جامعة عبد الحميد بن باديس مستغانم
كلية الحقوق والعلوم السياسية
مخبر القانون العقاري والبيئة

مشروع البحث التكويني الجامعي PRFU

"أنظمة الذكاء الاصطناعي بين تعزيز حماية حقوق الإنسان والتهديد بانتهاكها-دراسة استشرافية قانونية"-

الرقم: 108/ م ق ع ب/ 2025 مستغانم في: 09 جوان 2025

شهادة نشر فصل في كتاب

تشهد السيدة رئيسة مشروع الكتاب الموسوم ب " استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني أن الدكتور(ة) حجاب عبد الغني من جامعة المسيلة قد ساهم(ت) في تأليف فصل تحت عنوان:

The Role of Artificial Intelligence in Enhancing Digital Sovereignty and Cybersecurity: A Case Study of Algeria

من الكتاب الحامل للترقيم الدولي ISBN 978-9969-544-36-7

سلمت هذه الشهادة لاستعمالها في حدود ما يسمح به القانون.

رئيسة مشروع الكتاب

د. والي حاجة
أستاذة محاضرة
كلية الحقوق و العلوم السياسية
جامعة مستغانم

جامعة عبد الحميد بن باديس-مستغانم
كلية الحقوق والعلوم السياسية
مخبر القانون العقاري والبيئة

بالتعاون مع مشروع البحث التكويني الجامعي PRFU:
" أنظمة الذكاء الاصطناعي بين تعزيز حماية حقوق الإنسان والتهديد
بانتهاكها-دراسة استشرافية قانونية-"

دعوة للاستكتاب في كتاب جماعي ذو ترقيم دولي حول:

استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني

رئيسة الكتاب الجماعي:
الدكتورة وافي حاجة

جمع وتنسيق:
الدكتورة لطروش أمينة

توطئة:

إن ثورة تكنولوجيا المعلومات والاتصال التي مست مختلف دول العالم دون استثناء جعل هذه الأخيرة تعرف تطور في المفهوم التقليدي للسيادة الذي كان مرتبط بقدرة الدولة على تسيير شؤونها الداخلية والخارجية بطريقة منفردة ومستقلة دون المساس بها من قبل أيا كان، غير أن التطور الذي عرفه المجتمع الدولي بداية بالاعتراف بالعديد من الأشخاص كأشخاص فاعلين في المجتمع الدولي وصولا إلى العولمة وتسارع التحول الرقمي كل هذا ساهم في ظهور مفاهيم جديدة على غرار ما بات يعرف بالسيادة الرقمية، هذا من جهة.

من جهة أخرى أسهمت ثورة تكنولوجيا المعلومات والاتصال في حدوث طفرة في التهديدات الأمنية لتنتقل من البعد العسكري الى التهديدات السيبرانية حيث أن الدول في الوقت الراهن تواجه تحديات جديدة تهدد سيادتها الرقمية، والتي ترتكز على الحروب السيبرانية والهجمات الإلكترونية التي تستهدف أنظمتها الحيوية. وعليه لم تعد أساليب الدفاع التقليدية كافية لمجابهة هذه التهديدات المستجدة، لذا أصبحت أنظمة الذكاء الاصطناعي أداة أساسية لتعزيز القدرات الدفاعية الرقمية، قصد الكشف المبكر عن التهديدات والتعامل الفعّال معها في الوقت المناسب وبنجاعة كبيرة.

كل هذا جعل الذكاء الاصطناعي يحدث ثورة في مجال الأمن السيبراني من خلال تقديم حلول فعالة لمكافحة التهديدات السيبرانية بدءًا من الكشف عن التهديدات وحتى الاستجابة للحوادث، بحيث تعمل الأدوات والتقنيات المعتمدة على الذكاء الاصطناعي على تعزيز كفاءة وفعالية التدابير الأمنية ويتجلى ذلك من خلال التعامل مع كميات هائلة من البيانات، وتحديد التهديدات غير المعروفة، والتعلم المستمر والتكيف مع أساليب الهجوم الجديدة، كل هذا يجعل من أنظمة الذكاء الاصطناعي أداة لا تقدر بثمن في سبيل الكشف عن التهديدات السيبرانية والاستجابة لها بكفاءة وفعالية أكبر.

بذلك نجد أن مسألة تعزيز السيادة الرقمية في ظل تحديات الأمن السيبراني وفي عصر الذكاء الاصطناعي، تواجهها تحديات ورهانات عديدة، الأمر الذي يستدعي وضع سياسات واستراتيجيات دولية ووطنية عبر تحديد التطبيقات الحديثة للذكاء الاصطناعي في المجالات الأمنية، واقتراح حلول مبتكرة للتصدي للحروب السيبرانية مع الاخذ بعين الاعتبار بين الاستباقية والوقاية من التهديدات في الفضاء السيبراني، وحماية البيانات والمعطيات، والسهر على ترقية ونشر ثقافة رقمية أساسها التحسيس المستمر واليقظة الإعلامية لكل مؤسسات الدولة على اختلافها، وبطبيعة الحال كل هذا يستلزم تكاثف الجهود المؤسساتية والتشريعية لتعزيز السيادة الرقمية وتحقيق الأمن السيبراني في عصر الذكاء الاصطناعي.

أهداف الكتاب:

- التعرف على الذكاء الاصطناعي واستخداماته.
- التعرف على السيادة الرقمية.
- التعرف على الامن السيبراني وابعاده.
- تأثير استخدامات الذكاء الاصطناعي على السيادة الرقمية والأمن السيبراني.
- استكشاف دور الذكاء الاصطناعي في تعزيز الأمن السيبراني.
- السياسات والاستراتيجيات الدولية والوطنية المتبعة لتحقيق السيادة الرقمية وتعزيز الأمن السيبراني في ظل تنامي أنظمة الذكاء الاصطناعي.

الإشكالية:

ما هو دور أنظمة الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني؟ وكيف استطاعت الدول وبالأخص الجزائر في حماية سيادتها الرقمية في ظل بزوغ تهديدات أمنية ذات طابع رقمي؟

محاور الكتاب الجماعي:

المحور الأول: مفاهيم حول: الذكاء الاصطناعي-السيادة الرقمية-الأمن السيبراني.

المحور الثاني: تطبيقات الذكاء الاصطناعي المستخدمة في تحسين الأمن السيبراني وحماية السيادة الرقمية.

المحور الثالث: رهانات وتحديات استخدام الذكاء الاصطناعي في مجال الامن السيبراني.

المحور الرابع: السياسات الدولية والوطنية المتبعة لتحقيق السيادة الرقمية وتعزيز الأمن السيبراني .

شروط المشاركة:

- يجب أن تحتوي الصفحة الأولى من المداخلة على الاسم الكامل للباحث ورتبته العلمية ووظيفته، اسم الجامعة، البلد، المحور، عنوان المقال، البريد الإلكتروني والهاتف.
- أن يندرج البحث ضمن أحد محاور الكتاب الجماعي.
- أن تكون البحوث والدراسات أصيلة لم يسبق نشرها.
- أن يتصف البحث بمنهجية علمية محكمة.
- يقدم البحث باللغة العربية أو اللغة الإنجليزية، كما يقدم ملخص البحث باللغة العربية والإنجليزية، ولا تتجاوز كلماته **150** كلمة، مع إرفاقه بخمسة كلمات مفتاحية.
- أن لا يقل البحث أو الدراسة عن **15** صفحة وألا تتجاوز **20** صفحة.
- تكتب البحوث باللغة العربية بخط **Traditional Arabic** في المتن حجم **(16)**، و**(12)** في الإحالات والهوامش، مع استقلال كل صفحة بهوامشها وإحالاتها، أما البحوث باللغة الإنجليزية فيتم استخدام خط **Times New Roman** حجم **(12)** في المتن، و **(10)** في الإحالات والهوامش.
- هوامش الصفحة **2** سم من كل جانب.
- يتم وضع قائمة المراجع آخر البحث.

مواعيد مهمة:

آخر أجل لإرسال الورقة البحثية كاملة يوم 5 فيفري 2025

الرد على الأعمال العلمية المقبولة يوم 15 فيفري 2025

ترسل الأوراق البحثية إلى البريد الإليكتروني الآتي:

digitalsover.27@gmail.com

استخدامات الذكاء الاصطناعي

في

تعزيز السيادة الرقمية وتحقيق الأمن السيبراني

فصول في كتاب من تأليف مجموعة من المؤلفين

الإشراف العام على الكتاب: الدكتورة وافي حاجة

دار الأيمة للنشر والتوزيع
Editions LAIMMA

عنوان الكتاب: استخدامات الذكاء الاصطناعي
تعزيز السيادة الرقمية وتحقيق الأمن السيبراني في
اسم المؤلف: إشراف الدكتورة وافي حاجة
الحجم: 15,5 × 23,5
عدد الصفحات: 487
ISBN : 978-9969-544-36-7
منشورات دار لايمة، 2025
الإيداع القانوني: ماي-2025

للتواصل معنا

القليعة-تيبازة-الجزائر

الهاتف النقال: 550.085.725 (0) 213 +

WWW NLLIBRAIRIE.COM

المقدمة

إن الحمد لله، نحمده ونستعينه ونستغفره، ونعوذ بالله من شرور أنفسنا وسيئات أعمالنا، من يهده الله فلا مضل له، ومن يضلل فلا هادي له. وأشهد أن لا إله إلا الله وحده لا شريك له، وأشهد أن محمداً عبده ورسوله.

وبعد...

فإن ما يُكتب ويُسطر، إنما هو أثر من آثار الإنسان، وقد جرت سنة الله ألا يرتفع شيء إلا بفضل، ولا يثبت إلا بأصل، ولا يُبارك في عمل إلا بإخلاص، فما هذا الجهد إلا نفحة من فضل الله.

نسأله سبحانه أن يجعل هذا العمل خالصاً لوجهه الكريم، وأن ينفع به من قرأه، ويجعله شاهداً لا علينا، بل لنا يوم نلقاه، وهو أرحم الراحمين.

نحمد الله على إخراج هذا الكتاب العلمي حول استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني بمشاركة مجموعة من المؤلفين من داخل الجزائر وخارجها بالتعاون مع مشروع البحث التكويني الجامعي-PRFU- الموسوم ب «أنظمة الذكاء الاصطناعي بين تعزيز حماية حقوق الإنسان والتهديد بانتهاكها-دراسة استشرافية قانونية-" الموطن بمخبر القانون العقاري والبيئة.

إن ثورة تكنولوجيا المعلومات والاتصال التي مست مختلف دول العالم دون استثناء جعل هذه الأخيرة تعرف تطور في المفهوم التقليدي للسيادة الذي كان مرتبط بقدرة الدولة على تسيير شؤونها الداخلية والخارجية بطريقة منفردة ومستقلة دون المساس بها من قبل أيا كان، غير أن التطور الذي عرفه المجتمع الدولي بداية بالاعتراف بالعديد من الأشخاص كأشخاص فاعلين في المجتمع الدولي وصولا إلى العولمة وتسارع التحول الرقمي كل هذا ساهم في ظهور مفاهيم جديدة على غرار ما بات يعرف بالسيادة الرقمية، هذا من جهة.

من جهة أخرى أسهمت ثورة تكنولوجيا المعلومات والاتصال في حدوث طفرة في التهديدات الأمنية لتنتقل من البعد العسكري الى التهديدات السيبرانية حيث أن الدول في

الوقت الراهن تواجه تحديات جديدة تهدد سيادتها الرقمية، والتي ترتكز على الحروب السيبرانية والهجمات الإلكترونية التي تستهدف أنظمتها الحيوية. وعليه لم تعد أساليب الدفاع التقليدية كافية لمجابهة هذه التهديدات المستجدة، لذا أصبحت أنظمة الذكاء الاصطناعي أداة أساسية لتعزيز القدرات الدفاعية الرقمية، قصد الكشف المبكر عن التهديدات والتعامل الفعّال معها في الوقت المناسب وبنجاعة كبيرة.

كل هذا جعل الذكاء الاصطناعي يحدث ثورة في مجال الأمن السيبراني من خلال تقديم حلول فعالة لمكافحة التهديدات السيبرانية بدءًا من الكشف عن التهديدات وحتى الاستجابة للحوادث، بحيث تعمل الأدوات والتقنيات المعتمدة على الذكاء الاصطناعي على تعزيز كفاءة وفعالية التدابير الأمنية ويتجلى ذلك من خلال التعامل مع كميات هائلة من البيانات، وتحديد التهديدات غير المعروفة، والتعلم المستمر والتكيف مع أساليب الهجوم الجديدة، كل هذا يجعل من أنظمة الذكاء الاصطناعي أداة لا تقدر بثمن في سبيل الكشف عن التهديدات السيبرانية والاستجابة لها بكفاءة وفعالية أكبر.

بذلك نجد أن مسألة تعزيز السيادة الرقمية في ظل تحديات الأمن السيبراني وفي عصر الذكاء الاصطناعي، تواجهها تحديات ورهانات عديدة، الأمر الذي يستدعي وضع سياسات واستراتيجيات دولية ووطنية عبر تحديد التطبيقات الحديثة للذكاء الاصطناعي في المجالات الأمنية، واقتراح حلول مبتكرة للتصدي للحروب السيبرانية مع الاخذ بعين الاعتبار بين الاستباقية والوقاية من التهديدات في الفضاء السيبراني، وحماية البيانات والمعطيات، والسهر على ترقية ونشر ثقافة رقمية أساسها التحسيس المستمر واليقظة الإعلامية لكل مؤسسات الدولة على اختلافها، وبطبيعة الحال كل هذا يستلزم تكاثف الجهود المؤسساتية والتشريعية لتعزيز السيادة الرقمية وتحقيق الأمن السيبراني في عصر الذكاء الاصطناعي.

وعليه تتمحور الإشكالية الرئيسية لهذا الكتاب حول: ما هو دور أنظمة الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني؟ وكيف استطاعت الدول وبالأخص الجزائر في حماية سيادتها الرقمية في ظل بزوغ تهديدات أمنية ذات طابع رقمي؟

للإجابة على هذه الإشكالية تم تقسيم الكتاب إلى بابين كل باب يتناول ثمانية فصول، بحيث تطرقنا في الباب الأول إلى الإطار المفاهيمي والتشريعي للذكاء الاصطناعي والسيادة

الرقمية والأمن السيبيراني، في حين يتناول الباب الثاني آليات وتحديات الذكاء الاصطناعي في إطار تعزيز السيادة الرقمية وتحقيق الأمن السيبراني.

في ختام نشكر كل من ساهم وشارك في هذا الإنتاج العلمي الذي نتمنى أن يشكل إضافة في حقل البحث العلمي لاسيما القانوني منه.

