المجلة المغربية للدراسات القانونية والاقتصادية
ISSN(P) : 1142-2489
V2, Numéro 25, MARS 2026
المجلد 2، العدد 25، مارس 2026
ISSN(E) : 3085-4555
Revue Marocaine des Eudes Juridiques et Economiques

الذكاء الاصطناعي ركيزة استراتيجية لتعزيز الأمن السيبراني بالمغرب

Artificial Intelligence as a Strategic Pillar for Enhancing Cybersecurity in Morocco

موهيب عبد العزيز Abdelaziz MOUHIB

دكتور في الحقوق

أستاذ زائر بكلية العلوم القانونية

والسياسية الحسن الأول سطات

ملخص

إن الموازنة بين أهمية الاستفادة من الخدمات المتنوعة للذكاء الاصطناعي في توازن تام مع ضرورة خلق بيئة رقمية تتمتع بالأمن السيبراني ومدى قدرة التطور الرقمي على تشكيل رافعة استراتيجية لتعزيز المنظومة الأمنية في المملكة المغربية، خاصة في ظل سعيها لتحقيق أهداف برنامج "المغرب الرقمي 2025" يتطلب من المشرع بدل المزيد من المجهودات لمواكبة التطور التقني.

وتعد العلاقة بين الذكاء الاصطناعي والأمن السيبراني علاقة جدلية، فمن ناحية يُمثل الأول حليفًا استراتيجيًا قويًا من خلال إحداثه تحولاً جذرياً في آليات الدفاع، فهو يمكن أنظمة الأمن من الانتقال من الكشف التفاعلي القائم على التوقيعات إلى التحليل السياقي والاستباقي، باستخدام تقنيات مثل التعلم الآلي والتعلم العميق لاكتشاف الشذوذ والتهديدات الناشئة غير المعروفة سلفًا، كما أن الأتمتة الذكية للاستجابة للحوادث تعمل على تسريع احتواء الهجمات وتقليل الأضرار بشكل غير مسبوق.

ومن ناحية أخرى، يحمل الذكاء الاصطناعي في طياته بُعدًا تهديديًا وجوديًا، حيث يمكن للجهات الخبيرة تسخير نفس التقنيات لتطوير هجمات أكثر ذكاءً وتعقيدًا وتكيفًا، مثل البرمجيات الخبيثة متعددة الأشكال، وهجمات التصيد عالية التصديق باستخدام النماذج اللغوية، والتزييف العميق (Deepfakes) لأغراض التضليل والاستغلال.

من هذا المنطلق سنحاول دراسة الإطارين التشريعي والمؤسسي كأسس متينة[1]، لكنها تواجه تحديات ملازمة لتقنية الذكاء الاصطناعي نفسها، أبرز هذه التحديات تتمثل في الإشكاليات القانونية والأخلاقية، مثل إشكالية الخصوصية في ظل الحاجة الهائلة للبيانات، وتحيز الخوارزميات الذي قد يؤدي إلى ممارسات تمييزية، ومشكلة "الصندوق الأسود" التي تُضعف الشفافية وتُعقّد مسألة المساءلة القانونية عن القرارات والنتائج الخاطئة.

إن تعظيم الاستفادة من الذكاء الاصطناعي كرافعة للأمن السيبراني في المغرب يتطلب تبني نهج متكامل، لا يكفي تطوير البنى التقنية فقط، بل يجب مواكبته بتطوير مستمر للإطار التشريعي لمعالجة الثغرات القانونية الجديدة، وبناء القدرات البشرية المتخصصة، ووضع سياسات واضحة لأخلاقيات الذكاء الاصطناعي.

[1] نتحدث هنا عن القانونين: 05-20 و 08-09 وهيئات مثل CNDP وANRT.

الكلمات المفاتيح: الذكاء الاصطناعي، التحول الرقمي، الأتمتة الذكية، التهديدات السيبرانية، الاستباقية، رافعة استراتيجية.

Summary

Balancing the importance of leveraging diverse artificial intelligence services with the necessity of creating a secure digital environment, and harnessing technological development as a strategic lever to enhance the cybersecurity system in the Kingdom of Morocco—especially in light of its efforts to achieve the objectives of the "Digital Morocco 2025" program—requires Moroccan legislators to exert further efforts to keep pace with technological advancements.

The relationship between artificial intelligence and cybersecurity is dialectical. On one hand, AI represents a powerful strategic ally by fundamentally transforming defense mechanisms. It enables security systems to shift from reactive, signature-based detection to contextual and proactive analysis, using techniques such as machine learning and deep learning to detect anomalies and emerging, previously unknown threats. Moreover, the intelligent automation of incident response accelerates the containment of attacks and reduces damage in an unprecedented manner.

On the other hand, AI carries an existential threat dimension, as malicious actors can harness the same technologies to develop more intelligent, complex, and adaptive attacks. Examples include polymorphic malware, highly convincing phishing attacks using language models, Deepfakes for disinformation purposes, and the automation of reconnaissance and exploitation processes.

In the Moroccan context, we will attempt to examine the legislative and institutional frameworks (such as Laws 05-20 and 08-09, and bodies like the CNDP and ANRT) as solid foundations. However, these frameworks face challenges inherent to AI technology itself. The most prominent challenges include legal and ethical issues, such as privacy concerns amid the immense need

for data, algorithmic bias that may lead to discriminatory practices, and the "black box" problem, which undermines transparency and complicates legal accountability for erroneous decisions and outcomes.

Maximizing the benefits of AI as a lever for cybersecurity in Morocco requires adopting an integrated approach. It is not enough to develop technical infrastructures alone; this must be accompanied by continuous development of the legislative framework to address new legal gaps, building specialized human capacities, and establishing clear policies for AI ethics.

Keywords: Artificial Intelligence, Digital Transformation, Intelligent Automation, Cyber Threats, Proactivity, Strategic Lever.

مقدمة

يشهد العصر الرقمي الحالي تحولاً جوهرياً في طبيعة التهديدات الأمنية والآليات الدفاعية في الفضاء الإلكتروني، حيث أضحى الذكاء الاصطناعي بمثابة محور رئيسي في معادلة الأمن السيبراني المعاصرة. فمن ناحية، يمثل الذكاء الاصطناعي دعامة أساسية في بناء أنظمة دفاعية ذكية وقادرة على التكيف، تمكن من اكتشاف التهديدات الناشئة والاستجابة لها بسرعة تفوق القدرات البشرية. ومن ناحية أخرى، يخلق هذا الذكاء نفسه أبعاداً جديدة للتهديد، حيث يمكن للمهاجمين تسخير تقنياته لتطوير هجمات أكثر تعقيداً وتخفياً، بل وأتمتة عمليات الاختراق. وبالتالي، فإن العلاقة بين الذكاء الاصطناعي والأمن السيبراني هي علاقة ثنائية الوجه، تجمع بين عنصري الدفاع والهجوم في آن واحد. تهدف هذه الدراسة إلى تحليل طبيعة هذه العلاقة المعقدة، واستكشاف كيفية استغلال تقنيات الذكاء الاصطناعي في تعزيز الحماية الرقمية، إلى جانب تسليط الضوء على المخاطر والثغرات الأمنية الجديدة التي تثيرها، مما يضعنا أمام مشهد متطور تتقاطع فيه الفرص مع التحديات في معركة حماية الفضاءات الرقمية.

ويشكل التحول الرقمي أحد أبرز ملامح العصر الراهن، حيث أصبح الفضاء السيبراني ساحة حيوية للتفاعلات الاقتصادية والاجتماعية والأمنية. وفي خضم هذا التحول، برزت تهديدات إلكترونية متطورة تفرض على الدول تحديات غير مسبوقة في حماية سيادتها الرقمية ومصالحها الوطنية. وتأتي المملكة المغربية في صدارة الدول الساعية لمواكبة هذه المتغيرات من خلال تبني استراتيجية طموحة للتحول الرقمي تجسدت في برنامج "المغرب الرقمي 2025"، مما يجعل موضوع تأمين الفضاء السيبراني الوطني أولوية استراتيجية.

في هذا السياق، يبرز الذكاء الاصطناعي كتقنية محورية ذات تأثير مزدوج؛ فهو من ناحية يقدم أدوات متطورة لتعزيز القدرات الدفاعية والاستباقية في مواجهة الهجمات الإلكترونية، ومن ناحية أخرى يطرح إشكاليات قانونية وأخلاقية معقدة تتعلق بمساءلة الأنظمة الذكية والتحيز الخوارزمي واختراق الخصوصية.

من هنا، تبلورت إشكالية هذه الموضوع حول السؤال المحوري التالي: إلى أي حد يمكن للذكاء الاصطناعي أن يشكل رافعة استراتيجية لتعزيز منظومة الأمن السيبراني في المملكة المغربية؟

وتنبثق عن هذه الإشكالية الأسئلة الفرعية التالية:

- ✓ **ما هو الدور التحويلي الذي يلعبه الذكاء الاصطناعي في تطوير آليات الكشف عن التهديدات السيبرانية والاستجابة لها؟**
- ✓ **ما هي أبرز التحديات التي تواجه المنظومة الأمنية المغربية في مجال مواجهة التهديدات السيبرانية المعاصرة؟**
- ✓ **ما مدى ملاءمة الإطار القانوني والمؤسسي المغربي لاستيعاب تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني؟**

إن تحليل العلاقة التبادلية بين الذكاء الاصطناعي والأمن السيبراني، وتقييم مستوى جاهزية المنظومة الأمنية المغربية لتبني هذه التقنية، ووضع رؤية استشرافية لتطويرها، واعتمدت الدراسة المنهج الوصفي التحليلي لدراسة المفاهيم والإطار النظري، إلى جانب منهج دراسة الحالة لتطبيق هذه المفاهيم على السياق المغربي.

إن أهمية الذكاء الاصطناعي كركيزة استراتيجية لتعزيز الأمن السيبراني في طابعها البيني الذي يدمج بين التقنية والقانون، ومساهمتها في إثراء النقاش الأكاديمي حول آليات تأمين الفضاء الرقمي المغربي، وتقديم رؤية عملية لصانعي القرار.

ولمعالجة الإشكالية المحورية أعلاه سوف نقسم الموضوع إلى ثلاثة محاور، يتناول الأول الإطار النظري والمفاهيمي، ويحلل الثاني العلاقة الجدلية بين الذكاء الاصطناعي والتحديات الأمنية، بينما يركز الثالث على التشخيص التطبيقي للتجربة المغربية، وذلك وفق الشكل التالي:

المحور الأول: التأصيل النظري والمفاهيمي

يشهد العصر الرقمي تحولات جذرية في بنية المجتمعات والاقتصادات، مما جعل الفضاء السيبراني بيئة حيوية للتفاعلات البشرية والاقتصادية، إلا أن هذه البيئة تنطوي على مجموعة من التهديدات المتطورة التي تتطلب بدورها آليات دفاعية متقدمة، وفي هذا السياق، يبرز الذكاء الاصطناعي كتقنية ثورية قادرة على إعادة تعريف معايير الأمن السيبراني، من خلال تقديم حلول ذكية وقادرة على التكيف مع التعقيدات المتزايدة للهجمات الإلكترونية.

المطلب الأول: ماهية الذكاء الاصطناعي وأبعاده

مما لا يشك فيه أن الذكاء الاصطناعي (Artificial Intelligence) أضحى يشكل العمود الفقري والناظم التكنولوجي للثورة الصناعية الرابعة، التي تُعيد بدورها صياغة البنى الاقتصادية والاجتماعية والثقافية على مستوى العالم، ذلك أن الأمر ولا يقتصر هذا الحقل على كونه مجرد أداة تكنولوجية عابرة، بل هو حقل معرفي متعدد التخصصات (Interdisciplinary Field) يتقاطع فيه علم الحاسوب مع الفلسفة وعلم النفس العصبي والرياضيات واللغويات، ساعيًا إلى فهم الذكاء بماهيته وإمكانية محاكاته آليًا ويمكن تعريفه إجرائيًا بأنه: "فرع متخصص من فروع علم الحاسوب، يهتم بتصميم وتطوير الأنظمة الحاسوبية الذكية القادرة على أداء مهام كانت حكرًا على الذكاء البشري، كإدراك المحيط، والتعلم من التجربة، والاستدلال المنطقي، وفهم اللغات الطبيعية، وحل المشكلات المعقدة في ظل شروط عدم اليقين."[1]

الفرع الأول: التطور التاريخي والمراحل الرئيسية

مر تطور الذكاء الاصطناعي بمراحل تاريخية محورية بدءاً من الأفكار الأولى للعالم لان تورينج(Alan Turing) في الخمسينيات، مروراً بفترات المد والجزر التي عرفها المجال، ووصولاً إلى الطفرة الحالية المدعومة بتقنيات التعلم العميق والبيانات الضخمة، والتي أفرزت تطبيقات ملموسة في مجالات متعددة.

[1] – ستوارت راسل وبطر نورفيغ، الذكاء الاصطناعي: مقاربة حديثة، ترجمة: أحمد عبد الرحمن (الرياض: دار الحاسب النقي، 2020)، ص 45.

