



جامعة د/ مولاي الطاهر سعيدة

كلية الحقوق والعلوم السياسية
قسم الحقوق

تخصص:

قانون جنائي و علوم جنائية



عنوان المذكرة

واقع أمن المعلوماتي في ظل الذكاء الاصطناعي

تحت إشراف الأستاذة:

أ. عمارة فتيحة

إعداد الطالبين:

• مؤذن حبيب

• بن الدين فتحي



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



إهداء

أهدي هذا العمل المتواضع إلى:

إلى من كانا سبباً في وجودي، ومن علماني أن الدنيا كفاح وسلاحها العلم والمعرفة،
إلى من غمراني بدعواتهما، وكانا النور الذي أضاء دربي في كل خطوة.

إلى والديّ العزيزين أطال الله في عمرهما.

إلى زوجتي الغالية، التي كانت ولا تزال السند والدعم،
وشريكة كل لحظة تعب ونجاح.

إلى إخوتي وأخواتي،
إلى كل أفراد، عائلتي الكريمة،
الذين كانوا دائماً بجانبني بالدعاء والتشجيع.

إلى أصدقائي الأوفياء، الذين شاركوني الطريق وكانوا السند في مسيرتي.

إلى زملائي وزميلاتي في الدراسة،
مع كل الشكر والتقدير والاحترام.

إليهم جميعاً، أهدي هذا الجهد المتواضع،
راجياً من الله أن يتقبل ويجعل فيه نفعا وفائدة.

بن الدين فتحي

إهداء

إلى والديّ الحبيبين

من كانا سبباً في وجودي، ومن غمراني بحبهما، وسهرا من أجلي،
وكانا الدعاء الذي لا ينقطع، والعطاء الذي لا سيم له.
شكراً من القلب على كل ما قدمتما لي،
فما وصلتُ إلى هنا إلا بفضلكما وبعد توفيق الله.
أطال الله في عمركما وأدامكما لي سنداً وعوناً.

إلى زوجتي الغالية

رفيقة دربي، وسندي في كل خطوة، منحتني الحب والدعم والصبر الجميل،
وكانت لي العون والدافع للاستمرار.
شكراً لوجودك في حياتي، فأنت جزء من كل نجاح أحققه.

إلى ابنتي العزيزة

نبض قلبي، ونور عيني، ابتسامتك كانت دائماً مصدر إلهامي وقوتي،
من أجلك أسعى اليوم، ولأجلك أطمح غذا.
أدامك الله لي فرحاً وسعادة في حياتي.

إلى الأساتذة الكرام

منارة العلم والمعرفة، لكم مني كل التقدير والاحترام.
أشكركم على ما قدمتموه من علم ونصح وتوجيه طيلة مسيرتي الدراسية.

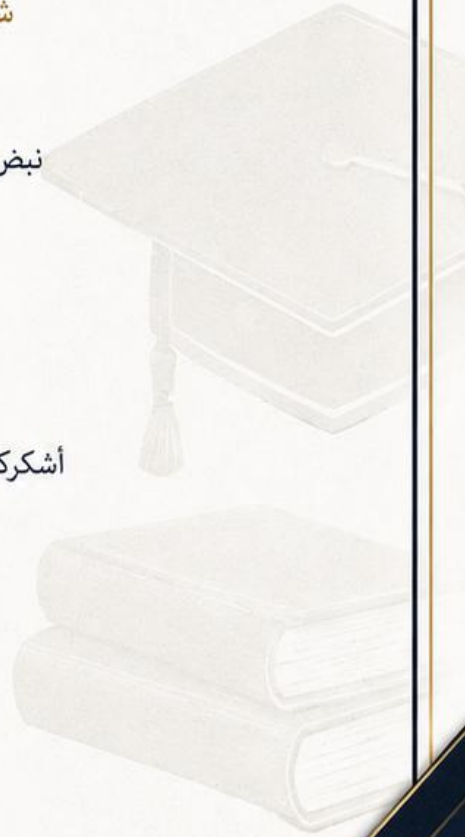
وبالأخص أستاذتي المشرفة

أ. عمارة فتيحة
على ما بذلته من جهد وإرشاد وتوجيه،
وعلى صبرها ودعمها، الكبير لإتمام هذه المذكرة.
جزاها الله عني كل خير.

إلى أصدقائي الأعزاء

الذين شاركوني أيام الدراسة، وكانت لهم بصمة جميلة في رحلتي،
بمواقفهم الصادقة، ودعمهم المعنوي، ورفقتهم الطيبة.
لكم مني كل المحبة والتقدير.

مؤذن حبيب



المقدمة

تعيش المجتمعات المعاصرة تحولاً رقمياً متسارعاً شمل مختلف مجالات الحياة، حيث أصبحت التكنولوجيا الحديثة عنصراً أساسياً في تسيير المؤسسات وتبادل المعلومات وتقديم الخدمات. وقد ساهم هذا التطور في ظهور تقنيات متقدمة كان لها أثر كبير في تغيير طبيعة العمل والتواصل واتخاذ القرار، ويأتي الذكاء الاصطناعي في مقدمة هذه التقنيات باعتباره من أبرز مظاهر الثورة الرقمية الحديثة. فلم يعد الذكاء الاصطناعي مجرد فكرة نظرية مرتبطة بالخيال العلمي، بل أصبح واقعاً عملياً حاضراً في مجالات متعددة، مثل الصحة، والتعليم، والاقتصاد، والإدارة، والأمن، والنقل، والإعلام، وغيرها من القطاعات التي تعتمد على البيانات والتحليل والتوقع.

ويقوم الذكاء الاصطناعي على قدرة الأنظمة الحاسوبية على معالجة كميات ضخمة من البيانات وتحليلها واستنتاج نتائج تساعد على اتخاذ القرارات أو التنبؤ بالمخاطر أو تحسين الأداء. وقد أدى التطور الكبير في تقنيات التعلم الآلي والتعلم العميق إلى توسيع نطاق استعمال هذه الأنظمة بصورة غير مسبوقة، مما جعلها أداة فعالة في دعم المؤسسات والأفراد وتسهيل العديد من العمليات المعقدة. غير أن هذا التطور السريع لم يخلُ من تحديات ومخاطر، خاصة في ظل الاعتماد المتزايد على الفضاء الرقمي وتوسع تداول المعلومات عبر الشبكات والأنظمة الإلكترونية.

وفي هذا السياق، برز الأمن المعلوماتي باعتباره من أهم القضايا المرتبطة بالتحول الرقمي، نظراً لما أصبحت تمثله المعلومات من قيمة استراتيجية بالنسبة للأفراد والمؤسسات والدول. فحماية البيانات والأنظمة والشبكات من الاختراق أو التلاعب أو التسريب أصبحت ضرورة حتمية لضمان استمرارية الخدمات وحماية الخصوصية والحفاظ على الثقة في البيئة الرقمية. كما أن تطور الهجمات السيبرانية وتعدد أساليب الاختراق جعل الوسائل التقليدية للحماية غير كافية في كثير من الأحيان، الأمر الذي دفع إلى البحث عن أدوات

أكثر قدرة على التحليل والكشف والاستجابة السريعة، وكان الذكاء الاصطناعي من أبرز هذه الأدوات.

وقد أصبح الذكاء الاصطناعي يستعمل بصورة متزايدة في مجال الأمن المعلوماتي، من خلال كشف الهجمات الإلكترونية، وتحليل السلوكيات المشبوهة، والتنبؤ بالتهديدات، ومراقبة الشبكات، وتحسين سرعة الاستجابة للحوادث الأمنية. إلا أن العلاقة بين الذكاء الاصطناعي والأمن المعلوماتي ليست علاقة إيجابية مطلقة، لأن هذه التقنية يمكن أن تستعمل أيضًا في تطوير هجمات أكثر خطورة وتعقيدًا، مثل الهجمات الآلية، والتصيد الاحتيالي الذكي، والتزييف العميق، وتحليل الثغرات الأمنية بصورة أسرع وأكثر دقة. ومن هنا تظهر الطبيعة المزدوجة للذكاء الاصطناعي، باعتباره أداة للحماية من جهة، ومصدرًا لتهديدات جديدة من جهة أخرى.

وتكمن أهمية هذا الموضوع في كونه يجمع بين مجالين يعدان من أكثر المجالات تأثيرًا في العصر الرقمي، وهما الذكاء الاصطناعي والأمن المعلوماتي، كما يكتسي أهمية علمية وعملية بالنظر إلى التوسع الكبير في استخدام الأنظمة الذكية داخل المؤسسات والقطاعات الحيوية، وما يرافق ذلك من مخاطر تتعلق بحماية البيانات والخصوصية والأمن السيبراني. كما أن دراسة هذا الموضوع تساعد على فهم طبيعة التحديات الجديدة التي فرضها الذكاء الاصطناعي على أنظمة الحماية التقليدية، وتبرز في الوقت نفسه الإمكانيات التي يوفرها لتعزيز أمن المعلومات ومواجهة التهديدات الرقمية الحديثة.

وانطلاقًا من ذلك، تتمثل إشكالية هذه الدراسة في التساؤل الآتي:

إلى أي مدى يساهم الذكاء الاصطناعي في تعزيز الأمن المعلوماتي، وما أبرز المخاطر والتحديات التي يطرحها في البيئة الرقمية؟

ويندرج ضمن هذه الإشكالية عدد من التساؤلات الفرعية، أهمها:

• ما المقصود بالذكاء الاصطناعي وما أبرز خصائصه وتطبيقاته؟

• ما مفهوم الأمن المعلوماتي وما العناصر التي يقوم عليها؟

- كيف يساهم الذكاء الاصطناعي في حماية الأنظمة والمعلومات؟
- ما المخاطر والتحديات الأمنية والقانونية المرتبطة باستعمال الذكاء الاصطناعي؟

وللإجابة عن هذه التساؤلات، تم الاعتماد على المنهج الوصفي التحليلي، من خلال عرض المفاهيم الأساسية المتعلقة بالذكاء الاصطناعي والأمن المعلوماتي، وتحليل العلاقة بينهما، ودراسة التطبيقات العملية والمخاطر المرتبطة باستخدام الأنظمة الذكية في المجال الأمني. وتهدف هذه الدراسة إلى توضيح مفهوم الذكاء الاصطناعي وبيان خصائصه وأهم تطبيقاته، مع إبراز طبيعة الأمن المعلوماتي وأبعاده المختلفة، ثم تحليل الدور الذي يؤديه الذكاء الاصطناعي في تعزيز الحماية الرقمية والكشف عن التهديدات الإلكترونية، إضافة إلى تسليط الضوء على أبرز التحديات والمخاطر التي قد تنتج عن سوء استخدام هذه التقنية أو الاعتماد المفرط عليها.

وقد تم تقسيم هذه الدراسة إلى ثلاثة فصول مترابطة، تناول كل فصل منها جانباً محدداً من الموضوع. حيث حُصص الفصل الأول لدراسة ماهية الذكاء الاصطناعي وتطبيقاته، من خلال بيان مفهوم الذكاء الاصطناعي وتطوره التاريخي، وشرح خصائصه التقنية، والتميز بينه وبين المفاهيم القريبة منه مثل تعلم الآلة والتعلم العميق والأتمتة والروبوتات، كما تم التطرق إلى تصنيفاته المختلفة وأبرز مجالات استخدامه، مع إبراز أهم المخاطر والتحديات المصاحبة لانتشاره.

أما الفصل الثاني فقد تناول مفهوم الأمن المعلوماتي في البيئة الرقمية وعلاقته بالذكاء الاصطناعي، حيث تم التطرق إلى تعريف الأمن المعلوماتي وتمييزه عن الأمن السيبراني، وشرح العناصر الأساسية التي يقوم عليها، والمتمثلة في السرية والسلامة والإتاحة، إضافة إلى بيان أهميته بالنسبة للأفراد والمؤسسات في ظل التوسع الرقمي. كما تناول الفصل طبيعة التهديدات والهجمات الإلكترونية الحديثة، وأثر الذكاء الاصطناعي في تغيير أساليب الحماية والهجوم داخل البيئة الرقمية.

في حين حُصص الفصل الثالث لدراسة دور الذكاء الاصطناعي في تعزيز الأمن المعلوماتي، وذلك من خلال تحليل أهم التطبيقات الأمنية القائمة على الأنظمة الذكية، مثل كشف الهجمات السيبرانية، وتحليل السلوك المشبوه، والاستجابة للحوادث الأمنية، وحماية الشبكات والبيانات. كما تم التطرق إلى التحديات القانونية والأخلاقية المرتبطة باستخدام الذكاء الاصطناعي في المجال الأمني، خاصة ما يتعلق بحماية الخصوصية، ومسؤولية القرارات الخوارزمية، وخطر التحيز والتلاعب بالمعلومات، إضافة إلى إبراز الحاجة إلى وضع أطر قانونية وتنظيمية تضمن الاستخدام الآمن والمسؤول لهذه التقنية.

الفصل الأول

الفصل الأول: ماهية الذكاء الاصطناعي وتطبيقاته

يُعدّ الفهم الدقيق لماهية الذكاء الاصطناعي وتطبيقاته خطوة تأسيسية لا غنى عنها قبل تناول دوره المباشر في مجال الأمن المعلوماتي. فمن غير الممكن تقييم أثر هذه التقنية أو ضبط مخاطر الاستفادة منها دون الإحاطة بطبيعتها التقنية، ومسارها التطوري، وخصائصها الوظيفية، والتميز بينها وبين المفاهيم القريبة منها. وانطلاقاً من ذلك، يُخصّص هذا الفصل لتأطير الذكاء الاصطناعي مفهوميًا وتطبيقيًا، حيث سيتناول في مبحثه الأول تعريفه وتطوره التاريخي وخصائصه الفنية والفرق بينه وبين المفاهيم المشابهة، بينما يُخصّص المبحث الثاني لتصنيفاته وأنواعه، وأبرز مجالات استعماله، والمخاطر العامة التي يثيرها انتشاره.

المبحث الأول: الإطار المفاهيمي للذكاء الاصطناعي

يمثل الذكاء الاصطناعي أحد أكثر المفاهيم التقنية حضورًا في النقاشات الحديثة، غير أن كثرة استعماله جعلت معناه يبدو أحيانًا واسعًا ومضطربًا، إذ يُستعمل للدلالة على برامج بسيطة تقوم بتنفيذ أوامر محددة، كما يُستعمل في الوقت نفسه للدلالة على أنظمة قادرة على التعلم والتحليل واتخاذ القرار. لذلك فإن تحديد مفهوم الذكاء الاصطناعي لا يكون بمجرد القول إنه “آلة تفكر”، بل ينبغي فهمه من خلال عناصره الأساسية، وهي: وجود نظام آلي، وجود بيانات يتعامل معها، وجود خوارزميات تعالج تلك البيانات، ووجود مخرجات قد تكون توقعات أو توصيات أو قرارات تؤثر في الواقع المادي أو الرقمي.

المطلب الأول: تعريف الذكاء الاصطناعي ومراحل تطوره التاريخي

يقصد بالذكاء الاصطناعي عمومًا قدرة الأنظمة الحاسوبية على أداء مهام كانت في الأصل تحتاج إلى قدر من الذكاء البشري، مثل التعلم، والاستنتاج، وفهم اللغة، والتعرف على الصور والأصوات، واتخاذ القرار. ولا يتعلق الأمر هنا بذكاء مطابق تمامًا للذكاء الإنساني، بل بقدرة تقنية مصممة لمعالجة البيانات واستخراج الأنماط منها، ثم تحويلها إلى نتائج قابلة للاستعمال في مجالات مختلفة. وقد عرّفت منظمة التعاون

الاقتصادي والتنمية نظام الذكاء الاصطناعي بأنه نظام قائم على الآلة، يستطيع وفق أهداف صريحة أو ضمنية أن يستنتج من المدخلات التي يتلقاها كيفية توليد مخرجات مثل التنبؤات أو المحتوى أو التوصيات أو القرارات التي يمكن أن تؤثر في بيئات مادية أو افتراضية، مع اختلاف هذه الأنظمة في درجة استقلاليتها وقدرتها على التكيف بعد تشغيلها¹.

ويظهر من هذا التعريف أن الذكاء الاصطناعي لا يقوم على عنصر واحد فقط، بل على علاقة مركبة بين البيانات والخوارزمية والهدف والنتيجة. فالآلة لا تعمل من فراغ، وإنما تحتاج إلى مدخلات تتعلم منها أو تستند إليها، ثم تنتج مخرجات قد تساعد الإنسان في الاختيار أو التوقع أو التصنيف. ولهذا فإن جوهر الذكاء الاصطناعي لا يكمن في شكل الجهاز أو البرنامج، بل في طريقة اشتغاله وقدرته على تحويل البيانات إلى معرفة عملية. وهذا ما يجعل الذكاء الاصطناعي مختلفًا عن البرامج التقليدية التي تكتفي بتنفيذ أوامر ثابتة، لأن النظام الذكي يستطيع في بعض صورته أن يتعلم من البيانات وأن يغير أدائه مع مرور الوقت أما من الناحية التاريخية، فإن فكرة الذكاء الاصطناعي لم تظهر فجأة مع التطبيقات الحديثة، بل تعود جذورها إلى حلم قديم بمحاكاة بعض القدرات الإنسانية بواسطة الآلة. غير أن البداية العلمية الواضحة ارتبطت بتطور علوم الحاسوب والرياضيات والمنطق، خاصة بعد طرح آلان تورنغ لفكرة اختبار قدرة الآلة على تقديم إجابات لا يستطيع الإنسان تمييزها عن إجابات البشر. وقد ساعد هذا التصور المبكر على فتح النقاش حول إمكانية اعتبار الآلة "ذكية" متى استطاعت إظهار سلوك قريب من السلوك الإنساني في الحوار أو حل المشكلات².

¹ Oecd Artificial Intelligence Papers ,Explanatory Memorandum on the Updated OECD Definition of an AI System, No. 8, 2024 ,p.7.

https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_3c815e51/623da898-en.pdf

² Jamie Berryhill and Authors , Hello, World: Artificial Intelligence and its Use in the Public Sector , OECD Working Papers on Public Governance No. 36, 2019 ,

وفي سنة 1956 برز استعمال مصطلح الذكاء الاصطناعي بصورة أوضح مع جون مكارثي، الذي عدّه علماً وهندسة لصناعة الآلات الذكية. ويكشف هذا التعريف المبكر أن الذكاء الاصطناعي لم يكن في بدايته مجرد تطبيق تجاري أو أداة جاهزة، بل كان مشروعاً علمياً يهدف إلى بناء أنظمة قادرة على إنجاز مهام ذهنية بطريقة آلية. ومع مرور الوقت، تطور هذا المجال من الأنظمة الرمزية التي تعتمد على قواعد منطقية مكتوبة سلفاً، إلى أنظمة التعلم الآلي التي تستخرج القواعد من البيانات، ثم إلى التعلم العميق الذي يعتمد على الشبكات العصبية لمعالجة مشكلات أكثر تعقيداً.