الدكتورة وافي حاجة

رئيسة مشروع البحث التكويني الجامعي-PRFU- الموسوم ب "أنظمة الذكاء الاصطناعي بين تعزيز حماية حقوق الإنسان والتهديد بانتهاكها"

-دراسة استشرافية قانونية-

المشرفة العامة على الكتاب

الباب الأول

الإطار المفاهيمي للذكاء الاصطناعي والسيادة الرقمية والأمن السيبراني

الفصل الأول

السيادة الرقمية والأمن السيبراني في عصر الذكاء الاصطناعي

-دراسة مفاهيمية وتحليلية للتحديات والفرص

- الدكتورة وافي حاجة

أستاذة محاضرة- أ-

مخبر القانون العقاري والبيئة

كلية الحقوق والعلوم السياسية جامعة عبد الحميد بن باديس-مستغانم-الجزائر

hadja.ouafi@univ-mosta.dz

الملخص

يشهد عالم اليوم ثورة رقمية وتقنية يرى الكثيرون أنها قد تقضي على الكثير من الحقوق التي يتمتع بها الانسان، وفي مقدمتها الحق في الخصوصية، خاصة في عصر الذكاء الاصطناعي، إلا أن الأمر قد يتعدى المساس بخصوصية الفرد الواحد، ليصل إلى انتهاك السيادة الرقمية للدول بشكل يمثل تهديدا لأمنها السيبراني. وعلى الرغم من الآثار السلبية للذكاء الاصطناعي، إلا أنه لا يمكن إنكار آثاره الايجابية على حفظ سيادة الدولة وتحقيق أمنها السيبراني، فأصبح بذلك الذكاء الاصطناعي أداة مزدوجة، تجمع بين التمكين السيبراني والتهديد للسيادة الرقمية، الأمر الذي يستوجب سن تشريعات وطنية واضحة ومتكاملة لتنظيم استخدام الذكاء الاصطناعي، بما يضمن الأمن السيبراني ويحافظ على السيادة الرقمية، وكذا تعزيز التعاون الدولي من أجل وضع قواعد قانونية ملزمة لحوكمة الذكاء الاصطناعي في الفضاء السيبراني.

مقدمة

شهد مجال الأمن السيبراني تحولا جذريا بفعل التطور المتسارع في تقنيات الذكاء الاصطناعي، لا سيما مع الانتشار الواسع لتطبيقاته في مختلف جوانب الحياة. فقد رافق هذا التأثير الإيجابي عدد من المزايا، لكنه في المقابل أفرز أيضاً بعض التحديات والسلبيات، خاصة فيما يتصل بأمن المعلومات والبيانات. ولم يعد التقدم التكنولوجي مجرد ميزة إضافية، بل أصبح سمة أساسية للقرن الحادي والعشرين، يتجلى في الاعتماد المتزايد على الأتمتة الإلكترونية في النظم الإدارية والمالية والأمنية على الصعيدين الوطني والدولي.

وفي هذا السياق، برز الذكاء الاصطناعي كأحد الأدوات الرئيسة التي تُستخدم في تعزيز الأمن السيبراني، من خلال قدراته الحاسوبية الهائلة، والتكامل المستمر بين الشبكات الذكية، إلى جانب تطور الأعمال الإلكترونية والاعتماد الواسع على رقمنة البيانات والمعلومات . كل ذلك يؤكد على فاعلية الأنظمة الإدارية والمالية والأمنية المبنية على تقنيات الذكاء الاصطناعي، رغم ما يطرحه ذلك من تحديات مستمرة في مجال حماية الأمن السيبراني.

الذكاء الاصطناعي يعد من أهم ملامح الثورة الصناعية الرابعة، لما له من تطبيقات واسعة في مختلف المجالات، تحول إلى أداة استراتيجية تعتمد عليها الدول والمؤسسات في الاقتصاد والصناعة والخدمات، وحتى في المجالات العسكرية والسياسية .ومن أهم المجالات التي يشهد فيها الذكاء الاصطناعي تأثيراً متزايداً، مجال الأمن السيبراني، الذي بات يشكل ركيزة أساسية من ركائز الأمن الوطني والشخصي.

ويكمن الدور الحيوي للذكاء الاصطناعي في قدرته على رصد التهديدات السيبرانية، وتحليلها، والتصدي لها بشكل فوري، مما يعزز من كفاءة النظم الأمنية، ويقلل من الاستجابة البشرية البطيئة. ويأتي هذا التداخل بين الذكاء الاصطناعي والأمن السيبراني نتيجة طبيعية، لأن كلا المجالين يعمل ضمن بيئة رقمية موحدة، هي الفضاء السيبراني .ففي هذا الفضاء، تتم معالجة البيانات، وتُدار الأنظمة، وتُخاض المعارك الرقمية، مما يجعل من الذكاء الاصطناعي عاملاً محورياً في حماية الأصول الرقمية، وتحقيق الاستقرار الأمني في العصر الرقمي.

بناء على ما تقدم نطرح الاشكالية التالية: هل تشكل تطبيقات الذكاء الاصطناعي في الأمن السيبراني نقلة نوعية في مفهوم السيادة الرقمية أم أنها تخلق تناقضات قانونية جديدة؟

يعتمد هذا البحث على منهجين تكامليين يتناسبان مع طبيعة المحاور المدروسة، حيث يستخدم المنهج الوصفي في المحور الأول لتقديم الإطار المفاهيمي والقانوني للسيادة الرقمية والأمن السيبراني، من خلال استعراض الأدبيات والمصادر القانونية ذات الصلة بشكل دقيق ومنظم. أما في المحور الثاني، فيعتمد البحث على المنهج التحليلي لدراسة تأثيرات الذكاء الاصطناعي، سواء الإيجابية أو السلبية، على الأمن السيبراني والسيادة الرقمية.

نتطرق من خلال هذا البحث إلى تقديم إطار قانوني مفاهيمي واضح لمفهومي السيادة الرقمية والأمن السيبراني في المحور الأول، ثم تحليل التأثيرات المتباينة للذكاء الاصطناعي على هذين المفهومين، سواء من حيث الفرص التي يقدمها في تعزيز الحماية السيبرانية، أو المخاطر التي قد تهدد استقرار السيادة الرقمية للدول ويكون ذلك ضمن المحور الثاني للدراسة.

المحور الأول

الإطار النظري لمفاهيم السيادة الرقمية والأمن السيبراني

يمثل الإطار النظري حجر الأساس لفهم مفهومي السيادة الرقمية والأمن السيبراني، حيث يشكلان بعدين مترابطين في الفضاء الرقمي الحديث. لذلك، يهدف هذا الإطار إلى تقديم دراسة مفصلة للمفاهيم الأساسية، وتحديد الخصائص القانونية والسياسية والأمنية التي تميز كلًا من السيادة الرقمية والأمن السيبراني، بما يهيئ الأرضية المناسبة لفهم تأثيرات الذكاء الاصطناعي التي ستتم مناقشتها لاحقًا.

أولا: السيادة الرقمية بين المفهوم وجدلية الاعتراف

سنناقش أولاً مفهوم السيادة بشكل عام، لننتقل بعد ذلك إلى تناول مفهوم السيادة الرقمية بوجه خاص. كما سنتناول جدلية الاعتراف بسيادة الدول على فضائها الرقمي.

1- مفهوم السيادة الرقمية

يرتبط مصطلح السيادة عموما، ارتباطا وثيقا بمفهوم الدولة أو السلطة العليا أو النظام السياسي القائم داخل الدولة. ونظرا لهذا الارتباط، فإن تحديد المفهوم الاصطلاحي للسيادة يختلف باختلاف الخلفيات الفلسفية والفكرية والسياسية، حيث يعرفه جان بودان (Jean Bodin):" السلطة العليا المطلقة والدائمة في الدولة التي لا تخضع لأي سلطة أخرى".[1] في حين يعرفها هوبز:» هي السلطة التي يطيعها الجميع دون استثناء والتي تمتلك الحق المطلق في سن القوانين وإجبار الأفراد على الطاعة."[2]

يتبين من خلال هذين التعريفين، إلى جانب تعريفات أخرى، أن مصطلحي "السيادة "و"السلطة العامة "غالبا ما يستعملان بمعنى واحد، إذ ينظر إليهما كوجهين لعملة

[1] Jean Bodin, Les Six Livres de la République, Librairie Arthème Fayard, Paris, 1986, p 78.

[2] توماس هوبز، اللفياثان الأصول الطبيعية والسياسية لسلطة الدولة، ترجمة دينا حرب، بشرى صعب، دار الفارابي، ص180، 2011.

واحدة، لكونهما يرتبطان بمفهوم السلطة السياسية العليا. غير أن بعض الباحثين يرون أن هذا الاستخدام المتبادل ينطوي على خلط بين الشيء ووصفه؛ فوفقًا لهذا الرأي، لا تعد السيادة سوى صفة تميز السلطة السياسية العليا القائمة داخل الدولة.

وبناءً على ذلك، يمكن التمييز بين مفهومين للسيادة:

• **المفهوم القانوني:** يعنى بإبراز السيادة كصفة ملازمة للدولة أو للسلطة العليا في إطار الدولة الحديثة، بما يعكس مبدأ المساواة بين الدول في المجتمع الدولي، بغض النظر عن شكل النظام السياسي أو حجم الإقليم.

• **المفهوم السياسي:** يرتبط بالقدرة الفعلية للدولة على فرض إرادتها داخليا وخارجيا، بما يعكس امتلاكها للقوة والسيطرة دون خضوع لأي سلطة خارجية أو داخلية، ما يجعل إرادتها فوق كل إرادة أخرى.

شهد مفهوم "السيادة" في النظام الدولي تحولاً كبيراً من كونه مطلقاً إلى نسبي، وذلك نظرًا للتغيرات العالمية المستمرة. ومن أبرز التطورات التي ساهمت في هذا التحول هو الفضاء السيبراني، الذي شكل تحدياً لمفهوم السيادة التقليدية في القانون الدولي. ويعد هذا التحدي من أبرز الدلائل على إعادة النظر في مفاهيم السيطرة والتحكم، حيث أضاف الفضاء السيبراني بعدا جديدا للتفاعلات الدولية، مما يتطلب إعادة تقييم آليات السيادة في هذا المجال[1].

بشكل عام، يستخدم لفظ السيادة الرقمية غالبًا للتعبير عن قوة الدولة واستقلاليتها في المجال اللامادي، كما يُستخدم أيضًا لوصف مختلف أشكال الاستقلالية والتحكم والسيطرة على البنى التحتية الرقمية، بما في ذلك التقنيات والمحتوى الرقمي ووسائل الاتصال وكل العناصر التي ترتبط بالمجال السيبراني وتتعلق به،[2] في حين ذهب البعض لاعتبار السيادة الرقمية تتمظهر في قيام الدولة ببسط سيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل في الإنترنت، حيث

[1] أنديرا عراجي، القوة في الفضاء السيبراني؛ فصل عصري من التحدي والاستجابة، دار ميرزا، بيروت، 2019، ص ص 83-86.

[2] فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية، المجلة الجزائرية للأمن الإنساني، المجلد الخامس، العدد 1، يناير 2020، ص 11.

انه لا وجود للسيادة الرقمية لولا وجود الإنترنت وتخطيه لحدود السيادة التقليدية المتمثلة في الفضاء المادي للدولة ضمن حدودها الإقليمية[1].

2- جدلية الاعتراف بسيادة الدول على فضائها الرقمي

اختلفت آراء علماء السياسة بشأن تأثير الأمن السيبراني على سيادة الدولة .فمن وجهة نظر دانيال لامباش، ساهم الفضاء السيبراني في تعزيز سيادة الدولة عبر دعم مفهوم" السيادة الإلكترونية "أو ما يعرف بـ» السيادة على البيانات"، والذي يعني فرض السيادة الوطنية داخل الفضاء السيبراني، أي تكوين مناطق ذات سيادة وطنية ضمن هذا الفضاء .ويعتمد هذا المفهوم على نظرية الممارسة والمفاهيم المزدوجة لإعادة التوطين، المعروفة أيضًا بـ» الأنطولوجيا الإقليمية."

وتشمل الأساليب التي تستخدمها الجهات الفاعلة، مثل الدول، لممارسة السيطرة على الفضاء السيبراني، قطع الإنترنت أثناء الأزمات السياسية، التحكم في البرمجيات والخوارزميات باستخدام تقنيات الذكاء الاصطناعي، وفرض رقابة مشددة على المحتوى، كما هو الحال في دول مثل تركيا وتايلاند. علاوة على ذلك، تلجأ بعض الدول إلى ممارسات مثل القرصنة الوطنية أو تطبيق قوانين"توطين البيانات" التي تمنع نقل البيانات عبر الحدود، كما هو الحال في روسيا والصين، ما يعكس قوة الدولة وسلطتها بشكل مستمر[2].

تملك الدول مجموعة من الأدوات التي تمكنها من إعادة تشكيل حدودها الوطنية داخل الفضاء السيبراني، وذلك عبر ممارسات تهدف إلى بسط سيطرتها الرقمية. من أبرز هذه الأدوات :حجب بروتوكولات الإنترنت الخاصة بمواقع معينة، ومراقبة الكلمات المفتاحية لرصد

[1] أحمد شحيرط، تحديات الإنترنيت لسيادة الدول (السيادة الرقمية)، مجلة البحوث القانونية والاقتصادية، الجزائر، المجلد الخامس، العدد 1، 2022، ص 305.

[2] بن قطاط خديجة، تداعيات الحروب السيبرانية على السيادة الرقمية، مجلة القانون العالم الجزائري والمقارن، جامعة سيدي بلعباس، المجلد 10، العدد 2، ديسمبر 2024، ص 288.

النقاشات المرتبطة بمواضيع تعتبرها الدولة حساسة أو تهديدا محتملا، فضلًا عن حظر الوصول إلى المنصات والمواقع التي تصنف على أنها تخريبية أو معادية للمصلحة العامة.[1]

تطرح إشكالية الاعتراف بالسيادة الرقمية للدول نتيجة للمواقف السلبية التي تتبناها بعض الأطراف الدولية، إذ لم تُقرّ جميع الدول بعد بهذا الشكل من السيادة داخل الفضاء السيبراني، نظرا لاختلاف السياسات والممارسات المتبعة من دولة لأخرى. فبينما ترى بعض الدول، مثل الولايات المتحدة الأمريكية، أن الفضاء السيبراني يعد من المشاعات العالمية، ولا يجوز إخضاعه لسيادة وطنية، تعتمد دول أخرى رؤية مغايرة، تعتبر أن بسط السيطرة على هذا الفضاء أمر ضروري للحد من تأثيراته وانعكاساته على أمن الدولة،[2] حيث تتبنى الصين سياسة صارمة في فرض السيطرة على الفضاء السيبراني، وهو ما يجسد رؤيتها الخاصة لمفهوم السيادة الرقمية .وفي السياق نفسه، يولي الاتحاد الأوروبي اهتمامًا بالغًا بحماية البيانات، ويتجلى ذلك من خلال تبنيه للائحة العامة لحماية البيانات، حيث يُنظر إلى البيانات على أنها جزء لا يتجزأ من السيادة الوطنية .وتُدرك هذه الدول أن الفضاء السيبراني قد يشكل تهديدًا مباشراً لأمنها القومي، ما يدفعها إلى اتخاذ تدابير مشددة لضبط تدفق المعلومات وحماية البنى التحتية الرقمية، إلى جانب سن تشريعات متنوعة لتعزيز أمن البيانات والسيادة الرقمية. وتؤدي هذه السياسات أحيانًا إلى نشوء نزاعات قانونية بين الدول، لاسيما فيما يخص تبادل البيانات عبر الحدود.

