنولوجيا المعلومات والاتصال، وتبادل الأدلة الإلكترونية في الجرائم الخطيرة[1].

وتظهر أهمية هذه الاتفاقية في مجال الذكاء الاصطناعي من عدة زوايا؛ فمن جهة، يمكن أن تستعمل الأنظمة الذكية في ارتكاب جرائم عابرة للحدود، مثل الاحتيال الإلكتروني الموجه، والتصيد الذكي، وتوليد هويات رقمية مزيفة، وأتمتة الهجمات. ومن جهة أخرى، قد تكون الأدلة المرتبطة بهذه الجرائم موزعة بين عدة دول أو منصات رقمية أو مزودي خدمات سحابية. لذلك فإن التعاون الدولي في حفظ الأدلة الإلكترونية وتبادلها يصبح ضرورة عملية وقانونية[2].

كما يجب أن يمتد التعاون الدولي إلى مجال حماية البيانات الشخصية، لأن الذكاء الاصطناعي يعتمد غالبا على تدفقات عابرة للحدود للبيانات، خاصة في الخدمات السحابية والمنصات الرقمية. ولذلك ينبغي أن تخضع عمليات نقل البيانات إلى الخارج لضمانات قانونية واضحة، وأن تراعي مستوى الحماية المتوفر في الدولة أو المنظمة المتلقية، وهو ما أقره القانون رقم 25-11 في الأحكام المتعلقة بنقل المعطيات إلى دولة أجنبية أو منظمة دولية[3].

وعليه، فإن تعزيز التعاون الدولي في مجال الأمن المعلوماتي يمثل شرطا أساسيا لحماية أمن المعلومات في ظل الذكاء الاصطناعي. غير أن هذا التعاون لا ينبغي أن يكون تقنيا وأمنيا فقط، بل يجب أن يكون قانونيا وحقوقيا أيضا، يوازن بين ملاحقة الجريمة وحفظ الأدلة من جهة، وحماية الخصوصية والبيانات والسيادة الرقمية من جهة أخرى [4].

---

[1] – الأمم المتحدة، "اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية"، المعتمدة بموجب قرار الجمعية العامة رقم 243/79 بتاريخ 24 ديسمبر 2024.

[2] – اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، 2024.

[3] – القانون رقم 25-11، الأحكام المتعلقة بنقل المعطيات إلى دولة أجنبية أو منظمة دولية.تنظم هذه الأحكام شروط نقل البيانات خارج الإقليم الوطني، وتربط ذلك بمستوى الحماية القانونية في الدولة أو المنظمة المتلقية.

[4] OECD, Recommendation of the Council on Artificial Intelligence, 2019/2024

الفرع الثاني: تحديث وتطوير التشريعات الوطنية لمواكبة الذكاء الاصطناعي

"يتجه التوجه التشريعي الحديث نحو إقرار 'الشخصية القانونية الافتراضية' للروبوتات الذكية، أو وضع صناديق تعويضات إجبارية لمواجهة المخاطر الناتجة عن هذه الأنظمة[1] ".

يعد تحديث التشريعات الوطنية أول آلية جوهرية لتطوير الحماية القانونية لأمن المعلومات في ظل الذكاء الاصطناعي، لأن النصوص القانونية القائمة، رغم أهميتها، وضعت في أغلبها لمواجهة أنماط تقليدية من المعالجة الرقمية أو الجرائم المعلوماتية، بينما أفرز الذكاء الاصطناعي واقعا تقنيا أكثر تعقيدا يقوم على الخوارزميات، والتعلم الآلي، وتحليل البيانات الضخمة، والقرارات الآلية، والتنبؤ بالسلوكيات، والمعالجة العابرة للحدود[2].

فالقانون الجزائري يتضمن حاليا عدة نصوص مهمة، منها القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والقانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والمواد 394 مكرر وما يليها من قانون العقوبات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات. غير أن هذه النصوص، على أهميتها، لا تشكل بعد قانونا خاصا وشاملا للذكاء الاصطناعي من حيث تعريفه، وتصنيف مخاطره، وتحديد شروط استعماله، وضبط مسؤولية المطور والمشغل والمسؤول عن المعالجة[3].

ويجب أن يتجه التحديث التشريعي إلى وضع تعريف قانوني واضح للذكاء الاصطناعي، لا يكون تقنيا مجردا، بل يربط النظام الذكي بقدرته على معالجة البيانات، والتعلم، والتنبؤ، وإنتاج مخرجات قد تؤثر في الحقوق والمراكز القانونية للأفراد. فغياب تعريف قانوني دقيق قد يؤدي إلى صعوبة تحديد نطاق التطبيق، وإلى اختلاف الجهات الإدارية والقضائية في تكييف الأنظمة المستعملة داخل المؤسسات[4].

كما ينبغي أن يقوم التحديث التشريعي على تبني مقاربة قائمة على المخاطر، بحيث لا تعامل جميع أنظمة الذكاء الاصطناعي بنفس الدرجة. فالأنظمة المستعملة في الأمن، والعدالة، والصحة، والتوظيف، والتعليم، والخدمات العمومية، أو المعالجة البيومترية، تطرح مخاطر أكبر من التطبيقات العادية. لذلك يجب

---

[1] – هشام محمد فريد، الذكاء الاصطناعي والقانون: دراسة مقارنة، دار النشر الجامعي، القاهرة، 2019، ص 92.

[2] – القانون رقم25 -11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، والمواد 394 مكرر وما يليها من قانون العقوبات الجزائري.

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

إخضاع الأنظمة عالية الخطورة لالتزامات مشددة، مثل التقييم المسبق، ودراسة الأثر، وجودة البيانات، والتوثيق، والرقابة البشرية، والتدقيق، وإمكانية تفسير القرار، والأمن السيبراني[1].