وقد عرف الذكاء الاصطناعي مراحل من الصعود والتراجع، إذ اصطدم في بداياته بمحدودية قدرات الحواسيب وضعف حجم البيانات المتاحة، ثم عاد بقوة مع تطور المعالجات وظهور البيانات الضخمة وانتشار الإنترنت. فكلما زادت القدرة على جمع البيانات وتخزينها ومعالجتها، اتسع مجال تطبيق الذكاء الاصطناعي، لأن هذه الأنظمة تحتاج إلى كميات معتبرة من البيانات حتى تكتشف العلاقات والأنماط وتبني نتائج أكثر دقة. ولذلك يمكن القول إن التحول الحقيقي للذكاء الاصطناعي لم يكن بسبب الخوارزميات وحدها، بل بسبب اجتماع ثلاثة عوامل: قوة المعالجة، وفرة البيانات، وتطور نماذج التعلم الآلي والتعلم العميق.¹

ومن خلال هذا التطور، انتقل الذكاء الاصطناعي من مجال البحث النظري إلى مجال الاستعمال اليومي، فأصبح حاضراً في محركات البحث، وأنظمة الترجمة، والمساعدات الرقمية، والتشخيص الطبي، والخدمات البنكية، والتعليم، والنقل،

p.12.

https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/hello-world_7734f030/726fd39d-en.pdf

¹ مريم قيس علوي، الذكاء الاصطناعي: تطوره، تطبيقاته وتحدياته، مجلة لباب للدراسات الاستراتيجية، العدد 20، مركز الجزيرة

للدراستات، 2023، ص 7-8. <https://2u.pw/dUu2V6>

والأمن السيبراني. وهذا الانتقال جعله تقنية عامة التأثير، أي أنه لا يخص قطاعاً واحداً، بل يمتد إلى مختلف المجالات التي تعتمد على البيانات والقرار. ومن هنا تزداد أهمية ضبط مفهومه، لأن غموض التعريف يؤدي غالباً إلى خلطه بمفاهيم قريبة مثل الأتمتة، أو تعلم الآلة، أو الروبوتات، أو البيانات الضخمة.

المطلب الثاني: الخصائص التقنية للأنظمة الذكية

تتميز الأنظمة الذكية بمجموعة من الخصائص التقنية التي تجعلها مختلفة عن البرامج التقليدية. وأول هذه الخصائص هو الاعتماد على البيانات، لأن النظام الذكي لا يستطيع أن يتعلم أو يتنبأ أو يصنف دون وجود بيانات كافية تمثل المجال الذي يعمل فيه. فالبيانات بالنسبة للذكاء الاصطناعي ليست مجرد مادة خام، بل هي الذاكرة التي يتغذى منها النظام، وكلما كانت البيانات أكثر جودة وتنوعاً وتنظيماً، زادت قدرة النظام على إنتاج نتائج أقرب إلى الواقع. ولهذا ترتبط فعالية الذكاء الاصطناعي ارتباطاً وثيقاً بجودة البيانات المستعملة في تدريبه أو تشغيله¹.

وتتمثل الخاصية الثانية في القدرة على التعلم، وهي الخاصية التي تميز كثيراً من الأنظمة الذكية عن البرمجيات العادية. فالبرنامج التقليدي ينفذ أوامر محددة كما كتبها المبرمج، أما نظام التعلم الآلي فيستطيع استخراج أنماط من البيانات وبناء نتائج اعتماداً على الأمثلة التي عولجت مسبقاً. ولا يعني ذلك أن النظام يفهم مثل الإنسان، بل يعني أنه يحسن أدائه من خلال التدريب والتكرار واكتشاف العلاقات الإحصائية داخل البيانات. ولهذا يعد تعلم الآلة أحد أهم المجالات التي يتم من خلالها توظيف الذكاء الاصطناعي لتحقيق أهداف عملية محددة.

¹ نزمين مجدي، الذكاء الاصطناعي وتعلم الآلة، سلسلة كتيبات تعريفية العدد 03، صندوق النقد العربي، 2020، ص 8.

<https://www.amf.org.ae/sites/default/files/publications/2021-12/artificial-intelligence-machine-learning.pdf>

وتظهر الخاصية الثالثة في القدرة على الاستنتاج وإنتاج المخرجات. فالذكاء الاصطناعي لا يكتفي بجمع البيانات، بل يحاول تحويلها إلى نتائج قابلة للاستعمال، مثل التنبؤ بوقوع خطر معين، أو اقتراح مسار مناسب، أو تصنيف رسالة إلكترونية على أنها آمنة أو خبيثة، أو تقديم توصية للمستخدم. وقد أوضحت منظمة التعاون الاقتصادي والتنمية أن النظام الذكي يستنتج من المدخلات التي يتلقاها كيفية توليد مخرجات تشمل التنبؤات والمحتوى والتوصيات والقرارات، وهو ما يبرز الطبيعة العملية لهذه الأنظمة

أما الخاصية الرابعة فهي الاستقلالية النسبية. فالأنظمة الذكية لا تعمل كلها بالدرجة نفسها من الاستقلال، إذ توجد أنظمة تحتاج إلى تدخل بشري مستمر، وأنظمة أخرى تستطيع تنفيذ عمليات معقدة دون إشراف مباشر في كل مرحلة. غير أن هذه الاستقلالية لا تعني غياب الإنسان تمامًا، لأن تصميم النظام، وتحديد أهدافه، واختيار بياناته، وتقييم نتائجه، كلها عمليات تعود في أصلها إلى تدخل بشري. ولذلك فإن الحديث عن استقلالية الذكاء الاصطناعي يجب أن يكون مضبوطاً، لأن النظام قد يعمل آلياً، لكنه يبقى مرتبطاً بمن صممه ومن وجه استعماله ومن يستفيد من نتائجه.

1

وتتمثل الخاصية الخامسة في القابلية للتكيف. فبعض أنظمة الذكاء الاصطناعي، خاصة القائمة على التعلم الآلي، يمكن أن تغير أداؤها بعد التشغيل نتيجة تعاملها مع بيانات جديدة أو بيئات مختلفة. وهذا يجعلها أكثر مرونة من الأنظمة الجامدة، لكنه في الوقت نفسه يثير مشكلات تتعلق بالرقابة والشفافية، لأن النظام الذي يتغير مع الزمن قد ينتج نتائج غير متوقعة أو يصعب تفسيرها بدقة. ولهذا تصبح قابلية التكيف ميزة تقنية من جهة، ومصدرًا للحذر من جهة أخرى، خصوصاً عندما

¹ OECD Artificial Intelligence Papers, op.cit,p.8.

تستعمل هذه الأنظمة في مجالات حساسة مثل الأمن المعلوماتي أو القرارات الإدارية أو الخدمات المالية

وتتميز الأنظمة الذكية كذلك بالقدرة على معالجة كميات ضخمة من البيانات في وقت قصير. وهذه الخاصية تجعلها مناسبة جدًا للمجالات التي تتغير بسرعة، مثل الأمن السيبراني، لأن الهجمات الرقمية قد تقع في ثوانٍ، وقد تمر عبر آلاف الإشارات والسجلات والاتصالات. لذلك تحتاج المؤسسات إلى أدوات قادرة على رصد الأنماط غير الطبيعية بسرعة تفوق قدرة الإنسان على المتابعة اليدوية. ومن هذه الزاوية، يصبح الذكاء الاصطناعي أداة تقنية تساعد على تحويل الفوضى الرقمية إلى مؤشرات قابلة للفهم والتحليل.

غير أن هذه الخصائص الفنية لا تجعل الذكاء الاصطناعي معصومًا من الخطأ. فالتائج التي يقدمها النظام قد تتأثر بجودة البيانات، أو بطريقة التدريب، أو بالتحيز الموجود داخل المعطيات، أو بسوء تصميم الخوارزمية. ولهذا لا ينبغي النظر إلى الذكاء الاصطناعي باعتباره بديلاً مطلقاً عن العقل البشري، بل باعتباره أداة قوية تحتاج إلى توجيه ورقابة وتقييم مستمر. وكلما زادت حساسية المجال الذي يستعمل فيه، زادت الحاجة إلى قواعد قانونية وأخلاقية وتقنية تضمن استعماله بطريقة آمنة.

المطلب الثالث: التمييز بين الذكاء الاصطناعي والمصطلحات التقنية القريبة

يقترب مفهوم الذكاء الاصطناعي من عدة مفاهيم تقنية، الأمر الذي يؤدي في كثير من الأحيان إلى الخلط بينها. وأول هذه المفاهيم هو تعلم الآلة. فتعلم الآلة ليس مرادفًا كاملاً للذكاء الاصطناعي، بل هو فرع من فروعها، يقوم على تمكين النظام من التعلم من البيانات واستخراج الأنماط منها دون الحاجة إلى برمجة كل قاعدة بشكل يدوي. لذلك يمكن القول إن كل نظام تعلم آلي يدخل ضمن مجال الذكاء

الاصطناعي، لكن ليس كل ذكاء اصطناعي قائمًا بالضرورة على تعلم الآلة، لأن بعض الأنظمة الذكية قد تعتمد على قواعد منطقية أو نماذج معرفية أخرى.¹

أما التعلم العميق فهو أضيق من تعلم الآلة، ويعد أحد فروع المتقدمة، إذ يعتمد على الشبكات العصبية الاصطناعية ذات الطبقات المتعددة لمعالجة مشكلات معقدة، مثل التعرف على الصور، وفهم اللغة الطبيعية، وتحليل الأصوات، واكتشاف الأنماط الدقيقة داخل البيانات. وتكمن أهميته في أنه مكن الأنظمة الذكية من تحقيق نتائج عالية في مجالات كانت صعبة سابقًا، لكنه يحتاج في العادة إلى بيانات كثيرة وقدرات حاسوبية كبيرة. وبذلك يكون الترتيب المفاهيمي الأدق هو أن الذكاء الاصطناعي هو المجال الأوسع، ثم يأتي تعلم الآلة داخله، ثم يأتي التعلم العميق باعتباره مجالًا أكثر تخصصًا²

ويختلف الذكاء الاصطناعي أيضًا عن الأتمتة. فالأتمتة تعني تنفيذ مهام محددة بصورة آلية وفق قواعد ثابتة ومسبقة، مثل إرسال رسالة تلقائية أو تشغيل آلة في وقت محدد. أما الذكاء الاصطناعي فيتجاوز التنفيذ الآلي البسيط إلى التحليل والتوقع والتكيف مع المعطيات. ومع ذلك، قد تتحول بعض تطبيقات الذكاء الاصطناعي مع مرور الوقت إلى أدوات عادية ينظر إليها الناس كأنها مجرد أتمتة، مثل الخرائط الرقمية أو أنظمة الاقتراح، لأن ما كان يبدو ذكيًا في مرحلة معينة يصبح مألوفًا مع كثرة الاستعمال

كما ينبغي التمييز بين الذكاء الاصطناعي والروبوتات. فالروبوت قد يكون آلة مادية تتحرك أو تنفذ أعمالًا معينة، لكنه لا يكون ذكيًا بالضرورة إلا إذا كان مزودًا بأنظمة قادرة على الإدراك أو التعلم أو اتخاذ القرار. وفي المقابل، قد يوجد الذكاء الاصطناعي دون أي شكل روبوتي، كما هو الحال في أنظمة تحليل البيانات، ومحركات

¹نزمين مجدي، المرجع السابق، ص 11.

²المرجع نفسه، ص 12.

التوصية، وأنظمة كشف الاحتيال، وبرامج الحماية الرقمية. لذلك فالروبوت هو وعاء مادي محتمل للذكاء الاصطناعي، وليس هو الذكاء الاصطناعي ذاته.

ويختلف الذكاء الاصطناعي كذلك عن البيانات الضخمة، رغم العلاقة القوية بينهما. فالبيانات الضخمة تعني وجود كميات هائلة ومتنوعة وسريعة التدفق من البيانات، أما الذكاء الاصطناعي فهو الوسيلة التي يمكن أن تستفيد من هذه البيانات لاكتشاف الأنماط وبناء التوقعات. فالبيانات وحدها لا تنتج معرفة إذا لم توجد أدوات تحليل مناسبة، والذكاء الاصطناعي لا يبلغ فعاليته دون بيانات كافية. ومن هنا تقوم العلاقة بينهما على التكامل لا الترادف، إذ توفر البيانات الضخمة المادة الخام، بينما توفر خوارزميات الذكاء الاصطناعي القدرة على التحليل والاستنتاج¹

كما يجب التمييز بين الذكاء الاصطناعي والخوارزمية. فالخوارزمية هي مجموعة خطوات أو تعليمات لمعالجة مشكلة معينة، وقد تكون بسيطة جدًا ولا علاقة لها بالذكاء الاصطناعي. أما الذكاء الاصطناعي فيستعمل خوارزميات أكثر تعقيدًا، غالبًا مرتبطة بالبيانات والتعلم والاستنتاج. لذلك فكل نظام ذكاء اصطناعي يعتمد على خوارزميات، لكن ليست كل خوارزمية تعد ذكاءً اصطناعيًا. وهذا التمييز مهم في مجال الأمن المعلوماتي، لأن الخلل قد يكون في الخوارزمية، أو في البيانات، أو في طريقة تدريب النظام، أو في البيئة التي يعمل داخلها.

ومن خلال ما سبق، يتضح أن الذكاء الاصطناعي مفهوم جامع، لكنه ليس كلمة سحرية تصلح لكل تقنية حديثة. فهو مجال يقوم على قدرة الأنظمة الآلية على معالجة البيانات واستنتاج النتائج والتكيف بدرجات مختلفة، بينما تبقى المفاهيم الأخرى مثل تعلم الآلة، والتعلم العميق، والأتمتة، والروبوتات، والبيانات الضخمة، مفاهيم قريبة منه لكنها لا تطابقه تمامًا. وبعد هذا التمييز ضروريًا قبل الانتقال إلى

¹ دحمان محمد، الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني والسياسي، المجلد 7 العدد 2، 2023، ص

443. <https://asjp.cerist.dz/en/article/236939>

دراسة تطبيقاته، لأن فهم المصطلحات بدقة يساعد على بناء تحليل صحيح لواقع الأمن المعلوماتي في ظل الذكاء الاصطناعي.

المبحث الثاني: تصنيفات الذكاء الاصطناعي ومجالات تطبيقاته

بعد تحديد مفهوم الذكاء الاصطناعي وتمييزه عن المفاهيم القريبة منه، يصبح من الضروري الانتقال إلى تصنيفاته وتطبيقاته، لأن الذكاء الاصطناعي لا يظهر في صورة واحدة، ولا يستعمل في مجال واحد. فهو قد يكون نظامًا بسيطًا يؤدي وظيفة محددة، وقد يكون نظامًا متقدمًا قادرًا على التعلم والتحليل والتكيف¹، كما قد يظهر في شكل تطبيقات يومية لا يشعر المستخدم أحيانًا أنها قائمة على خوارزميات ذكية. ومن هنا فإن دراسة تصنيفاته تساعد على فهم حدوده التقنية، أما دراسة تطبيقاته فتكشف أثره العملي في الحياة العامة، بينما يبين الحديث عن مخاطره أن هذه التقنية ليست محايدة دائمًا، بل تحمل معها تحديات أمنية وقانونية وأخلاقية تحتاج إلى ضبط ومتابعة.

المطلب الأول: مستويات الذكاء الاصطناعي: الضعيف، القوي، الفائق

يقسم الذكاء الاصطناعي عادة من حيث مستوى قدرته واستقلالته إلى ثلاثة أنواع رئيسية، وهي الذكاء الاصطناعي الضعيف، والذكاء الاصطناعي القوي، والذكاء الاصطناعي الفائق. وهذا التقسيم لا يقصد به أن بعض الأنظمة "ضعيفة" بمعنى أنها غير نافعة، بل المقصود أن قدرتها محصورة في مجال معين ولا تتجاوز المهمة التي صممت من أجلها. فالذكاء الاصطناعي الضعيف هو الشكل الأكثر انتشارًا في الواقع الحالي، لأنه يقوم على أداء مهمة محددة بدقة، مثل ترجمة نص، أو التعرف على وجه، أو اقتراح منتج، أو كشف رسالة احتيالية، أو تحليل سلوك المستخدم داخل منصة رقمية. وهو ذكاء متخصص، لا يملك وعيًا ولا فهمًا عامًا للواقع، وإنما يعمل داخل حدود البيانات والخوارزميات التي بني عليها. وقد أشار تقرير منظمة التعاون الاقتصادي والتنمية إلى أن أنظمة الذكاء الاصطناعي تنتج مخرجات مثل التنبؤات أو التوصيات أو

القرارات وفق أهداف محددة، وهو ما يوضح أن أغلب الأنظمة المستعملة حاليًا تعمل داخل نطاق وظيفي معين لا يتجاوز الغرض الذي صممت له¹.

ويظهر الذكاء الاصطناعي الضعيف في أغلب التطبيقات التي يستعملها الأفراد يوميًا، مثل محركات البحث، والمساعدات الصوتية، وأنظمة الملاحة، والتسويق الرقمي، وبرامج كشف الفيروسات، وأنظمة التعرف على الصور. فهذه الأنظمة قد تبدو ذكية لأنها تقدم نتائج سريعة ودقيقة في كثير من الأحيان، لكنها لا تفهم العالم كما يفهمه الإنسان، ولا تستطيع نقل خبرتها من مجال إلى آخر بشكل حر. فالنظام المصمم لكشف الاحتيال البنكي مثلاً لا يستطيع من تلقاء نفسه تشخيص مرض أو قيادة مركبة إلا إذا أعيد تصميمه وتدريبه لذلك الغرض. ولهذا فإن الذكاء الاصطناعي الضعيف هو ذكاء وظيفي مقيد، قوته في التخصص لا في العمومية.

أما الذكاء الاصطناعي القوي فيقصد به ذلك النوع الذي يفترض أن يمتلك قدرة عقلية عامة قريبة من القدرة الإنسانية، بحيث يستطيع الفهم والتعلم والتفكير والتكيف مع مشكلات متعددة دون أن يكون محصوراً في مهمة واحدة. وهذا النوع ما يزال في حدود البحث والنقاش النظري، لأنه يتجاوز مجرد تنفيذ تعليمات أو تحليل بيانات داخل مجال محدد، ويفترض وجود نظام قادر على التعامل مع المعرفة بطريقة واسعة ومرنة. ومن الناحية العلمية، لا يمكن القول إن الذكاء الاصطناعي القوي تحقق فعلاً في الواقع الحالي، لأن الأنظمة الموجودة، مهما بلغت قوتها، ما تزال تعتمد على البيانات والنماذج الاحتمالية ولا تملك وعياً ذاتياً أو فهماً إنسانياً كاملاً. ولذلك فإن الخلط بين الذكاء الاصطناعي الضعيف والذكاء الاصطناعي القوي يؤدي إلى مبالغة في تقدير قدرات الأنظمة الحالية.

¹ سعدي خليل و بن مهدي مرزوق، الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبراني، مجلة السلام للعلوم الإنسانية والاجتماعية، المجلد 6 العدد 1، جامعة الجزائر 3، 2022، ص144.