وعلى الرغم من تنامي الحاجة إلى التعاون الدولي لمواجهة التحديات السيبرانية العالمية، إلا أن هذا التعاون لا يخلو من التعقيد، بفعل التباينات القائمة في السياسات الوطنية .وتسعى العديد من الدول إلى فرض ولايتها القضائية على الفضاء الإلكتروني من خلال تنظيمه وفقًا لمعاييرها الوطنية، بهدف حماية هذا الفضاء من التهديدات التي قد تمس بثقة المجتمع الرقمي وسلامته وأمنه، خاصة في ظل تزايد وتيرة الهجمات السيبرانية[3].

---

[1] Daniel Lambach, "The Territorialization of Cyberspace", International Studies Review, Vol 22, Issue 3, September 2020, PP 482–506.

[2] أنديرا عراجي، المرجع السابق، ص 112.

[3] بن قطاط خديجة، المرجع السابق، ص 289.

ثانيا: مفهوم الأمن السيبراني وأبعاده الأساسية في الفضاء الرقمي

يشكل الأمن السيبراني أحد الركائز الأساسية لحماية الفضاء الرقمي، حيث يهدف إلى تأمين الأنظمة والشبكات والمعلومات من التهديدات المتزايدة في البيئة الرقمية، ويقوم على مجموعة من الأبعاد المتكاملة التي تضمن سلامة البيانات وسريتها وتوافرها.

1- مفهوم الأمن السيبراني

لقد شهد مصطلح الأمن السيبراني عدة تعريفات من جهات رسمية وغير رسمية، كما نجد له عدة تعريفات اصطلاحية، ويصبو تجسيد هذا المفهوم إلى تحقيق الكثير من الأهداف نظرا لأهميته.

أ- تعريف الأمن السيبراني

تم تعريفه من قبل الاتحاد الدولي للاتصالات بأنه "مجموعة الأدوات والسياسات ومفاهيم الأمن وتحفظات الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين"[1]، كما يعرف الأمن السيبراني حسب الهيئة الوطنية للأمن السيبراني بأنه: "تأمين كل الفضاء السيبراني الموجود و المترابط شبكياً من البنية التحتية لتقنية المعلومات، التي تشمل الإنترنت وشبكات الاتصالات، وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعايير والإجراءات المرتبطة بها".

يؤكد إدوارد أموروسو في *دليل هارفارد بزنس ريفيو* أن الأمن السيبراني يشمل "مجموعة الوسائل التي تهدف إلى الحد من أخطر الهجمات التي تستهدف البرمجيات أو أجهزة الحاسوب أو الشبكات." ويقوم هذا المفهوم على الإحساس الفعلي أو التصوري بغياب أو بضعف التهديدات، سواء كانت مادية أو رقمية، والتي قد تستهدف البنى التحتية للمجتمع المعلوماتي، خاصة في جوانبها الحساسة كالمجالات العسكرية، والاجتماعية، والثقافية،

[1] الاتحاد الدولي للاتصالات، مجموعة النصوص الأساسية للاتحاد الدولي للاتصالات التي اعتمدها مؤتمر المندوبين المفوضين، جنيف، 2019، ص748.

والاقتصادية، بغض النظر عن مصدر هذه التهديدات، داخلياً كان أو خارجياً، وهو ما يستدعي استعدادا وتفاعلا، سواء على المستوى الاجتماعي أو على الصعيد الرسمي، لمواجهتها والتصدي لها[1].

على الرغم من وجود عدة تعريفات للأمن السيبراني، إلا أنها تتلخص جميعها في مفهوم واحد: توفير الحماية السيبرانية بهدف ضمان توافر واستمرارية نظم المعلومات واتخاذ التدابير اللازمة لحماية الأفراد والدول من المخاطر السيبرانية[2].

ب-أهداف وأهمية الأمن السيبراني

يعنى الأمن السيبراني بحماية الأنظمة الحاسوبية من الوصول غير المشروع، ومنع العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل، كما يسعى إلى ضمان استمرارية الخدمات وعدم تعطيلها للمستخدمين المصرح لهم. وتشمل أهدافه الأساسية أيضا ضمان انسيابية انتقال المعلومات بشكل آمن ومرخص، واسترداد البيانات المسربة بأسرع وقت ممكن في حال وقوع اختراقات.

أما أهمية الأمن السيبراني، فتتجلى في تحقيق عناصر السلامة كحماية البيانات من الهجمات والقرصنة، وكذا تحقيق السرية لضمان عدم وصول غير المصرح لهم إلى المعلومات، كما تكمن أهميتها في الجاهزية من خلال توفير المعلومات عند الحاجة إليها. وتكمن فائدته كذلك في تقليل التهديدات والاختراقات، وحماية البيانات الحساسة، وضمان استمرارية عمل المؤسسات الرقمية دون انقطاع، خاصة فيما يتعلق بالخدمات الحيوية[3].

---

[1] حميدي حياة، طايلب نسيمة، مدخل مفاهيمي حول الأمن السيبراني، مجلة مدار للدراسات الاتصالية الرقمية، جامعة الجزائر 3، المجلد 2، العدد 2، نوفمبر 2022، ص 5.

[2] سي عبد القادر حنان، الأمن السيبراني وأثره على دول العالم، مجلة البصائر للدراسات القانونية والاقتصادية، جامعة عين تموشنت، المجلد 4، العدد 7، 2024، ص 23.

[3] حميدي حياة، طايلب نسيمة، المرجع السابق، ص ص 9، 10.

2- أبعاد الأمن السيبراني

تختلف أبعاد الأمن السيبراني من مجال لآخر:

أ. البعد العسكري:

نشأ الفضاء الإلكتروني في بيئة عسكرية، ثم انتقل إلى المجالات العلمية، وقد استخدم في تطوير القدرات العسكرية، حيث ظهر بوضوح في الصراع السيبراني بين روسيا وجورجيا، والهجمات على استونيا، والاختراقات النووية في إيران. يتميز الأمن السيبراني العسكري بقدرته على ربط الوحدات العسكرية بسرعة وفعالية، ما يسهم في اتخاذ القرارات وتحقيق الأهداف عن بُعد .وتجاهل هذا البعد يؤدي إلى مخاطر كبيرة من هجمات مضادة تستهدف البنية العسكرية.

ب. البعد الاقتصادي

أصبح الاقتصاد الرقمي قائمًا على المعرفة والتكنولوجيا، ما أدى إلى ازدياد الاعتماد على الإنترنت في إدارة المعاملات الاقتصادية والمالية. تشير الإحصائيات إلى النمو الهائل في التجارة الإلكترونية، لكن هذا النمو مهدد بارتفاع الجرائم السيبرانية، ما يحتم على الدول تعزيز معايير الأمن السيبراني لضمان استمرار النمو الاقتصادي وحماية البيانات والمعاملات[1].

ت. البعد الاجتماعي:

يتطلب تعزيز الأمن السيبراني وعيا مجتمعيا بأهمية الأمان الإلكتروني من خلال التثقيف المدني والحملات الإعلامية، مع التركيز على المسؤولية الفردية والجماعية. كما يجب ترسيخ الثقافة الأمنية ضمن الثقافة التكنولوجية، وضمان النفاذ الأمن إلى الشبكة العالمية من خلال مدونة أخلاقيات تحكم سلوك الفاعلين السيبرانيين.

[1] بارة سمير، الأمن السيبراني (cyber Security) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الانساني، جامعة باتنة، المجلد 2، العدد 2، 2017، ص ص 260، 262.

ث. البعد القانوني:

أفرز الفضاء السيبراني التزامات قانونية جديدة، كحق النفاذ إلى الإنترنت، وحماية المدونات والتجمعات الإلكترونية، وحقوق الملكية الفكرية، إلى جانب موجبات مثل حفظ البيانات والإبلاغ عن الجرائم الرقمية. ويتطلب الأمر ترسانة قانونية مرنة ومواكبة لهذه التحولات التقنية والاجتماعية لضمان الحماية القانونية في البيئة الرقمية[1].

ج. البعد السياسي

تلعب الشبكات الاجتماعية دورًا متزايدًا في الحياة السياسية، من خلال الحملات الانتخابية والاحتجاجات الإلكترونية، إلى جانب استخدامها من قبل الحكومات لنشر السياسات، أو من قبل الجماعات الإرهابية في التجنيد والتمويل. وهو ما يفرض على الدول تطوير استراتيجيات لحماية أمنها السيبراني من التدخلات والتهديدات السياسية والإرهابية عبر الفضاء الرقمي[2].

يظهر مما سبق أن الأمن السيبراني هو من مقومات الحفاظ على سيادة الدول على مجالها الرقمي، هذا المجال الذي شهد الكثير من المستجدات في عصر الذكاء الاصطناعي.

---

[1] إسلام فوزي، الأمن السيبراني الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي، المجلة الاجتماعية القومية، المجلد 56، العدد 2، مصر، ماي 2019، ص ص 113 ومايليها.

[2] بارة سمير، المرجع السابق، ص 260.

المحور الثاني

الذكاء الاصطناعي كفاعل مؤثر في بنية السيادة الرقمية والأمن السيبراني

مع تزايد الاعتماد على التكنولوجيا الرقمية في مختلف مجالات الحياة، برز الذكاء الاصطناعي كأحد أبرز التحولات التقنية التي تعيد تشكيل مفاهيم السيادة الرقمية والأمن السيبراني.

أولا: تعريف الذكاء الاصطناعي

لقد عرف عالم الكمبيوتر الأمريكي جون ماكرثي الذكاء الاصطناعي بأنه: "علم وهندسة صناعة الآلات الذكية وخاصة برامج الكمبيوتر الذكية"،[1] ويُعرف الذكاء الاصطناعي أيضاً على أنه "مجموعة متنوعة من الأساليب والتقنيات والأدوات لإنشاء النماذج وحل المشكلات عن طريق محاكاة سلوك الأشخاص المدركين"، كما يعرف بأنه أحد أبرز التطبيقات الحديثة لعلوم الحاسب الآلي، التي لها قدرات فائقة تحاكي قدرات الذكاء البشري والاستفادة منها تسهل العمل في مختلف مجالات الحياة البشر، وأنه النشاط المكرس لجعل الآلات ذكية، والذكاء هو تلك الجودة التي تمكن الكيان من العمل بشكل مناسب وببصيرة في بيئته". ويُقصد به أيضاً: "ذلك العلم الذي يهتم بصنع آلات ذكية تتصرف كما هو متوقع من الإنسان أن يتصرف ويتطرق الذكاء الاصطناعي[2]."

تم وضع عدد متنوع من التعريفات في مذكرة لجنة الأمم المتحدة للقانون التجاري الدولي في الدورة الحادية والخمسون لعام 2018، لكن لم تحظ بقبول عالمي، بأنه"...الذكاء الاصطناعي بشكل عام هو علم استنباط نظم قادر على حل المشاكل وأداء الوظائف بمحاكاة العمليات

---

[1] منسل كوثر، دور الإدارة الإلكترونية في الجزائر، نحو بروز قانون الإدارة الإلكترونية، أطروحة دكتوراه، تخصص قانون عام، قسم الحقوق، جامعة قالمة، كلية الحقوق والعلوم السياسية، قالمة، الجزائر، 2023، ص 471.

[2] أحمد عبد الفتاح حمدي الهنداوي، محمود مصطفى أحمد، الذكاء الاصطناعي وتطبيقاته في تطوير الإدارة الجامعية "رؤية مقترحة، جامعة الأزهر، العدد 92، الجزء 2، 2021، ص 484.

الذهنية، ويمكن تلقين الذكاء الاصطناعي كيفية حل مشكلة ما، ولكنه قادر أيضا على دراسة المشكلة ومعرفة كيفية حلها بمفرده دون تدخل بشري ويمكن للنظم المختلفة أن تبلغ مستويات مختلفة من التشغيل الذاتي وفي مقدورها أن تتصرف باستقلالية."[1]

وأوردت الأمم المتحدة تعريفا للذكاء الصناعي بأنه "التخصص في علم الحاسوب الذي يهدف إلى تطوير آلات وأنظمة بإمكانها أن تؤدي مهاما ينظر إليها على أنها تتطلب ذكاء بشريا، سواء كان ذلك بتدخل بشري محدود أو بدون تدخل بشري."[2]

أما بالرجوع إلى التشريعات فنجد أن المشرع الجزائري لم يضع تعريفا شاملا ودقيقا للذكاء الاصطناعي، إلا أنه نظم وبموجب القانون رقم 18-05 المؤرخ في 10 ماي 2018، والمتعلق بالتجارة الإلكترونية، إمكانية الاستناد إلى التكنولوجيات الحديثة، لاسيما البرمجيات الذكية، في إبرام العقود الإلكترونية. كما صدر المرسوم الرئاسي رقم 21-323 المؤرخ في 22 أوت 2021، الذي تم بموجبه إنشاء المدرسة الوطنية العليا للذكاء الاصطناعي.

وفي السياق ذاته، تم تنصيب المجلس العلمي للذكاء الاصطناعي كهيئة استشارية ذات طابع علمي، تُعنى بتطوير استخدامات الذكاء الاصطناعي، خصوصًا في مجالات التعليم، والصناعة، والاقتصاد. ويتولى هذا المجلس مهمة تشخيص الإمكانيات المادية والبشرية المتوفرة في هذا المجال، واقتراح برامج للتكوين، إلى جانب رصد فرص التعاون الدولي في مجال الذكاء الاصطناعي.

بالرجوع إلى التشريعات المقارنة نجد أن التشريع الأمريكي قد عرف الذكاء الاصطناعي في قانون لجنة الأمن القومي للذكاء الاصطناعي بأنه :" نظام اصطناعي يؤدي المهام في ظل ظروف متفاوتة وغير متوقعة دون إشراف بشري كبير، أو يمكنه التعلم من التجربة وتحسين الأداء عند تعرضه لمجموعات البيانات، نظام اصطناعي يتم تطويره في برامج الكمبيوتر، أو

---

[1] حمدان صدخان البزوني كاظم، أثر الذكاء الاصطناعي في نظرية الحق، المؤسسة الحديثة للكتاب، لبنان، 2023، ص 27.

[2] إخلاص مخلص إبراهيم، زياد طارق جاسم، "الذكاء الصناعي- جدلية الافتراض القانوني وصحة التصرفات- "، الوقائع الرسمية للمؤتمر الدولي السادس حول القضايا القانونية(ILIC2021) ،كلية القانون، جامعة تيشك الدولية، 25نوفمبر 2021.، تم الاطلاع يوم 20 ماي 2023، على الساعة 19.30، أنظر الموقع الالكتروني: https://conferences.tiu.edu.iq/ilic/wp-content/uploads/2022/01/15.pdf.

