The Role of Artificial Intelligence Technology in Achieving Cybersecurity Opportunities and Challenges[#]

Boukir Youssef[(1)*]

(1) Researcher, Faculty of Legal, Economic and Social Sciences, Sidi Mohamed Ben Abdellah University, - Fez.

Received: 1/2/2026
Accepted: 10/5/2026
Published: 23/7/2026

* *Corresponding Author:*
boukiryoussef587@gmail.com

DOI:
https://doi.org/10.59759/law.v5i2.1837

Abstract

Today, technology has become one of the most important tools for humanity—and indeed, an established reality in the contemporary world. Humanity can by no means live isolated from the digital world; without a doubt, we now live in a world dominated by the latest technologies in the telecommunications and information technology sector. Although artificial intelligence provides humanity with significant opportunities, it simultaneously poses a threat by contributing to the emergence of cyber threats and risks.

This requires working and focusing on building new skills for the digital future by utilizing artificial intelligence to enhance cybersecurity, in response to the emergence of cyber threats. These threats are considered dangerous phenomena that jeopardize national security and affect most vital sectors and critical infrastructure, without which human existence cannot continue.

Therefore, our paper aims to highlight the importance of using artificial intelligence to achieve and enhance cybersecurity, while primarily emphasizing the risks resulting from the use of AI applications. This necessitates exploring the best methods and strategies to mitigate the dangers of these threats.

[#] A special issue for the Third International Conference, entitled: **Artificial Intelligence, A Legal Vision Towards a Sustainable Future**.

Thus, after employing the descriptive-analytical approach and the inductive approach—as they are methodologies that align with our study's topic—the study concluded that AI applications are capable of predicting and countering cyber threats. This is achieved by training personnel and frameworks equipped to provide the necessary protection for the cyber infrastructure, given that the number of qualified professionals in the field is highly limited.
Keywords: Artificial Intelligence, Cybersecurity, Information Technology, Opportunities, Risks.
□

دور تكنولوجيا الذكاء الاصطناعي في تحقيق الأمن السيبراني
-الفرص والتحديات-

يوسف بوكير (1)

(1) باحث، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة سيدي محمد بن عبد الله، فاس.

ملخص

لقد باتت التكنولوجيا في وقتنا الراهن إحدى الوسائل الهامة للإنسانية بل أضحت حقيقة قائمة في العالم المعاصر، إذ لا يمكن بأي حال من الأحوال أن تعيش الإنسانية بمعزل عن العالم الرقمي، فبدون شك أصبحنا نعيش في عالم تهيمن عليه أحدث التقنيات الحديثة في قطاع الاتصالات وتكنولوجيا المعلومات، فعلى الرغم من إسهام الذكاء الاصطناعي في منح الإنسانية فرصا لا يستهان بها، إلا أنه في نفس الوقت يشكل تهديدا لها جراء مساهمته في بروز التهديدات والمخاطر السيبرانية.

الأمر الذي يفرض العمل والتركيز على بناء مهارات جديدة للمستقبل الرقمي من خلال الاستعانة بالذكاء الاصطناعي بغية تحقيق وتعزيز الأمن السيبراني جراء بروز التهديدات السيبرانية التي تعتبر من الظواهر الخطيرة التي تهدد أمن الدول والتي تطال معظم القطاعات الحيوية والبنية التحتية الحيوية للدول والتي لا يمكن للفرد الإنساني أن يستمر وجوده في ظل غيابها.

لهذا، تهدف ورقتنا إلى تسليط الضوء على أهمية استخدام الذكاء الاصطناعي في تحقيق وتعزيز الأمن السيبراني، مع إبراز بالأساس المخاطر الناتجة عن استخدام تطبيقات الذكاء الاصطناعي، الأمر الذي يفرض البحث عن أفضل السبل والاستراتيجيات للحد من خطورة هذه التهديدات.

إذا، وبعد توظيفنا للمنهج الوصفي التحليلي وكذا المنهج الاستقرائي على اعتبار أنها مناهج تتناغم وموضوع دراستنا، فقد توصلت الدراسة إلى أن تطبيقات الذكاء الاصطناعي قادرة على التنبؤ بالمخاطر والتهديدات

السيبرانية مع التصدي لها من خلال تدريب طاقات وأطر قادرة على توفير الحماية اللازمة للبنية التحتية السيبرانية على اعتبار أن عدد المحترفين المؤهلين في المجال جد محدود.