أولا: الأبعاد النظرية والتاريخية للذكاء الاصطناعي

تنبني فلسفة الذكاء الاصطناعي على سؤال جوهري طرحه "آلان تورينج" (Alan Turing) في مقاله seminal عام 1950: "هل يمكن للآلات أن تفكر؟"[1] والذي قاد إلى ما عُرف لاحقًا باختبار تورينج (Turing Test)، الذي يقيس قدرة الآلة على محاكاة الذكاء البشري إلى درجة لا يستطيع معها الإنسان التمييز بينها وبين بشري آخر في حوار نصي، وقد شهد المجمع الأكاديمي أولى ولاداته الرسمية في ورشة عمل "دارتموث" (Dartmouth Workshop) عام 1956، حيث صُكّ مصطلح "الذكاء الاصطناعي" رسميًا على يد جون مكارثي (John McCarthy)، لتبدأ معه حقبة من التفاؤل العلمي والاستكشاف النظري العميق.[2]

على المستوى النظري، يمكن تمييز مدرستين رئيستين داخل حقل الذكاء الاصطناعي:

1-الذكاء الاصطناعي الضيق (Weak AI أو Narrow AI): وهو الذكاء المصمم لأداء مهمة محددة أو نطاق ضيق من المهام، هذا النوع هو السائد حاليًا في جميع التطبيقات العملية، مثل أنظمة التوصية في "نتفليكس"، ومساعدات الصوتية مثل "سيري" و"أليكسا"، وأنظمة التعرف على الوجه، فهو يظهر ذكاءً في مجاله دون امتلاك وعي أو إدراك حقيقي.[3]

2-الذكاء الاصطناعي العام (Strong AI أو AGI- Artificial General Intelligence):

وهو الهدف النظري الطموح الذي يتصور أنظمة تمتلك ذكاءً مساوٍ للذكاء البشري في جميع الجوانب المعرفية، وقادرة على فهم العالم والتعلم وتطبيق المعرفة لحل أي مشكلة تواجهها، مع امتلاك وعي وإدراك ذاتي، وهذا النوع لا يزال حبيس المختبرات والأبحاث النظرية والفلسفية[4].

ثانيًا: المحاور التقنية الأساسية للذكاء الاصطناعي

يتفرع الذكاء الاصطناعي المعاصر إلى عدة تقنيات فرعية تشكل مجتمعةً أدواته التنفيذية وأبرزها:

1-تعلم الآلة (Machine Learning): وهو حجر الأساس الذي مكّن من القفزة النوعية الأخيرة في المجال، ويعتمد على فكرة تمكين الحواسيب من "التعلم" تلقائيًا من البيانات دون أن تكون مبرمجة بشكل صريح لكل مهمة من خلال الخوارزميات الإحصائية، تكتشف الأنظمة الأنماط في البيانات وتصنع تنبؤات أو قرارات بناءً عليها.[5]

2-التعلم العميق (Deep Learning): يُعد جزءًا متخصصًا ومتقدمًا من تعلم الآلة، يستخدم شبكات عصبية اصطناعية (Artificial Neural Networks) ذات طبقات متعددة (ومن هنا جاءت تسميته "عميق"). هذه الشبكات

[1] - Alan Turing, "Computing Machinery and Intelligence،" Mind, vol. 59, no. 236 (1950): pp. 433-460.

[2] - جون مكارثي وآخرون، "مقترح لبحوث الذكاء الاصطناعي في مؤتمر دارتموث"، 1955. (وثيقة تاريخية).

[3] - نيك بوستروم، الذكاء الخارق: مسارات، مخاطر، استراتيجيات، ترجمة: مُحَمَّد فتحي خضر (القاهرة: دار الكتب العلمية، 2018)، ص 78.

[4] - المرجع نفسه، ص 102.

[5] - بيتر هارينغتون، تعلم الآلة في العمل، ترجمة: سامي الثقفي (الدمام: مكتبة العبيكان، 2019)، ص 31.

تحاكي – بشكل مبسط جدًا – عمل الدماغ البشري، مما يمكنها من معالجة بيانات هائلة ومعقدة كالصور، والصوت، والنصوص، بفعالية غير مسبوقة.[1]

3–معالجة اللغة الطبيعية (Natural Language Processing –NLP): وهو الحقل المسؤول عن تمكين الحواسيب من فهم وتفسير وتوليد، والتفاعل مع اللغة البشرية (كالعربية والإنجليزية) بطريقة ذات معنى ومفيدة. تطبيقاته تشمل الترجمة الآلية، والتحليل الشعوري (Sentiment Analysis)، والمساعدات الذكية المتطورة.[2]

ثالثًا: الأبعاد التطبيقية والتأثير المجتمعي

تتسع دائرة تطبيقات الذكاء الاصطناعي لتمس كل قطاع تقريبًا، مما يجعله تكنولوجيا ذات أبعاد استراتيجية:

1–في القطاع الصحي: يساهم في التشخيص المبكر للأمراض (كسرطانات الجلد عبر تحليل الصور)، وتسريع اكتشاف الأدوية، والجراحة الروبوتية الدقيقة.

2–في القطاع المالي: يُستخدم في كشف الاحتيال، وتقييم المخاطر الائتمانية، والتداول الآلي.

3–في قطاع النقل: يشكل الأساس التقني للمركبات ذاتية القيادة وتحسين أنظمة إدارة المرور.

4–في مجال التعليم: يمكنه توفير تعليم مخصص (Personalized Learning) يتكيف مع سرعة واحتياجات كل طالب.

غير أن هذه الأبعاد الإيجابية تقابلها تحديات أخلاقية ومجتمعية جسيمة، تفرض نفسها على صانعي السياسات والباحثين، مثل: تحيز الخوارزميات (Algorithmic Bias)، وخصوصية البيانات، وأثر الذكاء الاصطناعي على سوق العمل واستقطاب الوظائف، والمساءلة القانونية والأخلاقية لقرارات الأنظمة الذاتية.[3]

الفرع الثاني: التصنيفات والأنواع الأساسية

يشهد العصر الراهن تطوراً متسارعاً في مجال الذكاء الاصطناعي، الذي لم يعد حكراً على أدبيات الخيال العلمي، بل أصبح واقعاً ملموساً يمس كافة مناحي الحياة، وقد استلزم هذا التطور إرساء تصنيفات منهجية تتيح فهم طبيعة هذه التقنيات وآليات عملها، وهو ما يعد مدخلاً ضرورياً لوضع الأطر التنظيمية والقانونية التي تحكمها، إذ تتباين المخاطر والفرص المرتبطة بتقنيات الذكاء الاصطناعي تبعاً لتباين أنواعها ودرجة تعقيدها ومن ثم، فإن تصنيف الذكاء الاصطناعي يعد الخطوة الجوهرية لتحديد نطاق المسؤولية القانونية، ودرجة الواجب الرقابي، وطبيعة الالتزامات الملقاة على عاتق المطورين والمشغلين.

أولا: التصنيفات المعيارية للذكاء الاصطناعي

[1]– يان ليكون ويوشوا بنجيو وجيوفري هينتون، "التعلم العميق"، مجلة نيتشر، مجلد 521، رقم 7553 (2015): ص 436-444.

[2]– دانييل جورافيسكي وجيمس مارتن، معالجة اللغة الطبيعية واللغويات الحاسوبية، ترجمة: مركز الملك عبد الله للدراسات اللغوية (الرياض: المركز، 2021)، ص 115.

[3]– "تقرير اللجنة العالمية لأخلاقيات المعرفة العلمية والتكنولوجيا (COMEST) حول أخلاقيات الذكاء الاصطناعي"، منظمة اليونسكو، 2019.

لا يوجد تصنيف واحد جامع للذكاء الاصطناعي، بل تتنوع التصنيفات بتنوع المعيار المعتمد في التمييز، ويمكن إبراز أبرز هذه التصنيفات على النحو التالي:

1–التصنيف وفقاً لدرجة القابلية للتطبيق (الذكاء الاصطناعي العام والضيق والفائق)

يعد هذا التصنيف من أكثر التصنيفات شيوعاً، حيث يقسم الذكاء الاصطناعي إلى ثلاثة أنواع بحسب نطاق المهام التي يستطيع أداءها مقارنة بالذكاء البشري[1]، فيمثل الذكاء الاصطناعي الضيق النمط السائد حالياً، وهو مصمم لأداء مهمة محددة أو مجموعة ضيقة من المهام، حيث يتفوق في أدائها لكنه يفتقر إلى التكيف مع مهام خارج نطاقه المبرمج[2].

أما الذكاء الاصطناعي العام، فهو نظام نظري يطابق القدرات الفكرية للإنسان، حيث يمكنه فهم العالم والتعلم وحل المشكلات المتنوعة بمستوى بشري[3]، في حين أن الذكاء الاصطناعي الفائق يفوق ذكاء الإنسان في جميع المجالات تقريباً، ويظل هذا النوع محض تخمين علمي تثار حوله تساؤلات فلسفية وقانونية عميقة بشأن إمكانية تنظيمه والسيطرة عليه[4].

2–التصنيف وفقاً للقدرة على التعلم والتكيف (الذكاء الاصطناعي الضعيف والقوي):

يقترب هذا التصنيف من سابقه، لكنه يركز على الطابع الفلسفي والوظيفي. فالذكاء الاصطناعي الضعيف يفترض أن الآلات يمكن أن تحاكي الذكاء البشري وتنفذ مهامًا ذكية دون أن تمتلك وعياً أو إدراكاً حقيقياً[5]. بينما يذهب الذكاء الاصطناعي القوي إلى إمكانية امتلاك الآلة لعقل ووعي يماثل الوعي البشري، بحيث تكون قادرة على التفكير والتخطيط وحل المشكلات بشكل مستقل[6]. وهذا التمييز له انعكاسات قانونية جسيمة، لا سيما فيما يتعلق بمسألة الشخصية القانونية للذكاء الاصطناعي والمسؤولية عن أفعاله.

3–التصنيف وفقاً للشفافية والقدرة على التفسير (الذكاء الاصطناعي الصندوق الأبيض والصندوق الأسود)

ينبع هذا التصنيف من الحاجة القانونية والتنظيمية الملحة لفهم آلية اتخاذ القرار داخل الأنظمة، خاصة في المجالات الحساسة مثل القضاء والطب والتمويل. فأنظمة الصندوق الأبيض تتميز بشفافيتها، حيث يمكن تتبع عملية الاستدلال والمنطق الذي اتبعته للوصول إلى مخرج معين[7]. في المقابل، تعتبر أنظمة الصندوق الأسود معقدة للغاية بحيث يصعب، إن لم يستحيل، فهم

---

[1] - Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson. p. 1020.

[2]– على سبيل المثال، أنظمة التوصية في منصات البيع الإلكتروني، أو أنظمة التعرف على الوجه.

[3] - Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford University Press. p. 22.

[4]– انظر: المادة 3 من مشروع الإطار التنظيمي الأوروبي للذكاء الاصطناعي (قانون الذكاء الاصطناعي) والذي يصنف أنظمة الذكاء الاصطناعي ذات المخاطر غير المقبولة، وهي تشمل نظرياً الأنظمة التي قد تهديد الحكم الذاتي البشري.

[5] - Searle, J. R. (1980). Minds, brains, and programs. Behavioral and Brain Sciences, 3(3), 417-424.

[6] - Kurzweil, R. (2005). The Singularity Is Near: When Humans Transcend Biology. Viking. p. 135.

[7]– انظر: المبادئ التوجيهية لأخلاقيات الذكاء الاصطناعي الصادرة عن اليونسكو، والتي تؤكد على ضرورة الشفافية وقابلية التفسير.

كيفية وصولها إلى قراراتها، كما هو الحال في بعض شبكات الخلايا العصبية العميقة[1]، وتثير هذه الأنظمة الأخيرة إشكاليات كبيرة تتعلق بحق المتأثر بالقرار في معرفة أسبابه، وإثبات الخطأ، وتطبيق مبدأ الشفافية.

ثانيا: الأنواع الأساسية لتقنيات الذكاء الاصطناعي من المنظور التقني

يتجلى الذكاء الاصطناعي عملياً عبر مجموعة من التقنيات والأساليب الحسابية، والتي تشكل البنية التحتية للتطبيقات المختلفة، ويمكن تصنيف هذه التقنيات إلى الأنواع الأساسية التالية:

1-التعلم الآلي: يمثل التعلم الآلي حجر الزاوية في معظم تطبيقات الذكاء الاصطناعي المعاصرة، وهو منهج يعتمد على تمكين الأنظمة من التعلم من البيانات وتحسين أدائها تلقائياً دون برمجتها صراحةً لكل مهمة[2]، ويتفرع من التعلم الآلي عدة أنماط أبرزها: التعلم تحت الإشراف حيث يتم تدريب النموذج على بيانات معلومة المخرجات، والتعلم غير الخاضع للإشراف الذي يكتشف الأنماط في البيانات غير المصنفة، والتعلم التعزيزي الذي يتعلم النموذج من خلال التفاعل مع بيئة ما للحصول على أكبر قدر من المكافآت[3]، وتجد هذه التقنيات تطبيقاتها في التنبؤ بالسلوكيات واكتشاف الاحتيال.

