

الحماية القانونية للأمن القومي (الحماية التقنية والتشريعية نموذجاً)

Legal protection of national security (technical and legislative protection as amodel)

عمر حماس^{1*}، المركز الجامعي مغنية، الجزائر، omar.hammas@yahoo.fr

omar.hammas@cumaghnia.dz

تاريخ قبول المقال: 2024/11/28

تاريخ إرسال المقال: 2024/08/01

الملخص:

إنّ ضمان الأمن القومي هو أحد مظاهر سيادة وقوة أي دولة في العالم، ولا يمكن تحقيقه إلا من خلال حمايته تقنيا وتشريعيا، فالحماية التقنية اليوم تتطلب استغلال التكنولوجيا بكل أشكالها وفي مقدمتها الذكاء الاصطناعي للوصول إلى حماية ولو جزئيا لأمنها القومي، فلا يمكن لأي دولة أن تحمي ذاتها وأفرادها تكنولوجيا ما لم تعتمد على تقنيات الذكاء الاصطناعي لما هذه الأخيرة من مزايا عديدة ودقيقة، كما يتطلب ضمان الأمن القومي أيضا حماية تشريعية من خلال قوانين داخلية والسعي إلى تكثيف الجهود الدبلوماسية في سبيل تخفيف من حدة المخاطر والهجمات السيبرانية، وهكذا تكون الدول في أمان بعيدا عن الصراع التكنولوجي وما يحمله من مخاطر وهجمات من الصعب اكتشافها .

الكلمات المفتاحية: الأمن القومي، الذكاء الاصطناعي، الحماية المادية والتقنية، الحماية التشريعية.

Abstract: Ensuring national security is one of the manifestations of the sovereignty and power of any country in the world, and it can only be achieved by protecting it technically and legally. Technical protection today requires exploiting technology in all its forms, most notably artificial intelligence, to achieve even partial protection of its national security. No country can protect Technology itself and its people Unless you rely on artificial intelligence techniques, because of the latter's numerous and precise advantages, ensuring national security also requires legislative protection through internal laws and seeking to intensify diplomatic efforts in order to mitigate the severity of risks and cyber attacks, and thus

* عمر حماس.

countries will be safe away from technological conflict. And what it carries Risks and attacks that are difficult to detect.

Key words : National security, artificial intelligence, physical and technical protection, legislative protection.

المقدمة:

شكل الذكاء الاصطناعي ثورة حقيقية على صعيد جميع المجالات الحيوية للدول وخصوصاً المجال الأمني فأحدث ثورة حقيقية في موازين القوى، وبدأت مظاهر حرب جديدة أساسها التكنولوجيا، هذه الحرب التي أطلق عليها بالحرب السيبرانية وتتمثل أسلحتها في مختلف الفيروسات والقنابل المنطقية والديدان والبرامج الخبيثة وغايتها الاختراق والتدمير، فكان لازماً إيجاد آليات توفر حماية وأمان من هذه الأسلحة الإلكترونية، وفعلاً سارعت الدول المتقدمة والنامية إلى حد سواء لتبني الذكاء الاصطناعي في مجال الأمن السيبراني والاهتمام بالذكاء الاصطناعي في منظومتها التعليمية والتكنولوجية والأمنية من أجل ضمان أمنها القومي، وهو ما تجسد من خلال مختلف برامج وتقنيات الذكاء الاصطناعي لمواجهة هذا العدو الخفي والذي قد يكون دولة أو حتى شخص عادي، إضافة إلى هذا سارعت مختلف التشريعات لسن قوانين تكون رادعة لكل من يمس بأمن هذه الدول وخاصة أن العالم اليوم أصبح مفتوحاً على مصرعيه، ولا يمكن الدول خاصة النامية منها اكتشاف أعدائها إذا لم تكن متسلحة تكنولوجياً وتشريعياً بل وأكثر من هذا السعي في دخول وولوج اتفاقيات ثنائية وإقليمية ودولية لعلها تتجو من مختلف الاعتداءات التكنولوجية والتي تحدث في كل وقت وحين وعلى مدار الساعة، والتسلح بالتكنولوجيا أضحت ضرورة حتمية خاصة في مجال الذكاء الاصطناعي، لأهميتها الجلية في مختلف المجالات الحيوية للدول وخاصة المجال الأمني، فضمن كل دولة أمنها وأمن أفرادها باستخدام تقنيات الذكاء الاصطناعي بشكل مظهر من مظاهر القوة والسيادة وضمن أمنها من خلال سن التشريعات التي تأتي رادعة لكل من يحاول الاعتداء تكنولوجياً بأي شكل من أشكال الاعتداء التكنولوجي، وبهذا تكون الدولة قد حصنت أمنها وأمن أفرادها، ومن هذه المنطلقات جاءت الإشكاليات التالية:

ما المقصود بالذكاء الاصطناعي والأمن القومي، وإلى أي مدى تتجلى أهمية الذكاء الاصطناعي والتشريع في ضمان الحماية من مختلف المخاطر الأمنية ؟

للإجابة على هذه الإشكالات، اتبعنا المنهج الوصفي لشرح مختلف المصطلحات التكنولوجية الحديثة، والمنهج التحليلي لتحليل النصوص القانونية المؤطرة لها، وعليه جاء المبحث الأول معنوناً بمفهوم الذكاء الاصطناعي والمخاطر الأمنية بينما عنون المبحث الثاني الحماية التقنية والتشريعية في مجال الأمن القومي.

المبحث الأول: مفهوم الذكاء الاصطناعي والمخاطر الأمنية

سننظر في هذا المبحث تعريف الذكاء الاصطناعي وخصائصه في المطلب الأول، وكذا مفهوم المخاطر الأمنية ومظاهرها في المطلب الثاني.

المطلب الأول: تعريف الذكاء الاصطناعي وخصائصه

في هذا المطلب نتطرق إلى تعريف الذكاء الاصطناعي (أولا) وخصائصه (ثانيا).