<https://asjp.cerist.dz/en/article/196713>

وتظهر أهمية هذا التمييز في مجال الأمن المعلوماتي، لأن التعامل مع نظام ذكي ضعيف يختلف عن التعامل مع نظام يملك قدرة عامة على التعلم واتخاذ القرار. فالأنظمة الأمنية الحالية القائمة على الذكاء الاصطناعي تستطيع كشف أنماط الهجوم أو التنبيه إلى سلوك مشبوه، لكنها لا تفكر بذاتها خارج حدود التدريب والبرمجة. لذلك يحتاج استعمالها إلى رقابة بشرية، خاصة عندما يتعلق الأمر بقرارات تمس حماية البيانات أو تعطيل حسابات أو تصنيف نشاط معين على أنه تهديد أمني. وقد ركز إطار إدارة مخاطر الذكاء الاصطناعي الصادر عن المعهد الوطني الأمريكي للمعايير والتكنولوجيا على ضرورة فهم مخاطر أنظمة الذكاء الاصطناعي وإدارتها لتعزيز الثقة فيها، وهو ما يؤكد أن هذه الأنظمة تحتاج إلى حوكمة ومتابعة لا إلى تسليم كامل بقراراتها.¹

أما الذكاء الاصطناعي الفائق فيمثل الصورة الأكثر تقدماً وافتراساً، ويقصد به ذكاء يتجاوز قدرات الإنسان في مختلف المجالات، سواء في التحليل أو الإبداع أو اتخاذ القرار أو حل المشكلات. وهذا النوع لا يوجد حالياً بصورة عملية، لكنه يحضر بقوة في النقاشات المستقبلية، خصوصاً عند الحديث عن مخاطر فقدان السيطرة على الأنظمة المتقدمة، أو استعمالها في الهجمات السيبرانية، أو تحويلها إلى أدوات مراقبة وتحكم واسع. لذلك فإن الذكاء الاصطناعي الفائق ليس موضوعاً تقنياً فقط، بل هو موضوع فلسفي وقانوني وأخلاقي أيضاً، لأنه يطرح سؤالاً خطيراً: إلى أي حد يمكن للإنسان أن يمنح الآلة قدرة على القرار دون أن يفقد السيطرة على نتائجها؟

وانطلاقاً من هذا التقسيم، يمكن القول إن واقعنا الحالي يقوم أساساً على الذكاء الاصطناعي الضعيف والمتخصص، مع تطور سريع في قدرات النماذج الحديثة التي أصبحت تنتج نصوصاً وصوراً وأكواداً وتحليلات أكثر تعقيداً. غير أن هذا التطور لا يعني بالضرورة الوصول إلى ذكاء إنساني كامل، بل يعني توسع قدرة الأنظمة على معالجة البيانات وتوليد مخرجات أكثر تنوعاً. ولذلك فإن دراسة الأمن المعلوماتي في ظل

¹ دحماني محمد، المرجع السابق، ص 447

الذكاء الاصطناعي يجب أن تنطلق من الواقع التقني الموجود، لا من التصورات الخيالية فقط، لأن الخطر الحقيقي اليوم لا يكمن في آلة واعية، بل في أنظمة قوية تستعمل بسرعة وبتكلفة منخفضة في الاختراق، والتضليل، وتحليل البيانات، وأتمتة الهجمات.

ومن جهة أخرى، يمكن تصنيف الذكاء الاصطناعي من حيث طريقة عمله إلى أنظمة تعلم آلي، وأنظمة تعلم عميق، وأنظمة معالجة لغة طبيعية، وأنظمة رؤية حاسوبية، وأنظمة خبيرة. وهذه التصنيفات التقنية مهمة لأنها تكشف طريقة اشتغال النظام. فالتعلم الآلي يعتمد على تدريب النموذج بواسطة البيانات، والتعلم العميق يعتمد على شبكات عصبية متعددة الطبقات، ومعالجة اللغة الطبيعية تهتم بفهم النصوص واللغة البشرية، أما الرؤية الحاسوبية فتتعلق بتحليل الصور والفيديوهات. وتفيد هذه التصنيفات في الأمن المعلوماتي لأن كل تقنية منها قد تستعمل في جانب دفاعي أو هجومي، فقد تستعمل معالجة اللغة الطبيعية لكشف الرسائل الاحتيالية، وقد تستعمل في المقابل لإنتاج رسائل تصيد أكثر إقناعاً.

المطلب الثاني: المجالات التطبيقية للذكاء الاصطناعي

تتعدد مجالات استخدام الذكاء الاصطناعي بصورة واسعة، لأن هذه التقنية أصبحت مرتبطة بكل نشاط يعتمد على البيانات أو القرار أو التوقع. ففي المجال الصحي مثلاً، يساعد الذكاء الاصطناعي في تحليل الصور الطبية، وتوقع بعض المخاطر الصحية، وتنظيم ملفات المرضى، ومساندة الطبيب في التشخيص. ولا يعني ذلك أن الآلة تحل محل الطبيب، بل إنها توفر له أداة تحليل إضافية قد تساعد على التقليل من الخطأ وتسريع القراءة، خاصة في الحالات التي تتطلب معالجة كمية كبيرة من المعطيات. وهنا تظهر قيمة الذكاء الاصطناعي كأداة مساعدة لا كسلطة مستقلة، لأن القرار الطبي يبقى محتاجاً إلى خبرة إنسانية ومسؤولية مهنية.

وفي المجال التعليمي، يستعمل الذكاء الاصطناعي في تخصيص المحتوى للمتعلمين، وتحليل مستوى الطالب، واقتراح تدريبات مناسبة، ومساعدة الأستاذ في

متابعة نقاط الضعف لدى المتعلمين. فبدل أن يكون التعليم غمطاً واحداً للجميع، تسمح الأنظمة الذكية ببناء مسارات أكثر مرونة، تراعي سرعة التعلم والفروق الفردية. غير أن هذا الاستعمال يثير بدوره إشكالات تتعلق بحماية بيانات الطلبة، وعدالة التقييم، وخطر الاعتماد المفرط على أدوات جاهزة قد تضعف الجهد الشخصي إذا لم تستعمل بضوابط واضحة.

أما في المجال الاقتصادي والمالي، فقد أصبح الذكاء الاصطناعي حاضراً في تحليل الأسواق، وإدارة المخاطر، وكشف الاحتيال، وخدمة الزبائن، والتسويق الموجه. وتستفيد المؤسسات المالية من قدرته على فحص معاملات كثيرة في وقت قصير، ورصد السلوك غير العادي الذي قد يدل على احتيال أو اختراق. ومن هذه الزاوية، يشكل الذكاء الاصطناعي أداة مهمة لحماية المعاملات، لكنه قد يتحول أيضاً إلى وسيلة تمييز أو استبعاد إذا كانت البيانات المستعملة في التدريب منحازة أو ناقصة. ولذلك فإن استعماله في المجال المالي يحتاج إلى شفافية ومراجعة، لأن الخطأ الخوارزمي قد ينتج عنه رفض خدمة أو تجميد عملية أو تصنيف شخص بطريقة غير عادلة.¹

وفي مجال الإدارة والخدمات العامة، يمكن للذكاء الاصطناعي أن يساعد على تحسين جودة الخدمة وتسريع معالجة الطلبات وتوجيه الموارد نحو الأولويات. وقد بين تقرير منظمة التعاون الاقتصادي والتنمية حول استعمال الذكاء الاصطناعي في القطاع العام أن هذه التقنية يمكن أن تساهم في تحسين تصميم الخدمات العامة وتحليل البيانات الحكومية، لكنها تحتاج إلى أطر واضحة حتى لا تتحول إلى مصدر للغموض أو ضعف المساءلة، كما أن استعمال الذكاء الاصطناعي في الإدارة يفرض ضرورة حماية المعطيات الشخصية، لأن المؤسسات العمومية تتعامل غالباً مع بيانات حساسة تخص المواطنين.

¹ جودي خرفية، هندسة الأمن السبراني في عصر الذكاء الاصطناعي: قراءة في أدوار واستراتيجيات البقطة الخوارزمية، المجلة الجزائرية للأمن الإنساني، المجلد 11 العدد 1، جامعة باتنة 1، 2025، ص 64.

وفي مجال الإعلام والاتصال، يستعمل الذكاء الاصطناعي في ترتيب المحتوى، واقتراح الأخبار، وتحليل اتجاهات الجمهور، وترجمة النصوص، وتوليد الصور والفيديوهات. وقد ساعد ذلك على تسريع إنتاج المحتوى وتوسيعه، لكنه فتح في المقابل بابًا خطيرًا أمام الأخبار المضللة، والتزييف العميق، والتلاعب بالرأي العام. فالنظام الذي يستطيع إنتاج نص مقنع أو صورة واقعية يمكن أن يستعمل في التوعية والمعرفة، كما يمكن أن يستعمل في التضليل وانتحال الهوية. ولهذا لم يعد خطر الذكاء الاصطناعي مرتبطًا بالاختراق التقني فقط، بل أصبح مرتبطًا أيضًا بالاختراق المعرفي، أي التأثير على قناعات الناس من خلال محتوى مصنوع بمهارة.¹

وفي مجال النقل، يساعد الذكاء الاصطناعي على تحسين الملاحية، وتوقع الازدحام، ومراقبة المركبات، وتطوير أنظمة القيادة المساعدة. وتقوم هذه التطبيقات على جمع بيانات من الطرق والمركبات والمستخدمين وتحليلها لإنتاج قرارات أو اقتراحات لحظية. غير أن هذا المجال يكشف أيضًا عن أهمية السلامة، لأن الخطأ في نظام ذكي داخل قطاع النقل قد يؤدي إلى أضرار مادية وبشرية. ولذلك فإن استعمال الذكاء الاصطناعي في الأنظمة المتصلة بالحركة والبنية التحتية يحتاج إلى اختبارات صارمة قبل اعتماده بشكل واسع.

أما في المجال الأمني، فيستعمل الذكاء الاصطناعي في تحليل المخاطر، ومراقبة الأنماط، والتعرف على السلوكيات المشبوهة، وكشف الهجمات السيبرانية، ومساعدة فرق الأمن على اتخاذ قرارات أسرع. وهنا تظهر صلته المباشرة بموضوع الأمن المعلوماتي، لأن الهجمات الرقمية الحديثة أصبحت أكثر سرعة وتعقيدًا من أن تواجه دائمًا بالطرق التقليدية. فالذكاء الاصطناعي يسمح بفحص سجلات ضخمة، ومقارنة ملايين الأحداث، واكتشاف الإشارات الضعيفة التي قد تسبق الهجوم. غير أن

¹ NIST, The NIST Cybersecurity Framework CSF 2.0, 2024, p.4.

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

استعماله الأمني يثير في المقابل خطر التوسع في المراقبة أو انتهاك الخصوصية إذا لم تضبط حدوده القانونية والأخلاقية¹.

ويمكن القول إن القاسم المشترك بين هذه التطبيقات كلها هو البيانات. فالذكاء الاصطناعي لا يشتغل في الفراغ، بل يحتاج إلى معطيات يتعلم منها أو يحللها. لذلك فإن توسع استعماله يعني توسع جمع البيانات ومعالجتها، وهذا ما يجعل الأمن المعلوماتي حاضراً في كل مجال من مجالات الذكاء الاصطناعي. فكلما توسعت التطبيقات الذكية، زادت الحاجة إلى حماية المعلومات من التسرب، والاختراق، والاستعمال غير المشروع، والتحيز، والتلاعب. ومن هنا تظهر العلاقة الوثيقة بين الذكاء الاصطناعي والأمن المعلوماتي: الأول يحتاج إلى البيانات حتى يعمل، والثاني يحمي تلك البيانات حتى لا تتحول إلى نقطة ضعف.

كما أن تطبيقات الذكاء الاصطناعي لم تعد محصورة في الدول المتقدمة أو الشركات الكبرى، بل بدأت تدخل إلى الحياة اليومية للمستخدمين العاديين من خلال الهواتف والمنصات والتطبيقات. وهذا الانتشار يجعل الوعي الأمني ضرورة عامة، لأن المستخدم لم يعد يتعامل مع برنامج بسيط، بل مع منظومات تجمع بياناته وتدرس سلوكه وتقتصر عليه محتوى أو خدمة أو قراراً. لذلك فإن الواقع الجديد يفرض على الباحث في الأمن المعلوماتي ألا يكتفي بدراسة الحماية التقنية، بل أن ينظر أيضاً إلى الثقافة الرقمية، وحقوق المستخدم، ومسؤولية المؤسسات التي تطور أو تستعمل هذه الأنظمة.

المطلب الثالث: التحديات والمخاطر المصاحبة لانتشار تقنيات الذكاء الاصطناعي

رغم الفوائد الكبيرة للذكاء الاصطناعي، فإن استعماله الواسع يطرح مجموعة من المخاطر العامة التي لا يمكن إهمالها. وأول هذه المخاطر هو خطر المساس بالخصوصية، لأن الأنظمة الذكية تحتاج إلى بيانات كثيرة حتى تعمل بدقة، وقد تشمل

¹ سعيدي خليل و بن مهدي مرزوق ، المرجع السابق، ص149

هذه البيانات معلومات شخصية أو سلوكية أو مالية أو صحية. وكلما توسع جمع البيانات، زاد احتمال إساءة استعمالها أو تسريبها أو ربطها ببيانات أخرى تكشف تفاصيل دقيقة عن حياة الأفراد. ولهذا تؤكد توصية اليونسكو بشأن أخلاقيات الذكاء الاصطناعي على ضرورة حماية حقوق الإنسان والكرامة والشفافية والرقابة البشرية عند تطوير واستعمال أنظمة الذكاء الاصطناعي.

ويعد التحيز من أخطر المشكلات المرتبطة بالذكاء الاصطناعي، لأن النظام قد ينتج قرارات غير عادلة إذا كانت البيانات التي تدرب عليها غير متوازنة أو تحمل انحيازات اجتماعية أو اقتصادية أو ثقافية. فالآلة لا تبدأ دائماً من الحياد، بل تتعلم من البيانات التي يزودها بها الإنسان، وإذا كانت هذه البيانات مشوهة أو ناقصة فإن النتائج ستكون بدورها مشوهة. وقد يظهر ذلك في التوظيف، أو منح القروض، أو تقييم المخاطر، أو تصنيف الأشخاص. ولذلك فإن العدالة في الذكاء الاصطناعي لا تتحقق بمجرد استعمال خوارزمية متقدمة، بل تحتاج إلى فحص البيانات، ومراجعة النتائج، وإتاحة آليات للاعتراض والتصحيح.¹

ومن المخاطر أيضاً ضعف الشفافية وصعوبة تفسير القرار الخوارزمي. فبعض أنظمة الذكاء الاصطناعي، خاصة القائمة على التعلم العميق، تنتج نتائج دقيقة لكنها لا تقدم دائماً تفسيراً واضحاً لكيفية الوصول إليها. وهذا يطرح مشكلة كبيرة عندما يؤثر القرار على حقوق الأفراد أو أمن المؤسسات. فإذا صنف نظام ذكي نشاطاً معيناً على أنه تهديد أمني، أو رفض طلباً، أو أوصى بإجراء معين، فإن السؤال يصبح: على أي أساس تم ذلك؟ ومن يتحمل المسؤولية إذا كان القرار خاطئاً؟ ولهذا تعد قابلية التفسير والشفافية من الشروط الأساسية لبناء الثقة في الأنظمة الذكية، خاصة في المجالات الحساسة.

¹ NIST, op.cit, p5

وتظهر مخاطر الذكاء الاصطناعي كذلك في إمكانية استعماله لأغراض خبيثة. فالخوارزميات نفسها التي تساعد على كشف الهجمات يمكن أن يستعملها المهاجمون لتطوير هجمات أكثر دقة. ويمكن استعمال الذكاء الاصطناعي في توليد رسائل تصيد مقنعة، أو إنشاء هويات وهمية، أو إنتاج برمجيات خبيثة، أو تحليل دفاعات المؤسسة لاكتشاف نقاط الضعف. وهذا يعني أن الذكاء الاصطناعي لا يزيد فقط من قدرة المدافعين¹، بل يزيد أيضًا من قدرة المهاجمين، مما يجعل الأمن المعلوماتي يدخل في سباق متواصل بين وسائل الحماية ووسائل الاعتداء.

ومن بين المخاطر المهمة أيضًا خطر الاعتماد المفرط على الأنظمة الذكية. فالمؤسسات قد تميل إلى الثقة الكاملة في نتائج الذكاء الاصطناعي بسبب سرعته ودقته الظاهرة، غير أن ذلك قد يؤدي إلى إضعاف الرقابة البشرية. فإذا أصبح الإنسان يكتفي بقبول ما تقترحه الآلة دون مراجعة، فقد تتحول التقنية من أداة مساعدة إلى سلطة فعلية غير خاضعة للنقاش. وقد نبه إطار إدارة مخاطر الذكاء الاصطناعي الصادر عن NIST إلى أن إدارة المخاطر تساعد على تعزيز موثوقية الأنظمة وبناء الثقة العامة فيها، وهو ما يدل على أن الذكاء الاصطناعي يحتاج إلى مراقبة مستمرة لا إلى استعمال عشوائي².

كما يطرح الذكاء الاصطناعي مخاطر تتعلق بالأمن المعلوماتي نفسه، لأن الأنظمة الذكية قد تكون هدفًا للهجوم. فقد يحاول المهاجم التلاعب ببيانات التدريب، أو إدخال بيانات مضللة تجعل النموذج يتخذ قرارات خاطئة، أو استغلال ثغرات في النموذج لاستخراج معلومات حساسة. وهذا النوع من المخاطر يختلف عن الهجمات التقليدية، لأنه لا يستهدف الخادم أو الشبكة فقط، بل يستهدف منطق النظام الذكي وطريقة تعلمه. ومن هنا تظهر الحاجة إلى حماية نماذج الذكاء الاصطناعي باعتبارها أصولًا معلوماتية حساسة، لا مجرد أدوات تقنية عادية.

¹ جودي خرفية، المرجع السابق، ص 69.

² OECD Artificial Intelligence Papers, op.cit, p.1.

وتبرز كذلك مخاطر قانونية وتنظيمية، لأن القوانين في كثير من الدول ما تزال تحاول اللحاق بسرعة التطور التقني. فالتشريعات التقليدية المتعلقة بحماية البيانات أو مكافحة الجرائم المعلوماتية قد لا تكون كافية دائماً لمعالجة قضايا مثل المسؤولية عن قرارات الذكاء الاصطناعي، أو ملكية البيانات المستعملة في التدريب، أو حدود المراقبة الآلية، أو استعمال التزييف العميق. ولذلك فإن الذكاء الاصطناعي يفرض على المشرع تحديث أدواته القانونية، حتى لا تبقى الحماية متأخرة عن الخطر. وتزداد أهمية هذا الأمر في الدول التي تعمل على بناء منظومات رقمية جديدة، لأن غياب الإطار القانوني الواضح قد يضعف الثقة في التحول الرقمي كله.