الكلمات المفتاحية: الذكاء الاصطناعي – الأمن السيبراني – تكنولوجيا المعلومات – الفرص – المخاطر.

المقدمة.

لقد شهدت الإنسانية خلال العقد الأخير موجة انتشار واسعة لتكنولوجيا الأجهزة الحاسوبية والشبكة المعلوماتية، والتي أدت إلى بروز مجالا جديدا يسمى " بالفضاء السيبراني". فبالرغم من أن الفضاء السيبراني يتميز بأخلاقيات ساهمت في تقدم الإنسانية من خلال الانفتاح الثقافي أو عن طريق محاولة التقليل من ظاهرة الأمية أو من خلال نشر المعلومة على وجه السرعة، إلا أن أخلاقيات الفضاء السيبراني أثارت نقاشا لكون الفضاء السيبراني مجالا بلا قيود خاصة وأنه لا يؤمن بالحواجز الجيوسياسية. لهذا تتاح للدول بل وحتى للفواعل من غير الدول فرصة الوصول إليه، بحيث يمكن أن ينشأ داخل هذا الميدان سيناريو النزاع المسلح وقيام الدول أو الأفراد بعملياتهم السيبرانية مما يجعل المدنيين يتعرضون لأضراره ويدفعون أفدح ثمن خاصة إذا تعلق الأمر باستهداف البنية التحتية الحيوية بهجمات سيبرانية[1]، لهذا تسعى العديد من الدول لمواجهة التحديات المتزايدة في الفضاء الرقمي من خلال تعزيز الأمن السيبراني والتي تلعب دورا كبيرا في حماية البيانات وخصوصية الإنسان من أخطار الهجمات السيبرانية.

أولا: الإطار العام للموضوع

تعود نشأة الأمن السيبراني إلى سبعينيات القرن الماضي، بعد أن ابتكر باحث يدعى "بوب توماس" برنامجا على الكومبيوتر يسمى « Creeper »، حيث ينتقل هذا البرنامج عبر شبكة « Arpanet » تاركا خلفه مسار تحركاته. أنشأ مخترع البريد الإلكتروني " توملينسون" برنامجا يسمى « Reaper » ويعد أول برنامج لمكافحة الفيروسات، لقد ظهرت برامج مضادات الفيروسات بالإنجليزية «Antivirus » كتجربة أولى عام 1987. يبدو أن جهود الأمن السيبراني في محاولة وقف هجمات التدمير والتخريب التي ما زالت تتطور وتتسع، والسبب في ذلك تطور قراصنة الإنترنت باستمرار.

لأجل ذلك، ينبغي على الخبراء والمتخصصين في المجال توجيه جهودهم للاستفادة من أحدث التقنيات المتوفرة للتقليل من حجم خطورة تلك الهجمات، ولتفادي الآثار التي قد تحصل في حال

نجحت أي واحدة من تلك الهجمات. تتجسد الجهود الحالية لمعظم الشركات والمؤسسات في محاولة دمج الذكاء الاصطناعي في عمليات مكافحة هجمات الفيروسات، من خلال إنشاء جدار أمني عالي المستوى والكفاءة للتقليل من الآثار الكارثية لأي هجمة إلكترونية، مثل قفل نظام المستخدمين لمنع أي عملية لسرقة البيانات[2].

ثانيا: أهمية الموضوع

تبرز أهمية الموضوع في ظل تصاعد الهجمات السيبرانية بين الدول عل نحو متزايد، الأمر الذي يفرض على الدول البحث عن كيفية مجابهة هذا النوع من الحروب وتحصين فضاءها السيبراني وتحقيق أمنها السيبراني، كما ترنو الدراسة إلى التعرف على تكنولوجيا المعلومات ودورها في تطوير استراتيجيات ترتكز بالأساس على الأساليب الحديثة بغية التصدي لأي هجمة سيبرانية متوقعة في المستقبل، كما تسعى الدراسة من زاوية أخرى، إلى الوقوف عند الدور الذي يمكن أن يلعبه الذكاء الاصطناعي في تحقيق الأمن السيبراني، مع رصد أهم المخاطر التي تؤثر على الحق في الخصوصية وحماية المعطيات الشخصية.