أولا: تعريف الذكاء الاصطناعي

1- التعريف الفقهي: تعددت التعاريف الفقهية للذكاء الاصطناعي ومن أهم التعاريف ما جاء به John Mc Carthy بأنه "علم وهندسة صنع الآلات الذكية"، وعرفه Minsky Lee Marvin بأنه "بناء برامج الكمبيوتر التي تتخبط في المهام التي يقوم بها البشر بشكل مرضي، لأنها تتطلب عمليات عقلية عالية المستوى مثل الإدراك الحسي"¹، كما عرفه بوردن على أنه "علم الحصول على الآلات وأنظمة الكمبيوتر لأداء المهام التي تتطلب ذكاء واعتاد البشر على القيام بها" وعرفه تريدينك، بأنه "عبارة عن مجموعة من التقنيات والمناهج الخاصة بالحوسبة، والتي تهتم بقدرة أجهزة الكمبيوتر على اتخاذ قرارات عقلانية قادرة على الاستجابة للظروف البيئية غير المتوقعة"²، وعرف الذكاء الاصطناعي على أنه "علم صنع الحواسيب للقيام بأشياء تتطلب ذكاء عندما يقوم بها الإنسان"³.

2- التعريف التشريعي: عرفته لجنة الأمم المتحدة للقانون التجاري الدولي، بأنه "علم استنباط نظم قادرة على حل المشاكل وأداء الوظائف بمحاكاة العمليات الذهنية"⁴، وعرفه البرلمان الأوروبي بتاريخ 16 فبراير 2017 من خلال تناول تنظيم قواعد القانون المدني بشأن الروبوتات والذكاء الاصطناعي، بأنه "العمل المستقل من خلال أجهزة الاستشعار أو عن طريق تبادل البيانات مع بيئتها والاتجار بتلك البيانات وتحليلها

¹ عبد الله سعيد عبد الله الوالي، المسؤولية المدنية عن أضرار تطبيقات الذكاء الاصطناعي في القانون الإماراتي، الطبعة الأولى، دار النهضة العلمية، الإمارات، 2021، ص ص. 28-29.

² مجدوب نوال، إشكالات المسؤولية القانونية عن تطبيقات نظم الذكاء الاصطناعي، الطبعة الأولى، المجموعة العلمية للطبع والنشر، مصر، 2022، ص. 15.

³ عبد السلام محمد رائد ستين، تطورات الاستخدام الاقتصادي للذكاء الاصطناعي، الطبعة الأولى، دار الأهرام للنشر والتوزيع والإصدارات القانونية، مصر، 2022، ص. 14.

⁴ عمر نافع رضا العباسي، النظام القانوني للذكاء الاصطناعي، دراسة مقارنة، الطبعة الأولى، المركز العربي للنشر والتوزيع، مصر، 2023، ص. 26.

لأغراض التعلم الذاتي من التجربة والتفاعل لتكييف سلوكها وإجراءاتها مع تلك البيئة⁵، ومن الدول الرائدة التي عرفت الذكاء الاصطناعي في تشريعاتها هي الولايات المتحدة الأمريكية وهذا في الفصل الثالث من قانون مستقبل الذكاء الاصطناعي لسنة 2017، وهذا على عكس المشرع الفرنسي الذي أشار إلى استحياء لمضمون الذكاء الاصطناعي والحريات⁶ ومن بين التشريعات العربية التشريع الأردني حيث لم يقدم تعريفاً واضحاً وصريحاً للذكاء الاصطناعي سواء في قانون حق المؤلف رقم 22 لسنة 1992 وقانون براءات الاختراع رقم 32 لسنة 1999، إلا أنه أتى على تعريف الوسيط الإلكتروني في المادة الثانية من قانون المعاملات الإلكترونية رقم 15 لسنة 2015، هذا التعريف الذي يعتبر قريباً اقرب إلى تعريف الذكاء الاصطناعي⁷، كما أن المشرع السعودي هو الآخر تبني الذكاء الاصطناعي وخير دليل على هذا هو منحه للروبوت صوفيا الجنسية السعودية في إطار مبادرة الاستثمار المستقبلي⁸.

ثانياً: خصائص الذكاء الاصطناعي

1- كفاءة ودقة الذكاء الاصطناعي: من أهم ميزات وخصائص الذكاء الاصطناعي بكفاءته العالية من خلال إدارة البيانات، كما أنه يعمل لمدة طويلة دون ملل أو تعب⁹ وتمتاز تقنياته بالقدرة على التفكير والإدراك والإبداع وفهم الأمور المرئية، كالتعرف على بصمات الصوت والصورة واكتساب المعرفة وتطبيقها، استخدام التجربة والخطأ لاستكشاف الأمور المختلفة، إضافة إلى استخدام الخبرات القديمة وتوظيفها في مواقف جديدة.

2- شمولية الذكاء الاصطناعي: من أهم مميزات الذكاء الاصطناعي وهو الشمولية من خلال اقتحامه جل المجالات السياسية والأمنية والاجتماعية بشقيه المجال الطبي والتعليمي والاقتصادي والقانوني، ففي المجال الطبي ما نجده في الذكاء الاصطناعي القوي من روبوتات طبية والمستخدم في الطب الإشعاعي، والجراحي والتشخيص الطبي وغيرها من المهام التي يقوم بها و نجد أيضاً الذكاء الاصطناعي في المجال

⁵ عمر نافع رضا العباسي، المرجع السابق، ص. 26.

⁶ محمود حسن السحلي، أساس المساءلة المدنية للذكاء الاصطناعي المستقل، قوالب تقليدية أم رؤية جديدة، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، مصر، المجلد 2، العدد 1، 2022، ص ص. 40-41.

⁷ مجدولين رسمي بدر، المسؤولية المدنية الناشئة عن استخدام تقنيات الذكاء الاصطناعي في التشريع الأردني، رسالة الماجستير في القانون الخاص، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2021-2022، ص. 14.

⁸ إياد مطشر صيهود، استشراف الأثر القانوني لتكنولوجيا الذكاء الاصطناعي، الانسالة، الروبوت الذكي، ما بعد الإنسانية، الطبعة الأولى، دار النهضة العربية للنشر والتوزيع، مصر، 2021، ص. 15.

⁹ عبد الله سعيد عبد الله الوالي، المرجع السابق، ص. 34.