الأجهزة المادية، أو أي سياق آخر يحل المهام التي تتطلب شبيهة بالبشر لكل استقبال، أو إدراك، أو تخطيط، أو تعلم، أو اتصال، أو فعل جسدي؛ نظام مصطنع للتفكير أو التصرف كإنسان بما في ذلك البنى المعرفية والشبكات العصرية؛ مجموعة من التقنيات، بما في ذلك التعلم الآلي، المصممة لتقريب مهمة معرفية؛ نظام مصطنع مصمم للعمل بشكل أصلي، بما في ذلك وكيل برمجيات ذكي أو روبوت مجسد يحقق الأهداف باستخدام الإدراك و التخطيط والاستدلال والتعامل و التواصل واتخاذ القرار".

ثانيا: الذكاء الاصطناعي كأداة استراتيجية لتعزيز السيادة الرقمية وصمود الأمن السيبراني

في عصر تتسارع فيه التكنولوجيا بشكل غير مسبوق، برز الذكاء الاصطناعي كأحد أبرز العوامل التي تشكل مستقبل الفضاء الرقمي، حيث تتجلى أدوار الذكاء الاصطناعي في تعزيز الأمن السيبراني وتحقيق السيادة الرقمية من خلال عدة تطبيقات رئيسية:

1. **إدارة البيانات الضخمة:** مع تزايد حجم الأنشطة اليومية عبر الإنترنت، يتم تبادل كميات هائلة من البيانات بين المستخدمين والبنية التحتية. هذا الكم الكبير يشكل تحدياً كبيرا لمحللي الأمن السيبراني في مراقبة كل التفاصيل وتقييم المخاطر المحتملة. هنا يظهر الذكاء الاصطناعي كحل مثالي، حيث يتمكن من مراقبة حركة البيانات وتحليل سلوك الخوادم بدقة، مما يتيح له الكشف التلقائي عن التهديدات المحتملة فور ظهورها. نظراً للكم الهائل من المعلومات المتاحة على شبكة الإنترنت، وتزايد حجم البيانات وانتشار البرمجيات المفتوحة المصدر، يواجه محللو الأمن السيبراني صعوبات كبيرة في رصد التهديدات الإلكترونية المرتبطة بهذه البيانات ضمن الإطار الزمني المناسب، لمواجهة هذا التحدي، تم تطوير نظام ذكي آلي يعتمد على تقنيات متقدمة لتحليل ومعالجة هذه البيانات، حيث يقوم باستخراج المحتوى الإلكتروني المهدد من المصادر العامة على الإنترنت باستخدام تقنية متقدمة تعرف باسم Doc2Vec، والتي تمكن من تمثيل النصوص بشكل فعّال لتحليلها واكتشاف التهديدات بدقة أكبر[1].

[1] Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada. Identification of cybersecurity specific content using the doc2vec language model. In 2019 IEEE 43rd annual com- puter software and applications conference (COMPSAC), volume 1, pages 396–401. IEEE, 2019.

2. **التنبؤ بالتهديدات المستقبلية:** حجم البيانات الضخم الذي يتعامل معه محللو الأمن يصعب معه التوقع المبكر للتهديدات .بفضل قدراته على معالجة كم هائل من المعلومات في وقت واحد، يمكن للذكاء الاصطناعي الكشف المبكر عن الأنشطة الخبيثة والتنبؤ بالهجمات المستقبلية .هذا يمكن الجهات الأمنية من اتخاذ إجراءات وقائية سريعة وفعالة، حيث يبقى الذكاء الاصطناعي في حالة تأهب مستمر لمواجهة أي تهديد محتمل وحماية البيانات والأنظمة.

3. **سرعة اكتشاف التهديدات:** الكشف السريع عن التهديدات يمثل عاملاً حاسماً في حماية النظم الرقمية. تشير الإحصائيات إلى أن 42% من المؤسسات تواجه زيادة في التهديدات التي تتطلب استجابة فورية. ويعد الذكاء الاصطناعي أداة قوية في هذا المجال، حيث يستطيع فحص كميات هائلة من البيانات بسرعة كبيرة لاكتشاف الهجمات السيبرانية. بالرغم من ذلك، يعاني 56% من المؤسسات من ضغوط كبيرة بسبب العبء التحليلي على فرق الأمن السيبراني، بينما يعجز 23%منهم عن التحقق الفعال من التهديدات. يوفر الذكاء الاصطناعي حلا لهذه التحديات عبر تحسين سرعة ودقة عمليات الكشف والاستجابة[1].

4. **الذكاء الاصطناعي كأداة استراتيجية في مكافحة الإرهاب تعزيزا للسيادة الرقمية:** أدى التقدم التكنولوجي في العصر الحديث إلى توسيع استخدامات الذكاء الاصطناعي ليصبح أداة محورية في دعم الأمن ومكافحة الإرهاب، خاصة من خلال قدرته على التفاعل مع وسائل الاتصال الحديثة وشبكات التواصل الاجتماعي، مما أتاح للأجهزة الأمنية كشف التهديدات المحتملة واعتراضها قبل وقوعها. يُستخدم الذكاء الاصطناعي في جمع وتحليل كميات ضخمة من البيانات، وتتبع المعلومات الدقيقة، والتعرف على الوجوه، ما يساعد في تحديد منفذي العمليات الإرهابية والمروجين لها. كما يساهم في تقليل هامش الخطأ خلال عمليات البحث والتحقيق والملاحقة، مما يعزز كفاءة الأجهزة الأمنية ويزيد من ثقة المواطنين بها. كذلك، يساعد الذكاء الاصطناعي في تصنيف الأفراد المعرضين للتأثير بالأفكار الهدامة وتوجيههم عبر برامج وقائية مخصصة، كما يمكنه تحليل الأدلة الرقمية لتحديد طبيعة الجماعة أو الشخص المتورط في أي مرحلة من مراحل تنفيذ العمل الإرهابي. ومن جهة أخرى، يستخدم الذكاء الاصطناعي لمنع انتشار المواد الدعائية على المنصات الرقمية كافيسبوك، من خلال مطابقة وتحليل الصور

[1] حسن نايف مبارك الحجرف، دور الذكاء الاصطناعي في تعزيز الأمن السيبراني، مجلة الدراسات الجامعية للبحوث الشاملة، المجلد 5، العدد 32، 2024، ص 14084.

ومقاطع الفيديو، وإنشاء قواعد بيانات لرصد الأنشطة المشبوهة[1]. ويعد تسخير هذه التقنيات في المجال الأمني ركيزة أساسية للحفاظ على السيادة الرقمية، حيث تمكن الدول من حماية فضائها الرقمي من التدخلات الخارجية والسيطرة على بياناتها الحساسة. كما يسهم الذكاء الاصطناعي في تحقيق الأمن السيبراني، من خلال قدرته على اكتشاف التهديدات الإلكترونية في الزمن الحقيقي والاستجابة السريعة لها، مما يشكل حصنا دفاعيا في مواجهة الهجمات الرقمية المتزايدة. غير أن هذا الاستخدام لا يخلو من تحديات، إذ بات بإمكان بعض التنظيمات غير الحكومية الحصول على تقنيات الذكاء الاصطناعي عبر السوق السوداء، ما يفرض تهديدا متزايدا ويثير مخاوف من عسكرة هذه التكنولوجيا بدل تسخيرها لأغراض تنموية. تعد النماذج التنبؤية المدعومة بالخوارزميات الذكية أداة فعالة لتحليل البيانات الرقمية الهائلة، مما يجعل الذكاء الاصطناعي عنصرا أساسيا في أي استراتيجية شاملة لتعزيز الأمن والاستقرار الرقمي[2].

5. إثبات الجرائم السيبرانية باستخدام الشبكات العصبية حفاظا على الأمن السيبراني:

تعد الشبكات العصبية أنظمة إلكترونية تحاكي بنية ووظائف الجهاز العصبي البيولوجي، وتستخدم بفعالية في تحليل البيئات السيبرانية المعقدة، خاصة في مجالات التنبؤ والتصنيف والكشف عن السلوك الإجرامي. ومن أبرز تطبيقاتها في إثبات الجرائم السيبرانية:

- شبكة Neuro Net: تعتمد على معالجة المعلومات الموزعة لرصد المخالفات السيبرانية، حيث تُصدر تنبيهات فورية وتُفعّل إجراءات مضادة .أثبتت كفاءتها في التصدي لهجمات حجب الخدمة، من خلال تصميم معرفات هوية عصبية تُميز وتُثبت مختلف أنواع الهجمات.

[1] سامح راشد، الذكاء الاصطناعي في مواجهة الإرهاب فرص وتحديات، دورية "آفاق استراتيجية"، مركز معلومات مجلس الوزراء، العدد 4، القاهرة ، أكتوبر 2021، ص 63.

[2] لمزيد من المعلومات ينظر: عادل عبد السميع عوض، دور الذكاء الاصطناعي في التنبؤ بمكافحة الارهاب، مجلة متون، جامعة سعيدة، المجلد 17، العدد 1، 2024.

• شبكة :IDS-NNM نظام يعتمد على الشبكات العصبية والنمذجة لإثبات محاولات الاختراق الإلكتروني بدقة عالية، دون تنبيهات كاذبة. كما طُوّرت أنظمة مشابهة للكشف عن حركة المرور المشبوهة باستخدام شبكات عصبية اصطناعية[1].

تُظهر هذه التطبيقات مدى فاعلية الشبكات العصبية في دعم الإثبات التقني للجرائم السيبرانية.

6. الذكاء الاصطناعي كأداة لتعزيز الأمن القومي: يساهم الذكاء الاصطناعي بشكل فعال في تعزيز الأمن القومي من خلال عدة فوائد رئيسية، أبرزها القدرة على التنبؤ والاستشعار المبكر للتهديدات عبر تحليل كميات ضخمة من البيانات واكتشاف الأنماط المحتملة، مما يساعد على إصدار تحذيرات استباقية. كما يستخدم في التعرف على الوجوه وتتبع المطلوبين، وتحسين نظم المراقبة الحدودية باستخدام تقنيات متقدمة، فضلا عن دوره في دعم الأمن السيبراني عبر رصد الهجمات الرقمية والتصدي لها بفعالية. ويعد الذكاء الاصطناعي أداة مهمة في دعم اتخاذ القرار الأمني، من خلال تقديم تحليلات وتوصيات دقيقة وسريعة، تسهم في مواجهة التحديات الأمنية بكفاءة أعلى[2].

ثالثا: الذكاء الاصطناعي بين تهديد السيادة الرقمية وتقويض الأمن السيبراني

رغم الفوائد الكبيرة التي يوفرها في تعزيز قدرات الدول والمؤسسات، إلا أن الذكاء الاصطناعي يحمل في طياته تحديات وتهديدات جدية تمس السيادة الرقمية وأمن الفضاء السيبراني.

1- **الذكاء الاصطناعي تهديد لاستقرار الدبلوماسية الدولية:** أضحى الاستخدام الضار للذكاء الاصطناعي في عدد متزايد من القطاعات – وعلى رأسها الأمن السيبراني والنفسي العالمي – أحد أبرز التحديات التي تستدعي إعادة تقييم السياسات الخارجية

[1] حمد عبد الله علي النيادي، الدليل السيبراني المستمد من الذكاء الاصطناعي، المجلة القانونية، جامعة القاهرة، المجلد 14، العدد 4، 2022، ص ص 1249- 1254.

[2] يمكن الاطلاع على: دبار محمد الأمين، بابو جمال الدين، تداعيات الذكاء الاصطناعي على الأمن القومي، مجلة القانون الخاص، جامعة الجلفة، المجلد 2، العدد 1، 2024، ص ص 102-103.

والدبلوماسية والتعاون الدولي .ويُعد هذا التهديد أحد المحركات المركزية لما بات يعرف بـ »الحرب الباردة التكنولوجية الجديدة"، حيث تتنافس القوى الكبرى على التفوق في مجال الذكاء الاصطناعي. وقد أسفر ذلك عن بروز قوى تقنية واقتصادية ناشئة تفرض تحولات في بنية النظام الدولي، مما يستوجب إعادة تعريف القواعد التي تنظم سلوك الفواعل الدولية التقليدية وغير التقليدية.

وفي هذا السياق، أصبحت الدول، بصفتها اللاعبين الأساسيين في العلاقات الدولية، مطالبة بمواجهة إشكاليات مستحدثة مثل السيادة على البيانات، والأمن السيبراني، والدبلوماسية الاصطناعية، والحرب الإلكترونية، وهي جميعها مفاهيم متشابكة مع الذكاء الاصطناعي. ويمثل هذا الواقع تحديا استراتيجيا جديدا قد يؤدي إلى اختلال التوازن الدولي، ويقوض الأطر القانونية والسياسية الكلاسيكية الحاكمة للعلاقات بين الدول[1].

2- أثر الذكاء الاصطناعي في تصاعد الهجمات السيبرانية وانتهاك السيادة الرقمية:

رغم أن أنظمة الأمن المبنية على الذكاء الاصطناعي صممت لحماية البنية التحتية الرقمية من التهديدات السيبرانية، إلا أن هذه الأنظمة قد تتحول إلى سلاح فعال في أيدي القراصنة، والمخترقين، وحتى بعض الأجهزة الاستخباراتية، حيث يمكن استغلال قدرات الذكاء الاصطناعي لشن هجمات احتيالية متقدمة، وتنفيذ تهديدات آلية، واستخدام الروبوتات الذكية في مهاجمة البنى التحتية الرقمية، كما تشمل الأساليب العدائية المتطورة القدرة على تعديل التعليمات البرمجية القابلة للتنفيذ، والتكيّف مع أنظمة التشغيل لتفادي الاكتشاف من قبل برامج الحماية، بل وحتى مهاجمة أنظمة الكشف ذاتها.

في المقابل، تعاني أنظمة الأمن المعتمدة على الذكاء الاصطناعي من محدودات تجعلها عرضة للخداع، لا سيما عند الاعتماد على بيانات تدريب غير دقيقة، أو مفرطة المعالجة، مما يؤدي إلى اتخاذ قرارات خاطئة. هذه الثغرات قد تستغل لتنفيذ هجمات سيبرانية مدمرة تؤدي

[1] Tamuno Miegbam, A., & Bariledum, K, Artificial Intelligence and Diplomacy in the 21st Century: The African Perspective, Central Asian Journal Of Theoretical And Applied Sciences 10(3), 2022, p 55.

إلى خسائر مادية جسيمة، كما تقوّض قدرة الدولة على حماية فضائها الرقمي، بما يهدد سيادتها الرقمية ويضعف أمنها السيبراني في مواجهة التهديدات المتزايدة والمعقدة[1].

3- **استخدام التنظيمات الإرهابية للذكاء الاصطناعي كتهديد مباشر للسيادة الرقمية والأمن السيبراني:** رغم تعدد الصكوك الدولية لمكافحة الإرهاب في إطار هيئة الأمم المتحدة، إلا أنها لا تتضمن التزامات ملزمة صريحة بشأن تجريم استخدام الإنترنت لأغراض إرهابية، وهو ما استغلته التنظيمات الإرهابية، وعلى رأسها تنظيم" داعش"، لتجنيد الأفراد وتدريبهم عن بعد عبر ما يعرف بـ» التدريب الجرمي الإلكتروني". ويعد هذا النمط من الاستخدام الرقمي غير المشروع وسيلة خطيرة لنشر الأيديولوجيا وتوسيع رقعة التأثير خارج الحدود الجغرافية، ما يشكل تهديدا مباشرا للسيادة الرقمية للدول[2].