ثالثا: الإشكالية

يلعب الذكاء الاصطناعي دورا مهما في تعزيز الأمن السيبراني، وبالتالي فإن الإشكالية الجوهرية للموضوع ستتكب حول مدى قياس نجاعة استخدام الذكاء الاصطناعي في تعزيز وتحسين الأمن السيبراني.

وتتفرع عن هذه الإشكالية الرئيسية جملة من التساؤلات الفرعية التي تتفاوت فيما بينها:

- ما المقصود بالأمن السيبراني؟
- أين تبرز أهمية الأمن السيبراني؟ وما أبعاده؟
- ما مجالات استخدام الذكاء الاصطناعي في تحقيق الأمن السيبراني؟
- وما المخاطر الناتجة عن استخدام تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني؟

رابعا: فرضيات الدراسة

لتفكيك الإشكالية المثارة أعلاه، تنطلق الدراسة من كون الذكاء الاصطناعي يقوم بمهام على درجة كبيرة من الأهمية في حماية البيانات الحساسة المرتبطة بالأفراد في ظل تنامي التهديدات

السيبرانية، إذ تعتمد هذه التقنيات على آليات متطورة. لكن في مقابل ذلك، تفترض الدراسة أن الوعي بخطورة التهديدات السيبرانية كافية لتجنيب البشرية من الحوادث السيبرانية وحماية أنظمتها وبياناتها.

خامسا: مناهج الدراسة

إن بناء أي دراسة علمية تحتاج إلى منهج يكون قادرا على تغطية عناصر البحث، لهذا فقد رأينا من الأنسب توزيع دراستنا على **المنهج الوصفي التحليلي** وكذا **المنهج الاستقرائي** حتى يتسنى لنا دراسة الظاهرة موضوع البحث دراسة تحليلية، وكذا تحديد المتطلبات التي يمكن من خلالها حماية الفضاء السيبراني من المخاطر السيبرانية.

سادسا: خطة الدراسة

نظرا لتعدد الجوانب التي تحيط بموضوع دراستنا، فقد ارتأينا توزيعها على الشكل التالي:

المطلب الأول: مفهوم الأمن السيبراني وأبعاده.

المطلب الثاني: دور الذكاء الاصطناعي في تعزيز الأمن السيبراني ومخاطره.

المطلب الأول: مفهوم الأمن السيبراني وأبعاده

يعد الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات، ونتيجة لأهمية الأمن السيبراني اليوم فقد جعلته العديد من الدول على رأس أولوياتها خاصة بعد بروز حروب جديدة تتمثل في الحروب الإلكترونية[3].

الفقرة الأولى: تعريف الأمن السيبراني

يقصد بالأمن السيبراني، حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات ويشار إليها « ICT » اختصارا لمصطلح « Information and communication technologies »، فالأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية وذلك من خلال مجموعة من الوسائل المستخدمة تقنيا وتنظيميا وإداريا في منع الوصول غير المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية ونظامية، وبذلك

فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصية وسرية من خلال اتباع التدابير والإجراءات اللازمة لحماية البيانات[4].

بينما عرفه « Edward amorso »، وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها[5]، ووفقا للتقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام 2010– 2011، عرف الأمن السيبراني بأنه: مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين[6].

الفقرة الثانية: أبعاد الأمن السيبراني

يطال الأمن السيبراني العديد من الأبعاد التي تسعى إلى محاولة التصدي للتهديدات السيبرانية والتي هي كالآتي:

- **البعد العسكري:** يكمن في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يسمح بتبادل المعلومات والأوامر وتدفقها، وهي الفكرة التي خلقت وطورت من أجلها الشبكات ومن بعدها الإنترنت وإصابة الأهداف عن بعد، إلا أنها تمثل كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيدا من الاختراق الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة " كالطائرات بدون طيار"، ويعد فيروس ستاكسنت » Stuxnet » بداية الاستعمال للقوة السيبرانية لتدمير البنية المادية وكذا مهاجمة حواسيب الطرد المركزي الإيراني[7].
- **البعد الاقتصادي:** نظرا لاستخدام أجهزة الكومبيوتر لتشغيل الصناعات وتنميتها ودفع الاقتصاد، سيصبح الإنترنت أساس التجارة والتمويل والمعاملات المالية، وكلها مرتبطة ببعضها البعض من خلال شبكات الكومبيوتر لتحقيق الأمن السيبراني خصوصا ما تعلق بالقطاع المالي[8].
- **البعد الاجتماعي:** تسمح طبيعة الإنترنت المفتوحة عبر الشبكات الاجتماعية بشكل خاص لكل مواطن، بأن يعبر عن تطلعاته السياسية وطموحاته الاجتماعية بأشكالها كافة، كذلك تشكل مشاركة جميع شرائح المجتمع ومكوناته وسيلة لإثراء هذا المجتمع وتطويره، بما تتيحه من فرص للاطلاع على الأفكار، والمعلومات المختلفة، إذ تكون حاجة الجميع في الحفاظ على استقرار