2-التعلم العميق: يعد التعلم العميق نوعاً متقدماً من التعلم الآلي، يستخدم شبكات عصبية اصطناعية ذات طبقات عديدة لمحاكاة الشبكة العصبية في الدماغ البشري[4]. تتيح هذه البنية المعقدة معالجة كميات هائلة من البيانات غير المهيكلة، مثل الصور والصوت والنصوص، مع تحقيق دقة عالية في مهام مثل التصنيف والتعرف على الأنماط. ومع ذلك، فإن قوة التعلم العميق تأتي على حساب الشفافية، حيث غالباً ما تتحول هذه الشبكات إلى أنظمة "صندوق أسود" يصعب تفسير قراراتها[5].

3-معالجة اللغة الطبيعية: تهدف هذه التقنية إلى تمكين الآلات من فهم اللغة البشرية الطبيعية (المكتوبة والمنطوقة) وتفسيرها وتوليدها[6]. وقد شهدت هذه المجالة قفزة نوعية مع ظهور النماذج اللغوية الكبيرة، مما أتاح تطوير مساعدين ذكيين متطورين، وأنظمة للترجمة الآلية فائقة الدقة، وتقنيات لتلخيص النصوص. وتثير هذه التقنية إشكاليات قانونية متعلقة بحقوق الملكية الفكرية على النصوص المولدة، ومخاطر التضليل ونشر المعلومات المغلوطة، وانتحال الشخصية.

---

[1] - Doshi-Velez, F., & Kim, B. (2017). Towards A Rigorous Science of Interpretable Machine Learning. arXiv preprint arXiv:1702.08608.

[2] - Mitchell, T. M. (1997). Machine Learning. McGraw-Hill. p. 2.

[3] - Sutton, R. S., & Barto, A. G. (2018). Reinforcement Learning: An Introduction (2nd ed.). The MIT Press. p. 1.

[4] - eCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

[5] - انظر: المادة 13 من اللائحة العامة لحماية البيانات في الاتحاد الأوروبي والتي تنص على "حق المعرفة" في حال اتخاذ قرارات آلية، مما يتعارض مع طبيعة أنظمة الصندوق الأسود.

[6] - Jurafsky, D., & Martin, J. H. (2023). Speech and Language Processing (3rd ed. draft). Pearson. Chapter 1.

4–الرؤية الحاسوبية: تمكن هذه التقنية الأنظمة من استخلاص المعلومات ذات المعنى من الصور الرقمية ومقاطع الفيديو وغيرها من المدخلات البصرية، ومحاكاة الإدراك البصري البشري[1]. تشمل تطبيقاتها التعرف على الوجوه، وتحليل الصور الطبية، وأنظمة القيادة الذاتية. وتعد من أكثر التقنيات إثارة للتحديات القانونية والتنظيمية، خاصة في مجالي الخصوصية (كالتعرف غير المصرح به على الوجوه) والسلامة الشخصية (كاعتمادها في المركبات ذاتية القيادة).

ويتضح من خلال هذا التحليل أن تصنيف الذكاء الاصطناعي ليس مجرد تمرين أكاديمي، بل هو أداة تحليلية محورية لتشريح الظاهرة وفهم أبعادها المتعددة. فالتصنيفات المعيارية (كالتعميم والقوة والشفافية) تقدم عدسات مختلفة لفهم الطبيعة القانونية والفلسفية لهذه الأنظمة ومدى الحاجة إلى تنظيمها. في حين أن فهم الأنواع التقنية الأساسية (كالتعلم الآلي والعميق ومعالجة اللغة) يسلط الضوء على الآليات التشغيلية والمخاطر المحددة المرتبطة بكل منها. ويؤكد هذا التباين بين الأنظمة على استحالة وجود نهج تنظيمي واحد ينطبق على جميع أشكال الذكاء الاصطناعي، مما يستدعي تبني تشريعات مرنة وقائمة على المخاطر، تأخذ في الاعتبار هذه الفروق الجوهرية في التصميم والوظيفة والقدرة.

ويشكل الذكاء الاصطناعي منظومة معقدة تتجاوز كونه مجرد ابتكار تكنولوجي، ليمسّ بشكل عميق البنى الاقتصادية والنسيج الاجتماعي والأمن القومي للدول وعليه، يتطلب فهم نطاقه الحقيقي تحليلاً شاملاً لأبعاده المتشابكة، والتي تفرض بدورها إطاراً قانونياً وتنظيمياً مرناً قادراً على مواكبة هذه التحولات الجذرية.

أولا: البُعد التقني – البنية التحتية والخوارزميات كموضوع للتنظيم

يتمثل الجوهر التقني للذكاء الاصطناعي في ثلاث ركائز أساسية: البيانات، الخوارزميات، والقدرة الحاسوبية. وتُعد هذه الركائز بمثابة "المواد الخام" للنظام، والتي تثير بدورها إشكاليات قانونية بالغة التعقيد.

أ–البيانات: ضرورة وحساسية: تُشكّل البيانات الوقود الأساسي لنماذج الذكاء الاصطناعي، سواءً كانت مُنظمة أو غير مُنظمة. هنا تبرز إشكالية التوافق بين جشع النظم للبيانات وبين حماية الحقوق الأساسية للأفراد، لاسيما الحق في الخصوصية. فعمليات جمع البيانات ومعالجتها تتطلب إطاراً قانونياً صارماً يستند إلى مبادئ "الشرعية والحدّ من الغرض والشفافية" التي أقرّها قانون حماية البيانات الشخصية في العديد من الدول[2]. كما تظهر تحديات تتعلق بجودة البيانات وتمثيليتها، حيث يمكن أن تؤدي البيانات المتحيزة إلى خلق "تحيز خوارزمي" يكرّس أشكالاً من التمييز، مما يستدعي تدخلاً تشريعياً لضمان "الإنصاف الخوارزمي".

[1] – Szeliski, R. (2022). Computer Vision: Algorithms and Applications (2nd ed.). Springer. p. 3.

[2] – انظر على سبيل المثال: القانون النموذجي العربي لحماية البيانات الشخصية الصادر عن جامعة الدول العربية، المادة (3) والتي تنص على أن معالجة البيانات الشخصية يجب أن تكون مشروعة وعادلة، وتجري لغرض محدد وواضح.

ب–الخوارزميات: الصندوق الأسود والمساءلة القانونية: تشكل تعقيدات الخوارزميات، وخاصة في تقنيات التعلّم العميق، ما يُعرف بـ "إشكالية الصندوق الأسود"، حيث يصبح من العسير تتبع كيفية اتخاذ القرار[1]. هذا الغموض يضعف من قدرة الأفراد على الطعن في القرارات الآلية التي تُؤثر في حقوقهم، كما يُصعّب عملية إثبات الخطأ وتحديد المسؤولية القانونية في حال وقوع ضرر، مما يستلزم تطوير نظريات قانونية جديدة للمساءلة، كالمسؤولية المطلقة أو المسؤولية المشتركة.

ج–البنية **التحتية الحاسوبية: الأمن السيبراني والسيادة الرقمية:** تعتمد النماذج المتطورة للذكاء الاصطناعي على بنى تحتية حاسوبية هائلة (مراكز بيانات، سحابة إلكترونية). ويجعل هذا الاعتماد الدول والشركات عُرضة لمخاطر أمنية وسياسية، مثل هجمات الحرمان من الخدمة أو التجسس الصناعي. من الناحية القانونية، تبرز قضايا "سيادة البيانات" وضرورة وضع معايير وطنية لأمن المعلومات وحماية البنى التحتية الحرجة[2].

ثانيا: البُعد الاقتصادي – إعادة هيكلة الأسواق والمنافسة

يُحدث الذكاء الاصطناعي تحولاً جذرياً في النماذج الاقتصادية، مما يفرض على المشرّع موازنة بين تحفيز الابتكار وضمان عدالة السوق.

أ–التحول في طبيعة العمل وحقوق العمال: يؤدي الأتمتة الذكية إلى إعادة تعريف العديد من الوظائف، بل وإلغاء بعضها، بينما يخلق وظائف جديدة. وهذا يستدعي تحديث التشريعات العمالية لمعالجة قضايا مثل: التدريب وإعادة التأهيل المهني، وحماية العمال في "اقتصاد المنصات" الذين يُدارون بواسطة خوارزميات، وضمان شروط عمل لائقة في بيئة العمل المستقبلية[3].

ب–التركيز السوقي ومكافحة الاحتكار: تمتلك الشركات التكنولوجية الكبرى التي تتحكم في البيانات والخوارزميات ميزة تنافسية هائلة، قد تؤدي إلى احتكارات طبيعية في أسواق الذكاء الاصطناعي. وهذا يتطلب من هيئات مكافحة الاحتكار

---

[1] – Burrell, Jenna. "How the machine 'thinks': Understanding opacity in machine learning algorithms." Big Data & Society 3.1 (2016). (تمت الترجمة والتلخيص). تشير الباحثة إلى أن عدم القدرة على تفسير آلية عمل الخوارزميات المعقدة يمثل تحدياً أساسياً للمساءلة.

[2] – European Union Agency for Cybersecurity (ENISA), "Artificial Intelligence Cybersecurity Challenges," 2020. (تمت الاستفادة من المفهوم). تؤكد الوكالة على أن الاعتماد على البنى التحتية السحابية يخلق نقاط ضعف مركزية يجب معالجتها بأطر قانونية.

[3] – International Labour Organization (ILO), "Work for a Brighter Future – Global Commission on the Future of Work," 2019. (تمت الاستفادة من التوصيات). دعت اللجنة إلى إعلان عالمي يضمن حماية العمال في اقتصاد الرقابة، والاعتراف بـ "الحد الأدنى من الحقوق الرقمية".

تبني منهجيات جديدة لتقييم عمليات الدمج والاستحواذ، لا تعتمد فقط على حصص السوق بل على "السيطرة على البيانات" و"الوصول إلى الشبكات العصبية للذكاء الاصطناعي"[1].

ج–الملكية الفكرية للإبداعات المنتجة بالذكاء الاصطناعي: يطرح إنتاج الذكاء الاصطناعي لأعمال أدبية أو فنية أو اختراعات إشكالية قانونية عميقة بشأن هوية "المخترع" أو "المؤلف". فهل تمنح براءة الاختراع لمالك النظام، أم للمبرمج، أم أن الإبداع يظل بلا حماية لأنه يفتقر إلى "اللمسة الإنسانية" التي تتطلبها قوانين الملكية الفكرية التقليدية؟[2]

ثالثا: البُعد الاجتماعي والأخلاقي – حماية القيم الإنسانية وصالح العامة

يُعتبر البعد الاجتماعي والأخلاقي أخطر الأبعاد، كونه يتعلق بالمبادئ الأساسية للمجتمع وكرامة الإنسان.

أ–العدالة والإنصاف ومكافحة التمييز: كما أشرنا، يمكن أن تكرس أنظمة الذكاء الاصطناعي التمييز على أساس الجنس أو العرق أو الدين إذا كانت البيانات التدريبية تحوي تحيزات، وهذا يتعارض مع الدساتير والقوانين التي تكفل مبدأ المساواة، لذلك يجب أن تفرض التشريعات عمليات تدقيق ومراجعة منتظمة للخوارزميات "لتقييم أثرها التمييزي المحتمل" قبل وبعد نشرها[3].

ب–الشفافية وإمكانية التفسير: يرتبط مبدأ الشفافية ارتباطاً وثيقاً بمبدأ سيادة القانون وبناء الثقة. يجب أن يكون للأفراد الحق في معرفة متى يتعاملون مع نظام ذكاء اصطناعي، والحصول على تفسير مفهوم للقرارات الآلية التي تُتخذ بحقهم، خاصة في المجالات شديدة الحساسية مثل الائتمان والتوظيف والعدالة الجنائية[4].

ج–الخصوصية والمراقبة الجماعية: تتيح تقنيات التعرف على الوجوه وتحليل المشاعر إمكانيات هائلة للمراقبة الجماعية من قبل الحكومات والشركات، مما يهدد الحريات المدنية ويخلق "مجتمع مراقبة". هنا، يتوجب على القضاء والمشرّع وضع ضوابط صارمة لتقييد استخدام هذه التقنيات بما يتناسب مع مبدأ "التناسبية" ويلتزم بضمانات المحاكمة العادلة[5].

رابعا: التطبيقات الاستراتيجية – تعزيز الأمن القومي وإدارة الموارد

يمثل الذكاء الاصطناعي أداة استراتيجية لتعزيز قدرات الدولة في المجالات الحيوية.

---

[1] - Crémer, Jacques, de Montjoye, Yves-Alexandre, and Schweitzer, Heike. "Competition policy for the digital era." European Commission, 2019. (تمت الاستفادة من الفكرة). يوصي التقرير بضرورة أن تركز قوانين المنافسة على هياكل السوق القائمة على البيانات.

[2]– على سبيل المثال، رفضت مكتب براءات الاختراع الأوروبي (EPO) والولايات المتحدة الأمريكية (USPTO) منح براءات اختراع سجل فيها الذكاء الاصطناعي كمخترع وحيد، مؤكدتين على ضرورة أن يكون المخترع "شخصاً طبيعياً".

[3]– انظر: المبادئ التوجيهية للأخلاقيات في الذكاء الاصطناعي الصادرة عن منظمة اليونسكو، والتي تؤكد على ضرورة إجراء تقييمات لأثر الذكاء الاصطناعي على حقوق الإنسان.