وقد بادرت بعض التشريعات، كقانون مكافحة الإرهاب البريطاني لعام 2000، والقرارات الإطارية للاتحاد الأوروبي، إلى تجريم هذه الأفعال، إلا أن غياب إطار دولي ملزم وموحد يُضعف فعالية المواجهة. كما أن الأدوات التقليدية للتحقيق باتت غير كافية أمام بيئة افتراضية منفتحة لا تعرف القيود، مما يعرض الأمن السيبراني للاختراق عبر منصات التدريب الرقمي المفتوحة. إن الاستخدام الإرهابي للإنترنت لا يهدد فقط أمن الدول بل يُقوّض قدرتها على فرض الرقابة الرقمية، ما يستدعي تطوير تقنيات رصد وتحليل ذكية قادرة على كشف الاستخدامات المشبوهة وحماية الفضاء السيبراني الوطني.

4- **مخاطر التحوّل الوظيفي في ظل الذكاء الاصطناعي:** أدى التوسع المتسارع في استخدام الذكاء الاصطناعي إلى تهديد واضح لهيكل الوظائف التقليدية، إذ باتت العديد من المهن الروتينية أو الخطرة مهددة بالاختفاء نتيجة حلول الآلة محل الإنسان، هذا التحول ينذر بتفاقم معدلات البطالة، لاسيما في الفئات الأقل تأهيلا رقميا، ويخلق فجوة اجتماعية واقتصادية متنامية بين من يمتلكون المهارات الرقمية ومن يستبعدون منها تدريجيا. كما أن هذا التحول قد يضعف القدرة الوطنية على الحفاظ على توازن سوق العمل، ويزيد من التبعية التكنولوجية

[1] مسيكة، محمد، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة الجزائر، المجلد 7، العدد 4، 2022، ص 458.

[2] سايمن شير كليف، استخدام الانترنت في أغراض إرهابية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، نيويورك، 2012، ص 31.

للخارج. وعلى الصعيد السيادي، فإن الاعتماد المفرط على تقنيات الذكاء الاصطناعي المستوردة يهدد السيادة الرقمية للدول التي لا تملك منظوماتها التقنية الخاصة، مما يجعلها عرضة للابتزاز التقني أو التجسس أو الاختراقات الأجنبية. كذلك، فإن إعادة هيكلة سوق العمل نحو الوظائف الرقمية دون حماية فعالة يجعل البنية التحتية أكثر عرضة للهجمات الإلكترونية، مما يضعف الأمن السيبراني ويعرض المؤسسات الحيوية لمخاطر شلل أو تسريب بيانات على نطاق واسع. إن هذه التغيرات لا تهدد فقط بارتفاع نسب البطالة أو تفاقم التفاوت الاجتماعي، بل تطرح أيضًا تحديات أمنية واستراتيجية، تمسّ صميم الاستقلال الوطني في العالم الرقمي[1].

5-تأثير الاختراق الاقتصادي الإلكتروني على سيادة الدول والأمن السيبراني: يسعى الاختراق الاقتصادي الإلكتروني إلى زعزعة أمن الدول وحكوماتها عبر استهداف معلوماتها الاقتصادية الحساسة، مما يعرضها للمساومة السياسية والاقتصادية. ويعد هذا الاختراق تهديدا خطيرا للاقتصاد الوطني، خاصة في غياب أنظمة أمن معلوماتية فعالة، حيث يؤثر على الموارد المالية للدول.

كما يستغل القراصنة الإلكترونيون الفئات الضعيفة داخل الدول النامية لإغرائهم بالمكاسب مقابل زعزعة الاستقرار ونشر أفكار تقوض شرعية الأنظمة، وقد وصف متحدث الكرملين هذا النوع من الاختراق بأنه شكل من أشكال الإرهاب والتهديد الأمني للدولة والمجتمع.

يمثل الاختراق الاقتصادي الإلكتروني أحد أخطر أشكال الهيمنة الحديثة، التي تحل محل أساليب السيطرة التقليدية كالاستعمار والحروب، معتمدين على التكنولوجيا والثورة المعلوماتية. وتشمل هذه التهديدات التدخل في الشؤون السياسية عبر منصات التواصل الاجتماعي، وانتهاك الخصوصية الوطنية من خلال احتكار شركات أجنبية للبنى التحتية الرقمية، مما يهدد السيادة الوطنية.

[1] دبار محمد الأمين، بابو جمال الدين، المرجع السابق، ص 104.

بذلك، رغم الفوائد العديدة لثورة المعلومات، فإنها تشكل في الوقت ذاته أداة للاختراق الرقمي والسيطرة غير المباشرة على الدول، عبر تجاوز الحدود الجغرافية وتحقيق نفوذ في الفضاء السيبراني.

الخاتمة

يظهر مما سبق، أن الذكاء الاصطناعي يعد فاعلا محوريا في تشكيل معالم السيادة الرقمية وتعزيز الأمن السيبراني. لقد ساعد الذكاء الاصطناعي في تحسين الدول قدراتها في الرصد والتنبؤ بالهجمات السيبرانية، وساهم في تطوير استراتيجيات متقدمة لحماية الفضاء الرقمي، إلا أن هذا التطور يطرح من جهة أخرى تحديات قانونية وأمنية معقدة، ترتبط بتقويض سيادة الدول، وتصاعد الهجمات السيبرانية، واحتكار التكنولوجيا من قبل كيانات غير خاضعة للرقابة الدولية في عصر الذكاء الاصطناعي.

وعليه توصلت الدراسة للنتائج التالية:

1. أصبح الذكاء الاصطناعي أداة مزدوجة، تجمع بين التمكين السيبراني والتهديد للسيادة الرقمية.

2. عجز الإطار القانوني الدولي عن مواكبة تسارع التطورات التقنية، مما يخلق فراغا تنظيميا في الفضاء السيبراني.

3. يمكن أن تتحول أدوات الذكاء الاصطناعي إلى وسائل هجومية في أيدي الفاعلين غير الحكوميين والتنظيمات الإرهابية.

4. يؤدي الاعتماد المفرط على تقنيات مستوردة إلى تهديد السيادة التقنية والرقمية للدول.

5. الذكاء الاصطناعي يحدث تحولا في البنية الاقتصادية والاجتماعية للدول، ما يستلزم تكيفا تشريعيا وهيكليا مستمرا.

بناء على ما تقدم نطرح بعض التوصيات كالآتي:

1. سن تشريعات وطنية واضحة ومتكاملة لتنظيم استخدام الذكاء الاصطناعي، بما يضمن الأمن السيبراني ويحافظ على السيادة الرقمية.

2. تعزيز التعاون الدولي من أجل وضع قواعد قانونية ملزمة لحوكمة الذكاء الاصطناعي في الفضاء السيبراني.

3. الاستثمار في البحث العلمي والتكوين لبناء قدرات وطنية ذات كفاءة عالية في تقنيات الذكاء الاصطناعي.

4. إنشاء أجهزة رقابة مستقلة تعنى بمتابعة استخدامات الذكاء الاصطناعي ومراقبة أخلاقيات التفاعل الرقمي.

5. التأكيد على السيادة الرقمية من خلال دعم إنتاج البرمجيات المحلية والبنى التحتية الرقمية الوطنية.

إن مواكبة العصر الرقمي تتطلب من الدول ليس فقط امتلاك الأدوات التقنية، بل أيضا وعيا قانونيا واستراتيجيًا يمكنها من حماية فضائها السيبراني، دون التفريط بسيادتها الرقمية أو أمنها القومي.

قائمة المصادروالمراجع

أولا: باللغة العربية:

أ- الكتب:

1- أنديرا عراجي، القوة في الفضاء السيبراني؛ فصل عصري من التحدي والاستجابة، دار ميرزا، بيروت، 2019.

2- توماس هوبز، اللفياثان الأصول الطبيعية والسياسية لسلطة الدولة، ترجمة دينا حرب، بشرى صعب، دار الفارابي، ص180، 2011.

3- حمدان صدخان البزوني كاظم، أثر الذكاء الاصطناعي في نظرية الحق، المؤسسة الحديثة للكتاب، لبنان، 2023.

ب- المقالات:

1- إسلام فوزي، الأمن السيبراني الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي، المجلة الاجتماعية القومية، المجلد 56، العدد 2، مصر، ماي 2019.

2- النيادي حمد عبد الله علي، الدليل السيبراني المستمد من الذكاء الاصطناعي، المجلة القانونية، جامعة القاهرة، المجلد 14، العدد 2022.

3- الهنداوي أحمد عبد الفتاح حمدي، محمود مصطفى أحمد، الذكاء الاصطناعي وتطبيقاته في تطوير الإدارة الجامعية "رؤية مقترحة، جامعة الأزهر، العدد 92، الجزء 2، 2021.

4- بارة سمير، الأمن السيبراني (cyber Security) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الانساني، جامعة باتنة، المجلد 2، العدد 2، 2017.

5- بن قطاط خديجة، تداعيات الحروب السيبرانية على السيادة الرقمية، مجلة القانون العالم الجزائري والمقارن، جامعة سيدي بلعباس، المجلد 10، العدد 2، ديسمبر 2024.

6- بيرم فاطمة، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية، المجلة الجزائرية للأمن الإنساني، المجلد الخامس، العدد 1، يناير 2020.

7- الحجرف حسن نايف مبارك، دور الذكاء الاصطناعي في تعزيز الأمن السيبراني، مجلة الدراسات الجامعية للبحوث الشاملة، المجلد 5، العدد 32، 2024.

8- حميدي حياة، طايلب نسيمة، مدخل مفاهيمي حول الأمن السيبراني، مجلة مدار للدراسات الاتصالية الرقمية، جامعة الجزائر 3، المجلد 2، العدد 2، نوفمبر 2022.

9- دبار محمد الأمين، بابو جمال الدين، تداعيات الذكاء الاصطناعي على الأمن القومي، مجلة القانون الخاص، جامعة الجلفة، المجلد 2، العدد 1، 2024.

10- راشد سامح، الذكاء الاصطناعي في مواجهة الإرهاب فرص وتحديات، دورية "آفاق استراتيجية"، مركز معلومات مجلس الوزراء، العدد 4، القاهرة، أكتوبر 2021.

11- سي عبد القادر حنان، الأمن السيبراني وأثره على دول العالم، مجلة البصائر للدراسات القانونية والاقتصادية، جامعة عين تموشنت، المجلد 4، العدد 7، 2024.

12- شحيرط أحمد، تحديات الإنترنيت لسيادة الدول (السيادة الرقمية)، مجلة البحوث القانونية والاقتصادية، الجزائر، المجلد الخامس، العدد 1، 2022 .

13- عوض عادل عبد السميع، دور الذكاء الاصطناعي في التنبؤ بمكافحة الارهاب، مجلة متون، جامعة سعيدة، المجلد 17، العدد 1، 2024.

14- مسيكة محمد، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة الجزائر، المجلد 7، العدد 4، 2022.

ت- أطروحات الدكتوراه:

- منسل كوثر، دور الإدارة الإلكترونية في الجزائر، نحو بروز قانون الإدارة الإلكترونية، أطروحة دكتوراه، تخصص قانون عام، قسم الحقوق، جامعة قالمة، كلية الحقوق والعلوم السياسية، قالمة، الجزائر، 2023.

ث- الوثائق والتقارير الدولية:

1- الاتحاد الدولي للاتصالات، مجموعة النصوص الأساسية للاتحاد الدولي للاتصالات التي اعتمدها مؤتمر المندوبين المفوضين، جنيف، 2019.

2- سايمن شير كليف، استخدام الانترنت في أغراض إرهابية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، نيويورك، 2012.

ج- المواقع الالكترونية:

- مخلص إبراهيم إخلاص، زياد طارق جاسم، "الذكاء الصناعي-جدلية الافتراض القانوني وصحة التصرفات-»، الوقائع الرسمية للمؤتمر الدولي السادس حول القضايا القانوني (ILIC2021)، كلية القانون، جامعة تيشك الدولية، 25نوفمبر 2021، تم الاطلاع يوم 20 ماي 2023، على الساعة 19.30، أنظر الموقع الالكتروني: https://conferences.tiu.edu.iq/ilic/wp-content/uploads/2022/01/15.pdf.

ثانيا: باللغة الأجنبية

Books :

- Bodin Jean, Les Six Livres de la République, Librairie AR thème Fayard, Paris, 1986.

Articles :

1- Lambach Daniel, "The Territorialization of Cyberspace", International Studies Review, Vol 22, Issue 3, September 2020.

2- Mendsaikhan Otgonpurev, Hasegawa Hirokazu, Yamaguchi Yukiko, and Shimada Hajime. Identification of cybersecurity specific content using the doc2vec language model. In 2019 IEEE 43rd annual com- puter software and applications conference (COMPSAC), volume 1, pages 396–401. IEEE, 2019.

3- Miegbam Tamuno, A., & Bariledum, K, Artificial Intelligence and Diplomacy in the 21st Century: The African Perspective, Central Asian Journal of Theoretical and Applied Sciences 10(3), 2022.

الفصل الثاني

تأصيل مفهوم السيادة الرقمية في الفقه الإسلامي وتعزيز آليات المواجهة السيبرانية.

"دراسة في قواعد الفقه ومقاصد الشريعة"

. الدكتور زيان سعيدي

دكتوراه تخصص علوم إسلامية-شريعة وقانون-

أستاذ محاضر-أ-كلية العلوم الإسلامية. جامعة الوادي

-البريد الإلكتروني المهني:saidi-ziane@univ-eloued.dz

-البرد الإلكتروني الشخصي: saidiziane1974@gmail.com

مقدمة

لا أحد يستطيع أن ينكر التَحوُّل الكبير الذي أحدثته الثورة المعلوماتية والإلكترونية في مختلف جوانب الحياة وجزئياتها سياسية واجتماعية واقتصادية وعلى مستويات متعددة.

وقد أدَّى هذا التطور التقني الرهيب إلى خلق نُظُم ومفاهيم جديدة كُرِّست من خلال الإقبال المتزايد على استعمال وسائل التواصل الاجتماعي على حساب مفاهيم تقليدية، بعضها من قبيل الثوابت والحقوق المجمع على عدم جواز المساس بها، كمفهوم السيادة التي تعتبر حقاً مقرَّراً لجميع الدول والأنظمة.

غير أن هذا المفهوم التقليدي لسيادة الدول، شهد هو الآخر تحوُّلا كبيرا في عصر الإنترنت واصطبغ بصبغة الرقمية، فظهر ما يسمى بالسيادة الرقمية.

ولم تَعُد التحديات التي تواجهها الدولة في محافظتها على سيادتها مقتصرة على الجانب الفيزيائي والمادي والذي يتمثل في تهديدات عسكرية بأسلحة فتاكة وجيوش جرارة، بل أصبحت تأتي عن طريق أجهزة حاسوبية وشاشات إلكترونية أسلحتها أنامل بسيطة تضغط على أزرار، وتعبث برموز، وتغيِّر شفرات، تدار المعركة فيها من أبعد مكان في غرف ضيقة بأبسط تجهيزات.