الفضاء السيبراني والمجتمع الذي يرتكز إليه. والمعلوم أن انفتاح مجتمع ما على مجتمع آخر، يؤسس لتبادل خبرات وأفكار، وتكون حاجات جديدة وآفاق تعاون وتكامل[9].

- **البعد القانوني:** إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع تشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان إلى الإطار القانوني الصارم للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها.[10]

المطلب الثاني: دور الذكاء الاصطناعي في تعزيز الأمن السيبراني ومخاطره

لقد أضحى توفير الأمن السيبراني مطلوبا على مستوى فردي بغرض حماية البيانات الشخصية وأيضا على مستوى جماعي بغية حماية أمن الدولة الإلكترونية وشبكاتها المالية والاقتصادية والعسكرية والتلفزيونية والإذاعية من الهجمات السيبرانية والقرصنة التي تنجم عنها خسائر تكلف الأفراد والشركات والدولة عشرات المليارات من الدولارات كل عام. ومن المتوقع، حسب المؤشر العالمي، تعرف التكلفة المقدرة للجرائم السيبرانية في سوق الأمن السيبراني ارتفاعا متزايدا بين عامي 2023 و2028 ليصل قدرها إلى 13.82 تريليون دولار أمريكي عام 2028. ولذلك لجأت جل الدول والشركات العالمية إلى تطوير أقسام جديدة متخصصة في الأمن السيبراني، سعيا منها لامتلاك قوة سيبرانية[11].

لهذا، سنحاول أن نسلط الضوء على الدور الذي يلعبه الذكاء الاصطناعي في تعزيز وتحقيق الأمن السيبراني في " الفقرة الأولى"، على أن نتطرق في " الفقرة الثانية " لمخاطر استخدام الذكاء الاصطناعي في الأمن السيبراني.

الفقرة الأولى: وظائف الذكاء الاصطناعي في تحقيق الأمن السيبراني

تتعدد وظائف الذكاء الاصطناعي في تحقيق الأمن السيبراني من خلال ما يلي:

أولا: التعامل مع كم هائل من البيانات

يعد وصول تطبيقات الذكاء الاصطناعي للبيانات الحساسة أمرا على درجة كبيرة من الأهمية بالنسبة للاقتصاد الرقمي[12]، فالفضاء الإلكتروني يتيح سيلا هائلا من البيانات والمعلومات المتدفقة حول العالم، وهي تلك المعلومات التي لا تقتصر على وجهة نظر الرسمية، بل تتعداها لتشمل دور

الأفراد في إنتاج المعلومات والترويج لها عبر الإنترنت، والتي كان لها دور كبير في تصاعد حجم المكاسب العالمية حيث بلغ عدد مستخدمي الإنترنت عالميا 58.3 مليون نسمة من إجمالي5.7 مليار، أضف إلى ذلك الملايين من مستخدمي الهواتف الذكية. ومستخدمي شبكات التواصل الاجتماعي ومحركات البحث ومواقع التجارة الإلكترونية. كل ذلك وغيره يلعب دورا كبيرا في جمع البيانات الشخصية، وتحليل هذه البيانات اعتمادا على برامج متقدمة في تحليل وتصنيف المحتوى وتطبيقات الذكاء الاصطناعي[13]. فالذكاء الاصطناعي يعد الخيار المثلى لاكتشاف المخاطر المحتملة التي تنشأ خلال الأنشطة اليومية ونقل البيانات، بفضل قدرته على مراقبة حركة المرور وتحليل نشاط الخادم بدقة وتحديد المخاطر المحتملة بشكل تلقائي[14].