[4]– ينص النظام الأساسي للاتحاد الأوروبي للذكاء الاصطناعي (AI Act) – في صيغته المقترحة – على أن أنظمة الذكاء الاصطناعي عالية الخطورة يجب أن تكون شفافة وقابلة للتفسير وتخضع لتدابير رقابية بشرية.

[5]– قضية المحكمة الأوروبية لحقوق الإنسان في قضية (Big Brother Watch and Others v. The United Kingdom [GC] (2021 أكدت على أن أنظمة المراقبة الجماعية يجب أن تكون منصوصاً عليها في قانون واضح، وضرورية في مجتمع ديمقراطي، ومتناسبة مع الهدف المشروع المراد تحقيقه.

أ–الذكاء الاصطناعي في الدفاع والأمن القومي: يُستخدم الذكاء الاصطناعي في تحليل البيانات الاستخباراتية، وتشغيل الأنظمة المستقلة (مثل الطائرات بدون طيار)، والوقاية من الهجمات السيبرانية. هذه التطبيقات تثير تساؤلات قانونية وأخلاقية عميقة، خاصة فيما يتعلق بـ "الأنظمة الذاتية القاتلة" وتفويض قرار استخدام القوة للآلة، مما يستدعي وضع أطر دولية ووطنية لـ "الرقابة البشرية ذات المعنى" على هذه الأنظمة[1].

ب–الذكاء الاصطناعي في الصحة العامة وإدارة الأزمات: أثبت الذكاء الاصطناعي فاعليته في تشخيص الأمراض وتسريع اكتشاف الأدوية وإدارة الموارد خلال الأوبئة والكوارث الطبيعية، التشريعات هنا يجب أن تركز على ضمان دقة هذه الأنظمة وسرية البيانات الصحية الحساسة، وتحديد المسؤولية في حال حدوث أخطاء تشخيصية.

ج–الذكاء الاصطناعي في تحقيق أهداف التنمية المستدامة: يمكن توظيف الذكاء الاصطناعي لتحسين إدارة الموارد الطبيعية ورفع كفاءة الطاقة وزيادة الإنتاجية الزراعية، يتطلب ذلك سياسات وطنية تشجع على البحث والتطوير في هذه المجالات وبناء الشراكات بين القطاعين العام والخاص لضمان توجيه التقنية لخدمة الصالح العام.

المطلب الثاني: مفهوم الأمن السيبراني وتجلياته المعاصرة

يُشكّل الأمن السيبراني (Cybersecurity) حجر الزاوية في بناء الثقة والاستقرار في الفضاء الإلكتروني المعاصر، الذي أصبح بدوره العصب الحياتي للمجتمعات الحديثة ومحركاً رئيسياً لكافة قطاعات العمل والاقتصاد والمعرفة، ولم يعد هذا المفهوم مقتصراً على حماية البيانات والمعلومات فحسب، بل تجاوز ذلك ليشمل حماية البنى التحتية الحيوية للأمم، واقتصادها الوطني، وأمنها القومي، بل ونسيجها الاجتماعي نفسه، ويمكن تعريفه إجرائياً بأنه "مجموعة الممارسات والتقنيات والآليات المصممة لحماية أنظمة الحاسوب، والشبكات، والبيانات، والبرامج من الهجمات، أو التلف، أو الوصول غير المصرح به، وذلك بهدف ضمان توافرها وسريتها وسلامتها."[2]

لقد تطور مفهوم الأمن السيبراني تطوراً جوهرياً متسارعاً، متجاوزاً مرحلة التركيز على تأمين الحدود التقليدية للشبكات (Network Security) أو مجرد مكافحة الفيروسات، ليدخل مرحلة أكثر تعقيداً واتساعاً. فالتجليات المعاصرة للأمن السيبراني تعكس طبيعة التهديدات المستجدة والبيئة الرقمية الديناميكية. ومن أبرز هذه التجليات:

- ✓ حماية البنى التحتية الحيوية الوطنية: تُعد هذه من أهم تجليات الأمن السيبراني في العصر الراهن، حيث تشمل حماية الأنظمة التي يعتمد عليها المجتمع وأمنه واقتصاده وصحته، ويشمل ذلك قطاعات الطاقة (المحطات الكهربائية وشبكات النقل) والمياه (محطات التحلية والتوزيع) والمواصلات (الطيران، السكك الحديدية، الموانئ) والخدمات المالية والمصرفية والرعاية

[1] – المبدأ الرابع من "مبادئ شارلوت فيل" حول الأسلحة الذاتية، والذي يؤكد على ضرورة أن تظل "الرقابة البشرية ذات المعنى" قائمة على قرار استخدام القوة.

[2] – المعهد الوطني للمعايير والتقنية (NIST)، الولايات المتحدة الأمريكية. (راجع: "Cybersecurity Framework" مع التعديلات اللغوية المناسبة للتعريف).

الصحية (المستشفيات وسجلات المرضى)[1]، فأي اختراق لهذه البنى قد يؤدي إلى شلل تام في الحياة اليومية، وخسائر اقتصادية فادحة، وحتى إلى أضرار بشرية وتهديد للأمن القومي.

✓ مواجهة تطور التهديدات السيبرانية المتطورة: لقد شهدت التهديدات تحولاً نوعياً من الهجمات العشوائية التي ينفذها أفراد إلى هجمات مُمنهجة ومدعومة من دول أو منظمات إجرامية منظمة، وتبرز هنا ظاهرة "البرمجيات الخبيثة للابتزاز" (Ransomware) التي تشفر بيانات الضحايا وطلب فدية مقابل فكها، مما أضر بالشركات الكبرى والمستشفيات والحكومات[2]، بالإضافة إلى هجمات "حجب الخدمة الموزع" التي تهدف لإغراق الخوادم بحركة مرور زائفة لتعطيلها وهجمات "التصيد" (Phishing) المتطورة التي تستهدف سرقة بيانات الاعتماد الحساسة عبر وسائل احتيالية شديدة التلاعب.

✓ الأمن السيبراني في ظل إنترنت الأشياء والتحول الرقمي: أدى الانتشار الهائل للأجهزة الذكية المترابطة عبر ما يعرف بـ "إنترنت الأشياء" (IoT) – بدءاً من الأجهزة المنزلية الذكية وصولاً إلى أجهزة الاستشعار في المدن الذكية والصناعة – إلى توسيع رقعة الهجوم بشكل غير مسبوق.

إن كل جهاز متصل بالإنترنت يمثل نقطة دخول محتملة للمخترقين إذا لم يتم تأمينه بشكل كاف[3]، كما أن التحول الرقمي الشامل للخدمات الحكومية والشركات واعتمادها على الحوسبة السحابية، يفرض متطلبات أمنية جديدة تتعلق بحماية البيانات المخزنة على المنصات السحابية وضمان خصوصية الأفراد.

✓ البعد الإنساني والاجتماعي للأمن السيبراني: لم يعد الأمن السيبراني مسألة تقنية بحتة، بل امتد ليشمل بعداً إنسانياً واجتماعياً عميقاً. فهو يتعلق بمكافحة الجرائم الإلكترونية التي تستهدف الأفراد مثل الاحتيال المالي والابتزاز الإلكتروني وانتحال الشخصية. كما يشمل حماية الفضاء الاجتماعي من خلال مكافحة خطاب الكراهية ونشر الشائعات والتضليل الإعلامي (Information Warfare) الذي يهدد الاستقرار الاجتماعي ويسعى لتقويض الثقة بين المواطنين ومؤسسات الدولة[4] وأصبح ما يُعرف بـ "الأمن السيبراني المجتمعي" مطلباً حيوياً لبناء مجتمع واعٍ ومقاوم لهذه المخاطر.

✓ الأمن السيبراني كرهان اقتصادي واستراتيجي: تحول الأمن السيبراني إلى عنصر أساسي في المنافسة الاقتصادية العالمية. فحماية أسرار التجارية والابتكارات التقنية والملكية الفكرية من عمليات التجسس الإلكتروني أصبحت ضرورة لاستمرارية الأعمال والمحافظة على الميزة التنافسية. كما أن امتلاك قدرات سيبرانية دفاعية وهجومية متطورة أصبح جزءاً من ميزان القوى بين الدول، حيث تُستخدم هذه القدرات في الصراعات الجيوسياسية، مما أدى إلى ظهور ما يُسمى بـ "استراتيجية الردع السيبراني"[5].

---

[1]– لمركز الوطني الإلكتروني، المملكة العربية السعودية. (وثائق استراتيجية الأمن السيبراني الوطني التي تؤكد على حماية البنى التحتية الحيوية).

[2]– تقرير سيماتنك عن تهديدات الأمن عبر الإنترنت (Internet Security Threat Report). (تقارير دورية توثق التصاعد الكبير في هجمات الـ Ransomware).

[3]– غارتنر (Gartner) وآي دي سي (IDC). (تقارير تحليلية حول نمو إنترنت الأشياء والتحديات الأمنية المصاحبة له).

[4]– اليونسكو (UNESCO). (دراسات حول تأثير التضليل الإعلامي والخطاب الرقمي على المجتمعات).

[5]– مركز الدراسات الاستراتيجية والدولية (CSIS). (أبحاث ونماذج عن استراتيجيات الردع السيبراني والصراع في الفضاء الإلكتروني بين الدول).

ويمكن القول إن مفهوم الأمن السيبراني قد تحول من كونه تخصصاً تقنياً هامشياً إلى استراتيجية وطنية شاملة ومتكاملة، تمس جميع مناحي الحياة، وتكمن صعوبة تحقيق هذا الأمن في الطبيعة العابرة للحدود للتهديدات وسرعة تطورها مقارنة بإجراءات الدفاع. لذلك، فإن المواجهة الفعالة تتطلب نهجاً تعاونياً يشمل تعزيز التشريعات وبناء الكفاءات البشرية وزيادة الوعي المجتمعي وتعزيز التعاون الدولي، والاستثمار المستمر في البحث والتطوير لابتكار حلول أمنية تكون في مستوى التحديات المستمرة والمتجددة التي يفرضها العالم الرقمي.

الفرع الأول: الإطار المفاهيمي المتطور

شكَّلت الثورة الرقمية تحوّلاً جذرياً في بنية المجتمعات الحديثة، فأضحت الفضاءات السيبرانية تشكل العمود الفقري للأنشطة الاقتصادية والاجتماعية والسياسية. وقد اقترن هذا التحول بظهور تهديدات متنوعة ومعقدة، استدعت تطوير مفهوم الأمن السيبراني من كونه مجرد أدوات تقنية لحماية الأنظمة، إلى إطار استراتيجي شامل ومتعدد الأبعاد.

لم يعد هذا المقتصر على تأمين البيانات والمعلومات فحسب، بل امتد ليشمل حماية البنى التحتية الحيوية والفضاء الرقمي الوطني، بل وأصبح ركيزة أساسية للأمن القومي في عصر العولمة الرقمية. يناقش هذا المطلب تطور هذا الإطار المفاهيمي، مستعرضاً تعريفاته المتعددة وأبعاده الرئيسية.

أولا: من الحماية التقنية إلى المفهوم الاستراتيجي الشامل

لقد تطور مفهوم الأمن السيبراني تطوراً ملحوظاً، متجاوزاً مرحلة التركيز على الجوانب الدفاعية والتقنية البحتة. ففي بداياته، كان يُختزل في "أمن المعلومات"، الذي يركز على حماية سرية وسلامة وتوافر البيانات من خلال أدوات مثل الجدران النارية وبرامج مكافحة الفيروسات[1] إلا أن توسع نطاق التهديدات، من جرائم إلكترونية فردية إلى عمليات التجسس الإلكتروني والحروب السيبرانية الممنهجة التي تستهدف دولاً بأكملها، أدى إلى ضرورة تبني نظرة أوسع.

فالأمن السيبراني، في مفهومه المعاصر، يُعرف بأنه "حماية الشبكات والأنظمة المعلوماتية والمكونات المادية والبرمجيات والبيانات من أي هجوم إلكتروني"[2] كما يعرفه البعض على أنه "مجموعة الوسائل التقنية والتنظيمية والإدارية التي تُستخدم لمنع الاستخدام غير المصرح به، واستعادة الأمن الإلكتروني، والتحقيق في الجرائم السيبرانية، لضمان توافر وسلامة وسرية المعلومات"،[3] وهذا التعريف يؤكد على الطبيعة المتعددة للتخصصات، التي تدمج بين التقنية والقانون والإدارة. وبالتالي، لم يعد الهدف مجرد ردع القراصنة، بل أصبح يشمل ضمان استمرارية الخدمات الحيوية وحماية الاقتصاد الوطني وصون السيادة الرقمية في مواجهة الفاعلين الحكوميين وغير الحكوميين على حد سواء.

ثانيا: الأبعاد الأساسية للإطار المفاهيمي المتكامل

[1] – الغامدي، خالد بن عبد الله. (2018). الأمن السيبراني: المفهوم والتحديات. مجلة البحوث الأمنية، 32(1)، 45.

[2] – الشهراني، فهد بن معيض. (2020). الإطار القانوني للأمن السيبراني في المملكة العربية السعودية. الرياض: دار الملك سعود، 33.

[3] – آل سعود، فيصل بن عبد الله. (2019). استراتيجيات الأمن السيبراني وحوكمتها. ورقة مقدمة إلى الملتقى العلمي للأمن السيبراني، الرياض، 17.