ويجب أن يشمل التحديث التشريعي كذلك إلزام المؤسسات العامة والخاصة بإجراء دراسة أثر قبل استعمال أنظمة الذكاء الاصطناعي في معالجة البيانات الشخصية أو حماية أمن المعلومات. فدراسة الأثر تسمح بتقدير المخاطر التي قد تمس الخصوصية أو الحريات أو سرية البيانات قبل بداية المعالجة، وتلزم المؤسسة بتحديد التدابير التقنية والتنظيمية اللازمة لتقليل تلك المخاطر. وقد خطا المشرع الجزائري خطوة مهمة في هذا الاتجاه بموجب القانون رقم 25-11 المعدل والمتمم للقانون رقم 18-07، حيث أدخل أحكاما حديثة تتعلق بمندوب حماية المعطيات، وخرق البيانات، ودراسة الأثر، وتوثيق عمليات المعالجة[2].

ومن الآليات المهمة أيضا إلزام الإدارات والمؤسسات بتعيين مندوب مختص بحماية المعطيات، تكون مهمته مراقبة الامتثال القانوني، وتقديم الاستشارة، والتنسيق مع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، والتأكد من احترام مبادئ الشفافية والتناسب والأمن. وتظهر أهمية هذا المندوب في كونه وسيلة داخلية للرقابة، تسمح بمنع المخالفة قبل وقوعها، لا بمجرد معالجتها بعد حدوث الضرر[3].

وعليه، فإن تحديث التشريعات الوطنية لمواكبة الذكاء الاصطناعي لا يعني إلغاء النصوص القائمة، بل يعني البناء عليها وتطويرها. فالقانون رقم 25-11 يوفر أساس حماية البيانات، والقانون رقم 09-04 يوفر أساس مكافحة الجريمة المعلوماتية، وقانون العقوبات يوفر أساس التجريم، غير أن المرحلة المقبلة تتطلب تنظيما خاصا بالذكاء الاصطناعي يحدد المخاطر، والالتزامات، والمسؤوليات، والضمانات، ويجعل الأمن المعلوماتي جزءا من شرعية استعمال الأنظمة الذكية لا مجرد إجراء تقني اختياري وفقا للمادة 41 مكرر [4].

[1] Regulation (EU) 2024/1689, Articles 6, 9, 10, 13, 14 and 15.

[2] – القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

[3] – القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، و القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، والمواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري.

[4] – المادة 41 مكرر من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الفرع الثالث: تحقيق التوازن بين حماية الأمن المعلوماتي وضمان الحقوق والحريات الفردية

"يجب ألا تتحول الرقابة الخوارزمية للأمن المعلوماتي إلى أداة لانتهاك الحريات الفردية؛ فالحماية القانونية يجب أن توازن بين متطلبات الأمن القومي والحق في سرية المراسلات[1] ".

يعد تحقيق التوازن بين حماية الأمن المعلوماتي وضمان الحقوق والحريات الفردية من أدق المسائل التي يطرحها الذكاء الاصطناعي، لأن الأمن المعلوماتي يمثل مصلحة عامة مشروعة، لكنه قد يتحول إلى مصدر خطر إذا استعمل لتبرير الرقابة الواسعة أو جمع البيانات دون حدود أو اتخاذ قرارات آلية تمس الأفراد دون ضمانات. ولذلك، فإن الإشكال لا يتمثل في الاختيار بين الأمن والحرية، بل في بناء نظام قانوني يسمح بتحقيق الأمن داخل حدود دولة القانون.

ويجد هذا التوازن أساسه في التعديل الدستوري لسنة 2020، خاصة المادة 47 التي كرست الحق في حماية الحياة الخاصة، وسرية المراسلات والاتصالات، وحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. فهذه المادة تجعل حماية الخصوصية والمعطيات الشخصية حقا دستوريا، ولا تسمح بالمساس به إلا وفق ما يقرره القانون وضمن الضمانات التي تحمي الحقوق الأساسية[2].

ويتحقق التوازن أولا من خلال مبدأ الشرعية، أي أن كل معالجة للبيانات أو مراقبة للاتصالات أو استعمال للذكاء الاصطناعي في مجال أمني يجب أن يستند إلى نص قانوني واضح. فلا يكفي القول إن النظام الذكي يهدف إلى حماية الأمن المعلوماتي، بل يجب أن يكون استعماله محددا في القانون، وأن تعرف الجهة المعنية نطاق المعالجة، والغرض منها، والمسؤول عنها، ومدة الاحتفاظ بالبيانات، ووسائل الطعن أو الاعتراض[3].

ويتحقق التوازن ثانيا من خلال مبدأ التناسب. فالإجراء الأمني يجب أن يكون مناسبا وضروريا لتحقيق الغرض المشروع، وألا يتجاوز ما تقتضيه الحاجة. فإذا كان الهدف هو حماية شبكة مؤسسة من الاختراق، فلا

[1] – سارة بوشتاتة، "التوازن القانوني بين الأمن السيبراني والخصوصية"، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة الجزائر 1، مج 58، ع 1، 2021، ص 401.

[2] – المادة 47 من التعديل الدستوري لسنة 2020..

[3] – المواد 7 و9 و32 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

يجوز جمع بيانات شخصية لا علاقة لها بهذا الغرض. وإذا كان الهدف هو كشف سلوك غير طبيعي داخل نظام معلوماتي، فلا ينبغي تحويل ذلك إلى مراقبة شاملة لحياة الموظفين أو المواطنين وفقا للمادة 09 [1].

ويتحقق التوازن ثالثا من خلال الرقابة القضائية والإدارية. فالقانون رقم 09-04، رغم أنه أجاز في حالات محددة مراقبة الاتصالات الإلكترونية والتفتيش والحجز داخل المنظومات المعلوماتية، إلا أنه قيد ذلك بضمانات، من بينها مراعاة سرية المراسلات والاتصالات، واشتراط الإذن المكتوب من السلطة القضائية المختصة في حالات المراقبة. وهذا يدل على أن المشرع حاول الجمع بين فعالية مكافحة الجريمة المعلوماتية وضمان الحقوق الدستورية وفقا للمواد من 3 إلى 6 من قانون رقم 09-04 [2].