الأمني من روبوتات عسكرية أمنية وتتمثل مهامها في تنبيه واستشعار أي أمر من شأنه المساس بالأمن في محيطها¹⁰، وفي المجال القانوني تتجسد مظاهر استخدامات الذكاء الاصطناعي في إبرام العقود الذكية، ومراجعة العقود.

3- الذكاء الاصطناعي تطبيقات مادية ومعنوية : ما يمتاز به الذكاء الاصطناعي أنه عبارة عن تطبيقات مادية ومعنوية، فتمثل التطبيقات المادية في السيارات ذاتية القيادة والطائرات المسييرة ذاتيا وكذا الروبوت الذكي، أما تطبيقات وأنظمة الذكاء الاصطناعي المعنوية فتتمثل في البرامج والخوارزميات¹¹.

4- استقلالية الذكاء الاصطناعي: من أهم ميزات الذكاء الاصطناعي هو تلك الاستقلالية التي يتمتع بها، فله القدرة على التصرف بشكل مستقل وتتجلى مظاهر استقلالية الذكاء الاصطناعي في العديد من المجالات كقيادة السيارة أو بناء محفظة استثمارية، ويتم تحديد الاستقلالية أيضا من خلال حجم الذي يملكه النظام وقدرته على التفاعل مع محيطه، إذ يمكن أن يحتوي الذكاء الاصطناعي على كثير من المستويات المتغيرة للاستقلالية التي يمنحها المصمم أو المبرمج، وكلما زاد الذكاء والقدرة على التفاعل زاد نطاق الخيارات المتاحة ومن ثم ازدادت الاستقلالية¹²، كذلك يمكن للذكاء الاصطناعي أن يتخذ القرار دون تدخل بشري، من خلال التعلم الآلي الذي يتخذ القرار المناسب¹³.

المطلب الثاني: مفهوم المخاطر الأمنية ومظاهرها

وسنتعرض إلى تعريف المخاطر الأمنية وخصائصها في الجزئية الأولى، ثم مظاهرها في الجزئية الثانية.

أولاً: تعريف المخاطر الأمنية وخصائصها

تعرف المخاطر الأمنية بالحروب السيبرانية والتي يركز مفهومها على اختراق مواقع الدول في العالم أو أنظمتها المعلوماتية، خاصة المتعلقة بالقطاعات الإستراتيجية كال دفاع والطاقة والاتصالات، وهذا بهدف التجسس عليها وتعطيل خدماتها أو سرقة معلوماتها، وعرف المختصين الحرب السيبرانية بأنها "الحرب التي تتم إدارتها في مجال الفضاء الرقمي، تمثل فيها الدول كفاعول رئيسية، حيث تستخدم الآليات والأسلحة

¹⁰ مجدولين رسمي بدر، المرجع السابق، ص.15 وما بعدها.

¹¹ أحمد علي حسن عثمان، انعكاسات الذكاء الاصطناعي على القانون المدني، دراسة مقارنة، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، مصر، المجلد 11، العدد 76، 2021، ص.1532.

¹² عمار كريم الفتلاوي، علي عبد الجبار رحيم المشهدي، المسؤولية المدنية عن تقنية الذكاء الاصطناعي المعقد دروب المعرفة للنشر، مصر، 2022، ص.17.

¹³ فاطمة عبد العزيز حسن احمد بلال، دور الذكاء الاصطناعي في تعزيز العدالة الناجزة أمام القضاء، دراسة مقارنة مع النظاميين القانوني والقضائي في دولة قطر، رسالة ماجستير في القانون الخاص، كلية القانون، جامعة قطر، 2022-2023، ص.35.

الالكترونية في الهجوم الذي يكون موجه أساسا إلى أجهزة الحاسب الآلي والشبكات الالكترونية الخاصة بالعدو أو الأنظمة الالكترونية وما تحتويه من معلومات والخاصة بالدول مما يحول دون استخدام هذه الأنظمة والأجهزة والشبكات أو تدميرها بالكامل¹⁴ وعليه و بمفهوم أوسع فإن المخاطر الأمنية تتمثل في مختلف الهجمات والاختراقات والتجسس الالكترونية والفيروسات والتعدي على خصوصية الأفراد والدول نتيجة الاستخدام الواسع والكبير للانترنت واستغلال مختلف التكنولوجيات الحديثة بما فيها الذكاء الاصطناعي، ويعد الحاسوب الآلي الأرض الخصبة لممارسة هذه الأفعال الغير مشروعة قانونا وأخلاقا نظرا لما تسببه من دمار وهلاك لمختلف القطاعات الحساسة في الدولة وخاصة في جانبها الأمني العسكري وجانبها الاقتصادي.

وتتميز المخاطر الأمنية بجملة من الخصائص نذكر منها ما يلي:

1- الخاصية التكنولوجية : ما يطبع المخاطر الأمنية أنها تستخدم فيها التكنولوجيا بشكل أساسي، مع الاعتماد على الانترنت، وفي هذا الصدد يتوقع خبراء أمن المعلومات أن تساهم تقنيات الذكاء الاصطناعي هي الأخرى في شن الهجمات الالكترونية، وعليه فمن الممكن أن يهاجم ذكاء اصطناعي، ذكاء اصطناعي آخر¹⁵.

2- الخاصية الدولية : ما يميز المخاطر الأمنية هو طابعها الدولي، فلا يمكن لأي دولة أي تسلل من مختلف الهجمات والاختراقات الالكترونية وغيرها من المخاطر، فهذا أولت مختلف الدول المتقدمة والنامية على حد سواء اهتماما بالغا بالذكاء الاصطناعي وعلى رأسهم الولايات المتحدة الأمريكية والصين، وهذا لاستخدامها في مجال حماية أمنهم القومي.

3- تعدد صور المخاطر الأمنية : ما يميز أيضا المخاطر الأمنية هو تعدد صورها وكل صورة تمثل نوع من العدوان التكنولوجي سواء على خصوصية الأفراد أو المنظمات أو الدول، ولكل من هذه الصور دور في مجال أو نطاق معين تبعا لما يصبو إليها مستخدموها، فهناك الاختراقات والجوسسة العسكرية والفيروسات بشتى أنواعها، وهناك العديد من صور المخاطر الأمنية.