ينبني الإطار المفاهيمي المتطور للأمن السيبراني على عدة أبعاد متكاملة، تجعله ركيزةً للأمن الشامل، وأبرزها:

1–البعد التقني: وهو الأساس الذي يقوم عليه الأمن السيبراني، ويشمل تطوير وتنفيذ الأدوات والتقنيات مثل أنظمة كشف التسلل، والتشفير، وتأمين البنى التحتية الحرجة، والتقنيات المتقدمة مثل الذكاء الاصطناعي لمكافحة الهجمات المعقدة.

2–البعد القانوني والتشريعي: يتمثل في وضع الأطر القانونية التي تجرم الأنشطة غير المشروعة في الفضاء السيبراني، وتنظم عمليات جمع الأدلة الرقمية (الإلكترونية)، وتعزز التعاون الدولي لمكافحة الجريمة السيبرانية العابرة للحدود.

3– البعد التنظيمي والإداري: ويتركز على وضع السياسات والاستراتيجيات الوطنية للأمن السيبراني، وإنشاء هياكل حوكمة واضحة (كالمراكز الوطنية للاستجابة للطوارئ السيبرانية)، ووضع معايير وإجراءات للمراقبة والتقييم المستمر لفعالية الإجراءات الأمنية.[1]

4–البعد البشري والثقافي: وهو بعد حاسم، إذ يهدف إلى بناء الوعي السيبراني وتنمية الكفاءات البشرية المتخصصة، فالإنسان غالباً ما يكون الحلقة الأضعف في السلسلة الأمنية، لذا أصبحت برامج التوعية ونشر الثقافة الأمنية بين المستخدمين والأفراد جزءاً لا يتجزأ من أي إطار أمني فعال.[2]

وعليه، فإن الطبيعة الديناميكية للتهديدات السيبرانية، التي تتطور باستمرار، تجعل من الإطار المفاهيمي للأمن السيبراني إطاراً متطوراً وغير ثابت، يتطلب مراجعة وتطويراً مستمرين للسياسات والاستراتيجيات والتقنيات، لمواكبة مشهد التهديدات المتغير وضمان تحقيق الأمن والاستقرار في الفضاءات السيبرانية.

الفرع الثاني: الأبعاد المتعددة للأمن السيبراني

لم يعد مفهوم الأمن السيبراني حكراً على الحماية التقنية للبيانات والشبكات فحسب، بل تجاوز ذلك ليشكل نظاماً معقداً ومتداخل الأبعاد، يؤثر ويتأثر بمختلف جوانب الحياة المعاصرة، لذلك، يقتضي التحليل العلمي تفكيك هذا المفهوم إلى أبعاده الرئيسية لفهم طبيعته الشمولية وآليات تعزيزه.

أولا: الأبعاد التقنية والتكنولوجية: البنية التحتية للحماية الرقمية

يشكل البعد التقني والتكنولوجي حجر الزاوية في بناء منظومة الأمن السيبراني، حيث يمثل خط الدفاع الأول ضد الهجمات الإلكترونية المتنامية، يتجلى هذا البعد في مجموعة من الآليات والبروتوكولات المصممة لحماية البنية التحتية الرقمية، والتي تشمل أجهزة الحواسيب والخوادم والشبكات والبيانات المخزنة والمتنقلة عبر الفضاء الإلكتروني، وتتمثل الركائز الأساسية لهذا البعد في تقنيات التشفير التي تضمن سرية وسلامة البيانات وجدران الحماية (Firewalls) التي ترشح حركة المرور الشبكية وأنظمة كشف ومنع التسلل (IDS/IPS) التي ترصد الأنشطة غير المشروعة، بالإضافة إلى برامج مكافحة البرمجيات الخبيثة، إلا أن التحدي الأكبر في هذا الإطار لا يكمن فقط في تطوير هذه الأدوات، بل في تحديثها المستمر لمواكبة أساليب الهجوم المتطورة، مما

[1] – الهيئة الوطنية للأمن السيبراني. (2021). الإطار العام لحوكمة الأمن السيبراني. المملكة العربية السعودية.

[2] – العتيبي، منصور بن سليم. (2022). دور الثقافة الأمنية في تعزيز الأمن السيبراني. مجلة جامعة الملك سعود –العلوم الإدارية، 34(2)، 112.

يستلزم تبني منهجيات استباقية كـ "الاختبار الاختراقي" (Penetration Testing) و"الذكاء الاصطناعي" للتنبؤ بالثغرات والتهديدات قبل استغلالها[1] وبالتالي، فإن قوة البعد التقني تقاس بمدى مرونته وقدرته على التكيف في مواجهة المشهد الديناميكي للتهديدات السيبرانية.

ثانيا: الأبعاد البشرية والتنظيمية: الإنسان كحلقة ضعف وقوة

على الرغم من أهمية الأدوات التقنية، يبقى العنصر البشري الحلقة الأكثر حساسية في معادلة الأمن السيبراني، فهو يشكل إما أقوى خط دفاع أو أكبر نقطة ضعف، يسلط هذا البعد الضوء على الجانبين البشري والتنظيمي، حيث يركز الأول على السلوكيات والممارسات الفردية للمستخدمين، فأغلب الاختراقات الأمنية، مثل هجمات التصيد (Phishing) والهندسة الاجتماعية، تعتمد على استغلال جهل المستخدم أو إهماله بدلاً من استغلال ثغرة تقنية.[2]

من هنا تبرز الحاجة الماسة لبرامج التوعية المستمرة وبناء الثقافة الأمنية التي تجعل من المستخدم "حارساً أول" للبيانات، أما الجانب التنظيمي، فيتعلق بوضع السياسات والإجراءات والهياكل الإدارية التي تنظم العمل داخل المؤسسات، وهذا يشيط تطبيق معايير وإطارات عمل مثل "أيزو 27001" (ISO/IEC 27001) للمنظومة الأمنية وتحديد المسؤوليات والصلاحيات وإجراء تدريبات محاكاة للهجمات ووضع خطط استجابة للحوادث، إن تكامل البعدين البشري والتنظيمي يخلق بيئة أمنية مرنة، حيث تتحول الثقافة الأمنية من مجرد التزام إلزامي إلى سلوك مؤسسي راسخ، مما يعزز المناعة الداخلية للمنظمة في مواجهة المخاطر[3].

ويُشكّل الأمن السيبراني في المملكة المغربية ركيزة أساسية ضمن الرؤية الاستراتيجية للتحول الرقمي، حيث عمل المشرع المغربي على بناء إطار تشريعي ومؤسسي متكامل يواكب التحديات الناشئة عن الفضاء الرقمي، وقد تبلور هذا الإطار من خلال سن نصوص قانونية مؤسسة، أبرزها القانون 05-20 المتعلق بالسلامة المعلوماتية والقانون 08-09 المتعلق بحماية المعطيات ذات الطابع الشخصي، إلى جانب إرساء بنية مؤسسية مختصة لتطبيق هذه النصوص وتنفيذ السياسات العمومية في هذا المجال.

أولاً: الإطار التشريعي: القوانين المؤسسة للأمن السيبراني

1- القانون 05-20 المتعلق بالسلامة المعلوماتية[4]

[1]- الزهراني، خالد بن عبدا لله. (2020). الأمن السيبراني: المفاهيم والتحديات. الرياض: دار جامعة الملك سعود للنشر. ص 145.

[2]- الشمري، فاطمة مُحَمَّد. (2019). "دور العامل البشري في تعزيز الأمن السيبراني: دراسة تحليلية". المجلة العربية لتقنية المعلومات والأمن السيبراني، 5(2)، 87-105.

[3]- الحمادي، ناصر إبراهيم. (2021). الإطار التنظيمي لحوكمة الأمن السيبراني في القطاع العام. أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية. ص 76.

[4]- قانون رقم 05.20 المتعلق بالسلامة المعلوماتية، الصادر بتنفيذه الظهير الشريف رقم 1.20.28 بتاريخ 19 فبراير 2020، الجريدة الرسمية عدد 6867 مكرر بتاريخ 24 فبراير 2020، ص 1187.

يُمثّل القانون 05-20 حجر الزاوية في المنظومة التشريعية المغربية للأمن السيبراني، حيث يهدف إلى ضمان "السلامة المعلوماتية" للمنظومات المعلوماتية للدولة والمؤسسات والهيئات العامة والخاصة، ولا يقتصر دوره على التجريم والعقاب، بل يتعداه إلى وضع إطار استباقي للوقاية والتدبير.

– **التجريم والعقاب**: وسّع القانون من نطاق الجرائم المعلوماتية المعاقب عليها، حيث شمل مجموعة من الأفعال الجرمية الجديدة مثل الدخول غير المشروع إلى منظومة معلوماتية، عرقلة سيرها وإدخال أو حذف معطيات بشكل غير مشروع[1]، كما عزز العقوبات السالبة للحرية والغرامات المالية وجعلها متناسبة مع خطورة هذه الجرائم وتأثيرها على المصالح الوطنية والأمن العام.

– **الوقاية والالتزام**: يُلزم القانون الأشخاص المعنويين الخاضعين لأحكامه، وخاصة المشغلين للمرافق الأساسية (المنشآت الحيوية)، باتخاذ جميع التدابير التقنية والتنظيمية الكفيلة بضمان سلامة وأمن منظوماتهم المعلوماتية[2]. كما فرض إبلاغ السلطات المختصة عن أي حادث له تأثير على السلامة المعلوماتية، مما يعكس نهجاً استباقياً في إدارة الأخطار السيبرانية.

–**الإجراءات الزجرية**: خوّل القانون للسلطات القضائية المختصة إمكانية اللجوء إلى تقنيات التحري الخاصة، مثل التطفل المعلوماتي، تحت رقابة قضائية صارمة، لمكافحة الجريمة المعلوماتية في إطار يحترم الضمانات القانونية.[3]

2–القانون 08–09 المتعلق بحماية المعطيات ذات الطابع الشخصي[4]:

يأتي هذا القانون كتتويج للجهود الرامية إلى حماية الحقوق الأساسية للأفراد، وخاصة الحق في الخصوصية، في سياق الاقتصاد الرقمي، وهو يستند إلى المعايير الدولية في هذا المجال، لا سيما التنظيم الأوروبي العام لحماية البيانات(GDPR) .

– **مبادئ أساسية لمعالجة المعطيات**: أرسى القانون جملة من المبادئ التي تحكم أي معالجة للمعطيات الشخصية، كالشفافية والقانونية والتناسب والحد من الغرض ودقة المعطيات وتحديد مدة حفظها،[5] كما اشترط الحصول على موافقة صريحة من الشخص المعني بالمعطيات قبل جمعها أو معالجتها.

– **ضمانات حقوق الأفراد**: كرّس القانون لحملة المعطيات الشخصية مجموعة من الحقوق، أبرزها الحق في الوصول إلى معطياتهم وحق التصويب وحق الحذف ("الحق في النسيان") وحق الاعتراض على المعالجة،[6] مما يعزز مركزهم كفاعلين رئيسيين في عملية المعالجة.

---

[1]– انظر: المادة 3-1 من القانون 05.20.

[2]– انظر: المادة 9 من القانون 05.20.

[3]– انظر: المادة 16 من القانون 05.20.

[4]– قانون رقم 09.08 المتعلق بحماية المعطيات ذات الطابع الشخصي، الصادر بتنفيذه الظهير الشريف رقم 1.09.15 بتاريخ 18 فبراير 2009، الجريدة الرسمية عدد 5714 بتاريخ 19 فبراير 2009، ص 935.

[5]– انظر: المادة 4 من القانون 09.08.

[6]– انظر: المواد من 24 إلى 28 من القانون 09.08.

– **الالتزامات المفروضة على المسؤول عن المعالجة:** فرض القانون على كل شخص ذاتي أو معنوي يقوم بمعالجة المعطيات الشخصية (المسؤول عن المعالجة) جملة من الالتزامات، أهمها إشعار الهيئة الوطنية للتحكم في حماية المعطيات ذات الطابع الشخصي (CNDP) قبل البدء في أي معالجة واعتماد تدابير أمنية تقنية ومادية لحماية هذه المعطيات من التسرب أو الضياع أو الوصول غير المشروع[1].

–**الهيئة الوطنية للتحكم في حماية المعطيات ذات الطابع الشخصي (CNDP):** أنشأ القانون هيئة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، مهمتها السهر على احترام أحكام القانون من خلال سلطاتها في المراقبة والتقييم والتوجيه والتوقيف، وكذلك سلطة فرض عقوبات إدارية مالية في حالة المخالفة[2].

ثانيا: الإطار المؤسسي: البنية الهيكلية لتدبير الأمن السيبراني

إلى جانب البنية التشريعية، تم إنشاء مجموعة من المؤسسات المتخصصة لتتكامل أدوارها في تأمين الفضاء الرقمي المغربي.

– **الوكالة الوطنية لتقنيي المعلومات (ANRT):** تلعب الوكالة دوراً محورياً في تنظيم قطاع الاتصالات وتقنية المعلومات وتضمن أمن وشبكات الاتصالات الوطنية، كما تساهم في تطوير معايير الأمن السيبراني والتوعية بمخاطر الفضاء الرقمي.