ولا يمكن إهمال المخاطر الأخلاقية المرتبطة بالكرامة الإنسانية والرقابة والمساواة. فالذكاء الاصطناعي قد يستعمل في تحسين الخدمات، لكنه قد يستعمل أيضاً في تتبع الأفراد وتصنيفهم والتأثير على اختياراتهم. وكلما أصبحت الأنظمة أكثر قدرة على تحليل السلوك، صار الإنسان أكثر عرضة لأن يتحول إلى مجموعة بيانات قابلة للتوقع والتوجيه. ولهذا تشدد اليونسكو على أن أخلاقيات الذكاء الاصطناعي يجب أن تقوم على حماية حقوق الإنسان والكرامة والعدالة والشفافية والمسؤولية، لأن التقنية لا ينبغي أن تتطور على حساب الإنسان¹

ومن خلال هذه المخاطر، يتضح أن الذكاء الاصطناعي ليس مجرد وسيلة تقنية محايدة، بل هو قوة جديدة تؤثر في طريقة جمع المعلومات ومعالجتها وحمايتها واستعمالها. فإذا أحسن توظيفه، استطاع أن يرفع مستوى الأمن المعلوماتي ويكشف التهديدات بسرعة وفعالية. أما إذا استعمل دون ضوابط، فقد يتحول إلى مصدر جديد للهجوم والتضليل والمراقبة وانتهاك الخصوصية. ولذلك فإن التحدي الحقيقي لا يكمن في رفض الذكاء الاصطناعي أو قبوله بشكل مطلق، بل في بناء استعمال مسؤول يوازن بين الابتكار والحماية، وبين الفعالية التقنية والحقوق الأساسية للأفراد.

¹جوادي خرفية، المرجع السابق، ص103

يتضح من خلال هذا الفصل أن الذكاء الاصطناعي يمثل مجالًا تقنيًا واسعًا يقوم على قدرة الأنظمة الآلية على معالجة البيانات واستنتاج النتائج وإنتاج توصيات أو قرارات في ضوء أهداف محددة. وقد تبين أن مفهومه لا يختلط بكل تقنية حديثة، بل ينبغي تمييزه عن تعلم الآلة، والتعلم العميق، والأتمتة، والروبوتات، والبيانات الضخمة، لأن هذا التمييز يساعد على فهم طبيعته وحدوده. كما تبين أن تطبيقاته أصبحت تمتد إلى الصحة، والتعليم، والاقتصاد، والإدارة، والإعلام، والنقل، والأمن، مما جعله عنصرًا مؤثرًا في مختلف جوانب الحياة الرقمية.

غير أن هذا الانتشار الواسع لا يخلو من مخاطر، إذ يثير الذكاء الاصطناعي إشكالات تتعلق بالخصوصية، والتحيز، والشفافية، والمسؤولية، والأمن، وإمكانية الاستعمال الخبيث. ولذلك فإن فهم ماهيته وتطبيقاته يعد خطوة أولى ضرورية قبل دراسة دوره في أمن المعلومات، لأن الذكاء الاصطناعي لا يمكن تقييمه في المجال الأمني إلا بعد إدراك طبيعته المزدوجة: فهو أداة للحماية من جهة، ومصدر لمخاطر جديدة من جهة أخرى.

الفصل الثاني

الفصل الثاني: الأمن المعلوماتي في البيئة الرقمية وعلاقته بالذكاء الاصطناعي

يمثل الأمن المعلوماتي في الوقت الحاضر أحد أعمدة الحياة الرقمية، لأن كل نشاط إلكتروني، مهما بدا بسيطاً، يقوم في النهاية على تبادل معلومات أو تخزينها أو معالجتها. ولم تعد المسألة مرتبطة بحماية جهاز معين أو برنامج واحد، بل أصبحت مرتبطة بحماية منظومة كاملة تشمل الإنسان، والبيانات، والشبكات، والبرمجيات، والبنية التحتية، والقواعد القانونية المنظمة للاستعمال. ومع دخول الذكاء الاصطناعي إلى هذا المجال، تغيرت طبيعة الأمن المعلوماتي من حماية تقليدية تعتمد على رد الفعل، إلى حماية أكثر ديناميكية تقوم على التحليل والتنبؤ واكتشاف الأنماط غير العادية.

وقد أكدت بعض الدراسات الحديثة أن العلاقة بين الذكاء الاصطناعي والأمن السيبراني أصبحت علاقة مزدوجة، إذ يمكن للذكاء الاصطناعي أن يساعد في كشف التهديدات وتعزيز الحماية، كما يمكن في المقابل أن يستعمل لتطوير هجمات أكثر سرعة وتعقيداً، وهو ما يجعل الأمن المعلوماتي أمام مرحلة جديدة لا تكفي فيها الوسائل الكلاسيكية وحدها.

المبحث الأول: مفهوم الأمن المعلوماتي وأبعاده

قبل البحث في أثر الذكاء الاصطناعي على الأمن المعلوماتي، يجب أولاً تحديد المقصود بالأمن المعلوماتي، لأن هذا المفهوم يتداخل مع عدة مصطلحات قريبة منه، مثل الأمن السيبراني، أمن الشبكات، حماية البيانات، أمن الأنظمة المعلوماتية، والجرائم المعلوماتية. وهذا التداخل لا يعني أنها مفاهيم متطابقة تمامًا، بل يعني أنها تدور حول مجال واحد هو حماية المعلومات والأنظمة التي تتعامل معها من كل اعتداء أو خلل أو استعمال غير مشروع. ولذلك فإن ضبط المفهوم في بداية هذا الفصل يساعد على فهم طبيعة التهديدات، والوسائل المعتمدة لمواجهتها، وموقع الذكاء الاصطناعي داخل هذا البناء الأمني الجديد.

المطلب الأول: تعريف الأمن المعلوماتي وتمييزه عن الأمن السيبراني

يقصد بالأمن المعلوماتي مجموعة التدابير التقنية والتنظيمية والقانونية التي تهدف إلى حماية المعلومات من الوصول غير المشروع، أو التعديل، أو الإتلاف، أو التعطيل، أو الإفشاء، سواء كانت هذه المعلومات محفوظة داخل أجهزة، أو منقولة عبر الشبكات، أو مستعملة داخل المؤسسات. فموضوع الأمن المعلوماتي هو المعلومة في ذاتها، أي المحافظة على قيمتها وسريتها وسلامتها وإتاحتها. ومن هنا فإن الأمن المعلوماتي لا يقتصر على الحماية الإلكترونية فقط، بل يشمل كذلك طرق حفظ الوثائق، وتنظيم صلاحيات الوصول، وتكوين المستخدمين، ووضع سياسات داخلية تمنع تسرب البيانات أو إساءة استعمالها¹.

أما الأمن السيبراني فيتعلق أكثر بحماية الفضاء السيبراني، أي البيئة الرقمية المتصلة بالشبكات والأنظمة والمنصات والخدمات الإلكترونية. فهو يهتم بحماية الحواسيب، والخوادم، والشبكات، والتطبيقات، والبنى التحتية الرقمية من الهجمات التي تقع عبر الوسائط الإلكترونية. ولذلك يمكن القول إن الأمن السيبراني أضيق من الأمن المعلوماتي من جهة، لأنه يركز على البيئة السيبرانية، لكنه أوسع من جهة أخرى عندما يتعلق بحماية البنية الرقمية الوطنية والقطاعات الحيوية. وهذا التمييز مهم، لأن المعلومة قد تتعرض للخطر حتى خارج الشبكة، بينما الهجوم السيبراني يفترض غالبًا وجود وسط رقمي أو اتصال إلكتروني.

ويظهر الفرق بين المفهومين من زاوية محل الحماية. فالأمن المعلوماتي يحمي المعلومة أينما وجدت، سواء كانت ورقية أو إلكترونية أو مخزنة داخل ذاكرة أو متداولة بين الأشخاص. أما الأمن السيبراني فيحمي الأنظمة والشبكات والخدمات الرقمية التي تمر عبرها المعلومات. ومع ذلك، فإن التطور الرقمي جعل الحدود بينهما أقل وضوحًا، لأن أغلب المعلومات اليوم أصبحت مخزنة أو متداولة رقميًا، وبالتالي صار الأمن المعلوماتي محتاجًا إلى الأمن السيبراني، وصار الأمن السيبراني بدوره لا معنى له إذا لم يكن هدفه النهائي حماية المعلومات.

وفي السياق الجزائري، يظهر استعمال مصطلح "أمن الأنظمة المعلوماتية" باعتباره مفهومًا قريبًا من الأمن المعلوماتي والأمن السيبراني معًا، لأنه يربط الحماية بالأنظمة التي تنتج المعلومات أو تعالجها أو تخزنها. وقد ورد في الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية أن الهدف العام يتصل بتعزيز القدرات التقنية والعملياتية للجزائر وتوفير بيئة ملائمة في مجال الأمن السيبراني، وهو ما يدل على أن الحماية لم تعد شأنًا تقنيًا معزولًا، بل أصبحت جزءًا من الأمن الوطني والتحول الرقمي¹. وقد نشر موقع وزارة الدفاع الوطني الجزائري هذه الاستراتيجية بوصفها إطارًا وطنيًا مرتبطًا بالمرونة السيبرانية وحماية البنية التحتية الرقمية.

ومن خلال ذلك، يظهر أن الأمن المعلوماتي يتكون من بعدين متكاملين: بعد وقائي يمنع الخطر قبل وقوعه، وبعد علاجي يتدخل بعد وقوع الحادث لتقليل آثاره واسترجاع الوضع الطبيعي. فالحماية لا تكون فقط بوضع كلمة مرور أو برنامج مضاد للفيروسات، بل ببناء سياسة شاملة تشمل تقييم المخاطر، وتحديد الصلاحيات، وتشفير البيانات، ومراقبة الدخول، وتدريب المستخدمين، ووضع خطط للاستجابة للحوادث. وهذا المعنى الواسع هو الذي يجعل الأمن المعلوماتي مجالًا مشتركًا بين التقنية والقانون والإدارة والسلوك البشري.

كما أن الأمن المعلوماتي لا ينجح إذا نظرنا إليه كمسؤولية قسم تقني فقط. فالمستخدم قد يكون أضعف حلقة في سلسلة الحماية عندما يفتح رابطًا مجهولًا، أو يستعمل

¹ وزارة الدفاع الوطني، الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029، 2025، ص 6.

https://www.mdn.dz/assi/nsiss_ar.pdf

كلمة مرور ضعيفة، أو يشارك معلومات حساسة دون تحقق. والمؤسسة قد تملك أنظمة متقدمة، لكنها تبقى معرضة للخطر إذا لم تكن لها سياسة واضحة لإدارة المعلومات. ومن هنا فإن الأمن المعلوماتي يتطلب ثقافة أمنية قبل أن يتطلب أدوات تقنية، لأن الأداة مهما كانت قوية لا تمنع الخطأ البشري إذا غابت اليقظة والتكوين.

وعند إدخال الذكاء الاصطناعي إلى هذا المجال، يصبح التمييز بين الأمن المعلوماتي والأمن السيبراني أكثر أهمية. فالذكاء الاصطناعي قد يستعمل لحماية المعلومات ذاتها، مثل تصنيف البيانات الحساسة أو كشف محاولات التسريب، وقد يستعمل لحماية الشبكات والأنظمة، مثل رصد الهجمات وتحليل السجلات الأمنية. وقد يستعمل أيضاً في الجانب الآخر من طرف المهاجمين، من خلال إنشاء رسائل تصيد دقيقة أو تحليل أنظمة الحماية لاكتشاف نقاط ضعفها. لذلك فإن الأمن المعلوماتي في ظل الذكاء الاصطناعي لم يعد مجرد حماية ضد خطر واضح، بل صار مواجهة ضد خطر يتعلم ويتطور ويتخفى.

المطلب الثاني: عناصر الأمن المعلوماتي: السرية، السلامة، الإتاحة

يقوم الأمن المعلوماتي في أساسه على ثلاثة عناصر رئيسية تعرف غالباً بثلاثية الحماية: السرية، والسلامة أو النزاهة، والإتاحة. وتمثل هذه العناصر الإطار الأول الذي تقاس من خلاله قوة أي نظام أمني، لأن فقدان واحد منها قد يؤدي إلى خلل خطير في حماية المعلومات. فالسرية تعني ألا تصل المعلومات إلا إلى الأشخاص أو الجهات المرخص لها، والسلامة تعني أن تبقى المعلومات صحيحة وغير معدلة بطريقة غير مشروعة، أما الإتاحة فتعني أن تكون المعلومات والأنظمة متوفرة عند الحاجة إليها من طرف أصحاب الحق في استعمالها.

تعد السرية أول عنصر من عناصر الأمن المعلوماتي، لأنها ترتبط بمنع الوصول غير المصرح به إلى البيانات. فالمعلومات قد تكون ذات طبيعة شخصية، أو مالية، أو مهنية، أو أمنية، وإذا وصلت إلى جهة غير مخولة فقد تستعمل في الابتزاز أو الاحتيال أو المنافسة غير المشروعة أو الإضرار بسمعة الأشخاص والمؤسسات. لذلك تعتمد السرية على وسائل متعددة، منها كلمات المرور، والتشفير، وتقنيات التحقق المتعدد، وتحديد الصلاحيات، ومراقبة الدخول

إلى قواعد البيانات. غير أن السرية لا تتحقق بالوسائل التقنية وحدها، بل تحتاج أيضًا إلى قواعد تنظيمية تمنع مشاركة المعلومات الحساسة دون مبرر.¹

وفي ظل الذكاء الاصطناعي، تزداد أهمية السرية لأن الأنظمة الذكية تتعامل غالبًا مع كميات ضخمة من البيانات. وكلما كانت البيانات أكثر تفصيلاً، زادت فائدتها في التدريب والتحليل، لكنها تصبح في الوقت نفسه أكثر خطورة إذا تسربت. فالبيانات التي تبدو عادية قد تكشف عند جمعها وتحليلها عن سلوك المستخدم، وميوله، وتحركاته، وعلاقاته، وربما حالته الصحية أو المالية. وهذا ما يجعل السرية في عصر الذكاء الاصطناعي لا تتعلق فقط بمنع سرقة ملف معين، بل بمنع إعادة تركيب صورة كاملة عن الشخص أو المؤسسة من خلال بيانات متناثرة.

أما السلامة أو النزاهة فتعني حماية المعلومات من التغيير أو التحريف أو الإتلاف غير المشروع. فقد تكون المعلومة سرية وغير مكشوفة، لكنها تفقد قيمتها إذا تم تعديلها دون علم صاحبها. ويظهر خطر المساس بالسلامة في القطاعات التي تعتمد على الدقة، مثل البنوك، والصحة، والتعليم، والإدارة، والأمن. فإذا تم تغيير رقم حساب، أو نتيجة تحليل طبي، أو سجل إداري، أو إعداد أمني، فإن الضرر قد يكون مباشرًا وخطيرًا. لذلك تهدف السلامة إلى ضمان أن تبقى البيانات صحيحة وكاملة وقابلة للاعتماد.

وتأخذ السلامة بعدًا جديدًا مع الذكاء الاصطناعي، لأن التلاعب قد لا يمس البيانات النهائية فقط، بل قد يمس البيانات المستعملة في تدريب النظام الذكي. فإذا تم إدخال بيانات مضللة إلى نموذج معين، فقد يتعلم النموذج بطريقة خاطئة وينتج قرارات غير دقيقة. وهذا النوع من الخطر خطير لأنه قد لا يظهر فورًا، بل يتسلل إلى منطق النظام نفسه. ولذلك فإن حماية سلامة البيانات في أنظمة الذكاء الاصطناعي تشمل حماية بيانات التدريب، وبيانات

¹ ناصر مراد، دور الأمن السبراني في حماية نظم المعلومات: تجربة الجزائر، مجلة اقتصاد المال والأعمال، المجلد 10، العدد 02، جامعة الوادي،

2025، ص 581-594. <https://asjp.cerist.dz/en/article/277651>

التشغيل، ونتائج النظام، وسجلات المراقبة، حتى لا تتحول الخوارزمية إلى قناة لإنتاج قرارات مشوهة.¹

أما الإتاحة فتعني ضمان وصول المستخدمين الشرعيين إلى المعلومات والخدمات عند الحاجة. فالنظام الآمن ليس هو النظام المغلق تمامًا، بل هو النظام الذي يحمي المعلومات وفي الوقت نفسه يسمح باستعمالها المشروع. وقد تتعرض الإتاحة للخطر من خلال الهجمات التي تعطل الخدمات، مثل هجمات حجب الخدمة، أو الأعطال التقنية، أو سوء إدارة الموارد، أو الكوارث التي تصيب البنية التحتية. وتكمن خطورة هذا العنصر في أن توقف الخدمة قد يسبب خسائر مالية وإدارية واجتماعية، حتى لو لم يقع تسريب للبيانات.

وتظهر أهمية الإتاحة بشكل خاص في المؤسسات التي تقدم خدمات رقمية مستمرة، مثل البنوك، والمستشفيات، والإدارات الإلكترونية، ومراكز البيانات. ففي هذه الحالات لا يكفي أن تكون البيانات سرية وسليمة، بل يجب أن تكون متاحة في الوقت المناسب. ولهذا تعتمد المؤسسات على النسخ الاحتياطي، وخطط استمرارية النشاط، ومراكز التعافي من الكوارث، وأنظمة المراقبة اللحظية. وقد يساعد الذكاء الاصطناعي هنا في توقع الأعطال، وتحليل الضغط على الأنظمة، واكتشاف المؤشرات المبكرة للهجمات التي تستهدف تعطيل الخدمة.

وتكشف هذه العناصر الثلاثة أن الأمن المعلوماتي يقوم على توازن دقيق. فالمبالغة في السرية قد تؤدي إلى تعطيل الإتاحة، والمبالغة في الإتاحة قد تضعف السرية، وإهمال السلامة يجعل البيانات المتاحة عديمة الثقة. لذلك فإن بناء نظام معلوماتي آمن يحتاج إلى سياسة متوازنة تراعي طبيعة البيانات، ومستوى الخطر، وحاجة المستخدمين، والبيئة القانونية. فالهدف ليس إغلاق المعلومات داخل قبة رقمي، بل جعلها قابلة للاستعمال دون أن تتحول إلى مدخل للضرر.

¹ زمورة جمال وبن عيسى ليلي، أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمة العمومية في الجزائر، مجلة البحوث الاقتصادية المتقدمة:

المجلد 07، العدد 02، 2022، ص 64. <https://asjp.cerist.dz/en/article/203547>

وقد أكدت الدراسات المتعلقة بالأمن السيبراني أن حماية المعلومات تقوم أساساً على ضمان هذه العناصر الثلاثة، لأن أي تهديد للسرية أو السلامة أو الإتاحة يمثل تهديداً مباشراً للنظام المعلوماتي ككل. وتزداد أهمية هذا التصور في ظل الذكاء الاصطناعي، لأن الخطر قد يضرب العناصر الثلاثة في وقت واحد: فقد يستعمل المهاجم نظاماً ذكياً لاخترق السرية، أو لتعديل بيانات التدريب بما يمس السلامة، أو لإطلاق هجمات آلية تعطل الإتاحة.¹

ومن هنا، لا يمكن تصور الأمن المعلوماتي في ظل الذكاء الاصطناعي دون حماية هذه الثلاثية. فالذكاء الاصطناعي قد يكون حارساً ذكياً لهذه العناصر عندما يستعمل في كشف التسربات، ومراقبة سلامة البيانات، وتوقع الأعطال. لكنه قد يكون أيضاً أداة تهديد عندما يستعمل في كسر السرية، أو التلاعب بالبيانات، أو تعطيل الخدمات. ولذلك فإن القيمة الحقيقية للذكاء الاصطناعي لا تتحدد بمجرد امتلاك التقنية، بل بطريقة إدماجها داخل سياسة أمنية واضحة، تراعي حقوق المستخدمين وتضع حدوداً لاستعمال البيانات.