ثانيا: مظاهر المخاطر الأمنية على نظم المعلومات السببرانية

¹⁴ دليلة العوفي، الحرب السببرانية في عصر الذكاء الاصطناعي، مجلة الحكمة للدراسات الفلسفية، مركز الحكمة للبحوث والدراسات، الجزائر، المجلد 9، العدد 02، 2021، ص ص. 782-783.

¹⁵ خالد ممدوح ابراهيم، التنظيم القانوني للذكاء الاصطناعي، الطبعة الأولى، دار الفكر الجامعي، مصر، 2022، ص. 98.

1-الاختراق : هو القدرة على الوصول إلى البيانات أو المعلومات بطريقة غير مشروعة، عن طريق ثغرات في نظام الحماية الخاص لأجهزة و الحاسوب واختراق الأجهزة وقواعد البيانات الخاصة بنظم معلومات السيبرانية، وهذه الثغرات غالبا ما تكون في المنافذ الخاصة بالجهاز، وهي بوابات للجهاز على الانترنت.

2-برامج ذات التحميل الذاتي : وهي برامج مخصصة للعمل في بيئة الانترنت، بحيث يتم إرسالها عبر الشبكة بكل سهولة، ويتم تحميلها على الحاسوب وكأنها معلومات مرسله دون أي مشاكل وصعوبات، وقد صممت هذه البرامج لتوفير السهولة والسرعة أثناء التصفح أو الإبحار في الشبكة، فتجعل من صفحات المواقع أكثر جاذبية وحركة ولذلك تحمست الشركات المنتجة للمتصفحات وقدمت الدعم لهذه التكنولوجيا ولكن صاحب هذه الانتشار سوء الاستخدام من قبل بعض المبرمجين والمستخدمين، مما تسبب في الكثير من المشاكل الأمنية لبقية المستخدمين¹⁶ ويطلق هذه البرامج بالبرامج الخبيثة¹⁷.

3-التجسس على البريد الالكتروني : إن التكنولوجيا الحالية أضحت غامضة وعسيرة ومن الصعب اكتشافها، فهناك برامج حاسوبية تثبت خلسة على أجهزة الحاسوب للتجسس على البريد الالكتروني المستخدم في المراسلات بين نظم المعلومات السيبرانية، وهذا من دون علم المستخدم سواء كان شخص أو منظمة، وتتجلى مهامها ليس فقط رصد البريد الالكتروني بل يتعدى هذا لجمع المعلومات الشخصية وميزة هذه البرامج أنها تظهر للمستخدم على شكل إعلان ما في طريقة فضولية أو مفاجئة، مما تجعل المستخدم متحمسا للاشتراك دون تفكير أو اخذ الحيطة¹⁸.

4-الفيروسات والجوسسة العسكرية : من أهم وأخطر البرامج وتتمثل أهدافها في تدمير من أجل إحداث أضرار جسمية بنظام الحاسوب سواء الأجهزة أو البرمجيات بمختلف أنواعها زمنها نظم المعلومات السيبرانية، وتتجلى أهم وسائل انتقال الفيروسات في قرصنة البرامج، الشبكات الإعلامية، البريد الالكتروني، والإرهاب فهناك جماعات إرهابية تقوم بتدمير المطارات واختطاف الطائرات وهذا بإدخال الفيروس إلى نظم المعلومات للدول المعادية كالفيروس الإسرائيلي الذي تم اكتشافه في الجامعة العربية بالقدس وتم تصنيفه كفيروس سياسي، كذلك هناك الجاسوسية العسكرية بحيث يتم فيه استخدام الفيروس في نقل الأسرار العسكرية، وفي ذات السياق أثارت الخصوصية قلقا قانونيا يتعلق بطائرات التجسس من دون طيار واستخدمات عسكرية أخرى خصوصا في ظل عدم وجود اتفاقيات دولية تحد من هذه التقنية، مما يشكل خطرا

¹⁶ علاء عبد الرزاق السالمي، المدخل إلى الذكاء الاصطناعي السيبراني، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، مصر، 2022، ص ص. 61-62.

¹⁷ دليلة العوفي، المرجع السابق، ص. 786.

¹⁸ علاء عبد الرزاق السالمي، المرجع نفسه، ص. 63.

دوليا على المدنيين وعلى الدول ورغم كل هذا فإن النظام العسكري يعد أقل عرضة للإصابة عن باقي النظم الطبيعية للعمل في هذا لنظام المتميز بالحزم والسرية والاستقلال عن باقي النظم¹⁹ وهناك عدد آخر من الوسائل لانتقال الفيروسات فالعالم اليوم أصبح قرية بالفعل وأصبح يعيش أخطار تكنولوجيا من الصعب اكتشافها إذا لم تكن متسلحا بالعلم.

المبحث الثاني: الحماية التقنية في مجال الأمن القومي

سارعت الدول المتقدمة أو النامية على حد سواء إلى تبني الذكاء الاصطناعي كآلية من آليات الحماية التقنية لحماية أمنها القومي باعتباره من الحلول الناجعة في وقتنا الحاضر، ولما يتميز به من سمات لها أثر ايجابي وفعالية اكبر في ضمان الأمن القومي، مدعوما بحماية تشريعية من جميع الأخطار المهددة لسلامة خصوصيات وأسرار هذه الدول وأفرادها وهذا ما سنكتشفه في هذا المبحث من خلال تعرضنا في المطلب الأول للحماية التقنية في مجال الأمن القومي، أما المطلب الثاني فخصصناه للحماية التشريعية في مجال الأمن القومي.

المطلب الأول: الحماية التقنية في مجال الأمن القومي

من أهم مظاهر الحماية التقنية للأمن القومي هي تلك الحماية التي تعتمد على التكنولوجيا الأكثر نجاعة وفعالية وهي تكنولوجيا الذكاء الاصطناعي، وزيادة على هذا تأتي حماية تقنية أخرى وهي الحماية المادية والفنية والمتمثلة في مزيج بين استخدام تكنولوجيات الذكاء الاصطناعي وتقنيات تكنولوجيا عادية، وهو ما سنراه في هذا المطلب من خلال تطرقنا إلى الذكاء الاصطناعي كآلية من آليات الحماية في مجال الأمن القومي ، إضافة إلى الحماية الفنية والمادية في مجال الأمن القومي.