– **اللجنة الوطنية لمكافحة الجرائم المعلوماتية (CNLCC):** تُعد هذه اللجنة آلية تنسيقية بين مختلف الفاعلين المؤسسيين المعنيين بمكافحة الجريمة المعلوماتية (وزارات الداخلية والعدل والاتصالات والوكالات المختصة)، تهدف إلى وضع استراتيجية وطنية في هذا المجال وتتبع تنفيذها وتعزيز تبادل المعلومات بين الجهات المعنية.[3]

– **الهيئة الوطنية للتحكم في حماية المعطيات ذات الطابع الشخصي (CNDP):** كما سبق الذكر، تشكل هذه الهيئة الركيزة المؤسسية لتطبيق قانون حماية المعطيات الشخصية، مما يجعلها فاعلاً أساسياً في حماية الخصوصية كأحد أركان الأمن السيبراني الشامل.

ويشهد الإطار التشريعي والمؤسسي المغربي للأمن السيبراني تطوراً ملحوظاً، يعكس إرادة سياسية راسخة لمواكبة متطلبات الرقمنة وتهديداتها، ويظل التحدي القائم في تعزيز التنسيق بين هذه المؤسسات ومواصلة تحديث النصوص القانونية لمسايرة التطورات التقنية المتسارعة، وبناء القدرات البشرية المتخصصة لضمان فعالية هذا الإطار في تحقيق السلامة المعلوماتية المنشودة.

[1]– انظر: المادتين 16 و 17 من القانون 09.08.

[2]– انظر: المواد من 31 إلى 38 من القانون 09.08.

[3]–: للمزيد من التفاصيل حول أدوار هذه اللجنة، يمكن الرجوع إلى المرسوم رقم 2.14.774 بتحديد اختصاصات وتنظيم اللجنة الوطنية لمكافحة الجرائم المعلوماتية

المحور الثاني: التفاعل الجدلي بين الذكاء الاصطناعي والأمن السيبراني

يمثل التفاعل بين الذكاء الاصطناعي والأمن السيبراني علاقة جدلية معقدة، تتسم بالثنائية والتأثير المتبادل، حيث لم يعد الذكاء الاصطناعي مجرد أداة مساعدة في يد المدافعين، بل أصبح سلاحاً ذا حدين يشكل معاً حجر الزاوية في معمارية الأمن الرقمي المعاصر.

فمن ناحية، يقدم الذكاء الاصطناعي، وتحديداً تقنيات التعلم الآلي والتعلم العميق، حزمة غير مسبوقة من الحلول الذكية القادرة على تعزيز الوقاية والكشف والاستجابة للتهديدات السيبرانية المتطورة، مما يضفي طابعاً استباقياً وذكياً على آليات الدفاع، ومن ناحية أخرى، فإن هذه التقنيات نفسها تمنح المهاجمين أدوات متقدمة لتطوير هجمات أكثر تطوراً وتكيفاً، تُعرف باسم "الهجمات الخبيثة المدعومة بالذكاء الاصطناعي"، مما يخلق حلقة مستمرة من التصعيد التكنولوجي بين الهجوم والدفاع.

إن العلاقة بين الذكاء الاصطناعي والأمن السيبراني هي علاقة جدلية – ديالكتيكية – يولد فيها كل تقدم في مجال دفاعي تحديات هجومية جديدة، والعكس صحيح. فالتقدم في تطوير أنظمة كشف التسلل القائمة على التعلم الآلي، على سبيل المثال، يحفز بدوره المهاجمين على تطوير تقنيات التهرب والتضليل (Adversarial Attacks) المصممة خصيصاً لخداع هذه الأنظمة،[1] هذه الديناميكية تضعنا أمام مشهد متقلب، حيث يصبح الذكاء الاصطناعي هو الساحة الجديدة للمواجهة، وهو المحرك الأساسي لتطور التهديدات، وفي الوقت ذاته، الحارس الأكثر فعالية ضدها.

لذلك، سنحاول تفكيك هذه العلاقة المعقدة وتحليلها من خلال مطلبين رئيسيين مترابطين، الأول يركز على دور الذكاء الاصطناعي كحليف استراتيجي للأمن السيبراني، حيث يستعرض الكيفية التي أحدثت بها هذه التقنيات ثورة في عمليات مراقبة الشبكة وتحليل السلوك لاكتشاف الشذوذ، وتسريع استجابة الحوادث من خلال الأتمتة الذكية، وتعزيز أمن الهوية عبر أنظمة المصادقة الحيوية، وتحليل الثغرات الأمنية بشكل استباقي. أما الثاني فيسلط الضوء على الوجه الآخر للذكاء الاصطناعي كتهديد وجودي، من خلال تحليل كيفية استغلال الجهات الخبيثة لهذه التقنيات في تنفيذ هجمات أكثر ذكاءً، مثل إنشاء البرمجيات الخبيثة المتطورة (Polymorphic and Metamorphic Malware)، وتطوير هجمات التصيد الاحتيالي الأكثر تصديقاً باستخدام تقنيات معالجة اللغة الطبيعية وإنشاء المحتوى العميق (Deep fakes)، وأتمتة عمليات استكشاف الثغرات واستغلالها[2].

المطلب الأول: الإمكانات الاستباقية للذكاء الاصطناعي

[1] - Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. D. (2011). Adversarial Machine Learning. Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence. (المرجع الأساسي لهجمات الخصومة في التعلم الآلي).

[2] - Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. arXiv preprint arXiv:1802.07228. (تقرير مؤسس حول الاستخدام الخبيث للذكاء الاصطناعي).

يشهد عصرنا الحالي تحوّلاً في طبيعة التهديدات التي تواجه الأمن القومي والمجتمعي، حيث أصبحت هذه التهديدات أكثر تعقيداً وتشابكاً، وغالباً ما تتسم بالسرعة والغموض، مما يجعل من أساليب المواجهة التقليدية غير كافية. في هذا السياق، يبرز الذكاء الاصطناعي ليس كأداة للاستجابة، بل كمحور أساسي لمنظومة استباقية[1] تهدف إلى توقع المخاطر ومنعها قبل أن يُعَدُّ الذكاء الاصطناعي، بمقدرته الفائقة على معالجة كميات هائلة من البيانات (Big Data)[2] بسرعات لا يمكن للعقل البشري مجاراتها، رافعةً نوعية في الانتقال من ثقافة رد الفعل إلى ثقافة الاستباق.

وتقوم الإمكانات الاستباقية للذكاء الاصطناعي على ثلاثة أركان رئيسية: التنبؤ، والوقاية، والتأهب، فمن خلال تقنيات التحليل التنبئي (Predictive Analytics) والتعلم الآلي (Machine Learning)، يمكن لنماذج الذكاء الاصطناعي اكتشاف الأنماط الخفية في البيانات التي تمر مرور الكرام على المحللين البشريين. هذا يتيح، على سبيل المثال لا الحصر، توقع الهجمات الإلكترونية من خلال رصد الشذوذ في حركة مرور البيانات (Network Traffic)، أو التنبؤ بانتشار الأوبئة من خلال تحليل بيانات البحث على الإنترنت وبيانات وسائل التواصل الاجتماعي، أو حتى توقع التهديدات المالية والاقتصادية مثل عمليات الاحتيال أو التقلبات السوقية الحادة.

وعليه، فإن هذا المبحث سيناقش الكيفية التي يُعيد بها الذكاء الاصطناعي تشكيل مفهوم الاستباقية، من خلال تحويل مجرى المعلومات من تدفق سلبي إلى مورد استراتيجي فاعل. سيسلط الضوء على الآليات التقنية التي تمكن من تحقيق هذه الاستباقية، مع تقديم أمثلة تطبيقية من مجالات متعددة مثل الأمن السيبراني، والصحة العامة، والأمن الوطني. كما سيتطرق إلى التحديات الأخلاقية والعملية المصاحبة لهذا التحول، مثل قضايا الخصوصية، والتحيز في الخوارزميات، وإشكالية المساءلة عند تفويض عمليات التوقع والمنع للآلات، الهدف النهائي هو تقديم رؤية متكاملة لدور الذكاء الاصطناعي كحجر زاوية في بناء أنظمة دفاع وحوكمة أكثر ذكاءً واستباقية في القرن الحادي والعشرين.

الفرع الأول: التحول في آليات الكشف والتحليل

يمكّن الذكاء الاصطناعي من تحليل كميات هائلة من البيانات لاكتشاف الأنماط غير الطبيعية والكشف عن التهديدات الناشئة بفعالية غير مسبوقة، حيث شكّل التطوّر المتسارع للتهديدات الإلكترونية، وتعقيد أساليبها، تحديًا جوهريًا أمام آليات الأمن التقليدية، التي لم تعد قادرة على مواكبة الحجم والذكاء المتزايد لهذه الهجمات. في هذا السياق، يبرز الذكاء الاصطناعي (Artificial Intelligence) كمنعطف حاسم، لا مجرد أداة تكميلية، بل كمُحوِّل جذري لطبيعة عمليات

[1] – عاشور، محمد. "الذكاء الاصطناعي وإدارة الأزمات: نحو نموذج استباقي." مجلة الدراسات المستقبلية، المجلد 12، العدد 2، 2022، ص 45-68.

[2] – Mayer-Schönberger, Viktor, and Kenneth Cukier. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt, 2013. (ترجمة: فايقة جرجس، "البيانات الضخمة: الثورة التي ستغير طريقة عيشنا وعملنا وفكرنا"، الدار العربية للعلوم ناشرون، 2014).

الكشف والتحليل. لم يعد التحول مقتصرًا على زيادة السرعة فحسب، بل تجاوزه إلى إعادة هندسة القدرة على فهم وإدراك التهديدات في بيئة رقمية تتسم بالضبابية والتعقيد.[1]

يمكّن الذكاء الاصطناعي من اختزال فجوة الزمن بين حدوث الهجوم واكتشافه، من خلال تمكين أنظمة الدفاع من تحليل كميات هائلة من البيانات لاكتشاف الأنماط غير الطبيعية والكشف عن التهديدات الناشئة بفعالية غير مسبوقة، مما يضع الأسس لما يُعرف بـ "المناعة الذاتية" للبنى التحتية الرقمية.[2]

أولا: التحول من الكشف القائم على التوقيع إلى التحليل السياقي

لطالما اعتمدت أنظمة الكشف التقليدية، مثل أنظمة كشف التسلل (Intrusion Detection Systems) القائمة على التوقيعات (Signature-based)، على مقارنة حركة المرور والسلوكيات بقوائم محددة مسبقًا للتهديدات المعروفة. هذا النهج، رغم فعاليته ضد الهجمات الشائعة، يتسم بالجمود ويتعذر عليه مواجهة الهجمات الصفرية (Zero-day Attacks) أو الهجمات المتطورة التي تتجنب استخدام توقيعات معروفة[3]، هنا يأتي التحول الذي يقوده الذكاء الاصطناعي، من خلال الانتقال من منطق "المطابقة" (Matching) إلى منطق "الاستدلال" (Inference). فتقنيات التعلم الآلي (Machine Learning) -وخاصة التعلم غير الموجّه (Unsupervised Learning) -تسمح للنماذج الحسابية ببناء فهم استباقي للسلوك "الطبيعي" baseline للشبكة والمستخدمين والتطبيقات. أي خلل أو انحراف طفيف عن هذا الأساس الذي تم تعلمه ذاتيًا، حتى لو لم يُسجل سابقًا في قوائم التهديدات، يُصنف على أنه شذوذ يستدعي الانتباه،[4] على سبيل المثال، يمكن للنموذج اكتشاف محاولة وصول غير اعتيادية لموظف في وقت غير معتاد، أو نقل بيانات بحجم غير مألوف، مما قد يشير إلى اختراق أو تهديد داخلي.

ثانيا: تمكين الكشف عن التهديدات الناشئة والمعقدة

تمتد قدرة الذكاء الاصطناعي لتتجاوز الكشف عن الشذوذ البسيط إلى مواجهة التهديدات المستعصية والبرمجيات الخبيثة متعددة الأشكال، هذه التهديدات تتغير ديناميكيًا وتتخفى ضمن الضجيج الرقمي العادي، مما يجعلها شبه خفية عن العين البشرية والأنظمة التقليدية. تعمل خوارزميات التعلم العميق، مثل الشبكات العصبية التلافيفية والشبكات العصبية المتكررة على

[1] – الأمن السيبراني في عصر الذكاء الاصطناعي: التحديات والفرص. مجلة جامعة الملك سعود –العلوم الهندسية، 32(2)، 155-167.

[2] - Miller, B. (2018). AI and the Future of Cybersecurity: The Predictive Paradigm. Cybersecurity Journal, 4(1), 22-35

[3] – الغامدي، فهد بن محمد. (2019). تقنيات التعلم الآلي في مواجهة الهجمات الإلكترونية المتطورة. ورقة مقدمة للمؤتمر السنوي للأمن المعلوماتي، الرياض.

[4] - Chen, L., & Zhang, H. (2021). Unsupervised Anomaly Detection for Network Traffic Using Deep Autoencoders. IEEE Transactions on Network and Service Management, 18(3), 3214-3225.