ويجب أن يمتد هذا المنطق إلى الذكاء الاصطناعي، بحيث لا يجوز اعتماد أنظمة ذكية في مجالات حساسة دون رقابة بشرية وقانونية. فالقرار الآلي الذي يمس حقا أو مركزا قانونيا يجب أن يكون قابلا للمراجعة، وأن يستطيع الشخص المعني الاعتراض عليه أو طلب تفسيره أو طلب تدخل بشري. وقد اتجه القانون رقم 25-11 المعدل والمتمم إلى منع تأسيس القرارات ذات الآثار القانونية على مجرد المعالجة الآلية التي تقيم بعض جوانب شخصية الفرد وفقا لما نصت عليه المادة 45 مكرر1 [3].

وعليه، فإن تحقيق التوازن بين حماية الأمن المعلوماتي وضمان الحقوق والحريات الفردية يقتضي اعتماد مقاربة قائمة على الشرعية، والتناسب، والشفافية، والرقابة، والمساءلة. فالذكاء الاصطناعي يجب أن يكون وسيلة لتعزيز أمن المعلومات وخدمة المرفق العام، لا أداة للتوسع في المراقبة أو تقليص الحقوق. وكلما كان استعمال الذكاء الاصطناعي أكثر تأثيرا في الأفراد، وجب أن تكون الضمانات القانونية أكثر قوة ووضوحا[4].

---

[1] – المادة 9 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[2] – المواد 3 و4 و5 و6 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] – المادة 45 مكرر 1 من القانون رقم 25-11 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

[4] Regulation (EU) 2024/1689, Articles 13 and 14.

تتعلق هذه المواد بالشفافية والرقابة البشرية في أنظمة الذكاء الاصطناعي، وهي مبادئ مقارنة تساعد على ضبط استعمال الأنظمة الذكية داخل حدود الحقوق والحريات

خلاصة الفصل الثاني :

مما سبق معالجته في هدا الفصل خلصنا على أن حماية أمن المعلومات في ظل الذكاء الاصطناعي أصبحت رهانا قانونيا واستراتيجيا يتجاوز البعد التقني، لارتباطها بحماية الحقوق والحريات وضمان الأمن الرقمي للدولة.

وقد أظهر أن المنظومة القانونية تقوم على تكامل بين الاتفاقيات الدولية والتشريعات الوطنية، حيث عزز المشرع الجزائري هذه الحماية من خلال دسترة الحق في حماية الحياة الخاصة والمعطيات الشخصية، وتجريم الاعتداءات على أنظمة المعالجة الآلية للمعطيات، مع إقرار ضمانات قانونية أساسية لحماية الخصوصية والبيانات الشخصية.

غير أن التطور المتسارع للذكاء الاصطناعي كشف عن تحديات قانونية معقدة، أبرزها صعوبة تحديد المسؤولية القانونية، وعدم كفاية التشريعات التقليدية لمواكبة الخوارزميات والقرارات الآلية والأنظمة عالية الخطورة، إضافة إلى إشكالات الإثبات الرقمي وحماية الدليل الإلكتروني.

كما أبرز الفصل ضرورة تحديث التشريعات الوطنية، وتعزيز الخبرة القضائية الرقمية والتعاون الدولي لمواجهة التهديدات السيبرانية العابرة للحدود.

وفي الأخير، فإن الحماية الفعالة لأمن المعلومات تظل رهينة بتحقيق توازن دقيق بين متطلبات الأمن المعلوماتي واحترام الحقوق والحريات، بما يضمن استعمالا آمنا ومسؤولا للذكاء الاصطناعي في إطار دولة القانون.

خاتمة

مما سبق البحث في هذه الدراسة يمكن القول أنه في ظل التحولات الرقمية المتسارعة التي يشهدها العالم المعاصر، أصبحت المعلومات تمثل إحدى أهم الثروات الاستراتيجية التي تعتمد عليها الدول والمؤسسات والأفراد في مختلف المجالات السياسية والاقتصادية والاجتماعية والأمنية، ومع التوسع الكبير في استعمال تكنولوجيات الإعلام والاتصال، وتزايد الاعتماد على الأنظمة المعلوماتية والوسائل الإلكترونية في إدارة المرافق والخدمات، برزت تحديات جديدة فرضت ضرورة توفير حماية فعالة للمعلومات والبيانات من مختلف أشكال الاعتداء أو الاختراق أو الاستغلال غير المشروع.

وقد أدى التطور الهائل في تقنيات الذكاء الاصطناعي إلى إحداث نقلة نوعية في مجال أمن المعلومات، حيث أصبحت الأنظمة الذكية قادرة على تحليل كميات ضخمة من البيانات، واكتشاف الأنماط غير العادية، والتنبؤ بالمخاطر، والكشف المبكر عن الهجمات السيبرانية، والاستجابة السريعة للحوادث الأمنية، وهو ما جعل الذكاء الاصطناعي أداة حديثة وفعالة لتعزيز الأمن المعلوماتي وحماية الأنظمة الرقمية.

غير أن هذا التطور التكنولوجي، ورغم ما يحمله من مزايا وإيجابيات، أفرز في المقابل مجموعة من الإشكالات القانونية والتقنية والأخلاقية، خاصة ما تعلق بحماية الخصوصية والمعطيات الشخصية، وصعوبة تحديد المسؤولية القانونية عن أفعال الأنظمة الذكية، إضافة إلى التحديات المرتبطة بالإثبات في الجرائم المعلوماتية، والتوازن بين متطلبات الأمن وحماية الحقوق والحريات الأساسية للأفراد.