أولاً: الذكاء الاصطناعي كآلية من آليات الحماية في مجال الأمن القومي

ساهم الذكاء الاصطناعي من خلال مختلف تقنياته ونظمه وخوارزمياته في إرساء قواعد أمنية مجابهة لكل احتمالات اعتداء تكنولوجياي كيفما كان شكله أو نوعه واكتشاف الهجمات والاختراقات الالكترونية حتى قبل وقوعها وهو ما سنستشفه من خلال عرض أهمية ودور الذكاء الاصطناعي من عدة جوانب كما يلي :

1- الذكاء الاصطناعي في مكافحة الهجمات والاختراقات السيبرانية

للذكاء الاصطناعي دور فعال وإيجابي في مجال الأمن السيبراني من خلال ما يقدمه من مزايا عديدة ، وتتجلى مساهمته من خلال دراسة البيانات الحالية وتحليلها والعمل على تنبؤ الهجمة قبل حدوثها، كما يقوم

¹⁹ عبد الله سعيد عبد الله الوالي، المرجع السابق، ص.46.

بتصيد هجمات جديدة لم يتم تعريفها في النظام من قبل، وكمثال على تلك الحالات هو قدرة الأنظمة على تصيد حالات تجسس السبيرياني على الدول والشركات التي لم تستطع أنظمة الحماية العادية تصيدها²⁰، كما يمكن للذكاء الاصطناعي محاربة القرصنة كما يمكن لبرامجه القدرة على التصدي للهجمات الالكترونية والتعامل معها بل وشن هجمات الكترونية تخترق النظم السبيريانية للخصوم²¹، فالسرعة ودقة الملاحظة التي يتسم بها الذكاء الاصطناعي في تحديد الاختراقات السبيريانية، كما يمكن استعمال أنظمة الذكاء الاصطناعي لتحليل الآثار المحتملة في مجال الأمن السبيرياني، وتعديل امتيازات الإذن بالدخول استنادا إلى الشبكة وموقع المستخدم²²، ومن الأمثلة عن الاختراقات التي يمكن للذكاء الاصطناعي التصدي لها هي تلك الاختراقات التي تمس المتجر الالكتروني وهذا في مجال التجارة الالكترونية، وللدخول من عمليات الاختراق والاحتيال هو تفعيل تطبيق الكابتشا CAPTCHA والغاية من هذا التطبيق هو التأكد من أن مستعمل صفحة الانترنت هو شخص وليس برنامج أو آلة يتصفح الانترنت بشكل أوتوماتيكي، واستغلالها لصد هجمات قرصنة سارقي المعلومات²³ وبالرغم من هذه القوة والدقة والسرعة التي يتمتع بها الذكاء الاصطناعي فإنه قد لا يتصدى لجميع الهجمات كتلك الهجمات الالكترونية الخطيرة جدا والتي تكون نسبة نجاحها عالية وهي الهجمات التي لم يتم تعريفها بالنظام من قبل ولم توضع طرق تصدي خاصة بها، وإنما هي ثغرة في نظام أو أسلوب هجمة مستحدثة بالكامل شبيهة لحد كبير بظهور مرض حديث أو فيروس جديد لم يتم تحديد لقاح ضده.

2- دور الذكاء الاصطناعي في الأمن السبيرياني

تتجلى مزايا الذكاء الاصطناعي في مجال الأمن السبيرياني من خلال عدة أوجه، فبداية يتم استخدام عمليات الدخول الحيوية لخلق عمليات تسجيل دخول آمنة وتتم عن طريق إما مسح بصمات الأصابع أو شبكة العيون أو طبعات اليد مع إمكانية استخدام هذا الأمر بمفرده أو مع كلمة مرور، وهو ما تجسد فعلا ونراه اليوم من تسجيل الدخول في الهواتف الذكية والحواسيب، ومع هذا فقد تعرضت شركات عدة لخروقات أمنية حيث عرضت عناوين البريد الالكتروني والمعلومات الشخصية وكلمات المرور للخطر، وقد أكد خبراء الأمن السبيرياني في عدة مناسبات أن كلمات المرور معرضة وبشكل كبير للهجمات السبيريانية، مما ينجر عنه تهديد للمعلومات الشخصية وبطاقات الائتمان وأرقام الضمان الاجتماعي وهي كلها أسباب تجعل تسجيل

²⁰ علاء عبد الرزاق السالمي، المرجع السابق، ص. 38.

²¹ عماد الدين حامد الشافعي، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، دراسة مقارنة، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، مصر، المجلد 2، العدد 3، 2019، ص 525، 526.

²² علاء عبد الرزاق السالمي، المرجع نفسه، ص ص. 38-39.

²³ خالد ممدوح ابراهيم، المرجع السابق، ص. 95.

الهوية الحيوية مساهمة ايجابية من قبل الذكاء الاصطناعي في الأمن السيبراني²⁴، ومع هذا فان الذكاء الاصطناعي وما يمتاز به من تقنيات كتقنيات التعلم الآلي والتي لها القدرة على تعلم وتحديد رسائل البريد الالكتروني العشوائي ورسائل الخداع من خلال تحليل هذه الرسائل عبر مجموعة كبيرة من أجهزة الكمبيوتر وله القدرة على التكيف مع الظروف المختلفة، فإن عوامل تصفية البريد العشوائي Gmail و Yahoo تقوم بأكثر من مجرد التحقق من رسائل البريد غير المرغوب فيها باستخدام القواعد الموجودة مسبقا، وفعلا قد نجح الذكاء الاصطناعي من خلال استخدام خوارزميات التعلم الآلي في تصفية 99,9 بالمئة من الرسائل غير المرغوب فيها في شركة Gmail²⁵.