وإذا كان الأمن القومي لأي دولة، مرتبط بمدى قدرته على المحافظة على سيادتها، فإن من مقتضيات المرحلة الراهنة تعزيز سيادتها على المستوى الرقمي تحقيقا لأمنها القومي الرقمي.

لأن أحد الأبعاد المهمة في تشكُّل مفهوم السيادة في الوقت الراهن، هو البعد الرقمي والتكنولوجي والذي يحتِّم على الدول التفكير في التعامل الايجابي معه، التعامل المتزن الذي يجمع بين ضرورة الاستخدام لهذه الفضاءات المعلوماتية وقدرتها على حماية أمنها السيبراني والمعلومات في ظل سيادتها الرقمية.

ولما كان الفقه الإسلامي بمرونته التشريعية واتساع قواعده وكلياته مستوعبا لجميع المستجدات التي تواجه الناس، فقد حاولتُ من خلال هذا البحث التأصيل لمفهوم السيادة

الرقمية في منظور الفقه الإسلامي واستعراض آليات المواجهة السيبرانية لمختلف الجرائم الالكترونية وتهديدات السيادة من المنظور نفسه.

فكان عنوانه:" تأصيل مفهوم السيادة الرقمية في الفقه الإسلامي وتعزيز آليات المواجهة السيبرانية دراسة في قواعد الفقه ومقاصد الشريعة.

الإشكالية: في ظل التحديات المتزايدة التي تواجه الدول الإسلامية وغيرها في المجال الرقمي، برزت الحاجة إلى تأصيل مفهوم السيادة الرقمية من منظور الفقه الإسلامي. ويثير هذا تساؤلات حول الجوانب الفقهية والمقاصدية التي يمكن أن تساهم في تأطير هذا المفهوم. كذلك، يتطلب الأمر دراسة مدى قدرة قواعد الفقه ومقاصد الشريعة على تعزيز منظومة الدفاع السيبراني لمواجهة الأخطار التي تهدد السيادة الرقمية للدول.

أهمية البحث: يجد البحث أهميته في النقاط التالية:

1-أهمية السيادة بشكل عام وأهميتها في المجال الرقمي لعظم مخاطر التهديدات السيبرانية.

2-ارتباط السيادة الرقمية بتحقيق الأمن القومي بالنظر إلى تطور شكل التهديدات والتحديات للدول.

3-أهمية التقعيد الفقهي والنظر المقاصدي في تحديد أبعاد هذا المفهوم.

هدف البحث: إن الهدف الأساسي الذي يسعى هذا البحث إلى تحقيقه، يتمثل في تحديد أثر التقعيد الأصولي والفقهي في التأصيل لمفهوم السيادة الرقمية، وأهمية الرجوع إلى الأحكام والاجتهادات الفقهية والأنظار المقاصدي لبناء منظومة هيكلية يمكن من خلالها مواجهة الجرائم الإلكترونية والتهديدات السيبرانية.

منهج البحث: تتطلب الإجابة عن هذه الإشكالية استخدام عدة مناهج:

1. المنهج الاستقرائي: لجمع النصوص الشرعية (آيات قرآنية وأحاديث نبوية) التي تتعلق بمفهوم السيادة، الحماية، والتعامل مع القضايا السيبرانية، ودراسة القواعد الفقهية والمقاصدية المتعلقة بالسيادة الرقمية.

2. المنهج التحليلي: لتحليل النصوص الشرعية والقواعد الفقهية ذات الصلة، وربطها بمفهوم السيادة الرقمية، ودراسة التطبيقات الحديثة لمواجهة التحديات السيبرانية في ضوء القواعد الفقهية ومقاصد الشريعة.

3. المنهج التأصيلي: لتأصيل مفهوم السيادة الرقمية من منظور الفقه الإسلامي، من خلال استنباط المبادئ والقواعد المستمدة من الشريعة، وصياغة الإطار الشرعي للمواجهة السيبرانية بناءً على القواعد الفقهية.

4. المنهج المقارن (عند الحاجة): لمقارنة السيادة الرقمية في الفقه الإسلامي مع المفاهيم القانونية أو التقنية المعاصرة لتعزيز فهم المفهوم الشرعي وتطوير آليات المواجهة.

خطة البحث: تشتمل خطة البحث على محاور ثلاثة:

المحور لأول: السيادة الرقمية في منظور الفقه الإسلامي (المفهوم والتأصيل). وتحته فروع.

المحور الثاني: التحديات السيبرانية للسيادة الرقمية وآليات المواجهة. وتحته فروع.

المحور الثالث: البعد المقاصدي وأثره في تعزيز السيادة الرقمية وتحديد نطاقها. وتحته فروع.

المحور الأول

السيادة الرقمية في منظور الفقه الإسلامي.

(المفهوم والتأصيل)

ثمة أبعادٌ ومُحدِّداتٌ مختلفة كثيرة يمكن من خلالها التأسيس لمفهوم السيادة بما في ذلك البُعد القانوني والبُعد السياسي والبُعد الجغرافي. غير أن هذا الزخم المتراكم من استخدامات وسائل التواصل الاجتماعي كان حاضراً بثقله كمعطى أساسي ومُحدِّدٍ مركزي في تشكيل مفهوم جديد للسيادة، وهو البعد الرقمي والذي كان نتاجه ما اصطلح عليه بالسيادة الرقمية.

وسوف نتناول من خلال هذا المحور الأول، علاقة مبدأ السيادة بالرقمنة من خلال تحديد مفهوم السيادة الرقمية، وبيان أثر البعد الرقمي في تشكل مفهوم السيادة بالرقمنة، ثم نحاول تحديد جوانب التأصيل الفقهي لمفهوم السيادة الرقمية من خلال عرض موقع السيادة الرقمية ضمن مراتب الحكم الشرعي، والأدوار الشرعية التي تناط بالدولة ممثلة في الحاكم أو في رئيس الدولة.

أولا: مبدأ السيادة وعلاقته بالرقمنة.

1-المفهوم التقليدي لمبدأ السيادة: يعتبر مفهوم السيادة بشكل عام أحد أهم المسائل المثارة في الفكر السياسي والتي ثار حولها جدل تاريخي كبير، خصوصا في أعقاب الثورة الفرنسية ونهاية الصراع بين الملوك والباباوات والإقطاعيين. وفيما يلي: تعريف للسيادة وعرض موجز لتشكل المفهوم السياسي والقانوني وفي الفكر الإسلامي لمبدأ السيادة.

- **تعريف السيادة لغة:** السيادة، الشرف والمجد. وساد يسُود سُودًا وسُؤْدَدًا وسِيادةً وسَيْدُودةً. والسَيِّد: هو الرئيس الذي فاق غيره بالعقل والمال، والدفع والنفع. وفي الحديث: «كُلُّ نَفْسٍ مِنْ بَنِي آدَمَ سَيِّدٌ، فَالرَّجُلُ سَيِّدُ أَهْلِهِ، وَالْمَرْأَةُ سَيِّدَةُ بَيْتِهَا».[1]

[1] ابن السني. عمل اليوم والليلة. برقم388 . ص346 ، وإسناده صحيح على شرط مسلم. انظر. السلسلة الصحيحة للألباني69/5

ويُطلق السَيِّد على الزوج، وفي التنزيل: وَأَلْفَيَا **سَيِّدَهَا لَدَى الْبَابِ﴾ [يوسف:25]**، لمعنى القَوَامة فيه.[1]

وعلى هذا، فإن المعاني التي تدور حولها السيادة لا تخرج عن استحقاق الشرف والمجد، وَوُفُور ما تتحقق به الغلبة ويُستَحَقُّ به التقديم من الرأي والمال والعقل، وما يتطلب التقديم من الدفع والنفع.

- **تعريف السيادة اصطلاحا**: يرتبط مصطلح السيادة بمفهوم الدولة أو السلطة العليا أو النظام السياسي الحاكم والسائد في البلد. وما دام الأمر كذلك، فإن تحديد المفهوم الاصطلاحي للسيادة يختلف بالنظر إلى المتغيرات الفلسفية أو الفكرية أو السياسية. وفيما يلي عرض لأهم التعريفات:

-تعريف جان بودان (Jean Bodin): "السلطة العليا المطلقة والدائمة في الدولة التي لا تخضع لأي سلطة أخرى".[2]

والملاحظ على هذا التعريف، أنه ربط مفهوم السيادة بمؤثرين اثنين: الإطلاق والدوام.

فالإطلاق معناه، ألا تكون هذه السلطة مقيدة بأي سلطة أخرى أو قوة داخلية كانت أو خارجية.

والدوام الذي يقتضي عدم القابلية للانتهاء والزوال أو الانتقال والتحوّل.

- **تعريف هوبز:** "هي السلطة التي يطيعها الجميع دون استثناء والتي تمتلك الحق المطلق في سن القوانين وإجبار الأفراد على الطاعة."[3]

---

[1] الزبيدي. تاج العروس 22/5

[2] Jean Bodin, Les Six Livres de la République, Librairie Arthème Fayard, Paris, 1986, p.

[3] توماس هوبز، اللفياثان الأصول الطبيعية والسياسية لسلطة الدولة، ترجمة دينا حرب، بشرى صعب. دار الفارابي 2011م. ص180

ويظهر من خلال هذا التعريفين وغيرهما من التعريفات الأخرى، استعمال مصطلح السيادة والسلطة العامة وهي السلطة السياسية بمعنى واحد. فهما وجهان لعملة واحدة.

ويرى بعض الباحثين أن استعمال المصطلحين في معنى واحد، هو خلط بين الشيء ووصفه. فالسيادة على هذا الاتجاه ليست إلا صفة تتمتّع بها السلطة السياسية العليا القائمة في الدولة.[1]

وعليه يمكن أن نفرق في تعريف السيادة بين مفهومين: قانوني وسياسي.

مفهوم قانوني: والذي يُعزّز كَوْن السيادة صفة من الصفات التي تتمتع بها الدولة أو السلطة العليا في منظور مفهوم الدولة الحديثة، بحيث تتساوى مع غيرها من الدول الأخرى بغضِّ النظر عن شكل السلطة القائمة أو المساحة الجغرافية.

أما بالنسبة للمفهوم السياسي، فتعني السيادة تمتُّع الدولة بالقوة والقدرة الفعلية على تأكيد حضورها الخارجي والداخلي، بحيث لا تخضع لأي سلطة خارجية كانت أو داخلية في اتخاذ أي إجراء يجعل إرادتها تسمو على كل إرادة.[2]

- مفهوم السيادة في الفكر الإسلامي:

إن المفهوم الإجرائي السابق الذي عُرِّفت به السيادة، ليس محلا للنزاع ولا مثارا للاختلاف حوله في المنظومة الفكرية الإسلامية. فتفسير السيادة بأنها السلطة العليا الحاكمة المطلقة التي لا تُنَازع في أمرها ولا تُعَارض في قرارها، المتفردة بالتشريع فيما يتعلَّق بتنظيم حياة المجتمع وإدارة شؤونه، أمر لا نزاع فيه ما دام الاتفاق على أن مصدر هذه السلطة العليا والمطلقة والمنفردة والدائمة هو الشرع. وهذا مضمون ما جاء في نصوص شرعية كثيرة: ﴿**إِنِ الْحُكْمُ إِلَّا لِلَّهِ**﴾ [الأنعام:57]» وَمَنْ **لَمْ يَحْكُمْ بِمَا أَنْزَلَ اللَّهُ فَأُولَئِكَ هُمُ الْكَافِرُونَ**﴾ [المائدة:44] ﴿**فَلَا وَرَبِّكَ لَا يُؤْمِنُونَ حَتَّى يُحَكِّمُوكَ فِيمَا شَجَرَ بَيْنَهُمْ ثُمَّ لَا يَجِدُوا فِي أَنْفُسِهِمْ حَرَجًا مِمَّا قَضَيْتَ وَيُسَلِّمُوا تَسْلِيمًا**﴾ [النساء:65].

---

[1] فتحي عبد الكريم . الدولة والسياسة في الفقه الإسلامي. ص13

[2] صلاح الصاوي. نظرية السيادة واثرها على شرعية الانظمة الوضعية. ص06

والصفة التي تثبت لمن يدير شؤون هذه السلطة، هي صفة وظيفية غايتها تحقيق مقاصد هذه السلطة العليا، من إقامة الدين وتنفيذ أحكامه، وتحقيق مصالح العباد، والمحافظة على حقوقهم وحماية حرياتهم...

فهما وظيفتان اثنتان تجتمعان في وظيفة واحدة وهي إقامة الإسلام. لان الإسلام دين ودولة.[1]

2-البعد الرقمي وأثره في تَشكُّل مفهوم جديد للسيادة:

إن تَشَكُّل مفهوم السيادة كغيره من المفاهيم الأخرى يخضع لعدد من المؤثرات والمتغيرات الاجتماعية والأحداث السياسية التي رافقت مختلف العلاقات والأوضاع الدولية. والسيادة التي سماها بعض الباحثين بالسيادة الصلبة تحولت بفضل السيطرة التي بسطها الذكاء الاصطناعي والثورة التقنية الهائلة التي اجتاحت الكرة الأرضية إلى سيادة سائلة ولينة.

وإذا كانت السيادة الصلبة تعني قدرة الدولة على بسط سيطرتها ونفوذها وإرادتها في حدود إقليمها الجغرافي، فإن هذه السلطة بدأت تتلاشى في ظل هذه الهيمنة الرقمية وانتشار مختلف أشكال الجرائم السيبرانية المهدِّدة لسيادتها.

وهنا برز مفهوم جديد للسيادة أسَّس له هذا الانتشار الواسع لوسائل الاتصال والتكنولوجيا، أُطلق عليه: مصطلح السيادة الرقمية أو السيادة الافتراضية، والتي تعني في مجملها قدرة الدولة على بسط نفوذها على إقليمها الافتراضي وتحقيق استقلالها المعلوماتي أو البيانات دفعاً ونفعاً.

فالتصدي للهجمات الإلكترونية ودفع أخطار التهديدات السيبرانية، من مقتضيات المحافظة على السيادة وتعزيزها. وبسط الدولة نفوذها في المجال المعلوماتي وقدرتها على التحكُّم في مختلف الأنظمة المعلوماتية على مستوى حدودها الجغرافية، وجه ثان في تعزيز مفهوم السيادة الرقمية.

---

[1] عبد القادر عوده. الإسلام وأوضاعنا السياسية. ص121

والإشكالية الكبيرة التي تواجهها الدول في تحقيق سيادتها المطلقة والتي تجعلها أكثر مسامية في تحصين نفوذها وتعزيز سلطتها، هو طبيعة الإنترنت باعتباره اختراعاً بشرياً متميزاً غير محدود، امتزجت فيه منافعه بدواهيه، وبقدر عموم النفع الذي يعود من ورائه بقدر الخطر الهائل الذي يحدثه في مجالات الحياة البشرية المتعددة. وإضافة إلى عدم المحدودية في عالم الإنترنت، يظهر تحدٍّ آخر ليس بأقل خطرا من هذا التحدي، وهو غياب الصفة القانونية المعنوية التي تمثله، مما يجعل الدول في مواجهة قوى بلا قيادة قانونية، فهي تجمعات كبرى لشبكات اتصال يغطي في مجموعها عموم الكرة الأرضية.