ومن خلال دراسة موضوع ''حماية أمن المعلومات في ظل الذكاء الاصطناعي''، تم التوصل إلى جملة من النتائج ، يمكن تلخيصها فيما يلي:

- أن أمن المعلومات لم يعد مجرد مسألة تقنية مرتبطة بحماية الأجهزة والبرمجيات، بل أصبح منظومة متكاملة تشمل الجوانب القانونية والتنظيمية والتقنية والبشرية، وتهدف إلى ضمان سرية المعلومات وسلامتها وتوافرها، مع حماية الأنظمة المعلوماتية من مختلف صور الاعتداء والاختراق.
- أن الذكاء الاصطناعي ساهم بشكل واضح في تطوير وسائل حماية أمن المعلومات، خاصة في مجال الكشف المبكر عن الهجمات السيبرانية، وتحليل السلوكيات المشبوهة، والتنبؤ بالمخاطر، والاستجابة الذكية للحوادث الأمنية، مما سمح بتحسين فعالية الأنظمة الأمنية وتقليل زمن الاستجابة للتهديدات.
- أن تقنيات التعلم الآلي وتحليل البيانات الضخمة أصبحت من أهم الوسائل الحديثة المستعملة في حماية الشبكات والأنظمة المعلوماتية، لأنها تمكن من اكتشاف الأنماط غير الطبيعية والتعامل مع الهجمات المتطورة التي يصعب على الوسائل التقليدية اكتشافها.
- أن المشرع الجزائري أدرك أهمية حماية أمن المعلومات والبيانات الشخصية، وهو ما تجسد من خلال مجموعة من النصوص القانونية، وعلى رأسها القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والقانون رقم 09-04 المتعلق بالوقاية من الجرائم

المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إضافة إلى التعديلات الحديثة التي جاء بها القانون رقم 25-11.

- أن التشريع الجزائري، رغم أهميته، لا يزال يحتاج إلى تطوير أكثر تخصصا لمواكبة التطور السريع للذكاء الاصطناعي، خاصة في المسائل المتعلقة بالشفافية الخوارزمية، والرقابة على الأنظمة الذكية، وتحديد المسؤولية القانونية الناتجة عن القرارات الآلية، وحماية الحقوق الرقمية للأفراد.
- أن الطابع العابر للحدود الذي تتميز به الجرائم المعلوماتية والاعتداءات السيبرانية يجعل من التعاون الدولي أمرا ضروريا وملحا، لأن مواجهة هذه الجرائم لا يمكن أن تتم بفعالية في إطار وطني ضيق فقط، بل تتطلب تنسيقا دوليا وتبادلا للمعلومات والخبرات والآليات التقنية والقانونية.
- أن استعمال الذكاء الاصطناعي في المجال الأمني، رغم أهميته، قد يؤدي إلى بعض المخاطر المرتبطة بالمراقبة المفرطة للأفراد، أو المساس بالخصوصية، أو التمييز الناتج عن الخوارزميات، وهو ما يفرض ضرورة إخضاع هذه التقنيات لضوابط قانونية وأخلاقية واضحة.

وانطلاقا من هذه النتائج، يمكن تقديم مجموعة من المقترحات التي قد تساهم في تعزيز الحماية القانونية لأمن المعلومات في ظل الذكاء الاصطناعي، وتتمثل أهمها فيما يلي:

- ضرورة إصدار تشريع جزائري خاص بالذكاء الاصطناعي يحدد مفهومه، ومجالات استعماله، والضوابط القانونية المرتبطة به، والمسؤولية المدنية والجزائية الناجمة عن استعماله .

- تعزيز الحماية القانونية للمعطيات الشخصية من خلال تفعيل دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، ومنحها صلاحيات أوسع في الرقابة والمتابعة .

- تطوير المنظومة الوطنية للأمن السيبراني، وتزويدها بوسائل تقنية حديثة تعتمد على الذكاء الاصطناعي للكشف المبكر عن التهديدات والهجمات الإلكترونية .

- وضع إطار قانوني ينظم استعمال الأنظمة الذكية في المجال الأمني، بما يضمن احترام الحقوق والحريات الأساسية، خاصة الحق في الخصوصية وحماية الحياة الخاصة .

- تعزيز التكوين والبحث العلمي في مجالات الأمن السيبراني والذكاء الاصطناعي داخل الجامعات والمؤسسات البحثية، باعتبارهما من المجالات الاستراتيجية المرتبطة بمستقبل الدول .

- نشر الثقافة الرقمية والأمنية بين الأفراد والمؤسسات، من خلال تنظيم حملات توعية وتكوين مستمر حول مخاطر الجرائم المعلوماتية وأساليب الوقاية منها .

- تشجيع المؤسسات العمومية والخاصة على اعتماد سياسات واضحة لأمن المعلومات، تتضمن إدارة المخاطر، وخطط الاستجابة للحوادث، وحماية البيانات الحساسة .

- دعم التعاون الدولي والإقليمي في مجال مكافحة الجرائم المعلوماتية وتبادل الخبرات والمعلومات التقنية والقانونية المتعلقة بالأمن السيبراني .

- تحديث وسائل الإثبات القانونية بما يتلاءم مع طبيعة الجرائم المرتبطة بالذكاء الاصطناعي والأدلة الرقمية، وتكوين القضاة وأجهزة الضبطية القضائية في هذا المجال .

- وضع آليات رقابية تضمن الشفافية في عمل الأنظمة الذكية، وتفادي الانحيازات أو الأخطاء التي قد تمس حقوق الأفراد أو تؤثر على القرارات الآلية .

وفي الأخير، يمكن القول إن الذكاء الاصطناعي يمثل سلاحا ذا حدين، فمن جهة يوفر إمكانيات هائلة لتعزيز أمن المعلومات وحماية الأنظمة الرقمية ومواجهة التهديدات السيبرانية، ومن جهة أخرى، يطرح تحديات قانونية وأخلاقية معقدة تتطلب تطوير التشريعات الوطنية والدولية بما يحقق التوازن بين متطلبات الأمن الرقمي وضمان احترام الحقوق والحريات الأساسية.