3- دور أنظمة وخوارزميات الذكاء الاصطناعي في كشف التهديدات السيبرانية

تتمثل أهمية الذكاء الاصطناعي أيضا من خلال الكشف عن التهديدات وغيرها من الأنشطة الضارة المحتملة، حيث تقوم شركات الأمن السيبراني بتعليم أنظمة الذكاء الاصطناعي للكشف عن الفيروسات والبرامج الضارة باستخدام خوارزميات معقدة تمكن من الذكاء الاصطناعي من تشغيل البرامج التي تستطيع التعرف عليها والتصدي لهذه الفيروسات، كما يمكن تدريب أنظمة الذكاء الاصطناعي على تحديد أصغر سلوكيات البرمجيات الخبيثة قبل أن تدخل النظام ثم تعزلهم عن هذا النظام، كما تقوم أنظمة التي تعمل على الذكاء الاصطناعي باستخدام استراتيجيات سريعة الاستجابة للحفاظ على حماية المؤسسات من خلال المعالجة الطبيعية التي تجمع تلقائيا عن الهجمات السيبرانية وأن هذه المعلومات بإمكانها إعطاء نظرة عن تحديد الحالات الشاذة والمشيرة إلا أنها هجمات إلكترونية²⁶، وتستخدم أنظمة الذكاء الاصطناعي في المصادقة لتوفير الإذن بالدخول إلى مستخدميها بحيث يتمتع مستخدمي الشركات بمستويات مختلفة من امتيازات المصادقة المعتمدة أيضا على الموقع الذي يدخلون من خلاله إلى البيانات عند استخدام الذكاء الاصطناعي، وتقوم المصادقة متعددة العوامل بجمع معلومات المستخدم لفهم سلوك هذا الشخص واتخاذ قرار بخصوص امتيازات الإذن بالدخول للمستخدم.

ثانيا: الحماية الفنية والمادية في مجال الأمن القومي

لا يكفي الذكاء الاصطناعي وحده في ضمان حماية تقنية كاملة لعدة أسباب من أهمها أنه قد لا تكون هذه التكنولوجيا في متناول جميع الدول وقد تكون تكنولوجيا الذكاء الاصطناعي غير كافية وحدها، فكان لازما

²⁴ علاء عبد الرزاق السالمي، المرجع السابق، ص.40.

²⁵ خالد ممدوح ابراهيم، المرجع السابق، ص.85-86.

²⁶ علاء عبد الرزاق السالمي، المرجع نفسه، ص.41 وما بعدها .

البحث في آليات أخرى تقنية تكون بمثابة آليات من آليات الحماية التقنية والتي لا يوفرها الذكاء الاصطناعي وحده فهي مزيج بين استخدامات الذكاء الاصطناعي والتقنيات التكنولوجية العادية المتاحة لجميع البشر، وكل هذا من أجل ضمان حماية فعالة للمعلومات وتكاملها والمتوفرة في نظم المعلومات السيبرانية، وهذه الإجراءات تكون فنية أو إجراءات مادية وإدارية.

1- الإجراءات المادية : الإجراءات المادية تشمل الأساليب والاستعدادات الاضطرارية وأساليب ضبط الوصول إلى لمواقع الأجهزة والوثائق للعاملين والخارجين غير المخولين، كوضع الأساليب والخطط والتوعية الأمنية ومعايير وضوابط أمنية للموقع والأفراد وغيرها، حيث قامت وزارة الدفاع الأمريكي بإنشاء إدارة خاصة سنة 2018 لتوطين المزيد من تكنولوجيا الذكاء الاصطناعي في نظم التسليح لمواجهة التهديدات، خاصة من جانب الصين وروسيا اللتين لديهما نفس النوعية من الاستراتيجيات لمواجهة السيطرة الأمريكية على الساحة الدولية²⁷، وما يؤكد هذا القول أيضا هو تحديث الولايات المتحدة الأمريكية الكثير من ابتكارات الذكاء الاصطناعي وانتشرت بسرعة لاسيما مع الضغوط الأكاديمية والتجارية القوية لجعل الذكاء الاصطناعي في متناول الجميع، إلا أن تزايد مبتكري الذكاء الاصطناعي وخبراتهم في دول أخرى كالصين يشكل إشارة على فقدان الولايات المتحدة الأمريكية ميزة المتحرك الأول في مجال الذكاء الاصطناعي²⁸

2- الإجراءات الفنية : إن الإجراءات الفنية التي يجب مراعاتها والاهتمام بها تشمل بداية توفير برمجيات ضبط الوصول للمعلومات وتساهم هذه البرمجيات في الحد من وصول مستخدم للمعلومات ومصادر النظام وبرامجه، مراقبة فعاليات المستخدم، والإنذار عن الاختراق، أما الإجراء الثاني للحماية الفنية فيتمثل في التشفير من خلال استخدام خوارزميات رياضية أو أجهزة ومعدات لغرض تشفير تنقل المعلومات أو تشفير المعلومات، وثالث إجراء حماية بوابة الدخول، ورابع إجراء هو إتباع الأساليب التي تؤكد موثوقية الرسائل من أنظمة المعلومات وأخير وخامسا الحماية من الفيروسات، وللاشارة فإن البرمجيات تتمثل في عدة تطبيقات تساهم في حماية نظم المعلومات السيبرانية، فهناك تطبيقات لحماية الهواتف الذكية، كتطبيق **AVG** المضاد للفيروسات ومهامه عديدة منها فحص ملفات التجسس والبرمجيات الضارة تلقائيا، أيضا تطبيق **Bitdtender** ويوفر حماية ضد الهجمات الضارة، وهناك تطبيق للتخلص من الفيروسات **BullGuard** وتطبيق **F.securr** وتطبيق **Kaspersky**، وهناك تطبيقات لحماية الحاسوب مثل تطبيق **Avast** وغيرها.

²⁷ م محمد عزام ، الذكاء الاصطناعي، مظلة حماية الأمن القومي في القرن الحادي والعشرين، مجلة السياسة الدولية، 8 أوت 2023، مقال منشور على الرابط التالي: <https://www.siyassa.org.eg/News/19653.aspx> ، تم الاطلاع عليه يوم 13 مارس 2024 على الساعة 12:00.

²⁸ دليلة العوفي، المرجع السابق، ص.789.