وخلاصة مفهوم السيادة الرقمية: هو قدرة الدول على تحكمها الكامل في إقليمها الافتراضي وتحقيق استقلالها في البيانات الرقمية وبسط سيطرتها ونفوذها في الفضاء الرقمي.

ثانيا: موقع السيادة الرقمية ضمن مراتب الحكم الشرعي.

إن التشريع الإسلامي هو المحدِّد الوحيد المكوِّن لمفهوم السيادة في المنظور الإسلامي. وتمتُّع الأمة أو الجماعة بالسيادة على قول بعض المفكرين، يمكن اعتباره مفهوما إجرائيا لمصطلح السيادة في الإسلام. لأن الأمة أو الجماعة ما هي إلا أداة لتحقيق سيادة التشريع الإسلامي، وأهم وظيفة من وظائف الحكومة في الإسلام، هي تنفيذ أحكام الشريعة الإسلامية، وهذا يتضمن أمرين اثنين: إقامة الدين والدنيا. وكل ما فيه تهديد لواحد منهما-الدين أو الدنيا-فصدُّه ومواجهته من أظهر واجبات الدولة ومقتضيات تمتُّعها بالسيادة على المعنى الذي بيناه.

وإذا كانت السيادة الرقمية تعني استقلال الدولة في إدارة بياناتها ومعلوماتها وبسط سيطرتها في الفضاء الافتراضي بما يمكِّنها من مواجهه الأخطار والتصدي للجرائم الإلكترونية، فإن هذا من أعظم واجبات الحكومة في الإسلام وفروض الولاية فيها.

وأغلب فقهاء الإسلام الذين كتبوا في الأحكام السلطانية عدَّدوا كثيرا من واجبات الإمامة ومسؤولياتها، إلا أنها ترجع إلى أمرين اثنين: إقامة الدين وتنفيذ أحكامه، وتحقيق مصالح العباد والمحافظة عليها.

ويندرج ضمن الأمر الثاني: درءُ كل المفاسد والمهدِّدات للأفراد والمجتمعات في أمنهم الديني أو الاجتماعي أو الفكري أو الاقتصادي أو السياسي...الخ.

ويقرر الماوردي رحمه الله في كتابه الأحكام السلطانية ما يمكن أن يُعتبر الأساس في تخليص الحكم الشرعي لتعزيز الدولة لسيادتها الرقمية. حيث ذكر عشرة من واجبات الحاكم ومهامه ومنها:» قوله: والخامس: تحصين الثغور بالعدة المانعة والقوة الدافعة حتى لا تظفر الأعداء بغرة ينتهكون فيها محرما، أو يسفكون فيها لمسلم أو معاهد دما".[1]

ومع تطور وسائل الاتصال التكنولوجي، فقد تحول فضاء الإنترنت إلى مسرح كبير لمختلف الاعتداءات والجرائم السيبرانية التي تمسّ الكليات الخمس التي جاءت الشريعة الإسلامية بمراعاتها. فالمواقع التي تشكك في الثوابت والعقائد، وتنتحل الإلحاد ونشر الإساءة إلى المقدسات الدينية على كثرتها لا يمكن الإحاطة بها. وضروب الاحتيال والخداع، واختراق الحسابات المالي، ونشر الفوضى والتحريض ضد الحكومات والأنظمة السياسية القائمة، ونشر البدع والضلالات الباطلة، وتشويه التصورات.... كلها جرائم تمسّ هذه الكليات الخمس. ومن أوجب واجبات الدولة تحصينها بالعدة المانعة والقوة الدافعة بتعبير الماوردي رحمه الله.

وفي الجملة، فإن كل جهد يتطلب بذله لتعزيز السيادة الرقمية تحقيقا لهذه المقاصد الشرعية يصير من الواجبات العينية باعتباره أهم وظائف السلطة العليا في الدولة الإسلامية، سواء على مستوى المراقبة للإقليم الافتراضي، أو على مستوى التدخل في توجيه الاستخدام الإيجابي لمختلف النظم والأجهزة المعلوماتية والإلكترونية.

وثمة جانب آخر يمكن أن يكون هو الآخر جانبا مهما من جوانب التأصيل لوجوب العمل على تعزيز السيادة بما في ذلك السيادة الرقمية، وهو تشريع الجهاد دفعا لضرر السائل وصدًّا لعدوانه وردًّا لفساده. قال تعالى: **﴿وَلَوْلَا دَفْعُ اللَّهِ النَّاسَ بَعْضَهُمْ بِبَعْضٍ لَفَسَدَتِ الْأَرْضُ﴾** [البقرة:252]. فالذَبُّ عن الحريم(الحرمات) وحماية البيضة هي الأخرى من واجبات الدولة ومن يتمتع بصفه السيادة.[2] والمقصود الأعظم صيان الحرمات من الانتهاك، وحفظ الحقوق من الاتلاف والضياع.

وإذا كان الواجب على الدولة بحكم سيادتها أن تؤمّن الطرق والمنافذ والمعابر ليسهل على الناس أن يتنقلوا ويسافروا آمنين مطمئنين على أنفسهم وأموالهم وأعراضهم، فإنه يدخل

---

[1] الماوردي. الأحكام السلطانية. ص40

[2] الماوردي. المرجع نفسه. ص40

ضمن هذا الواجب تأمين المنافذ والمعابر الإلكترونية ووسائل الاتصال العابرة للقارات والتي لا محدودية لتدفقها ولا لانتشارها، وخطرها ماحق وشرها في كل شيء وبالجميع لاحق. فإيضاح الحجة في مواطن الزيغ وبيان الصواب في مواضع الشبهات خصوصا في المواقع الإلكترونية المخصصة لهذا الغرض من أكد الفرائض على الدول بمقتضى السيادة التي تتمتع بها، حتى يكون الدين محروسا من كل خلل، وعموم الأمة ممنوعة من الزلل.

ولو رجعنا إلى التاريخ الإسلامي لوجدنا أمثلة كثيرة داعمة لهذه الوظيفة والواجب الشرعي للدولة المسلمة. فلما ظهر الخوارج بعد معركة صفين وانتشرت مقالتهم المنحرفة في تكفير المسلمين والحكام والخروج عليهم واتسعت دائرة فسادهم، تصدى لهم على ابن أبي طالب رضي الله عنه تأمينا للمسلمين من أفكارهم وحماية لهم من فسادهم وشرهم. فأرسل إليهم أولا ابن عباس ليناظرهم ويحاورهم محاورة علمية، فرجع من رجع، ومن رفض منهم العودة واستمر على إلحاق الأذى والضرر بالمسلمين قاتلهم في معركة النهروان.

ومن ذلك المناظرات العلمية التي كانت ترعاها الدولة الإسلامية في مختلف عصورها، العصر الأموي والعباسي وحتى في العصر المملوكي ضد التيارات الفكرية المنحرفة، هو الآخر شاهد على واجب التحصين الاجتماعي والعقلي والفكري الذي يجب أن تضطلع به الدولة وفق ما يمليه عليها مبدأ السيادة.

المحور الثاني

التحديات السيبرانية للسيادة الرقمية وآليات المواجهة.

لقد ألغى السلاح الافتراضي كل الفروق بين من يمتلك القوة المادية ويتحكم في الجيوش والجنود، وبين من لا يملك إلا عقله وجوارحه مجردا من كل قوه وخِلْواً من أي سلاح.

بل أصبح الفرد الواحد المدني أخطر على الدولة وأشد فتكا من جيوش جرارة وأسلحة دمار شامل، وعدته وعتاده حاسوب وشبكه إنترنت.

وقد أدَّت هيمنة الأجهزة والأنظمة الإلكترونية وبرامج الذكاء الاصطناعي إلى ظهور جرائم وتهديدات خطيرة زادت من هشاشة مبدأ السيادة وسيولتها في ظل تنامي جرائم الذكاء الاصطناعي وتزايد التهديدات السيبرانية.

ومن خلال هذا المحور سوف نشير إلى بعض تحديات السيادة الرقمية في المجال السيبراني، ثم تحديد آليات المواجهة السيبرانية لهذه التحديات من خلال استحضار أهم قواعد الفقه التي يمكن التخريج عليها في هذا المجال.

أولا: التحديات السيبرانية للسيادة الرقمية.

إنه بنفس القدر الذي تطورت فيه الخدمات الإلكترونية وألقت بظلالها على جميع مناحي الحياة الإنسانية تسهيلا وتيسيرا لشؤون الأفراد والدول، تطوَّرت معها التهديدات الإلكترونية، واتَّسعت دائرة الأخطار السيبرانية، وبشكل خاص على حقوق الدول في ممارسة سيادتها على إقليمها الرقمي. وفي اعتقادي أنه يمكن توزيع هذه التحديات التي تواجه السيادة الرقمية للدول على ثلاثة مستويات:

- على مستوى الهوية والمكوِّن الثقافي.

- على المستوى المادي والحسي ويشمل مختلف الجرائم على النفس وعلى المال وعلى العرض وعلى العقل.

- على مستوى التبعية وعدم القدرة على التحكم في مختلف أنظمة الذكاء الاصطناعي ووسائل التواصل الرقمية المختلفة.

1-السيبرانية على مستوى الهوية والمكوّن الثقافي:

لا أحد يستطيع أن ينكر تأثير العولمة في تغيير البنية الأساسية للهويات الثقافية لمختلف المجتمعات. فمنظومة القيم والتصورات التي تميز مجتمعاً ما ضمن خصوصياته التاريخية والحضارية، ويعبّر بها عن ذاته وجذوره وعُمقه، هي التي يمكن أن نطلق عليها مصطلح الهوية، والتي تتخذ من الدين واللغة والثقافة السائدة أشكالا وتمثُّلات لها.[1]

غير أنه في ظل تغوُّل العولمة-عن طريق اكتساح العالم الرقمي والافتراضي-أصبحت الخصوصيات والمحددات الثقافية لأي مجتمع أكثر هشاشة وأكثر عرضة للاختلال والاضطراب من أي وقت مضى.

لأن هذا الطوفان المتدفق من المعرفة الإنسانية في فضاءات النشر الالكتروني، هو اتجاه متزايد لخلق عالم بثقافة مفتوحة أو ثقافة بلا حدود. وهي فكرة-ثقافة بلا حدود-واكبت العولمة التي يروج لها المفكرون الغربيون.[2]

وقد يبدو لأول وهلة جمالية هذه الفكرة التي يتم تكريسها عن طريق العولمة-الثقافة المفتوحة أو الثقافة بلا حدود-والتي تعمل على الاجتماع الانساني وتفعيل القواسم الإنسانية المشتركة، وهي كثيرة: الحقوق الانسانية، الحريات، الكرامة. الخ. إلا أنه ما يُستبطن في هذه الفكرة من الشر والخطر كفيل بأن تتخذ له كافة الاجراءات للتصدي له وحماية المجتمعات منه. لأن هذا التعميم الثقافي أو العولمة الثقافية سيؤدي إلى فرض ثقافة واحده، وهي ثقافة الأقوى التي لا تقبل التبادل ولا التنوع. والقوة التي أعنيها هنا ليس مصدرها صوابية الفكرة نفسها المؤسسة للثقافة، بل من السيطرة المحكمة والتحكم الواسع في فضاءات النشر الرقمي. ولأن الإنسان في البعد الإلهي الإسلامي كائن كغيره من الكائنات الأخرى، يتأثر ويؤثر، ويتفاعل

[1] محمد عاره مخاطر العولمة.ص7

[2] نصار، جمال. (2015). الهوية الثقافية وتحديات العولمة. مركز الجزيرة للدراسات. تم الاسترجاع من https://studies.aljazeera.net/ar/issues/2015/01/201512895243715948.html.

مع ما حوله، تتحدد بالتالي شخصيته -ومنها هويته-وفقا لهذه الكيميا الكونية. لهذا نجد القرآن الكريم في آيات كثيرة يحذرنا فيها المولى سبحانه وتعالى وينهانا عن شهود المجالس التي يُسوَّق فيها للباطل ويزين فيها الشرك:" ﴿قَدْ نَزَّلَ عَلَيْكُمْ فِي الْكِتَابِ أَنْ إِذَا سَمِعْتُمْ آيَاتِ اللَّهِ يُكْفَرُ بِهَا وَيُسْتَهْزَأُ بِهَا فَلَا تَقْعُدُوا مَعَهُمْ حَتَّى يَخُوضُوا فِي حَدِيثٍ غَيْرِهِ إِنَّكُمْ إِذًا مِثْلُهُمْ﴾[النساء: 140] ﴿وَالَّذِينَ لَا يَشْهَدُونَ الزُّورَ وَإِذَا مَرُّوا بِاللَّغْوِ مَرُّوا كِرَامًا﴾ [الفرقان:72]

وفي حديث الصحيفة لما رأى النبي صلى الله عليه وسلم عمر بن الخطاب يقرأ شيئا من التوراة في صحيفة غضب وقال «أمتهوكون فيها يا ابن الخطاب؟ والذي نفسي بيده لقد جئتكم بها بيضاء نقية، لا تسألوهم عن شيء فيحدثونكم بحق فتكذبوا به أو بباطل فتصدقوا به، والذي نفسي بيده لو أن موسى كان حيا ما وسعه إلا أن يتبعني».[1]

إن تأثيرات العولمة وتهديداتها للهوية الثقافية، لا يمكن التقليل منها بتسطيحها، فتأثيرها قوي وعميق وعام وشامل يتصل بجميع الأبعاد الثقافية في المجتمع.

إن القهر والتعسف والسيطرة والغزو، هي الأوصاف المناسبة التي يمكن أن توصف بها العولمة. فالعولمة ما هي إلا شكل من أشكال الهيمنة بأبعادها المختلفة، وأخطرها البعد الهويات أو الثقافي. فهي تعني: " نفي الآخر وإحلال الاختراق الثقافي في محل الصراع الايديولوجي، كما تعني الهيمنة وفرض نمط واحد للاستهلاك والسلوك". [2]

وفي نفس الإطار يؤكد المفكر الإسلامي الكبير محمد عمارة هذا المعنى الحقيقي للعولمة فيقول في التفريق بين العالمي: والعولمة:"... وإن شئنا الدقة، فإنها– العولمة القسر والقهر والإجبار على لون من الخصوصية يعولهم القهر ليكون عالميا، العولمة قسر وقهر يُعولِم خصوصية حضارية بعينها عندما تجتاح خصوصية المقهورين. ففي العالمية يختار الإنسان، وفي العولمة لا خيار للإنسان الذي يحشر ويشحن في القطار الذي صنعه ويقوده الأقوياء".[3]

---

[1] ابن عبد البر. جامع بيان العلم وفضله2/805 برقم1497 والحديث حسنه ابن حجر في المطلب العالية12/617

[2] محمد عابد الجابري . العولمة والهوية الثقافية. عشر أطروحات في كتاب (العرب والعولمة). مركز دراسات الوحدة العربية. بيروت. 1998م. ص301

[3] محمد عماره. مخاطر العولمة. ص14

وقد ذكر الاستاذ محمد عمارة كثيرا من النماذج والشهادات على مقصديه المحور الثقافي والقضاء على كل الخصوصيات الثقافية الإسلامية والعربية في إطار ما يسمى بالعولمة.[1]

2-التهديدات السيبرانية على المستوى المادي (الجرائم السيبرانية).