وعليه، فإن تحقيق حماية فعالة لأمن المعلومات في ظل الذكاء الاصطناعي لا يمكن أن يتحقق بالاعتماد على الوسائل التقنية وحدها، بل يتطلب أيضا وجود إطار قانوني متكامل، وسياسات أمنية فعالة، وتعاون دولي مستمر، وثقافة رقمية واعية، حتى تتمكن الدول والمؤسسات من الاستفادة من مزايا الذكاء الاصطناعي دون الوقوع في مخاطره وانعكاساته السلبية.

قائمة المصادر والمراجع

قائمة المصادر

أولا–القران الكريم

سورة المجادلة، الآية 11

ثانيا– الإتفاقيات الدولية والمقارنة

1- الإعلان العالمي لحقوق الإنسان، المعتمد من الجمعية العامة للأمم المتحدة بتاريخ 10 ديسمبر 1948، المادة 12.

2- العهد الدولي الخاص بالحقوق المدنية والسياسية، المعتمد بتاريخ 16 ديسمبر 1966، دخل حيز النفاذ في 23 مارس 1976، المادة 17.

3- مجلس أوروبا، اتفاقية حماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، السلسلة الأوروبية للمعاهدات رقم 108، ستراسبورغ، 28 يناير 1981.

4- مجلس أوروبا، اتفاقية الجرائم الإلكترونية، بودابست، السلسلة الأوروبية للمعاهدات رقم 185، 23 نوفمبر 2001.

5- اللائحة (الاتحاد الأوروبي) 679/2016 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016، اللائحة العامة لحماية البيانات، الجريدة الرسمية للاتحاد الأوروبي، العدد119 L ، بتاريخ 4 مايو 2016.

6- مجلس أوروبا، البروتوكول المعدِّل لاتفاقية حماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، السلسلة الأوروبية للمعاهدات رقم 223، سنة 2018.

7- منظمة التعاون والتنمية الاقتصادية(OECD) ، توصية المجلس بشأن الذكاء الاصطناعي، المرجعOECD/LEGAL/0449 ، المعتمدة سنة 2019 والمحدَّثة سنة 2024.

8- اللائحة (الاتحاد الأوروبي) 1689/2024 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 13 يونيو 2024، والمتعلقة بوضع قواعد منسَّقة بشأن الذكاء الاصطناعي.

9- الأمم المتحدة، اتفاقية الأمم المتحدة لمكافحة الجرائم الإلكترونية، المعتمدة بموجب قرار الجمعية العامة رقم 243/79 بتاريخ 24 ديسمبر 2024.

ثالثا– الدستور

1- المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق ل30 ديسمبر سنة2020 المتعلق بإصدار التعديل الدستوري 2020 ، ، ج.ر.ج.ج، عدد 82 الصادر 15 جمادي الاولى 1442هـ الموافق ل30 ديسمبر 2020 المعدل و المتمم بموجب القانون رقم 26/04 المؤرخ في 26 مارس 2026، الجريدة الرسمية، العدد 22 بتاريخ 26 مارس 2026

رابعا– القوانين العادية

1- القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادرة بتاريخ 16 أوت 2009.

2- القانون رقم 15-04 المؤرخ في 1 فيفري 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 06، الصادرة بتاريخ 10 فبراير2015.

3- القانون رقم 18-04 المؤرخ في 10 ماي 2018، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 27 ، الصادرة بتاريخ 13 مايو 2018.

4- القانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 28، الصادرة بتاريخ 16 مايو 2018.

5- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 34، الصادرة بتاريخ 10 يونيو 2018. المعدل و المتمم بموجب القانون رقم 25-11 المؤرخ في 28 محرم عام 1447 الموافق 24 يوليو سنة 2025، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 48، الصادرة بتاريخ 24 يوليو 2025.

6-1- القانون رقم 24-06، المؤرخ في 19 شوال عام 1445 الموافق لـ 28أبريل سنة 2024، المتضمن قانون العقوبات الجزائري جريدة رسمية العدد 30 الصادرة بتاريخ 30 أبريل 2024 والذي تضمن تعديل وتتميم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966

خامسا- الأوامر

1- الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم بموجب القانون رقم 24-06 المؤرخ في 28 أفريل 2024 الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، العدد 30 الصادرة بتاريخ 30 أبريل 2024

2- الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975، المتضمن القانون المدني الجزائري، المعدل والمتمم بالقانون رقم 05-10 المؤرخ في 20 يونيو 2005 ، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، العدد 44 .

3- الأمر رقم 21-09 المؤرخ في 27 شوال عام 1442 الموافق 8 يونيو سنة 2021، المتعلق بحماية المعلومات والوثائق الإدارية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 45، الصادرة بتاريخ 9 يونيو 2021.

سادسا- المراسيم الرئاسية

1- المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية ، العدد 04 ، الصادرة بتاريخ 26 جانفي 2020 .

2- المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 86، الصادرة بتاريخ 11 نوفمبر 2021.

3- المرسوم الرئاسي رقم 22-187 المؤرخ في 18 ماي 2022، المتضمن تعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 35، الصادرة بتاريخ 24 ماي 2022.

سابعا– المراسيم التنفيذية

1- المرسوم التنفيذي رقم 16-134 المؤرخ في 25 أفريل 2016، المحدد لتنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 26، الصادرة بتاريخ 28 أبريل2016.

قائمة المراجع باللغة العربية

أولا– الكتب

1- أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، دار هومة للنشر، الجزائر، طبعة 15، 2016.

2- حيدر فالح سلمان، الخلود الرقمي – الذكاء الاصطناعي ومستقبل البشر، دار جامعة حمد بن خليفة للنشر، بدون طبعة ، بدون سنة نشر.

3- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية للطباعة والنشر، الإسكندرية، بدون طبعة ، 2008.

4- خالد ممدوح إبراهيم، أمن المعلومات، الدار الجامعية، الإسكندرية، طبعة1، 2008.

5- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، طبعة1، 2009.

6- خالد ممدوح، أمن المعلومات والخصوصية في ظل التحديات السيبرانية، دار الفكر الجامعي، الإسكندرية، طبعة 1، 2021.