المطلب الثالث: أهمية الأمن المعلوماتي في المؤسسات والأفراد

تزداد أهمية الأمن المعلوماتي كلما زاد اعتماد الأفراد والمؤسسات على الوسائل الرقمية. فالمؤسسة اليوم لا تحتفظ بمعلوماتها داخل ملفات ورقية فقط، بل تعتمد على قواعد بيانات، ومنصات تواصل، وحسابات مصرفية إلكترونية، وبرامج إدارة، وخوادم داخلية أو سحابية. وهذا التحول جعل المعلومات جزءاً من رأس مال المؤسسة، لأن فقدانها أو تسريبها أو تعطيلها قد يؤدي إلى خسائر مالية، واضطراب في العمل، وفقدان ثقة الزبائن، وربما مسؤولية قانونية. لذلك لم يعد الأمن المعلوماتي مسألة كمالية، بل أصبح شرطاً لاستمرار النشاط.

وبالنسبة للمؤسسات، يمثل الأمن المعلوماتي وسيلة لحماية الأسرار المهنية والبيانات المالية وملفات العمال والزبائن والعقود والمراسلات الداخلية. فإذا تعرضت هذه المعلومات للاختراق، فقد تستغل ضد المؤسسة في المنافسة أو الابتزاز أو التشهير. كما قد يؤدي تسرب

¹ بن برغوث ليلي، الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر، المجلة الدولية للاتصال الاجتماعي، المجلد 10 العدد 1، جامعة مستغانم، 2023، ص484. <https://revue.univ-mosta.dz/index.php/ijsc/article/view/1000/858>

بيانات الزبائن إلى إضعاف الثقة في المؤسسة، لأن المستخدم لا يتعامل مع الخدمة الرقمية فقط، بل يضع فيها جزءاً من حياته الخاصة. ومن هنا يصبح الأمن المعلوماتي عنصراً من عناصر السمعة، وليس مجرد إجراء تقني خلف الأبواب.

وتظهر أهمية الأمن المعلوماتي أيضاً في المؤسسات العمومية، لأن الإدارة الحديثة تتجه تدريجياً نحو الرقمنة. وعندما تصبح الخدمات الإدارية مرتبطة بالمنصات الرقمية، فإن حماية المعلومات تصبح مرتبطة بثقة المواطن في الدولة. فالسجلات المدنية، والبيانات الجبائية، والملفات الصحية، والوثائق الإلكترونية، كلها تحتاج إلى حماية قوية، لأنها تمس الحقوق والمراكز القانونية للأفراد. ولذلك فإن أي خلل في الأمن المعلوماتي داخل الإدارة قد لا يسبب ضرراً تقنياً فقط، بل قد يمس شرعية الخدمة العمومية وصدقيتها¹.

أما بالنسبة للأفراد، فإن الأمن المعلوماتي يحمي الهوية الرقمية والحسابات الشخصية والبيانات البنكية والصور والمراسلات والمعلومات الصحية والمهنية. فالإنسان في البيئة الرقمية يترك آثاراً كثيرة، وقد تستعمل هذه الآثار ضده إذا وقعت في يد غير آمنة. ومن أمثلة ذلك سرقة الحسابات، أو انتحال الهوية، أو الابتزاز الإلكتروني، أو الاحتيال المالي، أو نشر المعطيات الشخصية دون إذن. ولذلك فإن حماية الفرد لمعلوماته لم تعد أمراً اختياريّاً، بل صارت جزءاً من حماية حياته الخاصة.

ومع الذكاء الاصطناعي، يصبح الفرد أكثر عرضة لأشكال جديدة من المخاطر. فالتقنيات الذكية تستطيع تحليل السلوك، وتوقع الاهتمامات، وتخصيص المحتوى، بل وقد تستعمل في صناعة صور أو أصوات مزيفة. وهذا يجعل الأمن المعلوماتي مرتبطاً كذلك بحماية الشخصية الرقمية، لأن الاعتداء لم يعد يقتصر على سرقة كلمة مرور، بل يمكن أن يصل إلى صناعة هوية مزيفة أو محتوى مضلل باسم الشخص. ولهذا فإن الوعي الأمني لدى الأفراد يجب أن يتطور بقدر تطور الأدوات المستعملة ضدهم.

¹ Polona Car, Tristan Marcelin, Artificial Intelligence and Cybersecurity, 2024, p.1

وتكمن أهمية الأمن المعلوماتي كذلك في حماية الاقتصاد الرقمي. فالتجارة الإلكترونية، والدفع الإلكتروني، والخدمات البنكية عن بعد، والعمل عن بعد، والتعليم الرقمي، كلها تقوم على الثقة في سلامة الأنظمة وحماية البيانات. وإذا غابت هذه الثقة تراجع استعمال الخدمات الرقمية، وتضررت المؤسسات، وضعفت سرعة التحول الرقمي. لذلك فإن الأمن المعلوماتي ليس عائقاً أمام التطور، بل هو شرط له، لأن الرقمنة دون حماية تشبه بناء مدينة زجاجية بلا أبواب.

وفي الجزائر، أصبح الاهتمام الرسمي بأمن الأنظمة المعلوماتية أكثر وضوحاً من خلال تبني استراتيجية وطنية للفترة 2025-2029، وهو ما يعكس إدراكاً بأن الأمن الرقمي أصبح جزءاً من الأمن الوطني والتنمية الرقمية. فالاستراتيجية لا تتعلق بحماية أجهزة منفصلة، بل تهدف إلى بناء قدرة وطنية على الوقاية والاستجابة وتعزيز المرونة السيبرانية، خاصة أمام تزايد الاعتماد على الخدمات الرقمية والبنى التحتية المعلوماتية¹ وقد أشارت وزارة الدفاع الوطني إلى أن الاستراتيجية تمثل إطاراً شاملاً يهدف إلى ضمان المرونة السيبرانية الوطنية وحماية البنية التحتية الرقمية

كما أن أهمية الأمن المعلوماتي تتجلى في كونه مجاًلاً مشتركاً بين الدولة والقطاع الخاص والمجتمع. فالدولة تضع السياسات والقوانين، والمؤسسات تطبق الحماية داخل أنظمتها، والأفراد يلتزمون بسلوك رقمي واعٍ. وإذا ضعف طرف من هذه الأطراف، انعكس ذلك على الحماية العامة. فالمؤسسة التي لا تدرب عمالها تفتح باباً للاختراق، والمستخدم الذي لا يحمي حساباته قد يضر بنفسه وبغيره، والدولة التي لا تطور أطرها القانونية قد تترك فراغاً يستفيد منه المهاجمون.

وتزداد هذه الأهمية في ظل الذكاء الاصطناعي لأن الهجمات أصبحت أكثر قابلية للأتمتة. فالمهاجم لم يعد يحتاج دائماً إلى جهد يدوي كبير، إذ يمكنه استعمال أدوات ذكية لتوليد رسائل احتيالية كثيرة، أو البحث عن ثغرات، أو تحليل الضحايا، أو انتحال أنماط تواصل

¹ وزارة الدفاع الوطني، الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029، المرجع السابق، ص 5

حقيقية. وهذا يجعل المؤسسات والأفراد أمام خصم أسرع وأكثر قدرة على التكيف. وفي المقابل، يمكن للمدافعين أن يستعملوا الذكاء الاصطناعي لمواجهة هذه الهجمات، لكن ذلك يتطلب موارد بشرية مؤهلة، وبيانات جيدة، وقواعد واضحة، ونظام مراقبة مستمر.

ومن هنا يمكن القول إن الأمن المعلوماتي لم يعد مجرد حماية تقنية منعزلة، بل أصبح ثقافة وممارسة وسياسة عامة. فكل مؤسسة تحتاج إلى معرفة ما الذي تريد حمايته، ومن يحق له الوصول إليه، وما المخاطر المحتملة، وكيف تتصرف عند وقوع حادث. وكل فرد يحتاج إلى حد أدنى من الوعي بسلوكيات الحماية. وكل دولة تحتاج إلى رؤية وطنية تنظم الأمن الرقمي وتحمي البنية التحتية. وفي ظل الذكاء الاصطناعي، يصبح هذا كله أكثر إلحاحاً، لأن سرعة الخطر لا تترك وقتاً طويلاً للارتجال.¹

يتبين مما سبق أن الأمن المعلوماتي يقوم على حماية المعلومات من كل مساس يهدد سريتها أو سلامتها أو إتاحتها. كما تبين أن الأمن المعلوماتي أوسع من مجرد الحماية التقنية، لأنه يشمل الإنسان والمؤسسة والقانون والسياسة الأمنية. أما الأمن السيبراني فيرتبط أكثر بحماية الفضاء الرقمي والأنظمة والشبكات، لكنه أصبح متداخلاً مع الأمن المعلوماتي بسبب رقمنة أغلب البيانات والخدمات. وفي ظل الذكاء الاصطناعي، تزداد الحاجة إلى هذا التمييز، لأن التقنية الجديدة تستطيع أن تعزز الحماية من جهة، وأن تخلق تهديدات أكثر تعقيداً من جهة أخرى.

¹ National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework AI RMF 1.0, 2023, p.1 <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>

المبحث الثاني: آليات الذكاء الاصطناعي في تعزيز الأمن المعلوماتي

بعد تحديد مفهوم الأمن المعلوماتي وأبعاده الأساسية، يظهر أن الذكاء الاصطناعي لم يدخل هذا المجال باعتباره أداة عادية، بل باعتباره وسيلة قادرة على تغيير طريقة التفكير في الحماية نفسها. فالوسائل التقليدية في الأمن المعلوماتي كانت تعتمد في كثير من الأحيان على قواعد ثابتة، مثل التعرف على توقيع فيروس معروف، أو منع عنوان مشبوه، أو تطبيق سياسة دخول محددة. أما الذكاء الاصطناعي فينتجه إلى تحليل السلوك، واكتشاف الأنماط غير المألوفة، والتنبؤ بالخطر قبل أن يتحول إلى حادث كامل.

ولهذا، فإن قيمة الذكاء الاصطناعي في الأمن المعلوماتي تظهر في قدرته على التعامل مع كثافة البيانات وسرعة التهديدات. فالهجمات الحديثة لا تأتي دائماً في شكل واضح، بل قد تبدأ بإشارة صغيرة داخل سجل دخول، أو حركة غير مألوفة في الشبكة، أو رسالة تبدو عادية لكنها تحمل نية احتيالية. وقد أشار البرلمان الأوروبي إلى أن العلاقة بين الذكاء الاصطناعي والأمن السيبراني تقوم على ثلاثة أبعاد: أمن أنظمة الذكاء الاصطناعي نفسها، واستعمال الذكاء الاصطناعي لدعم الأمن السيبراني، واستعماله لأغراض خبيثة لإنتاج تهديدات جديدة.¹

المطلب الأول: الكشف الذكي عن التهديدات والهجمات

يعد كشف التهديدات من أهم المجالات التي استفاد فيها الأمن المعلوماتي من الذكاء الاصطناعي، لأن الهجمات الرقمية لم تعد تسير دائماً وفق نمط واحد يمكن التعرف عليه بسهولة. فقد يستعمل المهاجم أسلوباً جديداً، أو يغير شكل البرمجية الخبيثة، أو يخفي نشاطه داخل حركة عادية في الشبكة. ولهذا أصبحت الأنظمة الأمنية بحاجة إلى أدوات لا تنتظر ظهور الخطر بشكل كامل، بل تبحث عن مؤشرات صغيرة قد تدل على وجود اختراق أو محاولة تسلل.

¹ Polona Car, Tristan Marcelin, op.cit, p.4

وتقوم الأنظمة الذكية في هذا المجال على تحليل كميات كبيرة من البيانات الأمنية، مثل سجلات الدخول، وحركة الشبكة، وأنماط استعمال التطبيقات، ومحاولات الوصول إلى الملفات، وسلوك المستخدمين داخل النظام. ومن خلال هذه البيانات يمكن للنظام أن يبني صورة عامة عن السلوك الطبيعي، ثم ينبه إلى كل حركة تخرج عن هذا النمط. فإذا كان عامل في مؤسسة يدخل عادة من جهاز معين وفي وقت معين، ثم ظهر دخول مفاجئ من موقع بعيد أو في ساعة غير معتادة، فإن النظام الذكي يستطيع اعتبار ذلك مؤشراً يستحق الفحص.¹

وتظهر أهمية هذا الأسلوب في أن الهجوم لا يكشف فقط من خلال “اسم الفيروس” أو “توقيع البرمجية”، بل من خلال السلوك. فالبرمجية الخبيثة قد تغير اسمها وشكلها، لكن سلوكها داخل النظام قد يكشفها، مثل محاولة الوصول إلى عدد كبير من الملفات، أو إرسال بيانات إلى خادم خارجي، أو تعطيل بعض الخدمات الأمنية. ولذلك فإن التحليل السلوكي يسمح بالانتقال من حماية جامدة إلى حماية أكثر حركة ومرونة.

وقد أكدت دراسة دحماني محمد حول الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني أن التهديدات السيبرانية الحديثة تتميز بطبيعة مختلفة عن التهديدات التقليدية، لأنها تستهدف الأفراد والمؤسسات والدول من خلال الاختراقات والبرمجيات الخبيثة والاعتداءات الإلكترونية، وهو ما يجعل الاعتماد على تقنيات متقدمة في الرصد والتحليل ضرورة أمنية لا مجرد خيار تقني²

ولا يقتصر الكشف الذكي على مراقبة الهجمات الخارجية، بل يشمل أيضاً التهديدات الداخلية. فقد يكون الخطر صادراً عن مستخدم يملك صلاحيات داخل المؤسسة، سواء بسبب خطأ أو بسبب نية سيئة. وهنا يمكن للذكاء الاصطناعي أن يراقب تغير السلوك، مثل تحميل ملفات كثيرة في وقت قصير، أو الدخول إلى بيانات لا تتناسب مع طبيعة عمل

¹ زمورة جمال وبن عيسى ليلي، المرجع السابق، ص74

² دحماني محمد، الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني والسياسي، المجلد 7 العدد 2، جامعة الاغواط، 2023، ص

الموظف، أو استعمال حسابات خارج أوقات العمل المعتادة. وهذا النوع من المراقبة لا يعني اتهام الأشخاص مسبقاً، بل يعني بناء إنذار مبكر يمنع الضرر قبل توسعه.

كما تستفيد أنظمة كشف التهديدات من التعلم الآلي في تصنيف المخاطر حسب درجة الخطورة. فبدل أن تغرق فرق الأمن في آلاف التنبيهات اليومية، يمكن للنظام الذكي أن يرتبها حسب الأولوية، فيميز بين التنبيه البسيط والتهديد الذي يحتاج إلى تدخل عاجل. وهذا مهم جداً لأن كثرة التنبيهات قد تؤدي إلى إرهاق فرق الأمن، وقد تجعلهم يهملون إشارات خطيرة وسط ضجيج كبير من الإنذارات. ومن هنا يتحول الذكاء الاصطناعي إلى أداة تنظيمية كذلك، لأنه يساعد على توجيه الجهد البشري نحو ما يستحق المتابعة أولاً.

ويستعمل الذكاء الاصطناعي كذلك في كشف التصيد الإلكتروني، وهو من أكثر الهجمات انتشاراً وخطورة. فالرسائل الاحتيالية أصبحت أكثر إتقاناً، وقد تستعمل لغة قريبة من أسلوب المؤسسة أو الشخص المستهدف. وهنا تستطيع النماذج الذكية تحليل مضمون الرسالة، والروابط الموجودة فيها، وطريقة الكتابة، وسلوك المرسل، ومقارنتها بالرسائل المعتادة، ثم تحديد احتمال كونها محاولة احتيال. ومع تطور الذكاء الاصطناعي التوليدي، أصبح هذا المجال أكثر حساسية، لأن المهاجمين أنفسهم يستطيعون استعماله لصناعة رسائل تصيد أكثر إقناعاً¹.

وتبرز أهمية الكشف الذكي أيضاً في مواجهة الهجمات غير المعروفة سابقاً. فالوسائل التقليدية تكون فعالة غالباً ضد التهديدات المعروفة، لكنها تضعف أمام الهجمات الجديدة التي لم تسجل لها بصمة أمنية من قبل. أما الذكاء الاصطناعي فيمكنه الاعتماد على مؤشرات عامة للسلوك المشبوه حتى لو كان نوع الهجوم جديداً. ولهذا فإن دوره لا يقوم فقط على التعرف على الخطر المعروف، بل على الشك المنظم في كل سلوك غير مألوف.

¹ UNESCO, Recommendation on the Ethics of Artificial Intelligence, 2021, p.14 .

https://unesdoc.unesco.org/ark:/48223/pf0000381137_ara

غير أن هذا لا يعني أن الكشف الذكي معصوم من الخطأ. فقد ينتج النظام إنذارات كاذبة عندما يظن أن سلوكًا مشرورًا هو تهديد، وقد يفشل في كشف هجوم متقن إذا كان قريبًا جدًا من السلوك الطبيعي. لذلك يبقى دور الإنسان ضروريًا في التحقق والتحليل واتخاذ القرار النهائي. فالذكاء الاصطناعي هنا يعمل كعين رقمية واسعة، لكنه يحتاج إلى عقل بشري يقرأ النتائج ويقدر السياق ويمنع التسرع في الحكم.

ومن هذه الزاوية، يمكن القول إن الذكاء الاصطناعي يعزز الأمن المعلوماتي لأنه يرفع قدرة المؤسسات على رؤية ما لا يظهر بسهولة. فهو لا يلغي دور الخبراء، بل يمنحهم أدوات أوسع لتحليل الشبكات والبيانات والحسابات. وكلما كانت البيانات التي يتغذى عليها النظام دقيقة ومنظمة، كانت قدرته على كشف التهديدات أفضل. أما إذا كانت البيانات ناقصة أو ملوثة، فقد يتحول النظام نفسه إلى مصدر تقدير خاطئ، وهي نقطة تجعل جودة البيانات شرطًا أساسيًا لنجاح الحماية الذكية¹.

المطلب الثاني: الاستجابة الآلية للحوادث الأمنية

لا تكتمل فائدة الكشف عن التهديدات إذا لم ترافقه قدرة على الاستجابة السريعة. فبعض الهجمات الرقمية تتحرك بسرعة كبيرة، وقد تنتشر داخل النظام قبل أن يتمكن الإنسان من التدخل يدويًا. لذلك أصبحت الاستجابة الآلية للحوادث الأمنية من أهم مجالات توظيف الذكاء الاصطناعي، لأنها تسمح بتقليل الزمن الفاصل بين اكتشاف الخطر والتعامل معه.