ثانيا: تقليص وقت اكتشاف التهديد

يعد اكتشاف التهديدات بسرعة أمرا بالغ الأهمية، حيث أبلغ 42 في المائة من المنظمات عن زيادة في التهديدات الحساسة للوقت، والناس بطيؤون في تبنيها وهم دون المستوى الأمثل، ومن ناحية أخرى، يمكن للذكاء الاصطناعي فحص كميات كبيرة من البيانات في وقت واحد لاكتشاف التهديدات السيبرانية، وبالتالي تسهيل الأمن، وقد أفادت 56 في المائة من المؤسسات أنها غارقة في ملف تعريف التهديدات الذي يواجه المحللين السيبرانيين، إذ أفاد 23 في المائة منهم بأنهم غير قادرين على التحقق بشكل فعال من التهديدات المحددة[15].

ثالثا: توقع التهديدات المستقبلية

أمام تزايد اهتمام الإنسانية بتطبيقات الذكاء الاصطناعي، فقد أشارت دراسة صادرة عن معهد ماكينزي « Mckinsey global institute research » بحلول عام 2030 يتوقع أن يحقق الذكاء الاصطناعي إنتاجا اقتصاديا عالميا قدره 13 تريليون دولار سنويا[16]، فكمية البيانات التي يتعامل معها محللو الأمن السيبراني تحديا صعبا في التنبؤ بالتهديدات المستقبلية، إلا أن الذكاء الاصطناعي يستطيع معالجة حجما كبيرا من البيانات في وقت واحد، مما يمكن الكشف عن الأنشطة الضارة بفضل تحديد الإجراءات الوقائية والتهديدات المحتملة، إذ يمكن التقليل من الوقت المهدور والموارد البشرية، ويساعد البقاء يقظا من خلال اتخاذ الخطوات لحماية المؤسسة[17].

رابعا: دور الذكاء الاصطناعي في التصدي لفيروس كوفيد 19

لقد أكدت تجربة وباء كوفيد 19 أن الروبوت قادر على القيام بالعديد من المهام أثناء الأزمات كالكشف المبكر عن الوباء أو من خلال تحديد الأشخاص الذين يعانون من أعراض

الوباء، هذا وقد صرح السيد «Carol lago » وهو مستشار بقسم التطوير Grant Thornton » «يعتمد على استخدام الشبكات العصبية في تشخيص حالات المرضى وتوفير لهم مستوى كاف من الخدمة الصحية.[18]

الفقرة الثانية: مخاطر الذكاء الاصطناعي في علاقته بالأمن السيبراني

يصحب استخدام الذكاء الاصطناعي في علاقته بالأمن السيبراني العديد من التحديات التي سنحاول أن نقف عند أبرزها من خلال ما يلي:

أولا: مستقبل الأمن السيبراني مرتبط بالذكاء الاصطناعي

مع تزايد الهجمات الإلكترونية على المؤسسات والشركات في السنوات الأخيرة، أصبح واضحا أن الأسلوب الحالي للأمن السيبراني يعاني من ضعف في مواجهة التهديدات السيبرانية، وبعد الهجمات الأخيرة التي تمكن فيها قراصنة روس من اختراق عدد من الوكالات الحكومية الأمريكية، دعا العديد من الخبراء الأمنيين إلى إجراء تغيير جذري في استراتيجيات اكتشاف ومعالجة التهديدات الإلكترونية، بحيث يتم استبدال الاعتماد على مجموعات بيانات ثابتة بنماذج ذكاء اصطناعي مرنة قادرة على فهم السلوك الطبيعي وغير الطبيعي للموظفين[19].

في هذا الإطار، أشارت السيدة " أرتي بركار" نائبة رئيس القسم الأمني لشركة " أي بي ام"، إلى زيادة عدد الأجهزة المحمولة في مواقع العمل وتحول الشركات إلى استخدام تقنيات السحابة الإلكترونية، أدى إلى وجود عدد لا يحصى من الطرق للوصول إلى مساحات العمل الافتراضي وهو الأمر الذي يتيح فرص شن هجمات إلكترونية[20].