تحليل البيانات على مستويات مجردة ومتداخلة[1]، فبدلاً من فحص سطر واحد من الكود في ملف، يمكن للنموذج تحليل سلوك البرنامج ككل، أو تتبع سلسلة من الأحداث الموزعة عبر الزمن والشبكة لتكوين صورة متكاملة عن حملة هجومية معقدة. هذه الآلية التحليلية "الشبيهة بالبشر" في الربط بين الوقائع المتباعدة، ولكن بأداء وسرعة فائقتين، هي ما يوفر الفعالية "غير المسبوقة" في ملاحقة التهديدات الناشئة قبل أن تتحول إلى خروقات أمنية كبرى.[2]

إجمالاً، لم يعد التحول في آليات الكشف والتحليل بفضل الذكاء الاصطناعي ترفًا تقنيًا، بل أصبح ضرورة استراتيجية. فهو يحوّل الأمن السيبراني من نموذج دفاعي تفاعلي، يلهث وراء التهديدات بعد وقوعها، إلى نموذج استباقي تنبؤي قادر على تمييز إشارات الخطر من بين مليارات نقاط البيانات. هذه الثورة التحليلية، التي تجسدت في الانتقال من التوقيع إلى السياق، ومن المعلوم إلى المجهول، تُعيد تعريف معايير الكفاءة والفعالية في مواجهة مشهد التهديدات المتغير باستمرار، وتؤسس لمرحلة جديدة من التكيف والمرونة في الدفاع السيبراني.

الفرع الثاني: الأتمتة الذكية للاستجابة للحوادث

تمثل الأتمتة الذكية للاستجابة للحوادث نقلة نوعية في فلسفة الدفاع الإلكتروني، حيث لم يعد الذكاء الاصطناعي مجرد أداة مساعدة، بل أصبح حجر الزاوية في مواجهة التهديدات الإلكترونية المتسارعة والتعقيدة.

تتيح هذه الأنظمة تحويل المهام التشغيلية المتكررة والمعقدة إلى عمليات آلية ذكية، مما يرفع من كفاءة وفاعلية فرق الأمن السيبراني ويحولها من وضعية التفاعل مع الحوادث بعد وقوعها إلى موقع الاستباق والاحتواء الفوري، ويمكن إبراز هذا الدور من خلال النقطتين التاليتين:

أولا: التنسيق الآلي للعمليات (Security Orchestration) وتحسين زمن الاستجابة

تقوم الأتمتة الذكية على مبدأ "التنسيق الآلي" (Orchestration)، والذي يعني تكامل وتنسيق عمل الأدوات الأمنية المنفصلة – مثل أنظمة كشف التسلل (IDS)، وجدران الحماية (Firewalls)، ومنصات إدارة المعلومات والأحداث الأمنية (SIEM) – ضمن سير عمل (Workflow) موحد وآلي. يؤدي هذا التكامل إلى سد الفجوات التشغيلية والقضاء على "صرامة السياق" (Context Switches) التي يعاني منها المحلل البشري عند الانتقال بين واجهات أدوات متعددة.

فعلياً، عند حدوث حادث أمني، يستطيع نظام الأتمتة الذكية، من خلال واجهات برمجة التطبيقات (APIs)، أن يجمع تلقائياً بين مؤشر الخطر من نظام كشف التسلل، وسجلات التصفح المشبوهة من منصة SIEM، ليصدر أمراً آلياً إلى جدار الحماية بحظر عنوان IP مصدر الهجوم، كل ذلك في غضون ثوانٍ معدودة. هذه العملية، التي قد تستغرق دقائق أو ساعات

[1] - LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

[2] – البقمي، منصور بن عبد العزيز. (2022). التعلم العميق في تحليل السلوك السيبراني للكشف عن التهديدات المستعصية. رسالة دكتوراه غير منشورة، جامعة الملك فهد للبترول والمعادن.

إذا أُنجزت يدوياً، تُنجز آلياً بمعدل أسرع وبدرجة أعلى من الدقة، مما يحد بشكل كبير من "زمن الاحتواء" (Containment Time) وهو العامل الحاسم في تقليل الأضرار الناجمة عن الهجوم.[1]

ثانيا: التحليل الذكي للحوادث (Intelligent Analysis) والاستجابة الاستباقية

لا تقتصر الأتمتة الذكية على آلية التنفيذ فحسب، بل تمتد إلى "الذكاء" في التحليل واتخاذ القرار. حيث تُستغل تقنيات الذكاء الاصطناعي والتعلم الآلي (Machine Learning) لتحليل كميات هائلة من بيانات الحوادث والتهديدات، وتحديد الأنماط الخفية والروابط بين الحوادث المنفصلة التي قد تعجز العين البشرية عن إدراكها.

باستخدام نماذج التعلم الآلي المدربة على بيانات تاريخية، يمكن للنظام أن يصنف الحوادث تلقائياً حسب درجة خطورتها، ويميز بين الهجمات الحقيقية والإنذارات الكاذبة (False Positives)، بل ويتنبأ بمسارات الهجوم المحتملة[2] هذه القدرات التحليلية المتقدمة تمكن النظام من الانتقال من رد الفعل إلى الاستباق. على سبيل المثال، عند رصد سلوك غير طبيعي لجهاز ضمن الشبكة، يمكن للنظام لا أن يحجبه فحسب، بل وأن يفحص جميع الأجهزة التي أظهرت سلوكاً مشابهاً ويطبق عليها إجراءات وقائية مسبقة، مما يعطل حملة هجومية شاملة قبل أن تصل إلى ذروتها. وبذلك، لا تُختصر الأتمتة الذكية في التسريع الآلي للعمليات[3]، بل في إضافة طبقة من الذكاء الاستدلالي تجعل الاستجابة للحوادث أكثر ذكاءً ودقة واستباقية.

المطلب الثاني: التحديات والتهديدات السيبرانية المعاصرة

تمثل الفضاءات السيبرانية في العصر الراهن بيئة حيوية للمجتمعات والدول، ولكنها في الوقت نفسه تشكل حلبة لعدد متزايد من التحديات والتهديدات المعقدة التي تطورت بتسارع يوازي التطور التقني نفسه. لم تعد هذه التهديدات مقتصرة على الهجمات الفردية، بل تحولت إلى ظواهر منهجية تنطوي على أبعاد استراتيجية تمس الأمن القومي والاستقرار الاقتصادي والنسيج الاجتماعي، يتناول هذا المبحث بالتحليل أبرز هذه التحديات مصنفة وفق طبيعتها وأطرافها الفاعلة.

تشهد البيئة السيبرانية تصاعداً ملحوظاً في حدة التهديدات التي تنفذها دول أو كيانات مدعومة منها، مما حول الفضاء الإلكتروني إلى ساحة جديدة للتنافس الجيوسياسي.

الفرع الأول: تطور أنماط الهجمات الإلكترونية

تشهد الساحة السيبرانية تحولاً جوهرياً، لم يعد يقتصر على مجرد تطور تقني، بل أصبح ظاهرة استراتيجية معقدة تطال أمن الدول والمجتمعات على حد سواء، فقد تطورت التهديدات من أعمال فردية محدودة التأثير إلى هجمات منظمة ومنسقة، تُنفذ

[1] – فهد عبد الله الرشيد، الأمن السيبراني: المفاهيم والتطبيقات المتقدمة، (الرياض: دار جامعة الملك سعود للنشر، 2021)، ص 245.

[2] – محمد أمين السعيد، "دور الذكاء الاصطناعي في مواجهة الهجمات الإلكترونية متعددة المراحل"، المجلة الدولية للدراسات الأمنية، المجلد 8، العدد 2 (2022)، ص 118.

[3] – لينا محمود أحمد، "تأثير أنظمة الأتمتة الذكية SOAR على كفاءة مراكز العمليات الأمنية: دراسة تطبيقية"، مجلة آفاق الأمن المعلوماتي، المجلد 5، العدد 1 (2023)، ص 76.

بوسائل وأدوات متطورة، تستهدف البنى التحتية الحيوية والنظم المالية وحتى الاستقرار الاجتماعي والسياسي للدول. ويناقش هذا الفرع التطور النوعي للهجمات الإلكترونية أولا، كما يحلل الإطار القانوني لتصنيف هذه الأنماط ثانيا.

أولاً: التطور النوعي والتصنيفي للهجمات الإلكترونية

لم تعد الهجمات الإلكترونية حكراً على مجرمين أفراد يسعون لتحقيق مكاسب مادية سريعة، بل تجاوزت ذلك لتصبح أداة لفاعلين دولة وغير دولة، تتنوع دوافعهم بين السياسية والاقتصادية والعسكرية. ويمكن تصنيف هذا التطور في الأنماط الهجومية على النحو التالي:

1-من الجريمة الإلكترونية التقليدية إلى الجريمة الإلكترونية المنظمة: لقد شهدت الجريمة الإلكترونية قفزة نوعية من هجمات بسيطة مثل التصيد الاحتيالي (Phishing) وبرامج الفدية (Ransomware) الفردية، إلى عمليات إجرامية منظمة عابرة للحدود. تعمل هذه الشبكات بطريقة تشبه الشركات متعددة الجنسيات، متخصصة في تقديم خدمات القرصنة كخدمة (Hacking as a Service)، مما يوسع دائرة المخاطر ويجعل أدوات الهجوم متاحة لفاعلين أقل مهارةً[1]، وأصبحت الهجمات تستهدف بشكل منهجي قطاعات حيوية مثل الصحة والطاقة والخدمات المالية، مما يسبب خسائر اقتصادية فادحة ويعطل تقديم الخدمات الأساسية للمواطنين[2].

2-صعود حروب الشائعات والتأثير النفسي: يمثل هذا النمط تحدياً وجودياً للدول، فهو لا يستهدف الأنظمة التقنية بقدر ما يستهدف العقل الجمعي والمجال العام للمجتمع، من خلال استغلال منصات التواصل الاجتماعي وتقنيات التزييف العميق (Deepfakes)، يقوم الفاعلون الخصوم بنشر حملات منظمة للتضليل الإعلامي، تهدف إلى تقويض الثقة في المؤسسات الرسمية، وخلق حالة من الاستقطاب والفتنة الداخلية، والتأثير على نتائج الانتخابات[3].

هذه الهجمات، التي غالباً ما تكون ذات طابع "هجين"، تندرج تحت ما يعرف بـ "حروب ما بعد الحقيقة"، حيث يصبح فيها التلاعب بالتصورات وسيلة حرب أكثر فعالية من الأسلحة التقليدية في كثير من الأحيان.

3-تطور أدوات التجسس الإلكتروني والاستخباراتية: تحول التجسس الإلكتروني من مجرد سرقة بيانات إلى عمليات استخباراتية استباقية ومعقدة. لم يعد يقتصر على اختراق الشبكات لسرقة المعلومات، بل يتعداه إلى عمليات "الهجوم الصامت" (Low and Slow Attacks) التي تهدف إلى التسلل والبقاء لفترات طويلة داخل الشبكات المستهدفة لجمع معلومات استخباراتية حساسة أو وضع أبواب خلفية (Backdoors) لاستخدامها في هجمات مستقبلية[4]. كما برزت ظاهرة "التجسس

---

[1]- أحمد محمد السيد، "الجريمة الإلكترونية المنظمة: الطبيعة والإطار القانوني"، مجلة الأمن السيبراني، العدد 5، (2022)، ص 45.

[2]- تقرير البنك الدولي، "التكلفة الاقتصادية للجريمة الإلكترونية في المنطقة العربية"، (واشنطن: 2023)، ص 12.

[3]- فاطمة الزهراء عبد الرحمن، "حروب الشائعات في الفضاء السيبراني: دراسة في آليات المواجهة"، مجلة الدراسات الإعلامية والأمنية، المجلد 10، العدد 1، (2021)، ص 78.

[4]- معهد الأمن السيبراني الدولي، "تقرير التهديدات السيبرانية العالمية 2024"، (لندن: 2024)، ص 23.

الاقتصادي"، حيث تستهدف الهجمات مراكز الأبحاث والشركات المتقدمة تقنياً لسرقة حقوق الملكية الفكرية والأسرار التجارية، مما يؤثر على الميزان التنافسي الاقتصادي بين الدول.

ثانياً: الإطار القانوني لتصنيف أنماط الهجمات الإلكترونية

يطرح التطور السابق للهجمات تحديات جسيمة أمام القانون الوطني والدولي، مما استدعى تطوير أطر قانونية لتكييف هذه الأفعال وتصنيفها تمهيداً للمساءلة عنها. وينقسم هذا الإطار إلى مستويين:

1-التكييف القانوني على المستوى الوطني: تسعى معظم الدول إلى سن تشريعات وطنية لمكافحة الجريمة الإلكترونية، تحاول من خلالها مواكبة هذه الأنماط المتطورة. فتم تعريف الأفعال المجرمة لتشمل الوصول غير المشروع، الاعتداء على سلامة البيانات، والابتزاز الإلكتروني، والتجسس الاقتصادي[1]، كما تعمل الدول على تجريم أفعال نشر الشائعات والتضليل الإعلامي عندما تهدد الأمن الوطني أو النظام العام، مستندة في ذلك إلى قوانين العقوبات العامة أو تشريعات مكافحة الجريمة الإلكترونية[2]. ومع ذلك، تبقى التحديات قائمة، خاصة فيما يتعلق بتحديد نطاق الاختصاص القضائي في الجرائم العابرة للحدود، وصعوبة جمع الأدلة الرقمية وتقديمها أمام القضاء، والحفاظ على التوازن بين متطلبات الأمن واحترام حقوق الإنسان وخصوصية الأفراد.