ويقصد بالاستجابة الآلية أن تقوم الأنظمة الأمنية بتنفيذ إجراءات معينة بمجرد ظهور مؤشر خطر، مثل عزل جهاز مصاب، أو إيقاف حساب مشبوه، أو منع اتصال خارجي، أو نقل ملف إلى منطقة آمنة، أو إرسال تنبيه عاجل إلى فريق الأمن. ولا يعني ذلك ترك القرار كله للآلة، بل يمكن أن تكون الاستجابة على درجات: فبعض الحالات البسيطة تعالج آليًا،

¹ بن أحمد فاطمة الزهراء و صحراوي بن شبيحة، الذكاء الاصطناعي وتحسين الأمن السيبراني للمنظمات: دراسة حالة شركة مايكروسوفت، مجلة البشائر الاقتصادية، المجلد 11 العدد 1، جامعة بشار، 2025، ص283. <https://asjp.cerist.dz/en/article/266184>

وبعض الحالات المتوسطة تحتاج إلى موافقة بشرية، أما الحالات الخطيرة فتجمع بين التدخل الآلي والتحقيق البشري العاجل.

وتظهر أهمية هذه الآلية في أن الهجوم الناجح غالبًا يستفيد من عامل الوقت. فكل دقيقة تأخير قد تسمح للمهاجم بتوسيع نطاق الاختراق، أو سرقة بيانات أكثر، أو تعطيل خدمة مهمة. لذلك فإن الذكاء الاصطناعي يساعد على تحويل الأمن المعلوماتي من رد فعل بطيء إلى استجابة أسرع وأكثر تنظيمًا. وقد أكد تقرير المنتدى الاقتصادي العالمي أن تأمين استعمال الذكاء الاصطناعي داخل المؤسسات يحتاج إلى الجمع بين إجراءات ما قبل التشغيل وإجراءات ما بعد التشغيل، أي إدخال الحماية منذ مرحلة التصميم مع الاستمرار في المراقبة والاستجابة والتعافي بعد التشغيل

وتسمح الاستجابة الذكية كذلك بتقليل أثر الخطأ البشري. ففي حالات الضغط، قد يتأخر الموظف في قراءة التنبيه أو يخطئ في تقدير خطورته. أما النظام الذكي فيستطيع تنفيذ إجراءات أولية بسرعة كبيرة، خاصة إذا كانت القواعد محددة مسبقًا. فإذا تم اكتشاف حساب يحاول الدخول عشرات المرات بكلمات مرور مختلفة، يمكن للنظام أن يوقفه مؤقتًا قبل أن ينجح الهجوم. وإذا ظهر جهاز يرسل بيانات غير معتادة إلى خارج الشبكة، يمكن عزله حتى يتم التحقيق في سبب ذلك.

ومع ذلك، يجب أن تكون الاستجابة الآلية مضبوطة حتى لا تتحول إلى مصدر اضطراب. فإذا كان النظام شديد الحساسية فقد يعطل حسابات سليمة أو يوقف خدمات ضرورية بسبب إنذارات كاذبة. لذلك تحتاج المؤسسات إلى تحديد مستويات الخطر بدقة، وربط كل مستوى بإجراء مناسب، مع ترك مساحة للتدخل البشري في القرارات الحساسة. فالاستجابة الذكية لا تعني السرعة فقط، بل تعني السرعة المتوازنة مع الدقة والرقابة.¹

¹ بلشير يعقوب، الجريمة السيبرانية في عصر الذكاء الاصطناعي: قراءة في التحديات والمخاطر المستجدة، مجلة حقوق الإنسان والحريات العامة، المجلد

10 العدد 2، جامعة مستغانم، 2025، ص242. <https://asjp.cerist.dz/en/article/281940>

وتفيد أنظمة الذكاء الاصطناعي أيضًا في تحليل الحادث بعد وقوعه، لأنها تستطيع تتبع مسار الهجوم، ومعرفة نقطة البداية، وتحديد الملفات أو الحسابات التي تأثرت، واقتراح إجراءات المنع المستقبلية. وهذا الجانب مهم لأن الحادث الأمني لا ينتهي بمجرد إيقاف الهجوم، بل يجب فهمه حتى لا يتكرر. فكل حادث هو درس أمني، والذكاء الاصطناعي يساعد على استخراج هذا الدرس من كمية كبيرة من السجلات والمعطيات.

كما تساهم الاستجابة الذكية في دعم خطط استمرارية النشاط. فإذا تعرضت خدمة معينة لهجوم، يمكن للنظام أن يساعد على توجيه الحركة إلى خوادم بديلة، أو تفعيل نسخ احتياطية، أو ترتيب الأولويات حسب أهمية الخدمات. وهذا يجعل الأمن المعلوماتي مرتبطًا بالمرونة، أي قدرة المؤسسة على مواصلة العمل رغم وقوع الحادث. فالهدف ليس منع كل خطر بصورة مطلقة، لأن ذلك غير ممكن عمليًا، بل بناء قدرة على تقليل الضرر واسترجاع الوضع بسرعة.

وفي مجال المؤسسات الصغيرة والمتوسطة، قد يكون الذكاء الاصطناعي مفيدًا لأنه يعوض جزئيًا نقص الخبراء الأمنيين. فليست كل مؤسسة قادرة على تشغيل فريق أمن كبير طوال اليوم، لكن يمكنها الاعتماد على أدوات ذكية للمراقبة والتنبيه والاستجابة الأولية. ومع ذلك، لا ينبغي أن يؤدي هذا إلى وهم الاكتفاء بالأداة، لأن أي نظام يحتاج إلى إعداد صحيح وتحديث ومراجعة. فالأداة الأمنية التي لا يفهمها صاحبها تشبه قفلاً فاخرًا ترك مفتاحه في الباب.¹

وتظهر هنا أهمية الحوكمة الداخلية، لأن الاستجابة الآلية يجب أن تكون جزءًا من سياسة مكتوبة توضح من يملك صلاحية تعطيل الحسابات، ومتى يتم عزل الأجهزة، وكيف يتم إعلام المسؤولين، وكيف تحفظ الأدلة الرقمية بعد الحادث. فغياب هذه السياسة قد يجعل الاستجابة عشوائية، حتى لو كانت الأدوات متقدمة. لذلك فإن الذكاء الاصطناعي لا يعوض التنظيم، بل يحتاج إليه حتى يعمل بطريقة سليمة.

¹ زمرة جمال وبن عيسى ليلي، المرجع السابق، ص 87

ومن جهة أخرى، يمكن استعمال الذكاء الاصطناعي في اختبار جاهزية الاستجابة الأمنية، من خلال محاكاة هجمات محتملة وقياس سرعة النظام في التعامل معها. وهذا يساعد المؤسسة على معرفة نقاط الضعف قبل أن يستغلها المهاجم الحقيقي. فالأمن الجيد لا ينتظر الكارثة حتى يتعلم منها، بل يصنع سيناريوهات تدريبية تكشف الضعف في وقت آمن. وهنا يصبح الذكاء الاصطناعي أداة وقائية وتدريبية في الوقت نفسه¹.

ومن خلال ما سبق، يظهر أن الاستجابة الآلية للحوادث الأمنية تمثل مرحلة متقدمة من الأمن المعلوماتي، لأنها لا تكتفي بمعرفة الخطر، بل تنتقل إلى احتوائه وتحليله وتقليل آثاره. غير أن نجاحها يتوقف على التوازن بين الآلة والإنسان، وبين السرعة والرقابة، وبين الحماية واستمرارية الخدمة. فإذا تحقق هذا التوازن، أصبح الذكاء الاصطناعي قادرًا على دعم المؤسسات في مواجهة بيئة رقمية تتحرك بسرعة البرق وتترك آثارها في صمت.

المطلب الثالث: تحليل البيانات والتنبؤ بالمخاطر الأمنية

يمثل التنبؤ بالمخاطر الأمنية أحد أهم التحولات التي أدخلها الذكاء الاصطناعي على مجال الأمن المعلوماتي. فالحماية التقليدية كانت تميل إلى التعامل مع الخطر بعد وقوعه أو عند ظهوره بشكل واضح، أما الذكاء الاصطناعي فيحاول قراءة المؤشرات المبكرة التي قد تدل على خطر قادم. وهذا التحول مهم لأن المؤسسات لم تعد تحتاج فقط إلى معرفة ما حدث، بل تحتاج إلى توقع ما قد يحدث حتى تستعد له قبل فوات الأوان.

وتعتمد القدرة التنبؤية على تحليل البيانات التاريخية والحالية معًا. فالنظام الذكي يدرس الحوادث السابقة، وأنماط الهجمات، وسلوك المستخدمين، والثغرات المتكررة، وحركة الشبكة، ثم يحاول استخراج علاقات يمكن أن تساعد على توقع احتمال وقوع هجوم جديد. فمثلاً، إذا لاحظ النظام زيادة غير معتادة في محاولات فحص المنافذ، أو تكرار محاولات الدخول

¹ ابن برغوث ليلي، المرجع السابق، ص 450.

الفاشلة، أو ارتفاع حجم حركة البيانات في اتجاه معين، فقد يعتبر ذلك مؤشراً على هجوم قادم أو اختبار تمهيدي من طرف المهاجم.

ولا يتعلق التنبؤ هنا بمعرفة المستقبل بصورة قطعية، بل بتقدير الاحتمالات. فالذكاء الاصطناعي لا يقول إن الهجوم سيقع حتماً، بل يرفع درجة الانتباه إلى وجود ظروف تشبه ظروف هجمات سابقة. وهذا مفيد جداً في إدارة المخاطر، لأن المؤسسة تستطيع توزيع مواردها حسب مستوى الخطر، بدل التعامل مع كل التنبيهات بالدرجة نفسها. فالأمن المعلوماتي لا يقوم فقط على امتلاك أدوات كثيرة، بل على معرفة أين يجب استعمالها ومتى.

وفيد تحليل البيانات كذلك في بناء خريطة للمخاطر داخل المؤسسة. فقد يكشف النظام أن بعض الأقسام أكثر تعرضاً لمحاولات التصيد، أو أن بعض الأجهزة لم تحدث منذ مدة، أو أن بعض المستخدمين يملكون صلاحيات أوسع مما يحتاجون إليه. ومن خلال هذه النتائج يمكن للمؤسسة أن تعالج نقاط الضعف قبل أن تتحول إلى باب للاختراق. وهنا يظهر الذكاء الاصطناعي كأداة تشخيص، لا كأداة دفاع فقط.¹

وقد أكد المنتدى الاقتصادي العالمي أن المؤسسات التي تعتمد الذكاء الاصطناعي تحتاج إلى فهم السياق الذي يؤثر في الخطر السيبراني، وتحديد المخاطر والثغرات المحتملة، وتقييم آثارها، ثم اختيار وسائل التخفيف المناسبة طوال دورة حياة النظام.

وهذا المعنى ينسجم مع فكرة أن التنبؤ الأمني لا يكون إجراء منفصلاً، بل جزءاً من إدارة متكاملة للمخاطر.

كما يمكن للذكاء الاصطناعي أن يساعد في تحليل التهديدات الخارجية، مثل متابعة الأخبار الأمنية، وقواعد بيانات الثغرات، وتقارير البرمجيات الخبيثة، والأنشطة المشبوهة على الشبكات. فبدل أن تبقى المؤسسة معزولة داخل نظامها، تستطيع ربط حمايتها بالمشهد الأمني

¹ بن أحمد فاطمة الزهراء و صحراوي بن شيخة، المرجع السابق، ص283.

العام. فإذا ظهرت ثغرة خطيرة في برنامج تستعمله المؤسسة، يمكن للنظام أن يرفع مستوى الخطر تلقائيًا وينبه المسؤولين إلى ضرورة التحديث أو عزل بعض الخدمات.¹

ويظهر دور التنبؤ أيضًا في حماية البنية التحتية الحساسة، مثل الطاقة، والاتصالات، والبنوك، والخدمات الحكومية. فهذه القطاعات لا تحمل الانتظار حتى يقع الهجوم، لأن الضرر قد يمس المجتمع كله. لذلك تحتاج إلى مراقبة مستمرة وتحليل مسبق للمخاطر. وكلما كانت البيانات المتاحة أكثر تنظيمًا وتكاملاً، أمكن للذكاء الاصطناعي أن يقدم قراءة أفضل للوضع الأمني.

غير أن التنبؤ بالمخاطر يطرح بدوره تحديات مهمة. أولها أن جودة التوقع مرتبطة بجودة البيانات. فإذا كانت البيانات ناقصة أو قديمة أو غير ممثلة للواقع، فإن التوقعات ستكون ضعيفة. وثانيها أن المهاجمين قد يحاولون خداع النماذج الذكية بإرسال بيانات مضللة أو خلق سلوكيات مصطنعة تجعل النظام يخطئ في تقدير الخطر. وثالثها أن الإفراط في التنبؤ قد يؤدي إلى قلق أمني دائم يجعل المؤسسة تتعامل مع الاحتمالات كأنها حقائق مؤكدة.²

ولذلك يجب أن يبقى التنبؤ الأمني أداة مساعدة في اتخاذ القرار، لا بديلاً عن التقييم البشري. فالخبير الأمني يستطيع قراءة السياق الذي قد لا تفهمه الخوارزمية، مثل ظروف العمل، أو طبيعة المشروع، أو حساسية البيانات، أو وجود تغييرات داخلية في المؤسسة. فإذا اجتمع التحليل الآلي مع الخبرة البشرية، أصبحت إدارة المخاطر أكثر توازناً وواقعية.

ومن جهة أخرى، يمكن استعمال التنبؤ الأمني في التخطيط المالي والإداري. فالمؤسسة التي تعرف أكثر مصادر الخطر تستطيع توجيه ميزانيتها نحو الحماية الأكثر حاجة، بدل شراء أدوات كثيرة دون خطة واضحة. كما يمكنها ترتيب برامج التكوين حسب المخاطر الفعلية، فإذا كانت الهجمات الأكثر تكرارًا تستهدف البريد الإلكتروني، يصبح تدريب العمال على

¹ ناصر مراد، المرجع السابق، ص 71

² بن برغوث لبلي، المرجع السابق، ص 450.

كشف التصيد أولوية. وإذا كانت الثغرات مرتبطة بتحديثات الأنظمة، تصبح إدارة التحديثات أولوية.¹

وفي ظل الذكاء الاصطناعي، يصبح تحليل البيانات والتنبؤ بالمخاطر أشبه برادار داخل العاصفة الرقمية. فهو لا يمنع العاصفة من الوجود، لكنه يمنح المؤسسة فرصة رؤية اتجاهها قبل أن تصطدم بها. وكلما كان هذا الرادار مضبوطاً ومراقباً، كانت فائدته أكبر. أما إذا ترك دون مراجعة، فقد يرى خطراً حيث لا يوجد خطر، أو يغفل عن خطر حقيقي يتخفى خارج أنماطه السابقة.

يتبين من خلال هذا المبحث أن الذكاء الاصطناعي يعزز الأمن المعلوماتي عبر ثلاث آليات أساسية: الكشف الذكي عن التهديدات، والاستجابة الآلية للحوادث، وتحليل البيانات للتنبؤ بالمخاطر. وهذه الآليات تجعل الحماية أكثر سرعة ومرونة وقدرة على التعامل مع الهجمات الحديثة. غير أن نجاحها لا يتحقق بمجرد استعمال أدوات ذكية، بل يتوقف على جودة البيانات، ووضوح السياسات الداخلية، ووجود رقابة بشرية، وربط الذكاء الاصطناعي بإدارة شاملة للمخاطر. فالذكاء الاصطناعي لا يلغي الحاجة إلى الإنسان، بل يجعل دوره أكثر دقة؛ ينتقل من المتابعة اليدوية المتعبة إلى التحليل والتقدير واتخاذ القرار.

¹ حياة حميدي. نسيم طايبل، مدخل مفاهيمي حول الأمن السيبراني، مجلة مدار للدراسات الاتصالية الرقمية، المجلد 2 العدد 2، جامعة الجزائر3،

المبحث الثالث: تحديات الأمن المعلوماتي في ظل الذكاء الاصطناعي

رغم أن الذكاء الاصطناعي يمنح الأمن المعلوماتي أدوات قوية في الرصد والتحليل والاستجابة، إلا أنه في الوقت نفسه يخلق تحديات جديدة أكثر تعقيدًا من التحديات التقليدية. فالخطر لم يعد يأتي فقط من مهاجم يستعمل برنامجًا خبيثًا معروفًا، بل أصبح يمكن أن يأتي من خوارزمية قادرة على توليد رسائل احتيالية مقنعة، أو تحليل الضحايا بدقة، أو تقليد الصوت والصورة، أو البحث الآلي عن الثغرات. ومن هنا يظهر أن الذكاء الاصطناعي لا يدخل مجال الأمن المعلوماتي كوسيلة دفاع فقط، بل يدخل أيضًا كقوة يمكن أن يستغلها المهاجم، مما يجعل البيئة الرقمية أكثر حساسية وتشابكًا.¹

¹ المرجع نفسه، ص 13

والتحدي الحقيقي في هذا المجال أن الذكاء الاصطناعي يرفع مستوى السرعة والتعقيد في آن واحد. فالهجوم الذي كان يحتاج إلى وقت وجهد ومعرفة تقنية واسعة، أصبح في بعض صورته قابلاً للتنفيذ بوسائل أسهل وأسرع. كما أن الدفاع لم يعد يستطيع الاعتماد على الوسائل القديمة وحدها، لأن المهاجم نفسه يتطور ويستعمل أدوات قادرة على التعلم والتكيف. لذلك فإن الأمن المعلوماتي في ظل الذكاء الاصطناعي يشبه سباقاً مفتوحاً بين طرفين: طرف يستعمل التقنية للحماية، وطرف يستعملها لاختراق الحماية.

المطلب الأول: مخاطر الهجمات المدعومة بالذكاء الاصطناعي

تعد الهجمات المدعومة بالذكاء الاصطناعي من أخطر التحديات التي تواجه الأمن المعلوماتي، لأنها تجعل الاعتداءات الرقمية أكثر دقة وانتشاراً وقدرة على التخصيص. فالمهاجم لم يعد مضطراً إلى إرسال رسالة احتيالية عامة إلى عدد كبير من الأشخاص على أمل أن يقع بعضهم في الفخ، بل يمكنه استعمال أدوات ذكية لتحليل معلومات الضحية وصياغة رسالة تناسب وظيفته أو اهتماماته أو طريقة تواصله. وبهذا يصبح الاحتيال أكثر قرباً من الواقع، وأكثر قدرة على خداع المستخدم، خصوصاً عندما تبدو الرسالة مكتوبة بلغة سليمة وتحمل تفاصيل مقنعة.

ويظهر هذا الخطر بوضوح في التصيد الإلكتروني، لأن الذكاء الاصطناعي التوليدي يستطيع إنتاج نصوص طبيعية يصعب أحياناً تمييزها عن رسائل حقيقية. وقد كان التصيد سابقاً يكشف أحياناً من خلال الأخطاء اللغوية أو الصياغة الركيكة، أما اليوم فقد أصبحت الرسائل الاحتيالية أكثر جودة، وقد تحمل أسلوباً رسمياً أو مهنيّاً أو شخصياً بحسب الهدف. وهذا يعني أن معيار الانتباه إلى الأخطاء اللغوية لم يعد كافياً، بل أصبح من الضروري الاعتماد على تحقق متعدد، ومراقبة الروابط، وفحص المرسل، وتدريب المستخدمين على الشك المنظم لا على الثقة السريعة.