ثانيا: الذكاء الاصطناعي كبديل لكلمات المرور في حماية البيانات والحق في الخصوصية

يخلق الذكاء الاصطناعي تحديات جديدة للقانون الدولي لحقوق الإنسان، بل ويشكل خطرا على الحرية والحق في الخصوصية، فجعل البيانات العلمية مفتوحة للجميع ينتج عنه مخاطر جديدة تتعلق بسيادة الدول على البيانات، وهو أحد أساب الصراع بين الصين والولايات المتحدة الأمريكية حيث اتهم الرئيس الأمريكي دونالد ترامب وإدارته الصين بالفشل في مشاركة بياناتها بشفافية مع دول أخرى[21]، فحسب اعتقاد " أرتي بركار" إذا أراد قراصنة الإنترنت اختراق فقاعة الذكاء الاصطناعي التي تحمي المستخدم فلن تكون مراقبة عاداته الرقمية كافية وحدها ، بل سيحتاجون أيضا إلى مراقبة تحركات هذا المستخدم لمعرفة أدق خصوصياته. وأوضحت أن الذكاء

الاصطناعي ليست تقنية جامدة، فهو يتطور باستمرار وفق البيانات التي يتلقاها، ومن تم فإننا نحتاج إلى إجراء تحليلات لملايين التهديدات المحتملة التي تحدث كل يوم[22].

هذا، وقد اختتمت " بركار" مقالها بالقول إن العصر الذي كانت فيه الأجهزة الموثوقة وكلمات المرور التي تتكون من 14 حرف كافية لضمان الأمن قد انتهى، ويجب علينا التفكير بشكل جدي في الوصول إلى تقنيات قادرة على التكيف بسرعة، لأنه مثلما تتغير نماذج العمل على نحو متزايد تتغير كذلك التكتيكات التي يتبعها قراصنة الإنترنت لاختراقها[23].

خاتمة

يعد الذكاء الاصطناعي من أبرز مخرجات الثورة الصناعية الرابعة إذ حقق هذا الأخير نجاحات لم تستطع الإنسانية تحقيقها، فقد سارعت العديد من الدول إلى توظيف هذه التقنية في مجال الأمن السيبراني إلا أن مثل هذه التقنيات تحتاج إلى إطار قانوني ينظمها، إذ حان الوقت لتظافر جهود الدول بغرض مجابهة ومواجهة التهديدات السيبرانية التي تجتاح ليست الدول الضعيفة فحسب بل تمتد أيضا للدول التي تبسط سيطرتها على الفضاء السيبراني. فعلى الرغم من المكتسبات أو الفوائد التي تقدمها تطبيقات الذكاء الاصطناعي في هذا الخصوص إلا أن استخدامها يشكل من زاوية أخرى تحديات ومخاطر على الأمن السيبراني لا سيما فيما يتعلق ببيانات وخصوصية الإنسان.

لأجل ذلك، فقد توصلت دراستنا لبعض الملاحظات التي يمكن إجمالها فيما يلي:

- ضرورة سن تشريعات تساير التطوير السريع الذي تشهده تطبيقات الذكاء الاصطناعي.
- الاستفادة من تجارب الدول السباقة، كالصين والولايات المتحدة الأمريكية وسنغفورة.
- تأطير كوادر متخصصة في مجال الذكاء الاصطناعي ونشر ثقافته على نطاق واسع.
- التشجيع على استخدام الذكاء الاصطناعي والتحسيس بخطورة المس بخصوصية وبيانات الأفراد.

المصادر والمراجع المعتمدة

❖ **الكتب:**

- عادل عبد الصادق،" الإرهاب الإلكتروني: القوة في العلاقات الدولية – نمط جديد وتحديات مختلفة"، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، الطبعة الأولى 2009.
- عادل عبد الصادق،" الاقتصاد الرقمي – تحديات السيادة السيبرانية "، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، 2020.
- فاطمة رومات،" العلاقات الدولية وتحديات الذكاء الاصطناعي"، مكتبة الألفية، 2024.
- محمد فارس العمارات – إبراهيم الحمامصة،" الأمن السيبراني – المفهوم وتحديات العصر"، دار الخليج للنشر والتوزيع، الطبعة الأولى، 2022.