7- خالد ناصر السيد، أصول الذكاء الاصطناعي، مكتبة الرشد، الرياض، بدون طبعة، 2004.

8- رامي متولي القاضي، المسؤولية القانونية عن أخطاء الذكاء الاصطناعي، دار الجامعة الجديدة، الإسكندرية، بدون طبعة ، 2020.

9- عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، طبعة1، 2003.

10- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، طبعة1، 2006.

11- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي: دراسة قانونية متعمقة في القانون المعلوماتي، دار الفكر الجامعي، الإسكندرية، بدون طبعة ، 2006.

12- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، بدون طبعة ، 2007.

13- عبد الملك الدناني، خالد درار، عمر بن عمر، تقنيات الذكاء الاصطناعي وتطبيقاته في المجال الإعلامي بالدول العربية، دار شهر زاد للنشر والتوزيع، عمان، طبعة1، 2025.

14- عمار بوضياف، المعاهدات الدولية وأثرها في القوانين الداخلية، دار ريحانة، الجزائر، طبعة2، 2017.

15- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، بدون طبعة ، 2004.

16- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، طبعة 2، 2012.

17- محمد كمال الصاوي، الدليل الرقمي وإجراءات التحقيق في الجرائم التكنولوجية، مطبعة المعارف، القاهرة، 2021.

18- مروان محمد عبده، المسؤولية المدنية والجنائية في جرائم الحاسب الآلي، دار الكتب القانونية، مصر، طبعة1، 2018.

19- منال بومعراف، الذكاء الاصطناعي رؤية متعددة التخصصات، كتاب جماعي دولي محكم، المركز الديمقراطي العربي للدراسات الإستراتيجية والاقتصادية والسياسية، برلين، طبعة1، أفريل 2024.

20- نهال عبد القادر المومني، الجرائم المعلوماتية, دار الثقافة للنشر والتوزيع، عمان، طبعة1، 2008.

21- وافي حاجة، استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني، منشورات دار لايمة، الجزائر، 2025.

22- يونس عرب، جرائم الكمبيوتر والإنترنت، اتحاد المصارف العربية، بيروت، طبعة1، 2001.

23- يونس عرب، موسوعة القانون وتقنية المعلومات: قانون الكمبيوتر، اتحاد المصارف العربية، بيروت، طبعة1، 2002.

ثانيا: المقالات في المجلات العلمية

1- بليان مسعود، عكنوش نبيل، «أمن الوثائق والمعلومات الإلكترونية واستراتيجيات حفظها في الأرضية الرقمية لقطاع التربية»، مجلة المعيار، مجلة 25، عدد59، 2021.

2- سهيلة بضياف وآمنة حمراني، «أمن المعلومات في الجزائر – الإجراءات والتحديات»، المجلة الجزائرية للأمن والتنمية، مجلة 09، عدد 16، جانفي 2020.

3- سارة بوشتاتة، «التوازن القانوني بين الأمن السيبراني والخصوصية»، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة الجزائر 1، مجلة 58، عدد 01، 2021.

4- علي بن خلفان بن علي الهنائي، «تطبيقات الذكاء الاصطناعي في المجال الأمني: دراسة مطبقة على دول مجلس التعاون لدول الخليج العربية»، مجلة الدراسات القانونية والاقتصادية، مجلة 10، عدد 04، 2024.

5- فيلالي أسماء، شليل عبد اللطيف، «تهديدات أمن المعلومات وسبل التصدي لها»، مجلة البشائر الاقتصادية، مجلة 04، عدد 03، 2017.

6- قدافيه أمينة، «استراتيجية أمن المعلومات»، مجلة أبعاد اقتصادية، مجلة 06، عدد01،

7- قندوز فتيحة، «الجوانب القانونية لاستخدام الذكاء الاصطناعي»، المجلة الجزائرية للحقوق والعلوم السياسية، الجزائر، مجلة 09، عدد 01، 2024.

8- ليلى بن شيخ، «الآليات القانونية لحماية البيانات الشخصية في التشريع الجزائري»، مجلة الدراسات القانونية والسياسية، جامعة الوادي، مجلة 05، عدد 02، 2019.

9- ياسين بن ورزق، «التحديات القانونية للذكاء الاصطناعي»، مجلة الاجتهاد للدراسات القانونية، المركز الجامعي تمنراست، عدد 12، 2022.

ثالثا– الرسائل و المذكرات الجامعية

مذكرات ماجيستير

1-خالد ياسين الشيخ، أمن نظم المعلومات والرقابة (التحكم)، مذكرة ماجستير، جامعة دمشق، المعهد العالي للتنمية الإدارية، 2010.

2-وفاء شويتامي، الحماية القانونية للبيانات الشخصية في المعاملات الإلكترونية، مذكرة ماجستير، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر 1،2015.

مذكرات ماستر

1- عبد الباسط عيساوي، سفيان زيتون، آثار الذكاء الاصطناعي على الأمن السيبراني: دراسة حالة الجزائر، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، 2024.

رابعا- الملتقيات والمؤتمرات والتقارير والمعايير

1- أحمد الحصيني، مقدمة أمن المعلومات، منتدى الرياض الاجتماعي الثالث: المجتمع والتقنية – مجلة تحديات وآفاق، جانفي 2020.

2- محمد طول، أمل بكار، أساسيات حول الذكاء الاصطناعي – إطار مفاهيمي، ملتقى وطني افتراضي حول استخدامات الذكاء الاصطناعي كضمان لجودة التعليم العالي والبحث العلمي، 7 نوفمبر 2022.

3- مبسوطة حمد الحاسي، استراتيجية التكامل بين الذكاء الاصطناعي والأمن السيبراني في رصد ومواجهة الهجمات السيبرانية المبكرة، المؤتمر الدولي الأول للتعليم الإلكتروني وتكنولوجيا المعلومات، جامعة الزاوية، ليبيا، 2025.