كما يمكن استعمال الذكاء الاصطناعي في إنشاء هويات مزيفة أكثر إقناعاً. فقد يستطيع المهاجم توليد صورة شخصية، أو إنشاء حسابات تبدو حقيقية، أو صياغة محادثات طويلة

لإقناع الضحية. وتزداد الخطورة عندما يرتبط ذلك بالترتيب العميق، لأن الصوت أو الصورة قد يستعملان لخداع موظف أو فرد أو مؤسسة. فإذا تلقى موظف اتصالاً بصوت يشبه صوت مديره ويطلب منه تحويل أموال أو إرسال ملف حساس، فإن الخطر هنا لا يعود تقنياً فقط، بل يصبح نفسياً واجتماعياً كذلك.¹

ومن المخاطر الخطيرة أيضاً استعمال الذكاء الاصطناعي في أتمتة البحث عن الثغرات. فالمهاجم يستطيع استخدام أدوات ذكية لمسح مواقع وخوادم وتطبيقات كثيرة في وقت قصير، وتحليل النتائج، وترتيب الأهداف الأكثر ضعفاً. وهذا يرفع حجم الهجمات ويجعل المؤسسات الصغيرة عرضة للخطر، حتى لو لم تكن مستهدفة بذاتها، لأنها قد تقع ضمن مسح آلي واسع يبحث عن أي باب مفتوح. وهنا يتحول الذكاء الاصطناعي إلى أداة توسع نطاق الاعتداء، لا مجرد أداة تزيد دقته.

وقد يستعمل الذكاء الاصطناعي كذلك في تطوير برمجيات خبيثة أكثر قدرة على التخفي. فالبرمجية قد تغير سلوكها بحسب البيئة التي توجد فيها، أو تؤخر نشاطها حتى لا تكتشف، أو تحاول تقليد سلوك عادي داخل النظام. وهذا يجعل وسائل الكشف التقليدية أقل فعالية، لأنها تعتمد غالباً على أنماط معروفة أو توقعات ثابتة. أما الهجوم الذكي فقد يتغير ويتكيف، فيصبح اكتشافه محتاجاً إلى تحليل سلوكي عميق ومراقبة مستمرة.

وتظهر خطورة هذه الهجمات أيضاً في أنها قد تستهدف أنظمة الذكاء الاصطناعي نفسها. فقد يحاول المهاجم التلاعب ببيانات التدريب حتى يتعلم النموذج بطريقة خاطئة، أو إدخال مدخلات مصممة لخداعه، أو استخراج معلومات من النموذج إذا كان قد تدرب على بيانات حساسة. وهذا النوع من الهجمات يختلف عن اختراق قاعدة بيانات عادية، لأنه يضرب منطق النظام الذكي وقدرته على إصدار نتائج صحيحة. فإذا كان النظام يستعمل في الأمن المعلوماتي، فإن خداعه قد يجعل الحماية نفسها تتحول إلى نقطة ضعف.²

¹ بن أحمد فاطمة الزهراء و صحراوي بن شيخة، المرجع السابق، ص286.

² بلشير يعقوب، المرجع السابق، ص256.

ومن جهة أخرى، لا تقتصر الهجمات المدعومة بالذكاء الاصطناعي على المؤسسات الكبيرة، بل تمس الأفراد أيضاً. فالأفراد يستعملون هواتفهم وحساباتهم وتطبيقاتهم البنكية ومنصاتهم الاجتماعية يومياً، وكلها تحتوي على معلومات يمكن استغلالها. ومع توفر أدوات توليد النصوص والصور والصوت، يصبح من السهل صناعة سيناريوهات احتيال شخصية، مثل رسالة من قريب، أو إعلان عمل، أو رابط مسابقة، أو طلب دفع عاجل. ولذلك فإن الأمن المعلوماتي في هذا السياق لا يعتمد فقط على الأنظمة التقنية، بل يحتاج إلى وعي اجتماعي واسع.

ويجب التنبيه إلى أن الخطر لا يأتي من الذكاء الاصطناعي في ذاته، بل من طريقة استعماله. فالأداة التي تكشف البرمجيات الخبيثة يمكن أن تستعمل لتحسينها، والأداة التي تحلل السلوك لحماية المستخدم يمكن أن تستعمل للتلاعب به، والنموذج الذي يكتب نصاً تعليمياً يمكن أن يكتب رسالة احتيالية. ولهذا فإن المشكلة ليست في وجود التقنية وحدها، بل في غياب الضوابط والرقابة والوعي. فكل تقنية قوية تحمل في داخلها احتمالين: أن تكون قفلاً للباب، أو نسخة من المفتاح في يد غير آمنة.

ومن هنا، فإن مواجهة الهجمات المدعومة بالذكاء الاصطناعي تتطلب تطوير أدوات دفاعية موازية، وتحديث أنظمة المراقبة، وتدريب المستخدمين، ووضع سياسات واضحة لاستعمال الذكاء الاصطناعي داخل المؤسسات. كما تتطلب التعاون بين الجهات التقنية والقانونية، لأن كثيراً من هذه الهجمات لا يمكن مواجهتها بالبرامج وحدها. فالتزيف العميق، وانتحال الهوية، والاحتيال الذكي، والتلاعب بالبيانات، كلها تحتاج إلى حماية تقنية وردع قانوني وتوعية مستمرة.

المطلب الثاني: إشكالات الخصوصية وحماية البيانات

تعد الخصوصية من أكثر القضايا حساسية في ظل الذكاء الاصطناعي، لأن هذه التقنية تقوم في جزء كبير من فعاليتها على جمع البيانات وتحليلها. وكلما زادت البيانات، تحسن أداء النظام في التوقع والتصنيف والتوصية، لكن في المقابل زادت احتمالات المساس بالحياة الخاصة. فالبيانات لم تعد تقتصر على الاسم أو العنوان أو رقم الهاتف، بل أصبحت تشمل السلوك الرقمي، والموقع، وعمليات البحث، والاهتمامات، والصور، والمحادثات، والعلاقات، والأنماط

اليومية. وهذا يجعل حماية البيانات مسألة مرتبطة بالكرامة والحرية، لا بمجرد حفظ ملفات إلكترونية¹.

وتظهر الإشكالية الأولى في كثافة جمع البيانات. فالكثير من التطبيقات والمنصات تجمع بيانات واسعة عن المستخدمين، أحياناً أكثر مما يحتاجه تقديم الخدمة. ومع إدخال الذكاء الاصطناعي، تصبح هذه البيانات مادة للتحليل والاستنتاج، وقد تستخرج منها نتائج لم يقدمها المستخدم مباشرة. فالشخص قد لا يصرح بحالته الصحية أو وضعه المالي أو ميوله، لكن النظام قد يستنتج ذلك من سلوكه الرقمي. وهنا لا يكون الخطر في البيانات المفردة فقط، بل في القدرة على ربطها وتحليلها لإنتاج معرفة دقيقة عن الفرد.

وتظهر الإشكالية الثانية في مسألة الموافقة. فكثير من المستخدمين يوافقون على شروط طويلة دون قراءتها، أو لا يفهمون فعلياً كيف ستستعمل بياناتهم. وفي ظل الذكاء الاصطناعي، تصبح الموافقة أكثر تعقيداً، لأن البيانات قد تستعمل لاحقاً في تدريب نموذج أو تحسين خوارزمية أو إنتاج خدمة جديدة لم تكن واضحة وقت الجمع. ولذلك فإن الموافقة الشكلية لا تكفي دائماً لحماية الخصوصية، بل يجب أن تكون مبنية على وضوح وشفافية وقدرة حقيقية على الاختيار.

أما الإشكالية الثالثة فتتعلق بالاحتفاظ بالبيانات. فكلما احتفظت المؤسسة ببيانات أكثر ولمدة أطول، زاد حجم الخطر في حالة الاختراق أو التسريب. كما أن الاحتفاظ ببيانات قديمة قد يؤدي إلى نتائج غير عادلة إذا استعملت لاحقاً في التقييم أو التصنيف. ومن هنا تظهر أهمية مبدأ تقليل البيانات، أي ألا تجمع المؤسسة إلا ما تحتاج إليه فعلاً، وألا تحتفظ به إلا للمدة الضرورية. وهذا المبدأ يصبح أكثر أهمية في أنظمة الذكاء الاصطناعي، لأن الجمع المستمر للبيانات قد يدفع بعض الجهات إلى جمع كل شيء دون تقدير كافٍ للمخاطر².

¹ بن برغوث لبلي، المرجع السابق، ص 454.

² بلشبير يعقوب، المرجع السابق، ص 262.

وتتعلق الإشكالية الرابعة بالبيانات الحساسة. فبعض المعطيات تحتاج إلى حماية أكبر، مثل البيانات الصحية، والبيانات البيومترية، والبيانات المالية، والبيانات المتعلقة بالأطفال. وإذا استعملت هذه البيانات في أنظمة ذكية دون ضمانات صارمة، فقد ينتج عنها ضرر كبير. فالنظام الذي يتعامل مع بصمة الوجه أو الصوت لا يتعامل مع كلمة مرور يمكن تغييرها بسهولة، بل مع جزء من هوية الإنسان. وإذا تسربت هذه المعطيات، فقد يكون الضرر طويل الأمد وصعب الإصلاح.

وتطرح الخصوصية كذلك إشكالا داخل المؤسسات. فالذكاء الاصطناعي قد يستعمل لمراقبة أداء العمال، وتحليل سلوكهم، وقياس إنتاجيتهم، وربما توقع احتمال مغادرتهم للعمل أو ارتكابهم خطأ. ورغم أن المؤسسة قد تبرر ذلك بالحماية أو تحسين الأداء، إلا أن التوسع في المراقبة قد يخلق بيئة عمل خانقة ويضعف الثقة بين العامل والمؤسسة. لذلك يجب أن يكون استعمال الذكاء الاصطناعي في المراقبة الداخلية محدودًا ومتناسبًا ومعلنًا، لا أن يتحول إلى عين رقمية لا تنام.¹

وفي المجال الأمني، تبدو الخصوصية أكثر تعقيدًا، لأن الحماية تتطلب أحيانًا مراقبة حركة الشبكة وسجلات الدخول وسلوك المستخدمين. غير أن هذه المراقبة يجب ألا تتحول إلى جمع مفرط لكل التفاصيل الشخصية دون ضوابط. فالأمن لا يبرر دائمًا انتهاك الخصوصية، بل يجب أن يقوم على التناسب: كل إجراء أمني يجب أن يكون ضروريًا ومناسبًا للخطر الذي يواجهه. وإذا أمكن تحقيق الحماية بوسيلة أقل مساسًا بالخصوصية، فإنها تكون أولى.

كما تظهر مشكلة الشفافية في حماية البيانات. فالمستخدم أو العامل أو الزبون يحتاج إلى معرفة نوع البيانات التي تجمع عنه، وسبب جمعها، ومدة الاحتفاظ بها، ومن يملك حق الوصول إليها، وهل تستعمل في تدريب أنظمة ذكية أم لا. وغياب هذه المعلومات يجعل العلاقة بين الفرد والمؤسسة غير متوازنة، لأن المؤسسة تعرف الكثير عن الفرد، بينما لا يعرف هو إلا القليل عن طريقة استعمال بياناته. وهذا الخلل في المعرفة قد يتحول إلى خلل في السلطة.

¹ ناصر مراد، المرجع السابق، ص 583.

ولا يمكن فصل الخصوصية عن الأمن المعلوماتي، لأن كل تساهل في حماية البيانات يفتح الباب أمام الاستغلال. فإذا تعرضت قاعدة بيانات تحتوي على معلومات شخصية للاختراق، فإن الضرر لا يتوقف عند المؤسسة، بل ينتقل إلى الأفراد الذين قد يواجهون الاحتيال أو الابتزاز أو انتحال الهوية. ومع الذكاء الاصطناعي، يمكن للمهاجم أن يستغل البيانات المسربة بطريقة أكثر خطورة، من خلال تحليلها وتصنيف الضحايا وترتيبهم حسب قابلية الاستهداف¹.

ومن هنا، فإن حماية الخصوصية في ظل الذكاء الاصطناعي تحتاج إلى مقارنة مزدوجة: تقنية وقانونية. فمن الناحية التقنية يجب اعتماد التشفير، وإخفاء الهوية، وتقليل البيانات، وتحديد الصلاحيات، ومراقبة الوصول. ومن الناحية القانونية يجب وضع قواعد واضحة حول جمع البيانات واستعمالها ونقلها والاحتفاظ بها، مع ضمان حق الأفراد في الإعلام والاعتراض والتصحيح والمحو عند الاقتضاء. أما من الناحية الأخلاقية، فيجب أن تقوم المعالجة على احترام الإنسان لا على تحويله إلى ملف قابل للاستغلال.

وبذلك يتضح أن الخصوصية ليست عقبة أمام الذكاء الاصطناعي، بل هي شرط لاستعماله بشكل مشروع وموثوق. فإذا شعر الأفراد أن أنظمتهم الذكية تراقبهم دون حدود، فسيفقدون الثقة في الخدمات الرقمية. أما إذا بنيت هذه الأنظمة على الشفافية والحماية والتناسب، فإنها تستطيع أن تحقق الفائدة دون سحق المساحة الشخصية للمستخدم. فالثقة الرقمية لا تولد من قوة الخوارزمية وحدها، بل من شعور الإنسان أن بياناته ليست غنيمة مفتوحة في سوق الخوارزميات.

المطلب الثالث: صعوبات التنظيم القانوني والأخلاقي

يمثل التنظيم القانوني والأخلاقي للذكاء الاصطناعي في مجال الأمن المعلوماتي تحديًا كبيرًا، لأن القانون بطبيعته يحتاج إلى وقت في الصياغة والمناقشة والتطبيق، بينما تتطور التقنية بسرعة كبيرة. وهذا الفرق في السرعة يجعل المشرع أحيانًا يلاحق واقعًا سبق أن تغير. فما إن توضع قاعدة لتنظيم خطر معين حتى تظهر صورة جديدة للخطر، سواء من خلال أداة توليد محتوى،

¹ بلشبير يعقوب، المرجع السابق، ص 266.

أو تقنية تزيف، أو طريقة هجوم، أو نموذج ذكي جديد. ولذلك فإن القانون في هذا المجال يحتاج إلى مرونة كافية تسمح له بمرافقة التطور دون أن يفقد وضوحه.

وتظهر صعوبة التنظيم أولاً في تحديد المسؤولية. فإذا تسبب نظام ذكاء اصطناعي في خطأ أمني، فمن المسؤول؟ هل هو مطور النظام، أم المؤسسة التي استعملته، أم الشخص الذي أدخل البيانات، أم المسؤول الذي اعتمد النتيجة، أم النظام نفسه؟ من الناحية القانونية لا يمكن تحميل الآلة مسؤولية مستقلة بالطريقة التي يتحملها الإنسان، لكن في الوقت نفسه لا يمكن تجاهل أن القرار قد يكون نتاج عملية آلية معقدة. لذلك تحتاج المسؤولية في هذا المجال إلى توزيع دقيق، يراعي دور كل طرف في التصميم والتشغيل والمراقبة.

وتزداد المشكلة عندما تكون أنظمة الذكاء الاصطناعي غامضة أو يصعب تفسيرها. فإذا لم يكن من الممكن معرفة سبب القرار، يصبح إثبات الخطأ أو التقصير أكثر صعوبة. فكيف يطعن الفرد في قرار خوارزمي لا يعرف أساسه؟ وكيف تثبت المؤسسة أنها لم تحمل إذا كان النظام نفسه لا يقدم تفسيراً واضحاً؟ ولهذا فإن الشفافية وقابلية التفسير ليستا مسألتين تقنيتين فقط، بل هما ضرورتان قانونيتان لحماية الحقوق وتحديد المسؤوليات.

وتظهر صعوبة أخرى في اختلاف القوانين بين الدول. فالبيانات قد تجمع في دولة، وتعالج في دولة ثانية، وتخزن في دولة ثالثة، ويستعملها نظام تابع لشركة عابرة للحدود¹. وهذا يجعل تطبيق القانون الوطني وحده غير كافٍ دائماً، لأن الخطر يتجاوز الحدود بسرعة، بينما إجراءات المتابعة القضائية والتعاون الدولي قد تكون بطيئة ومعقدة. ولذلك يحتاج الأمن المعلوماتي في ظل الذكاء الاصطناعي إلى تعاون دولي، خاصة في الجرائم المعلوماتية العابرة للحدود وحماية البيانات.

أما من الناحية الأخلاقية، فإن التحدي يتمثل في ضمان ألا تتحول الحماية الأمنية إلى ذريعة للمراقبة الواسعة. فبعض المؤسسات أو الدول قد تستعمل الذكاء الاصطناعي بحجة الأمن،

¹ بلشير يعقوب، المرجع السابق، ص 254.

بن أحمد فاطمة الزهراء وصحراوي بن شبيحة، المرجع السابق، ص 286.

لكنها توسع من مراقبة الأفراد وجمع بياناتهم وتحليل سلوكهم. وهنا يظهر السؤال الأخلاقي الصعب: كيف نحمي المجتمع من المخاطر الرقمية دون أن نحول كل فرد إلى موضوع مراقبة مستمرة؟ فالحرية لا تعيش جيدًا داخل قفص ذكي، حتى لو كان القفص مصنوعًا من خوارزميات براءة.

وتبرز الأخلاقيات أيضًا في مسألة العدالة وعدم التحيز. فإذا استعمل نظام ذكي لتقييم المخاطر الأمنية، فقد يصنف بعض الأشخاص أو المناطق أو السلوكيات على أنها أخطر من غيرها بناءً على بيانات منحازة. وهذا قد يؤدي إلى قرارات غير عادلة، مثل مراقبة فئة معينة أكثر من غيرها، أو حرمان بعض المستخدمين من خدمات، أو الاشتباه في أشخاص بسبب أنماط إحصائية لا تعبر عن ذنب حقيقي. لذلك يجب أن تخضع الأنظمة الذكية لاختبارات دورية تكشف الانحياز وتراجع النتائج.

كما أن تنظيم الذكاء الاصطناعي في الأمن المعلوماتي يحتاج إلى الموازنة بين الابتكار والحماية. فالتشدد القانوني المفرط قد يعيق تطوير حلول أمنية مهمة، بينما التساهل الكبير قد يفتح الباب للاستغلال والانتهاك. ولذلك ينبغي أن تقوم القواعد القانونية على مبدأ التناسب: كلما زاد خطر النظام الذكي، زادت درجة الرقابة المطلوبة. فالأنظمة التي تتعامل مع بيانات حساسة أو قرارات أمنية مؤثرة يجب أن تخضع لشروط أقوى من التطبيقات البسيطة محدودة الأثر.

وفي السياق الجزائري، تزداد الحاجة إلى تطوير الإطار القانوني والمؤسسي بما يساير التحول الرقمي والتهديدات الجديدة. فوجود استراتيجية وطنية لأمن الأنظمة المعلوماتية يمثل خطوة مهمة، لكنه يحتاج إلى دعم تشريعي وتنظيمي وتكويني مستمر حتى يتحول إلى ممارسة فعلية داخل الإدارات والمؤسسات. فالنصوص والسياسات لا تكفي إذا لم ترافقها كفاءات بشرية، ووسائل تقنية، وثقافة أمنية، وآليات تنفيذ ومراقبة.