المطلب الثاني: الحماية التشريعية في مجال الأمن القومي

يعد سن التشريعات في مجال حماية الأمن القومي مظهر من مظاهر سيادة الدولة، وحفاظها على أمنها القومي بغض عن النظر إن كانت هذه الدولة متقدمة أو نامية، حيث سارعت مختلف الدول وخاصة النامية لسن تشريعات تكون جدار أمان لمنظومتها المعلوماتية، فقضية الأمن القومي أضحت قضية دولية وجب مراعاتها وهو ما تحقق فعلا من خلال تطرق التشريعات لها سواء كانت منظمات دولية أو دول، وهو ما سنطرق اليه بالتفصيل من خلال التعرض للحماية التشريعية للمنظمات الدولية والتشريع الأمريكي، إضافة إلى الحماية التشريعية الأوروبية والعربية.

أولا: الحماية التشريعية للمنظمات الدولية والتشريع الأمريكي

سعت مختلف التشريعات وكذا مختلف المنظمات الدولية إلى سن قوانين لحماية الأمن القومي فأصدرت بذلك جملة من القوانين وخاصة تلك الجرائم المتعلقة بالحواسيب وهو ما سنستعرضه من خلال التطرق إلى مختلف التشريعات كما يلي :

1- التشريعات الدولية : تشمل التشريعات الدولية مختلف القرارات الصادرة عن المنظمات الدولية وعلى رأسهم منظمة الأمم المتحدة، حيث أصدرت هذه الأخيرة قرار وهذا بمناسبة المؤتمر الثامن لمنع الجريمة ومعاملة السجناء المنعقد في هافانا سنة 1990، يدعو هذا القرار إلى ضرورة دراسة ووضع الإجراءات اللازمة للحد من جرائم الحواسيب وتشريع القوانين لمكافحة عمليات إساءة استخدام الحواسيب وتحديث القوانين الوطنية لهذا الغرض.

2- التشريع الأمريكي: تعد الولايات المتحدة الأمريكية من الدول الأوائل التي سنت قوانين في مجال حماية المعلومات، فبداية الأمر كان هناك اختلاف وتباين في قوانين جرائم الحاسوب من ولاية لأخرى، لكن مع أواخر سنة 1984 تم ميلاد أول قانون فيدرالي لجرائم الحصول أو الوصول غير المخول إلى معلومات مصنفة عن الأمن القومي وصدر أيضا قانون آخر سنة 1986.

ثانيا: الحماية التشريعية الأوروبية والعربية

1- التشريعات الأوروبية : من التشريعات الأوروبية التشريع الفرنسي والذي أصدر سنة 1988 قانونا والمتعلق ببعض جرائم المعلوماتية وخصص له بابا مستقلا، ويعتبر القانون الفرنسي رقم 19 لسنة 1988 من القوانين التي عالجت الاعتداء على البرامج والمعلومات في القرن العشرين وجرم تحليل وتعطيل أو إفساد

تشغيل نظم الحواسيب أو استخدام أو تعديل أو محو البيانات وتزوير المستندات الصادرة بواسطة الحاسوب وتجريم بعض الأساليب التقنية الجديدة في الاعتداء مثل الفيروسات²⁹.

2- التشريعات العربية : إن التشريعات العربية هي الأخرى في ظل التحولات التكنولوجية الحاصلة والتحول من النظام العام التقليدي إلى النظام العام الإلكتروني قامت بوضع قوانين لحماية المعطيات، فلا يكفي حماية نظام الحكومة الإلكترونية من خلال تجريم بعض الأعمال العدوانية والضارة التي تحدث في مجال تقنية المعلومات ووضع عقوبات رادعة لها، بل يجب تطوير نظام وقائي متكامل يهدف إلى تأمين شبكة المعلومات ومنع وقوع الجرائم الإلكترونية أو الذكية، وفي إطار الحماية التشريعية العربية فقد أصدرت عدد الدول العربية قوانين، حيث اصدر المشرع المصري قانون تنظيم الاتصالات رقم 10 لسنة 2003 الخاص بتأمين نقل وتبادل المعلومات والقانون رقم 15 لسنة 2004 بخصوص تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية الانترنت،، أيضا تعد دولة الإمارات العربية هي الأخرى من الدول العربية التي شرعت قوانين لمكافحة الجريمة المعلوماتية والتصدي لأخطارها منها القانون العربي الاسترشادي الصادر سنة 2003 بخصوص مكافحة جرائم تقنية المعلومات المعتمد بموجب قرار مجلس وزراء العدل العرب المنعقد في دورته التاسعة عشرة في أكتوبر 2003 ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين في سنة 2004، كما أصدر التشريع الإماراتي القانون رقم 2 لسنة 2006 الخاص بمكافحة جرائم تقنية المعلومات ليليه إصدار القانون رقم 03 لسنة 2012 الخاص بإنشاء الهيئة الوطنية للأمن الإلكتروني، بعدها وفي سنة 2012 صدر المرسوم الاتحادي رقم 5 لسنة 2012 المتعلق بمكافحة جرائم تقنية المعلومات ،وتم أيضا إصدار المرسوم الاتحادي رقم 2 لسنة 2018 الخاص بتعديل المرسوم الاتحادي رقم 5 لسنة 2012³⁰ ، وبالنسبة للتشريع الجزائري فقد أصدر القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها³¹.

²⁹ علاء عبد الرزاق السالمي، المرجع السابق، ص. 59 وما بعدها.

³⁰ محمد حمدي عبد العليم علام، الإستراتيجية القانونية للذكاء الاصطناعي وتطبيقاته، دروب المعرفة للنشر والتوزيع، مصر، 2024، ص. 165 وما بعدها.

³¹ أنظر القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية العدد 47 والمؤرخة في 16 أوت 2009.