4- أبوستول فاسيليف وآخرون، **التعلّم الآلي العدائي: تصنيف ومصطلحات الهجمات وسبل التخفيف منها**، NIST AI 100-2e2025، المعهد الوطني للمعايير والتكنولوجيا، 2025.

5- معيار ISO/IEC 27001:2022 ، **أمن المعلومات والأمن السيبراني وحماية الخصوصية — نظم إدارة أمن المعلومات — المتطلبات**، المنظمة الدولية للتوحيد القياسي، 2022.

6- معيار ISO/IEC 27002:2022 ، **أمن المعلومات والأمن السيبراني وحماية الخصوصية — ضوابط أمن المعلومات**، المنظمة الدولية للتوحيد القياسي، جنيف، 2022.

7- معيار ISO/IEC 27701:2019 ، **تقنيات الأمن — امتداد لمعياري ISO/IEC 27001وISO/IEC 27002لإدارة معلومات الخصوصية**، المنظمة الدولية للتوحيد القياسي، جنيف، 2019.

8 -كارين سكارفون وموروغياه سوبايا، **دليل إدارة كلمات المرور في المؤسسات**، منشور NISTالخاص رقم 800-118، المعهد الوطني للمعايير والتكنولوجيا، 2009.

9- المعهد الوطني للمعايير والتكنولوجيا، **إطار إدارة مخاطر الذكاء الاصطناعي AI RMF 1.0**، NIST AI 100-1، وزارة التجارة الأمريكية، يناير 2023.

10-المعهد الوطني للمعايير والتكنولوجيا، **إطار الأمن السيبراني NIST CSF 2.0** ، ورقة بيضاء في الأمن السيبراني صادرة عن NIST ، 26 فبراير 2024.

11- معهد ستانفورد للذكاء الاصطناعي المرتكز على الإنسان، **تقرير مؤشر الذكاء الاصطناعي لسنة 2026**، 2026.

12- فنسنت سي. هو، ديفيد فيرايولو، ريك كون، آدم شنيتزر، كينيث ساندلين، روبرت ميلر، كارين سكارفون، **دليل تعريف التحكم في الوصول القائم على السمات (ABAC) واعتباراته**، منشور NIST الخاص رقم 800-162، المعهد الوطني للمعايير والتكنولوجيا، 2014.

13- فنسنت سي. هو، دي. ريتشارد كون، ديفيد إف. فيرايولو، جيفري فواس، **التعلّم الآلي للتحقق من سياسات التحكم في الوصول**، NISTIR 8360، المعهد الوطني للمعايير والتكنولوجيا، 2021.

خامسا– المواقع الإلكترونية

1- المنصة الوطنية للمجلات العلمية ASJP: https://www.asjp.cerist.dz

2- موقع جمعية الحماية الرقمية: https://hemaya.org.sa

قائمة المراجع باللغة الأجنبية :

1-Alex Krizhevsky, Ilya Sutskever, Geoffrey E. Hinton, ImageNet Classification with Deep Convolutional Neural Networks, NeurIPS, 2012

2- Clarence Chio and David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms, O'Reilly Media, 1st Edition, 2018.

3 - Ethem Alpaydin, Introduction to Machine Learning, MIT Press, 4th Edition, 2020 .

4- Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning, MIT Press, 2016.

5- Murat Kantarcioglu and Bhavani Thuraisingham, Data Mining for Security Applications, IOS Press, Amsterdam, 2008.

6-Soma Halder and Sinan Ozdemir, Hands-On Machine Learning for Cybersecurity, Packt Publishing, 1st Edition, 2018.

7- Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach, 4th ed., Pearson, 2021.

8- Sumeet Dua and Xian Du, Data Mining and Machine Learning in Cybersecurity, CRC Press, 1st Edition, 2011.

فهرس المحتويات

فهرس المحتويات

العنوان	الصفحة
شكر وعرفان	
إهداء	
قائمة المختصرات	
مقدمة	أ
الفصل الأول :الإطار النظري لأمن المعلومات في مجال الذكاء الاصطناعي	**4**
المبحث الأول :الإطار المفاهيمي لأمن المعلومات في مجال الذكاء الاصطناعي	5
المطلب الأول :مفهوم أمن المعلومات	6
الفرع الأول :تعريف أمن المعلومات	6
أولا :المقصود بأمن المعلومات	6
ثانيا :خصائص أمن المعلومات	9
الفرع الثاني :أهمية وأهداف أمن المعلومات	10
أولا :أهمية أمن المعلومات	10
ثانيا :أهداف أمن المعلومات	10
الفرع الثالث :مخاطر أمن المعلومات	11
المطلب الثاني :الذكاء الاصطناعي	13
الفرع الأول :تطور الذكاء الاصطناعي	13
أولا: مراحل تطور الذكاء الاصطناعي	13
ثانيا :تعريف الذكاء الاصطناعي	15
ثالثا :خصائص الذكاء الاصطناعي	15
الفرع الثاني :أنواع الذكاء الاصطناعي	16
الفرع الثالث :تطبيقات الذكاء الاصطناعي في مجال أمن المعلومات	16
المبحث الثاني :دور الذكاء الاصطناعي في تعزيز أمن المعلومات	18
المطلب الأول :آليات الذكاء الاصطناعي في الكشف عن التهديدات المعلوماتية	19
الفرع الأول :الكشف المبكر عن الهجمات والاختراقات السيبرانية	19
الفرع الثاني :تحليل السلوكيات غير الطبيعية والتنبؤ بالمخاطر	20
الفرع الثالث :الاستجابة الذكية للحوادث الأمنية واحتواؤها	21
المطلب الثاني :مساهمة الذكاء الاصطناعي في تطوير وسائل حماية أمن المعلومات	22
الفرع الأول :استخدام الذكاء الاصطناعي في أنظمة المصادقة والتحكم في الولوج	23
الفرع الثاني :حماية الشبكات والبيانات بواسطة تقنيات التعلم الآلي	24