كما أن التنظيم الأخلاقي لا يجب أن يبقى خطابًا عامًا، بل ينبغي أن يتحول إلى قواعد عملية داخل المؤسسات. ويظهر ذلك في وضع موثيق لاستعمال الذكاء الاصطناعي، وتحديد

البيانات المسموح بجمعها، ومنع استعمال الأدوات الذكية غير المرخصة في معالجة معلومات حساسة، وتدريب العمال على مخاطر إدخال بيانات المؤسسة في منصات خارجية، وتحديد المسؤول عن مراجعة مخرجات الأنظمة الذكية. فالأخلاق في المجال الرقمي لا تكون جميلة بمجرد كتابتها، بل تصبح نافعة عندما تدخل في الإجراءات اليومية.

ومن التحديات المهمة أيضاً صعوبة الإثبات في الجرائم المدعومة بالذكاء الاصطناعي. فالترزيف العميق قد يجعل الصوت أو الصورة غير كافيين كدليل مباشر، والرسائل المولدة آلياً قد تصعب نسبتها إلى شخص معين، والهجمات الآلية قد تمر عبر خوادم متعددة في دول مختلفة. وهذا يفرض تطوير الخبرة الرقمية وأدوات التحقيق، حتى يستطيع القضاء والجهات المختصة التعامل مع الأدلة الجديدة دون تسرع أو عجز¹.

وفي النهاية، يمكن القول إن التنظيم القانوني والأخلاقي للذكاء الاصطناعي في الأمن المعلوماتي ليس مسألة تكميلية، بل هو جزء من الحماية نفسها. فالأنظمة الذكية مهما بلغت قوتها تحتاج إلى حدود، والمسؤوليات تحتاج إلى تحديد، والبيانات تحتاج إلى ضمانات، والأفراد يحتاجون إلى حقوق واضحة. وإذا غاب التنظيم، قد تتحول التقنية إلى قوة منفelte؛ وإذا حضر التنظيم بوعي ومرونة، أمكن للذكاء الاصطناعي أن يكون حليفاً للأمن المعلوماتي بدل أن يصبح خصماً متخفياً في ثوب الحداثة.

¹ صدراتي محمد، نحو إطار قانوني للذكاء الاصطناعي، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 10 العدد 1، جامعة الاغواط، 2026،

ص1893. <https://asjp.cerist.dz/en/article/290152>

الخاتمة

تكشف مخرجات هذه الدراسة بوضوح أن إشكالية الأمن المعلوماتي في عصر الذكاء الاصطناعي قد تجاوزت بكثير حدودها التقنية الضيقة، لتتبلور كقضية استراتيجية مركبة تتقاطع فيها ديناميكيات متعددة، تتراوح بين البنى التحتية الرقمية المتطورة، والأطر القانونية المتحولة، والآليات التنظيمية المستجدة، والاعتبارات الأخلاقية المؤثرة في تشكيل الممارسات المؤسسية. وفي ظل التحول الرقمي المتسارع الذي يشهده العالم المعاصر، غدت البيانات العنصر الحيوي الذي تُغذى به الأنظمة الذكية عملياتها، مما يحول حماية المعلومات من مجرد إجراء وقائي تكميلي إلى ركيزة أساسية لا غنى عنها لضمان استدامة الخدمات الرقمية، وتعزيز الثقة المؤسسية وثقة العملاء، وصون الحقوق الأساسية للأفراد والكيانات على حد سواء.

وقد أسفرت التحليلات المعتمدة في هذا البحث عن تجلية الطبيعة الثنائية والمزدوجة التي يتسم بها الذكاء الاصطناعي في الحقل الأمني؛ فمن ناحية، يتجلى كآلية دفاعية متقدمة قادرة على إحداث نقلة نوعية في منظومات الحماية، من خلال تمكينها من الرصد الاستباقي للأنماط التهديدية، وتحليل السلوكيات غير الاعتيادية بدقة عالية، والاستجابة التلقائية والسريعة للحوادث الأمنية، والتنبيه بالمخاطر المحتملة قبل تجسدها الفعلي على أرض الواقع. ومن ناحية أخرى، يُبرز البحث كيف يمكن توظيف هذه القدرات ذاتها كأداة هجومية مُضاعفة للخطر عندما تقع في أيدي الجهات الخبيثة، حيث تُسهم في أتمتة عمليات الاختراق، وصياغة هجمات التصيد الاحتيالي ذات الطابع الشخصي والمقنع، واستغلال تقنيات التزييف العميق لخلق سيناريوهات تضليلية معقدة، فضلاً عن استهداف نماذج التعلم الآلي ذاتها عبر أساليب متطورة، مثل تصميم البيانات أو التلاعب بمعاملات الخوارزميات.

كما بيّنت الدراسة أن المبادئ التأسيسية للأمن المعلوماتي، والمتتمثلة في ثلوث السرية والسلامة والإتاحة، قد اكتسبت أبعاداً هيكلية وتشغيلية أكثر تعقيداً في البيئات

المعتمدة على الذكاء الاصطناعي. ذلك أن البيانات لم تعد تُعامل ككيانات ساكنة أو أرشيفية فحسب، بل تحولت إلى مورد تحليلي ديناميكي يخضع لعمليات معالجة متواصلة، واستنتاج آلي، وتغذية راجعة تعيد تشكيل سلوك النماذج الذكية باستمرار. وعليه، فإن أي اختراق أو خلل في منظومة الحماية لم يعد يقتصر أثره المباشر على تسريب المعلومات أو تعطيل الخدمات، بل قد يمتد إلى تشويه مخرجات التحليلات، وتضليل عمليات صنع القرار على المستويين الاستراتيجي والتشغيلي، أو إحداث انتهاكات منهجية وعميقة للخصوصية تتجاوز الحدود التقليدية للتدخل في الشؤون الفردية.

واستنادًا إلى هذه المعطيات المتراكمة، يتضح جليًا أن التصدي الفعال لتحديات الأمن المعلوماتي في ظل تسارع وتيرة الذكاء الاصطناعي لا يمكن أن يركز على الحلول التقنية بمعزل عن غيرها، بل يستلزم تبني رؤية تكاملية وشاملة تجمع بين تطوير البنى التحتية الدفاعية القائمة على الخوارزميات المتقدمة، وبناء القدرات البشرية من خلال برامج التوعية والتأهيل المستمر، وتحديث الأطر التشريعية والتنظيمية لمواكبة المستجدات الرقمية، وإرساء معايير أخلاقية رصينة تضبط استخدام الأنظمة الذكية وتوجهها نحو الصالح العام. فمهما بلغت التقنية من مستويات التعقيد والكفاءة، فإنها تبقى قاصرة عن ضمان الأمن الشامل ما لم تخضع لإشراف بشري واعٍ ورقابة مؤسسية مستدامة تحول دون انحرافها من أداة حماية إلى مصدر تهديد غير متوقع.

وبناءً على ما تقدم، يمكن التأكيد على أن الذكاء الاصطناعي لا يجسد تهديدًا وجوديًا مطلقًا، ولا يُقدّم في المقابل حلًا سحريًا أو نهائيًا لإشكاليات الأمن الرقمي، بل يظل أداة محايدة نسبيًا يتشكل أثرها الفعلي تبعًا للإطار الحوكمي، والضوابط التشغيلية، والأخلاقيات المرافقة لتوظيفه. فعندما يُدمج ضمن منظومة أمنية واعية تقوم على مبادئ الشفافية، والمساءلة، وحماية الخصوصية، وتصميم الأنظمة بأمان منذ مرحلة التأسيس، فإنه يُسهم بشكل فعال في رفع مناعة البنى الرقمية وتعزيز القدرة على التصدي للتهديدات المعقدة والمستجدة. وفي المقابل، فإن تبني هذه التقنيات دون ضوابط رقابية

أو معايير تشغيلية واضحة قد يفتح مسارات جديدة للاختراق المنهجي، والمراقبة غير المشروعة، وتآكل الخصوصية الفردية والمؤسسية على نطاق واسع.

وانطلاقاً من هذه الاستنتاجات، تطرح الدراسة مجموعة من التوصيات العملية والسياسية التي من شأنها ترسيخ بيئة أمنية متوازنة وقادرة على الصمود في وجه التحولات التكنولوجية المتسارعة، وأبرزها: تعزيز الوعي الأمني الرقمي على المستويين المؤسسي والفردى، وتطوير الكفاءات البشرية المتخصصة في مجال تقاطع الأمن المعلوماتي وتقنيات الذكاء الاصطناعي، واعتماد سياسات حوكمة بيانات شاملة تضمن الجودة والشفافية والمساءلة في دورة حياة البيانات، وتحديث النصوص التشريعية الوطنية والدولية بما يتوافق مع طبيعة الجرائم الرقمية الناشئة وآليات المساءلة المرتبطة بالأنظمة الذاتية. كما تؤكد الدراسة ضرورة تشجيع الاستخدام المسؤول للذكاء الاصطناعي في التطبيقات الدفاعية والأمنية، مع الإبقاء على آليات الرقابة البشرية والتدقيق الدوري بوصفها ضماناً أساسية. وأخيراً، تبرز الحاجة الملحة إلى بناء شبكات تعاون مؤسسي متعددة القطاعات تربط بين الجهات التقنية والقانونية والإدارية والأكاديمية، نظراً لأن الأمن المعلوماتي في عصر الذكاء الاصطناعي لم يعد مسؤولية جهة منعزلة، بل أصبح مسؤولية جماعية تتطلب يقظة مؤسسية مستمرة، ومرونة تشغيلية عالية، وتوازناً استراتيجياً دائماً بين متطلبات الابتكار التكنولوجي ومعايير الحماية والأمن الرقمي.

قائمة المصادر والمراجع

أولاً: الكتب العربية

- نزمين مجدي، الذكاء الاصطناعي وتعلم الآلة، سلسلة كتيبات تعريفية، العدد 03، صندوق النقد العربي، 2020.

- مريم قيس علوي، الذكاء الاصطناعي: تطوره، تطبيقاته وتحدياته، مجلة لباب للدراسات الاستراتيجية، مركز الجزيرة للدراسات، 2023.

- عبد الفتاح بيومي حجازي، الأمن السيبراني وحماية المعلومات، دار الفكر الجامعي، مصر.

- محمد الهادي حمودة، أمن المعلومات والشبكات، دار الجامعة الجديدة.

- علي محمد السلمي، التحول الرقمي والأمن السيبراني، دار التعليم الجامعي.

ثانياً: المقالات العلمية

- دحماني محمد، “الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني”، مجلة الفكر القانوني والسياسي، المجلد 7، العدد 2، 2023.

- سعيدي خليل، وابن مهدي مرزوق، “الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبراني”، مجلة السلام للعلوم الإنسانية والاجتماعية، المجلد 6، العدد 1، 2022.

- جودي خرفية، “هندسة الأمن السيبراني في عصر الذكاء الاصطناعي: قراءة في أدوار واستراتيجيات اليقظة الحوازمية”، المجلة الجزائرية للأمن الإنساني، المجلد 11، العدد 1، 2025.

- زمورة جمال، وابن عيسى ليلي، “أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمة العمومية في الجزائر”، مجلة البحوث الاقتصادية المتقدمة، المجلد 07، العدد 02، 2022.

- ناصر مراد، “دور الأمن السيبراني في حماية نظم المعلومات: تجربة الجزائر”، مجلة اقتصاد المال والأعمال، المجلد 10، العدد 02، 2025.

- بن برغوث ليلي، “الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر”، المجلة الدولية للاتصال الاجتماعي، المجلد 10، العدد 1، 2023.

- أحمد شوقي، “الذكاء الاصطناعي ومستقبل الأمن المعلوماتي”، مجلة الدراسات القانونية المعاصرة، 2024.
- كريم بوعلام، “الهجمات السيبرانية المدعومة بالذكاء الاصطناعي”، مجلة العلوم الأمنية، 2023.
- عبد القادر بوحفص، “التحديات القانونية للذكاء الاصطناعي”، مجلة القانون والتكنولوجيا، 2024.
- سارة بن عيسى، “حماية البيانات الشخصية في البيئة الرقمية”، مجلة الحقوق والعلوم السياسية، 2022.

ثالثًا: التقارير والدراسات الدولية

- OECD Artificial Intelligence Papers, *Explanatory Memorandum on the Updated OECD Definition of an AI System*, No. 8, 2024.
- Jamie Berryhill et al., *Hello, World: Artificial Intelligence and its Use in the Public Sector*, OECD Working Papers on Public Governance, No. 36, 2019.
- NIST, *The NIST Cybersecurity Framework CSF 2.0*, 2024.
- UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 2021.
- ENISA, *Artificial Intelligence Cybersecurity Challenges*, 2023.
- IBM Security, *Cost of a Data Breach Report*, 2024.
- Microsoft Security, *Cyber Signals Report*, 2024.
- World Economic Forum, *Global Cybersecurity Outlook*, 2025.

رابعًا: النصوص القانونية والاستراتيجيات الرسمية

- وزارة الدفاع الوطني الجزائرية، الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029، 2025.

- القانون الجزائري المتعلق بحماية المعطيات ذات الطابع الشخصي.
- القوانين المتعلقة بمكافحة الجرائم الإلكترونية في الجزائر.
- التوجيهات الأوروبية المتعلقة بحوكمة الذكاء الاصطناعي وحماية البيانات.

خامسًا: المواقع الإلكترونية

- موقع منظمة التعاون الاقتصادي والتنمية: <https://www.oecd.org> OECD
- موقع المعهد الوطني الأمريكي للمعايير والتكنولوجيا: <https://www.nist.gov> NIST
- موقع اليونسكو: <https://www.unesco.org> UNESCO
- منصة المجلات العلمية الجزائرية: <https://www.asjp.cerist.dz> ASJP
- Google Scholar: <https://scholar.google.com>
- موقع وزارة الدفاع الوطني الجزائرية: <https://www.mdn.dz>
- موقع ENISA: <https://www.enisa.europa.eu>
- موقع IBM Security: <https://www.ibm.com/security>
- موقع Microsoft Security: <https://www.microsoft.com/security>

سادسًا: الرسائل الجامعية

- بن يوسف أحمد، “دور الذكاء الاصطناعي في تعزيز الأمن السيبراني”، رسالة ماستر، جامعة الجزائر، 2024.
- خديجة بوعلام، “الأمن المعلوماتي في ظل التحول الرقمي”، مذكرة ماستر، جامعة وهران، 2023.
- يوسف مرابط، “التحديات القانونية للذكاء الاصطناعي”، أطروحة دكتوراه، جامعة قسنطينة، 2025.

سابعًا: المراجع الأجنبية

- Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach*, Pearson Education.

- Kevin Mitnick, *The Art of Invisibility*, Little, Brown and Company.
 - William Stallings, *Network Security Essentials*, Pearson.
- Bruce Schneier, *Data and Goliath*, W.W. Norton & Company.
- Ian Goodfellow, Yoshua Bengio & Aaron Courville, *Deep Learning*, MIT Press.
- Thomas H. Davenport, *Artificial Intelligence for the Real World*, Harvard Business Review.
 - Nick Bostrom, *Superintelligence*, Oxford University Press.
 - Kai-Fu Lee, *AI Superpowers*, Houghton Mifflin Harcourt.
- Tarleton Gillespie, *Custodians of the Internet*, Yale University Press.
 - Luciano Floridi, *The Ethics of Artificial Intelligence*, Oxford University Press.

المختصر	المعنى باللغة العربية	المعنى باللغة الأجنبية
AI	الذكاء الاصطناعي	Artificial Intelligence
ML	تعلم الآلة	Machine Learning
DL	التعلم العميق	Deep Learning
NLP	معالجة اللغة الطبيعية	Natural Language Processing
CS	الأمن السيبراني	Cyber Security
IS	أمن المعلومات	Information Security
IT	تكنولوجيا المعلومات	Information Technology
NIST	المعهد الوطني للمعايير والتكنولوجيا	National Institute of Standards and Technology
OECD	منظمة التعاون الاقتصادي والتنمية	Organisation for Economic Co-operation and Development
UNESCO	منظمة الأمم المتحدة للتربية والعلم والثقافة	United Nations Educational, Scientific and Cultural Organization
VPN	الشبكة الافتراضية الخاصة	Virtual Private Network
IDS	نظام كشف التسلل	Intrusion Detection System
IPS	نظام منع التسلل	Intrusion Prevention System
IoT	إنترنت الأشياء	Internet of Things
Big Data	البيانات الضخمة	Big Data
Firewall	جدار الحماية	Firewall
Malware	البرمجيات الخبيثة	Malware
Phishing	التصيد الاحتيالي	Phishing
Deepfake	التزييف العميق	Deepfake

قائمة المختصرات

الفهرس

5	المقدمة.....
10	الفصل الأول: ماهية الذكاء الاصطناعي وتطبيقاته.....
10	المبحث الأول: الإطار المفاهيمي للذكاء الاصطناعي.....
10	المطلب الأول: تعريف الذكاء الاصطناعي ومراحل تطوره التاريخي.....
13	المطلب الثاني: الخصائص التقنية للأنظمة الذكية.....
15	المطلب الثالث: التمييز بين الذكاء الاصطناعي والمصطلحات التقنية القريبة.....
18	المبحث الثاني: تصنيفات الذكاء الاصطناعي ومجالات تطبيقاته.....
18	المطلب الأول: مستويات الذكاء الاصطناعي: الضعيف، القوي، الفائق.....
21	المطلب الثاني: المجالات التطبيقية للذكاء الاصطناعي.....
24	المطلب الثالث: التحديات والمخاطر المصاحبة لانتشار تقنيات الذكاء الاصطناعي.....
30	الفصل الثاني: الأمن المعلوماتي في البيئة الرقمية وعلاقته بالذكاء الاصطناعي.....
31	المبحث الأول: مفهوم الأمن المعلوماتي وأبعاده.....
31	المطلب الأول: تعريف الأمن المعلوماتي وتمييزه عن الأمن السيبراني.....
33	المطلب الثاني: عناصر الأمن المعلوماتي: السرية، السلامة، الإتاحة.....
36	المطلب الثالث: أهمية الأمن المعلوماتي في المؤسسات والأفراد.....
40	المبحث الثاني: آليات الذكاء الاصطناعي في تعزيز الأمن المعلوماتي.....
40	المطلب الأول: الكشف الذكي عن التهديدات والهجمات.....
43	المطلب الثاني: الاستجابة الآلية للحوادث الأمنية.....
46	المطلب الثالث: تحليل البيانات والتنبؤ بالمخاطر الأمنية.....
50	المبحث الثالث: تحديات الأمن المعلوماتي في ظل الذكاء الاصطناعي.....
50	المطلب الأول: مخاطر الهجمات المدعومة بالذكاء الاصطناعي.....
53	المطلب الثاني: إشكالات الخصوصية وحماية البيانات.....
56	المطلب الثالث: صعوبات التنظيم القانوني والأخلاقي.....
60	الخاتمة.....
63	قائمة المصادر والمراجع.....
67	قائمة المختصرات.....
68	الفهرس.....