❖ **الأطروحات الجامعية:**

- طيب الهرمودي،" الأمن السيبراني وحماية الحياة الخاصة والمعطيات الشخصية بدولة الإمارات العربية المتحدة على ضوء الاتفاقيات الدولية والتشريعات الوطنية"، أطروحة لنيل الدكتوراه في القانون العام والعلوم السياسية، جامعة محمد الخامس – الرباط، كلية العلوم القانونية والاقتصادية والاجتماعية أكدال، 2024.
- المقالات العلمية:
- إسماعيل زروقة،" الفضاء السيبراني والتحول في مفاهيم القوة والصراع "، مجلة العوم القانونية والسياسية، المجلد 10، العدد 1، أفريل 2019.
- آسيا السبتي – عمر بوقريط،" دور الذكاء الاصطناعي في تحقيق الأمن السيبراني"، المجلة الدولية للبحوث القانونية والسياسية، المجلد 8، العدد 3، ديسمبر 2024.
- حسام محمد نبيل عبد الرؤوف مرسي،" الأمن السيبراني (ضرورته – متطلبات تحقيقه)، مجلة كلية الدراسات العليا، العدد24، مارس 2016.
- خليل سعيدي – مرزوق بن مهدي،" الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبراني"، دراسات في حقوق الإنسان، المجلد 6، العدد 1، جوان 2022.
- عبد القادر لشقر – إدريس عبادي،" الحماية القانونية للأمن السيبراني"، مجلة البوغاز للدراسات القانونية والقضائية، العدد 34، يونيو 2024.

- محمد دحماني،" الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني"، مجلة الفكر القانوني والسياسي، المجلد السابع، العدد الثاني، 2023.
- مني عبد الله السمحان،" متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، مجلة كلية التربية، جامعة المنصورة، العدد 111، يوليوز 2020.
- هاله سعد مجبل،" الذكاء الاصطناعي ودوره في إدارة مخاطر الأمن السيبراني"، جامعة كربلاء، كلية التربية للعلوم الإنسانية، 2024.

ثانيا: المراجع باللغة الأجنبية

❖ **Libros :**

- Robert walters – Marko novak, » Cyber security, artificial intelligence, data protection the law », Springer, 2021.
- Articlos cientificos y estudios :
- Paola tolavera miranda ," son los ciberataques un peligo inmiente del siglo 21 – la pertinencia de comunicacion politica para su estudio", Academia, 2018.
- Grant thornton, » perspectiva del covid 19 – tecnología e innovación contra el coronavirus », abril 2020.

الهوامش

1 فهي تشكل كل المرافق والخدمات والشبكات وأدوات تكنولوجيا المعلومات التي في حالة تدميرها أو توقفها عن العمل ستخلف آثارا على الإنسان وصحته ورفاهه الاقتصادي، بل وحتى أداء مؤسسات الدولة. لهذا نقترح بعض المؤسسات والشبكات التي تندرج ضمن قائمة البنية التحتية الحيوية مثل:

- شبكة المياه والمعالجة والتخزين.
- محطات توليد الطاقة.
- تكنولوجيا الاتصالات والمعلومات "ICT".
- قطاع الصحة.
- وسائل النقل بشتى أنواعه وكذا أنظمة التحكم في حركة المرور.
- النظام المالي والأجهزة البنكية.

للاطلاع أكثر ينظر:

Paola tolavera miranda ," son los ciberataques un peligo inmiente del siglo 21 – – la pertinencia de comunicacion politica para su estudio", Academia, 2018, P:6y7, Articulo publicado enlace: https://unam.academia.edu/PaolaTalaveraMiranda :2024 – 06 – 23، la hora: 12.45.

ومن جهة أخرى تعرفها اللجنة الأمريكية للبنية التحتية الحيوية بأنها:" شبكات مستقلة يعود ملكية معظمها في الدول المتقدمة للقطاع الخاص وتتضمن النظم والعمليات التي تعمل بصورة مترابطة ومنتظمة لضمان تقديم وتوزيع الخدمات والسلع الأساسية، فالبنية التحتية عبارة عن إطار من الشبكات المستقلة والنظم المتوافقة من عمل الصناعات والمؤسسات وتوزيع القدرات الخاصة بتدفق السلع والخدمات الأساسية اللازمة لتحقيق الأمن الاقتصادي والقدرة على الدفاع.

- للاطلاع أكثر ينظر: عادل عبد الصادق،" الإرهاب الإلكتروني: القوة في العلاقات الدولية – نمط جديد وتحديات مختلفة"، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، الطبعة الأولى 2009، ص 375.

2 طيب الهرمودي،" الأمن السيبراني وحماية الحياة الخاصة والمعطيات الشخصية بدولة الإمارات العربية المتحدة على ضوء الاتفاقيات الدولية والتشريعات الوطنية"، أطروحة لنيل الدكتوراه في القانون العام والعلوم السياسية، جامعة محمد الخامس – الرباط، كلية العلوم القانونية والاقتصادية والاجتماعية أكدال، 2024، ص 47 وبعدها.