فهرس المحتويات

الفرع الثالث :مزايا اعتماد الذكاء الاصطناعي في مجال أمن المعلومات	25
الفصل الثاني :الإطار القانوني لحماية أمن المعلومات في ظل الذكاء الاصطناعي	**26**
المبحث الأول :التنظيم القانوني لحماية أمن المعلومات	27
المطلب الأول :الأساس القانوني الدولي والوطني لحماية أمن المعلومات	28
الفرع الأول :الاتفاقيات والمعايير الدولية في مجال الأمن السيبراني وحماية البيانات	28
الفرع الثاني :التشريعات الوطنية الخاصة بحماية المعطيات والبيانات الشخصية	32
الفرع الثالث :القوانين الوطنية المتعلقة بمكافحة الجرائم المعلوماتية	38
المطلب الثاني :الحماية القانونية للخصوصية والبيانات الشخصية	44
الفرع الأول :الأساس القانوني للحق في الخصوصية الرقمية	44
الفرع الثاني :الضمانات القانونية لمعالجة وحماية البيانات الشخصية	47
الفرع الثالث :المسؤولية القانونية عن انتهاك أمن المعلومات وخرق الخصوصية	50
المبحث الثاني: خاطر و افاق حماية أمن المعلومات في ظل الذكاء الاصطناعي	53
المطلب الأول :التحديات القانونية في مجال الذكاء الاصطناعي	53
الفرع الأول :صعوبة تحديد المسؤولية القانونية عن أفعال الأنظمة الذكية	54
الفرع الثاني :قصور وعدم ملاءمة التشريعات الحالية للتطور التكنولوجي	56
الفرع الثالث: صعوبة الإثبات في الجرائم المرتبطة بالذكاء الاصطناعي	58
المطلب الثاني :آليات وآفاق تطوير الحماية القانونية لأمن المعلومات في مجال الذكاء الاصطناعي	60
الفرع الأول : :تعزيز التعاون الدولي في مجال الأمن المعلوماتي	61
الفرع الثاني: :تحديث وتطوير التشريعات الوطنية لمواكبة الذكاء الاصطناعي	63
الفرع الثالث :تحقيق التوازن بين حماية الأمن المعلوماتي وضمان الحقوق والحريات الفردية	64
خاتمة	70
قائمة المصادر والمراجع	73
فهرس المحتويات	83
ملخص	85

الملخص

يشهد أمن المعلومات في العصر الحديث أهمية متزايدة باعتباره من أبرز التحديات القانونية والتقنية التي فرضها التطور الرقمي المتسارع، خاصة مع الانتشار الواسع لتقنيات الذكاء الاصطناعي، فقد ساهمت هذه التقنيات في تعزيز حماية الأنظمة المعلوماتية من خلال الكشف المبكر عن التهديدات السيبرانية، تحليل المخاطر الرقمية، والاستجابة السريعة للهجمات الإلكترونية، مما أدى إلى رفع مستوى فعالية الأمن السيبراني وتحسين آليات حماية البيانات.

وفي المقابل أثار استخدام الذكاء الاصطناعي العديد من الإشكالات القانونية المرتبطة بحماية المعطيات الشخصية والحق في الخصوصية داخل البيئة الرقمية، الأمر الذي يفرض ضرورة تطوير الأطر القانونية بما يواكب التحولات التكنولوجية الحديثة، ففعالية أمن المعلومات لا تتحقق فقط بالاعتماد على الوسائل التقنية المتطورة، وإنما تتطلب أيضاً توفير حماية قانونية صارمة تضمن مكافحة الجرائم الإلكترونية وتنظيم استخدام البيانات الرقمية ، و من جهة أخرى فان تحقيق أمن معلومات فعال يستوجب ايجاد توازن بين متطلبات الأمن الرقمي داخل البيئة الرقمية.

وتهدف هذه الدراسة إلى إبراز مدى إسهام تقنيات الذكاء الاصطناعي في ضمان وتعزيز أمن المعلومات وحماية البيانات، وبيان دورها في حفظ سرية المعلومات وسلامتها وتوافرها، مع تقييم مدى كفاية أو قصور الآليات القانونية والتقنية المعتمدة في مواجهة المخاطر والتحديات الناجمة عن استخدام هذه التقنيات، واقتراح السبل الكفيلة بتعزيز الحماية القانونية والتقنية بما يحقق أمنًا معلوماتيًا أكثر فعالية.

الكلمات المفتاحية :أمن المعلومات، الذكاء الاصطناعي، الأمن السيبراني ، الحماية القانونية.

Abstract

Information security has become a critical issue in the contemporary digital era, representing one of the most significant legal and technological challenges arising from rapid digital transformation, particularly with the widespread adoption of Artificial Intelligence (AI) technologies. AI has played a vital role in enhancing the security of information systems by enabling the early detection of cyber threats, analyzing digital risks, and providing rapid responses to cyberattacks. These capabilities have significantly improved the effectiveness of cybersecurity and strengthened data protection mechanisms.

However, the increasing use of AI has also generated complex legal challenges concerning the protection of personal data and the right to privacy within the digital environment. Consequently, there is a pressing need to develop legal frameworks capable of keeping pace with technological advancements while ensuring the responsible use of AI technologies. Effective information security depends not only on advanced technological solutions but also on comprehensive legal protection that addresses cybercrime, regulates the processing and use of digital data, and safeguards individuals' fundamental rights. Therefore, achieving a secure digital environment requires striking an appropriate balance between cybersecurity requirements and the protection of privacy and other fundamental rights.

This study aims to examine the extent to which artificial intelligence technologies contribute to ensuring and strengthening information security and data protection. It further analyzes their role in maintaining the confidentiality, integrity, and availability of information, while evaluating the effectiveness of the existing legal and technical mechanisms in addressing the risks and challenges associated with the use of these technologies. In addition, the study explores the adequacy of the current regulatory framework and proposes recommendations for enhancing both legal and technical safeguards to achieve a higher level of information security

Keywords: Information Security; Artificial Intelligence (AI); Cybersecurity; Legal Protection; Personal Data Protection