2-التصنيف في إطار القانون الدولي: على المستوى الدولي، لا يزال هناك جدل فقهي وقانوني حول كيفية تطبيق قواعد القانون الدولي، ولا سيما قانون استخدام القوة (Jus ad Bellum) والقانون الدولي الإنساني(Jus in Bello) ، على الفضاء السيبراني. المحاولة الأبرز في هذا الصدد جاءت من خلال "إطار التصنيف" الذي وضعته مجموعة الخبراء الحكوميين التابعة للأمم المتحدة، والذي يميز بين عدة مستويات للأنشطة العدائية في الفضاء السيبراني[3]:

-أنشطة الجريمة الإلكترونية: وهي تخضع أساساً للقوانين الوطنية ومعاهدات التعاون القضائي.

- أنشطة التجسس الإلكتروني: والتي تعتبرها معظم الدول ممارسة سيادية غير محظورة طالما لم ترقى إلى مستوى "استخدام القوة".

-أنشطة تصل إلى حد "استخدام القوة" (Use of Force): وهي الهجمات الإلكترونية ذات العواقب الوخيمة والمماثلة في تأثيرها للقوة العسكرية التقليدية، والتي قد تبرر للدولة اللجوء إلى حق الدفاع الشرعي وفقاً للمادة 51 من ميثاق الأمم المتحدة.

---

[1] - المادة (3) من قانون مكافحة الجرائم الإلكترونية الأردني رقم (15) لسنة 2019.

[2] - المادة (7) من نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية.

[3] - United Nations General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/76/135, (2021), para 13.

– **أنشطة تصل إلى حد "استخدام القوة** :(**Use of Force**) "وهي الهجمات الإلكترونية ذات العواقب الوخيمة والمماثلة في تأثيرها للقوة العسكرية التقليدية، والتي قد تبرر للدولة اللجوء إلى حق الدفاع الشرعي وفقاً للمادة 51 من ميثاق الأمم المتحدة.

– **الهجمات الإلكترونية خلال النزاعات المسلحة**: والتي تخضع عند تطبيقها للقانون الدولي الإنساني، مما يفرض التمييز بين الأهداف العسكرية والمدنية، وتحريم الهجمات العشوائية أو التي تسبب أضراراً.[1]

الفرع الثاني: التحديات المرتبطة بالذكاء الاصطناعي

يواجه استخدام الذكاء الاصطناعي في الأمن السيبراني جملة من التحديات الجوهرية التي تهدد بتحويله من أداة لحماية الفضاء الإلكتروني إلى مصدر للمخاطر والمشكلات القانونية والأخلاقية. ويمكن تقسيم هذه التحديات على النحو التالي:

أولاً: التحديات القانونية والأخلاقية

تتمثل أبرز التحديات في هذا الإطار في الإشكاليات المتعلقة بالخصوصية والتحيز الخوارزمي، والتي تثير تساؤلات عميقة حول مدى توافق تقنيات الذكاء الاصطناعي مع الأطر القانونية والقيم الأخلاقية.

1– إشكاليات الخصوصية وحماية البيانات:

يؤدي الاعتماد على الذكاء الاصطناعي في الأمن السيبراني، خاصة في مجال التحليلات التنبؤية والكشف عن التهديدات، إلى معالجة كميات هائلة من البيانات الشخصية والحساسة، مما يثير إشكاليات قانونية عميقة تتعلق بالخصوصية[2]. فتقنيات مثل التعلم الآلي تتطلب تغذيتها ببيانات ضخمة – بما في ذلك البيانات الشخصية – لتدريب النماذج وتحسين دقتها. هذا يجعل عملية جمع البيانات ومعالجتها وتخزينها تتعارض مع مبدأي الحد الأدنى من البيانات والغرض المحدد اللذين تنص عليهما تشريعات حماية البيانات مثل النظام الأوروبي العام لحماية البيانات[3]. كما أن استخدام تقنيات المراقبة الاستباقية التي تعتمد على الذكاء الاصطناعي، مثل تحليل أنماط السلوك للكشف عن الأنشطة الخبيثة، يخلق حالة من المراقبة الدائمة التي تهدد الحريات الفردية وتخلق "مجتمع مراقبة" رقمي، مما يستدعي إعادة النظر في الأطر القانونية المنظمة لعمليات المراقبة الإلكترونية لضمان تحقيق التوازن بين مقتضيات الأمن واحترام الحق في الخصوصية[4].

2– تحدي التحيز الخوارزمي والتمييز:

---

[1]– البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1977، المادة 48 (مبدأ التمييز) والمادة 51 (حظر الهجمات العشوائية).

[2]– المادة 12 من الإعلان العالمي لحقوق الإنسان: "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه...". انظر أيضاً: المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية.

[3]– المادة 5(1) من النظام الأوروبي العام لحماية البيانات (GDPR) والتي تنص على مبادئ "الحد الأدنى من البيانات" و"تحديد الغرض".

[4]– عبد الله بن خليل الظاهري، "الحق في الخصوصية المعلوماتية في مواجهة تقنيات الذكاء الاصطناعي"، مجلة جامعة الشارقة للعلوم القانونية، المجلد 18، العدد 2، 2021، ص 45.

ينشأ التحيز في أنظمة الذكاء الاصطناعي المستخدمة في الأمن السيبراني من تحيز البيانات التي تُدرب عليها هذه الأنظمة، أو من تحيز الخوارزميات نفسها[1]. فعلى سبيل المثال، إذا تم تدريب نظام للكشف عن الهجمات الإلكترونية باستخدام بيانات غالبيتها من هجمات originating من مناطق جغرافية معينة، فقد يصبح النظام أكثر ميلاً لتصنيف الأنشطة القادمة من تلك المناطق على أنها خبيثة، حتى لو كانت مشروعة. هذا التحيز يؤدي إلى نتائج تمييزية، حيث قد يتم حرمان مستخدمين أبرياء من الخدمات أو وضعهم تحت المراقبة المكثفة بناءً على خلفياتهم أو مواقعهم فقط[2]، من الناحية القانونية، يثير هذا التحدي مسألة الامتثال لمبادئ المساواة وعدم التمييز المنصوص عليها في الدساتير والتشريعات الوطنية والمواثيق الدولية لحقوق الإنسان، كما يضعف شرعية القرارات الأمنية المتخذة بناءً على هذه الأنظمة ويقوض الثقة فيها.

ثانياً: التحديات التشغيلية والمساءلة القانونية

ترتبط هذه الفئة من التحديات بالتعقيد التقني الذاتي لأنظمة الذكاء الاصطناعي وآلية عملها، وما يترتب على ذلك من صعوبات في إخضاعها للمساءلة والفهم البشري.

1- إشكالية المساءلة والشفافية (مشكلة الصندوق الأسود)

تتمثل أحد أكبر العوائق القانونية أمام استخدام الذكاء الاصطناعي في الأمن السيبراني فيما يعرف بـ "مشكلة الصندوق الأسود"، حيث يصعب – بل وقد يستحيل – فهم كيفية وصول النماذج المعقدة، خاصة شبكات الأعصاب الاصطناعية العميقة، إلى قرار أو توصية معينة[3]. هذا الغياب للشفافية يخلق إشكالية قانونية جسيمة في تحديد المسؤولية عند وقوع خطأ، مثل عندما يفشل نظام في كشف هجوم إلكتروني أو عندما يصنف نشاطاً مشروعاً خطأً على أنه تهديد. فمن المسؤول عن الضرر الناتج؟ هل هو مطور الخوارزمية، أم مالك البيانات المستخدمة في التدريب، أم المستخدم النهائي للنظام؟[4] يصعب تطبيق قواعد المسؤولية التقليدية (المسؤولية التقصيرية والعقدية) في هذه الحالة بسبب استقلالية النظام وعدم القدرة على إثبات خطأ بشري محدد. مما يستدعي تطوير أطر قانونية جديدة، مثل مفهوم "المسؤولية الموضوعية" أو إنشاء صندوق تعويضات خاص، لتغطية الأضرار الناجمة عن أنظمة الذكاء الاصطناعي المستقلة[5].

2- التحديات التشغيلية والاعتماد المفرط

---

[1]- سارة مُحَمَّد العتيبي، "التحيز في الخوارزميات: دراسة في المسببات والآثار وآليات المواجهة"، مجلة البحوث القانونية والاقتصادية، المجلد 42، العدد 3، 2022، ص 112.

[2]- المادة 2 من الإعلان العالمي لحقوق الإنسان: "لكل إنسان حق التمتع بجميع الحقوق والحريات المذكورة في هذا الإعلان، دونما تمييز من أي نوع...".

[3]- أحمد قاسم الجوارنة، "مسؤولية الأضرار الناشئة عن الذكاء الاصطناعي: دراسة تحليلية في إطار القانون المدني"، مجلة العلوم القانونية، المجلد 55، العدد 1، 2023، ص 78.

[4]- فاطمة الزهراء بلعربي، "إشكالية تحديد المسؤولية المدنية عن أضرار الذكاء الاصطناعي"، مجلة القانون والأعمال، العدد 15، 2022، ص 34.

[5]- التقرير الصادر عن لجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال) حول المسؤولية المدنية عن أنظمة الذكاء الاصطناعي المستقلة، 2023.

من الناحية التشغيلية، يؤدي الاعتماد المفرط على أنظمة الذكاء الاصطناعي إلى إضعاف المهارات البشرية التحليلية في مجال الأمن السيبراني، مما يخلق "ثقافة الرضا الكاذب" حيث يعتمد المحللون بشكل أعمى على مخرجات النظام دون تمحيص نقدي. علاوة على ذلك، فإن هذه الأنظمة نفسها معرضة لهجمات خبيثة مصممة خصيصاً لخداعها، مثل هجمات "البيانات الخادعة" (Adversarial Attacks)، حيث يقوم المهاجمون بتعديل طفيف على بيانات الإدخال لتضليل النظام وجعله يتصرف بشكل خاطئ[1]، هذا يضعف الفعالية العامة للنظام ويخلق نقطة ضعف جديدة يمكن استغلالها، قانونياً، يثير هذا السؤال حول "واجب العناية" الملقى على عاتق مقدمي خدمات ومشغلي هذه الأنظمة في تأمينها وصيانتها بشكل مستمر ضد مثل هذه الهجمات المعروفة، والفشل في ذلك قد يترتب عليه مسؤوليتهم عن الأضرار الناجمة[2].

خاتمة:

خلاصة القول إن الذكاء الاصطناعي يمثل بالفعل رافعة استراتيجية ذات طابع ثنائي، تجسّد علاقة جدلية مع الأمن السيبراني، فمن جهة، يقدم إمكانات استباقية غير مسبوقة، تمكن من تحويل آليات الدفاع من النمط التفاعلي القائم على التوقيعات إلى النمط التنبؤي السياقي، مستفيداً من تقنيات التعلم الآلي والتعلم العميق في كشف الشذوذ والتهديدات الناشئة وتسريع عمليات الاستجابة للحوادث عبر الأتمتة الذكية، وهذا ما يجعله حليفاً لا غنى عنه في تعزيز المناعة الرقمية للدول.

غير أن هذه الإمكانات لا تخلو من مخاطر وتحديات جسيمة فالوجه الآخر للذكاء الاصطناعي يكمن في كونه أداة فتاكة في يد الجهات الخبيثة، يمكن تسخيرها لتطوير هجمات أكثر ذكاءً وتكيفاً، كالبرمجيات متعددة الأشكال وهجمات التصيد عالية التصديق والتزييف العميق، كما تبرز تحديات قانونية وأخلاقية ملحة، تتعلق بإشكاليات الخصوصية في ظل الحاجة الماسة للبيانات، وتحيز الخوارزميات، ومشكلة "الصندوق الأسود" التي تُضعف الشفافية وتُعقّد مسألة المساءلة القانونية.

وعلى مستوى التشريع المغربي، رغم امتلاكه إطاراً تشريعياً ومؤسسياً متيناً (كالقانون 05-20 والقانون 08-09 وهيئات مثل CNDP وANRT)، فإنه يواجه ذات التحديات العالمية المرتبطة بطبيعة هذه التقنية الثورية، مما يستدعي تبني نهج متكامل وشامل لا يقتصر على تطوير البنى التقنية فحسب، بل يمتد ليشمل مواكبة مستمرة للإطار التشريعي لسد الثغرات الجديدة، وبناء القدرات البشرية المتخصصة، ووضع سياسات واضحة لأخلاقيات الذكاء الاصطناعي.

[1] – خالد سليمان الرشيدي، "تهديدات الأمن السيبراني للذكاء الاصطناعي: هجمات البيانات الخادعة نموذجاً"، المؤتمر السعودي للأمن السيبراني، 2022، ص 5.

[2] – المادة 164 من النظام الأساسي للحكم في المملكة العربية السعودية (الصادر بالمرسوم الملكي رقم أ/٩١): "التقاضي مكفول للجميع...". مما يفترض وجود جهة مسؤولة يمكن مقاضاتها لتعويض الضرر.