3 محمد فارس العمارات – إبراهيم الحمامصة،" الأمن السيبراني – المفهوم وتحديات العصر"، دار الخليج للنشر والتوزيع، الطبعة الأولى، 2022، ص 25.

4 مني عبد الله السمحان،" متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، مجلة كلية التربية، جامعة المنصورة، العدد 111، يوليوز 2020، ص9.

5 إسماعيل زروقة،" الفضاء السيبراني والتحول في مفاهيم القوة والصراع "، مجلة العوم القانونية والسياسية، المجلد 10، العدد 1، أفريل 2019، ص 1021.

6 مني عبد الله السمحان،" متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، مرجع سابق، ص 10.

7 محمد فارس العمارات – إبراهيم الحمامصة،" الأمن السيبراني – المفهوم وتحديات العصر"، مرجع سابق، ص 27.

8 محمد دحماني،" الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني"، مجلة الفكر القانوني والسياسي، المجلد السابع، العدد الثاني، 2023، ص 603.

9 حسام محمد نبيل عبد الرؤوف مرسي،" الأمن السيبراني (ضرورته – متطلبات تحقيقه)، مجلة كلية الدراسات العليا، العدد24، مارس 2016، ص 349.

10 إسماعيل زروقة،" الفضاء السيبراني والتحول في مفاهيم القوة والصراع "، مرجع سابق، ص 1023.

11 عبد القادر لشقر – إدريس عبادي،" الحماية القانونية للأمن السيبراني"، مجلة البوغاز للدراسات القانونية والقضائية، العدد 34، يونيو 2024، ص109.

12 Robert walters – Marko novak, » Cyber security, artificial intelligence, data protection the law », Springer, 2021, p: 7.

13 عادل عبد الصادق،" الاقتصاد الرقمي – تحديات السيادة السيبرانية "، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، 2020، ص 42.

14 هاله سعد مجبل،" الذكاء الاصطناعي ودوره في إدارة مخاطر الأمن السيبراني"، جامعة كربلاء، كلية التربية للعلوم الإنسانية، 2024، مقال متاح على الرابط التالي: https://cohe.uokerbala.edu.iq/wp، تم الاطلاع عليه بتاريخ: 2025 – 3 – 16، على الساعة: 12 :56.

15 محمد دحماني،" الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني"، مرجع سابق، ص 605.

16 Robert walters – Marko novak, » Cyber security, artificial intelligence, data protection the law », op. cit, p: 61.

17 هاله سعد مجبل،" الذكاء الاصطناعي ودوره في إدارة مخاطر الأمن السيبراني"، مرجع سابق.

18 Grant thornton, » perspectiva del covid 19 – tecnología e innovación contra el coronavirus », abril 2020, estudio esta publicado enlace: https://www.grantthornton.es/contentassets/12c9e2e520554e30815b9dbdc5b83dc1/consultoria_covid19.pdf, ha sido visto: 16 – 2 – 2025, la hora: 18:00.

19 آسيا السبتي – عمر بوقريط،" دور الذكاء الاصطناعي في تحقيق الأمن السيبراني"، المجلة الدولية للبحوث القانونية والسياسية، المجلد 8، العدد 3، ديسمبر 2024، ص 427، مقال متاح على الرابط

التالي: https://asjp.cerist.dz/en/article/263597، تم الاطلاع عليه بتاريخ: 2025 – 2 – 16، على الساعة، 54: 19.

20 خليل سعيدي – مرزوق بن مهدي،" الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبراني"، دراسات في حقوق الإنسان، المجلد 6، العدد 1، جوان 2022، ص 35، مقال متاح على الرابط التالي: https://n9.cl/typ5li، تم الاطلاع عليه بتاريخ: 2025 – 2 – 17، على الساعة: 54: 20.

21 فاطمة رومات،" العلاقات الدولية وتحديات الذكاء الاصطناعي"، مكتبة الألفية، 2024، ص 80.

22 آسيا السبتي – عمر بوقريط،" دور الذكاء الاصطناعي في تحقيق الأمن السيبراني"، مرجع سابق، ص 427.

23 خليل سعيدي – مرزوق بن مهدي،" الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبراني"، مرجع سابق، ص 36.