الخاتمة:

تحصيلا لما جاء في الورقة البحثية فان العالم اليوم يشهد ثورة تكنولوجية والتي من مفرزاتها الذكاء الاصطناعي وما أحدثه ويحدثه في تغيير موزاين القوى وكذا مفاهيم القوة، فالبرغم ما تقدمه تكنولوجيات الذكاء الاصطناعي للعالم من مزايا عديدة إلا أنها هذا لا ينفي عن هذه التكنولوجية الخطورة التي قد تفرزها في جميع المجالات الحيوية وخاصة في المجال الأمني وكل ما يتعلق بالأمن القومي للدول لذلك كان من الضروري توفير حماية لخصوصية الأفراد وسرية المعلومات الأمنية. وخلاصة لما جاء في الورقة البحثية توصلنا إلى النتائج التالية :

أولاً : تعدد المخاطر الأمنية وتنوعها وامتياز كل شكل من أشكال هذه المخاطر بمهام خاصة حسب الغرض والهدف المرجو منها .

ثانياً :الذكاء الاصطناعي آلية من آليات الفعالة في إرساء قواعد حماية وأمان قوية بفضل ما يمتاز به من تقنيات تساهم في صد مختلف الهجمات والاختراقات.

ثالثاً:اهتمام شديد بتكنولوجيا الذكاء الاصطناعي من الدول الرائدة تكنولوجيا وعسكريا كالولايات المتحدة الأمريكية والصين مما يؤكد أهمية الذكاء الاصطناعي.

رابعاً: تجند دول العالم المتقدمة والنامية من خلال إصدار تشريعات تكون بمثابة جدار آمان لحماية منظومتها الأمنية وخصوصية أفرادها وكل هذا يطلق في نطاق الأمن القومي.

ومن خلال هذه النتائج توصلنا إلى التوصيات التالية :

أولاً: ضرورة منح أهمية بالغة أكثر للذكاء الاصطناعي والأمن السيبراني لأهميتهما على صعيد المحالات من خلال تكوين المورد البشري، وفتح مدارس أخرى جهوية في هاذين المجالين .

ثانياً :إبرام اتفاقيات ثنائية، إقليمية ودولية قصد الحد من مختلف الهجمات والاختراقات والتي قد تكون سببها الدول المعادية.

ثالثاً: ضرورة سن قوانين تشريعية أكثر حزما وردعا لمجرمي المعلوماتية، وضمانا لحماية أمنية لخصوصية الأفراد والدولة.

رابعاً:حتمية التسلح بالذكاء الاصطناعي من أجل حماية المنظومة الأمنية للدولة وحماية خصوصية أفرادها في ظل الصراع التكنولوجي القائم والتهديدات الأمنية الحاصلة.

قائمة المصادر والمراجع:

أولاً: النصوص القانونية

- القانون رقم 04-09 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية العدد 47 والمؤرخة في 16 أوت 2009.

ثانياً: الكتب

- إياد مطشر صيهود، استشراف الأثر القانوني لتكنولوجيا الذكاء الاصطناعي، الانسالة، الربوت الذكي، ما بعد الإنسانية، الطبعة الأولى، دار النهضة العربية للنشر والتوزيع، مصر، 2021.
- خالد ممدوح ابراهيم، التنظيم القانوني للذكاء الاصطناعي، الطبعة الأولى، دار الفكر الجامعي، مصر، 2022.
- عبد السلام محمد رائد ستين، تطورات الاستخدام الاقتصادي للذكاء الاصطناعي، الطبعة الأولى، دار الأهرام للنشر والتوزيع والإصدارات القانونية، مصر، 2022.
- عبد الله سعيد عبد الله الوالي، المسؤولية المدنية عن أضرار تطبيقات الذكاء الاصطناعي في القانون الإماراتي، الطبعة الأولى، دار النهضة العلمية، الإمارات، 2021.
- علاء عبد الرزاق السالمي، المدخل إلى الذكاء الاصطناعي السيبراني، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، مصر، 2022.
- عمار كريم الفتلاوي، علي عبد الجبار رحيم المشهدي، المسؤولية المدنية عن تقنية الذكاء الاصطناعي المعقد دروب المعرفة للنشر، مصر، 2022.
- عمر نافع رضا العباسي، النظام القانوني للذكاء الاصطناعي، دراسة مقارنة، الطبعة الأولى، المركز العربي للنشر والتوزيع، مصر، 2023.
- مجدوب نوال، إشكالات المسؤولية القانونية عن تطبيقات نظم الذكاء الاصطناعي، الطبعة الأولى، المجموعة العلمية للطبع والنشر، مصر، 2022.
- محمد حمدي عبد العليم علام، الإستراتيجية القانونية للذكاء الاصطناعي وتطبيقاته، دروب المعرفة للنشر والتوزيع، مصر، 2024.

ثالثاً: الرسائل والمذكرات

- فاطمة عبد العزيز حسن احمد بلال، دور الذكاء الاصطناعي في تعزيز العدالة الناجزة أمام القضاء، دراسة مقارنة مع النظاميين القانوني والقضائي في دولة قطر، رسالة ماجستير في القانون الخاص، كلية القانون، جامعة قطر، 2022-2023.

- مجدولين رسمي بدر، المسؤولية المدنية الناشئة عن استخدام تقنيات الذكاء الاصطناعي في التشريع الأردني، رسالة الماجستير في القانون الخاص، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2021-2022.

رابعاً: المقالات

- أحمد علي حسن عثمان، انعكاسات الذكاء الاصطناعي على القانون المدني، دراسة مقارنة ، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، مصر، المجلد 11، العدد 76، 2021.
- دليلة العوفي، الحرب السيبرانية في عصر الذكاء الاصطناعي، مجلة الحكمة للدراسات الفلسفية، مركز الحكمة للبحوث والدراسات، الجزائر، المجلد 9، العدد 02، 2021.
- عماد الدين حامد الشافعي، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، دراسة مقارنة، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، مصر، المجلد 2، العدد 3، 2019.
- محمود حسن السحلي، أساس المساءلة المدنية للذكاء الاصطناعي المستقل، قوالب تقليدية أم رؤية جديدة، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، مصر، المجلد 2، العدد 1، 2022.

خامساً: المواقع الإلكترونية

- م محمد عزام ، الذكاء الاصطناعي، مظلة حماية الأمن القومي في القرن الحادي والعشرين، مجلة السياسة الدولية، 8 أوت 2023، مقال منشور على الرابط التالي : <https://www.siyassa.org.eg/News/19653.aspx>، تم الاطلاع عليه يوم 13 مارس 2024 على الساعة 12:00.