إن بسط الدولة لسلطانها الرقمي على إقليمها ورعاياها، تعزيز لسيادتها الرقمية. وكل أشكال الاعتداءات الرقمية أو الجرائم الإلكترونية التي تمس الأفراد أو حتى كيانات الدولة ومؤسساتها الحيوية، يمثل تهديدا لصلابة سيادتها الرقمية.

وتختلف الجرائم الإلكترونية بحسب دوافع أصحابها وبواعثهم إلى ارتكاب هذه الجرائم.

فقد يكون الدافع للجريمة الإلكترونية ماليا، وقد يكون الدافع عقديا أو فكريا(إيديولوجيا)، وقد يكون الدافع عسكريا أو سياسيا...الخ.

ويعتبر الدافع المالي أقوى الدوافع إلى الاعتداءات الإلكترونية. وتؤكد الإحصائيات الرسمية أن أكبر نسبة من الجرائم الإلكترونية كانت بسبب الحصول على الأموال. وتقدر البيانات أن نسبة الخسائر المادية نتيجة الاعتداءات على الأرصدة البريدية والبنكية جاوزت خمس مليارات عالميا. وفي الولايات المتحدة الأمريكية وحدها تجاوزت حالات الاعتداءات بسرقة البيانات الشخصية للبطاقات المالية 10 ملايين عملية.[2]

وقد تكون الاعتداءات الإلكترونية بهذا الدافع عن طريق اختراق أنظمة المصارف والبنوك والتلاعب بها. وقد تمكَّن عدد من القراصنة بتحويل مبالغ ضخمة من بنوك عالمية إلى أرصدة أخرى مما كبدها خسائر مالية فادحة.

ومن هذا القبيل قرصنة المعلومات والبيانات السرية والاستفادة منها في الابتزاز المادي أو المساومة على مصالح معينة استراتيجية أو الضغط لتمرير مشاريع محددة وغيرها.

---

[1] المرجع السابق. ص20 وما بعدها.

[2] عبد العزيز إبراهيم الشبل. الاعتداد الالكتروني دراسة فقهية. ص40

وأخطر هذه الاعتداءات الإلكترونية ما يتعلق منها بالمجال العسكري عن طريق التلاعب بالأنظمة الإلكترونية للأسلحة، والذي قد يسبب خسائر بشريه كثيرة، إضافة إلى التلاعب بالمرافق الحيوية والبنية التحتية مثل الطاقة والمياه والكهرباء. الخ.

ويمكن تحديد سبعة أنواع من الهجمات السيبرانية العسكرية:

- التجسُّس عن طريق سرقة المعلومات والأسرار والبيانات الخاصة.

- التخريب عن كثيرة، إضافة طريق نشر فيروسات ونحوها.

- هجمات رفض الخدمة (DOS) عن طريق إغلاق المواقع الإلكترونية بطلبات مزيفة للمستخدمين.

- الهجوم على شبكات الطاقة الكهربائية.

- الهجمات الدعائية بنشر الأكاذيب وإثاره الفتن والتحريض.

- الاضطرابات الاقتصادية عن طريق تعطيل الأسواق المالية والبورصات.

- الهجمات المفاجئة بغرض إضعاف العدو وقد تكون مقدمة لحرب ميدانية.[1]

3-التحديات السيبرانية على مستوى التبعية التكنولوجية:

الحقيقة التي لا مراء فيها أن تكنولوجيا الاتصال والاعلام والمعلومات، تخضع في الاستخدام والتوجيه والتحكم للدول الكبرى وشركاتها الضخمة. وبدهي أن تفرض شروطها على من يريد من الدول اقتناء هذه التكنولوجيا والاستفادة منها، وطبيعي أيضا أن تحرص على إبقائها خاضعه لها، دائرة في الفلك الذي تحدده لها.

[1] Hiranyaprayoon, A., et al. (2024). Exploring the vital role of facilitator organizations in supporting cancer patient care. *Journal of Healthcare Management*, 44(1), 1-10. https://doi.org/10.1007/s43999-024-00052-y.

وإذا كان من مقومات السيادة قدرة الدولة على تأكيد ذاتها في المجال الدولي بكل حريه، فإن الأمر لا يبدو سهلا في ظل ضعف بنيه تحتية وقاعده اجتماعية هشة وتبعيه مطلقه بما في ذلك التبعية التكنولوجية، خصوصا وأن بعض المكونات الأساسية للأنترنت تدار خارجا النطاق القانوني الدولي عن طريق ما يسمى الأيكان ICAAN.[1]

والحقيقة التي يؤكدها بعض الباحثين، أنه ما دمنا لسنا قادرين على الإنتاج في المجال التكنولوجي وعاجزين عن توفير البيئة المناسبة لاستنباتها وغير قادرين على مواطنتها وتعزيز ثقافة المواطنة الرقمية، فإننا بالمحصِّلة لا نستطيع توظيفها التوظيف الأمثل والاستفادة منها بشكل يجنّبنا المزالق الخطيرة المهددة لهويتنا وكينونتنا الثقافية.[2]

إن واحدا من أهم مضامين السيادة الرقمية، الاستقلالية. بل قد تكون من مرادفاتها التي تتيح لدولة ذات سيادة حقيقية في المجال الرقمي أن تتخذ قراراتها ومواقفها بكل حرية واختيار بما في ذلك التعامل مع الشركات الكبرى المنتجة للتكنولوجيا، وتلك التي تقوم بإدارة مواقع التواصل الاجتماعي. وأكبر عائق يحول دون ذلك، سيطرة الطرف الأقوى المصنّع والمُنتج والمُصدِّر لهذه التكنولوجيا، والذي لا يتيح أي فرصة لتطويع منجزاته التكنولوجية التي يهدف من ورائها بسط سيطرته ونفوذه على المستقبِل والمستورِد لهذه التكنولوجيا الخاصة به.

ثانيا: آليات المواجهة السيبرانية في المنظور الإسلامي.

إن حجم التهديدات التي تخلفها الاعتداءات والجرائم الإلكترونية المختلفة، يُظهر بوضوح أهمية الجهود التي ينبغي أن تبذلها الدول لبسط سيادتها على إقليمها الافتراضي، سواء على المستوى التقني والفني أو على المستوى التشريعي أو على المستوى الفكري والثقافي.

فالمواجهة الحقيقية تقتضي إعدادا كاملا على كافة المستويات، وبما أن هذه التحديات والتهديدات تحمل معها مخاطر كبيرة على الأمن القومي بمختلف أبعاده، فإنه موازاة مع حجم هذه

[1] ذنون جاسم، فائز. (2015). تأثير الإنترنت على مبدأ السيادة. مجلة كلية الحقوق بجامعة النهرين, 2, ص338

[2] اليحياوي، يحيى. "التبعية التكنولوجية الجديدة." الموقع الإلكتروني, 2024, elyahyaoui.org. تاريخ الزيارة: 2025/01/15 الساعة: 11:00

التهديدات والمخاطر يكون حجم الإعداد والمواجهة. قال تعالى: ﴿وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ﴾ [الأنفال:60]

والذي يتعين علينا التركيز عليه هنا، تصفيف آليات المواجهة في المنظور الفقهي الإسلامي من خلال قواعد الفقه وكلياته التشريعية وصولا إلى تكوين هيكل للمواجهة السيبرانية في المنظور الإسلامي.

إن أهم قاعدة فقهية يتم استحضارها في تعزيز سند المواجهة لمختلف التحديات والتحديدات بما في ذلك التهديدات في المجال الرقمي:

1-قاعدة تصرفات السلطة منوطة بالمصلحة:

وتعتبر هذه القاعدة من أهم قواعد الولايات العامة والخاصة في الفقه الإسلامي. والنص الفقهي لهذه القاعدة كما ذكرها الفقهاء:" تصرف الامام على الرعية منوط بالمصلحة". وقد نص عليها الشافعي وغيره.[1]

ومن الأدلة التي تؤصِّل لهذه القاعدة: قوله صلى الله عليه وسلم: «ما من عبد يسترعيه الله رعية يموت يوم يموت وهو غاش لرعيته إلا حرم الله عليه الجنة».[2]

لأن من واجبات من تقلَّد السلطة أن ينصح للرعية ويعمل على حمايتهم وصيانة حقوقهم وأخلاقهم وهويتهم بشكل عام. «ما من أمير يلي أمر المسلمين، ثم لا يجهد لهم، وينصح، إلا لم يدخل معهم الجنة».[3]

وهذه القاعدة كما قال الزحيلي: ترسم حدود الإدارات العامة والسياسة في تصرفات الولاة والحكام على الرعية. والمبنى الأساسي في صحة التصرفات الإدارية والتنظيمية هو المصلحة جلباً والمفسدة درءاً.

---

[1] الزحيلي. القواعد الفقهيه وتطبيقاتها.494/1

[2] صحيح البخاري2614/6برقم7631 صحيح مسلم87/1برقم280

[3] صحيح مسلم88/1برقم283

ومقتضى هذه القاعدة، أن كل ما يحقق مصلحة أو يدرئ مفسدة من التنظيمات أو السياسات أو التشريعات يتعيَّن على الحاكم فعله وعلى الرعية الالتزام به.

وإذا كان الحدُّ من التهديدات الرقمية يقتضي سنَّ تشريعات وقوانين تنظيمية وإدارية على المستوى الوطني أو المشاركة في اتفاقيات مكافحة الجرائم الإلكترونية إقليمية ودولية، فإن ذلك من واجبات الحاكم بمقتضى السيادة والسلطة الممنوحة له والمفوضة إليه، وتفريعاً على هذه القاعدة الفقهية.

ومما يعزِّز شرعية المشاركة في المجال الدولي عن طريق الدخول في هذه الاتفاقيات لمكافحة الجرائم والاعتداءات الإلكترونية، مشاركه النبي صلى الله عليه وسلم في حلف الفضول الذي عقدته قريش نصرة للمظلوم ومواجهة للظالم وفيه قال صلى الله عليه وسلم: «شهدت حلفا في الجاهلية في دار ابن جدعان لو دعيت إليه اليوم لأجبت، رد الفضول إلى أهلها، وألا يقر ظالم مظلوما».[1]

2-قاعده إزالة الضرر ودفعه:

والضرر، هو كل مفسدة تلحق بالغير سواء كانت في نفسه أو في ماله أو في دينه أو في عقله.

والجرائم الإلكترونية شاملة في أضرارها ومفاسدها لسائر الكليات التي جاءت الشرائع والملل جميعا بحفظها. وقد ذكر الفقهاء كثيرا من القواعد المتعلقة بإزالة الضرر ودفعه، منها القاعدة الأمّ أو القاعدة الأساسية والتي يندرج تحتها قواعد فرعية أخرى وهي قاعدة: " لا ضرر ولا ضرار". وأصلها لفظ حديث نبوي.[2] وهذه القاعدة تضمنت حكما عاما، وهو أنه لا ضرر على المعنى الذي بيناه في الشريعة. وتصدير القاعدة بصيغه نفي الجنس مبالغة في النهي والزجر. ونفي الضرر يفيد دفعه قبل وقوعه وهو الجانب الوقائي، ورفعه بعد وقوعه وهو الجانب العلاجي. ومنه القاعدة الفقهية:" الضرر يزال".

---

[1] الفاكهي. أخبار مكة276/3

[2] مسند أحمد267/3 ، سنن ابن ماجة430/3 وحسنه ابن الصلاح. انظر. ابن الملقن. خلاصة البدر المنير438/2

وتأسيسا على هذه القاعدة، فإنه يتعين على السلطة الحاكمة توفير كافة التدابير والإجراءات الوقائية التي تقطع الطريق أمام المفسدين والمجرمين عن طريق تعزيز منظومتها الأمنية المتخصصة لمواجهة التهديدات السيبرانية الداخلية والخارجية، وتفعيل المنظومة العقابية الرادعة والزاجرة على أصحاب الجرائم الإلكترونية.

وكل جريمة إلكترونية تقابلها غالبا جريمة تقليدية. والذي يتعين على الفقهاء والمجتهدين بذل الوُسع والجُهد في تحقيق مناطات هذه الجرائم الإلكترونية، وتكييفها بما يتوافق مع المنصوص عليه من العقوبات الشرعية. لأن القاعدة الفقهية: «لا جريمة ولا عقوبة الا بنص". وهي قاعدة مقررة في الشريعة الإسلامية وحتى في القوانين الوضعية، وشواهدها في النصوص الشرعية كثيرة.[1]

فإذا كانت الجريمة الإلكترونية متضمنة لقذف وتشهير ورمي بالفاحشة، فعقوبة القذف الجلد ورد الشهادة.

وإذا كانت الجريمة الإلكترونية سرقة وتوافرت فيها شروطها، فالعقوبة القطع.

وإذا كان العدوان من قبل ذي شوكة ومَنَعَة ومجاهرة كما هو حال أغلب جرائم الحاسب الآلي فالعقوبة عقوبة حرابة: قتل أو صلب أو قطع للأيدي والأرجل من خلاف.

وما لا يقابله عقوبة نصية من الجرائم الإلكترونية، فالمقرر عند الفقهاء التعزير بكل وسيلة ما لم يكن منهيا عنه في الشريعة إذا تحقق معها الردع والزجر للجاني ولغيره كما في جرائم التجسس، وانتهاك الخصوصية، وانتحال الشخصية، وإنشاء المواقع الإباحية، ونشر الفواحش، وسرقة البيانات الخاصة والمعلومات السرية، والعبث بالمرافق الحيوية وغيرها.

3-قاعدة الوسائل لها أحكام المقاصد:

وهذه القاعدة من أهم قواعد الفقه الإسلامي التي لها حضور قوي في مجال السياسة الشرعية. ومعنى هذه القاعدة، أن حكم الوسيلة يتحدد بحكم ما قصد منها. فإن كان المقصود مشروعا، كانت الوسيلة إليه مشروعة وما لا فلا. فالأمر بالشيء أمر به وبما لا يتم إلا به،

[1] عبد القادر عوده . التشريع الجنائي الإسلامي مقارنا بقانون الوضعي. 117/1. . محمد ابو زهره . الجريمة والعقاب.ص133

والنهي عن الشيء نهي عنه وعن كل ما يؤدي إليه. وعليه يتحدد حكم استعمال هذه الوسائل والوسائط الإلكترونية. فإن كان استعمالها مشروعا وآمنا ومُحقِّقا للعدل وجالبا للمصالح، تعيَّن ذلك على القادر والمستطيع. ولهذا فإن من لوازم السيادة ومقتضياتها في المجال الرقمي، إنشاء المواقع الإلكترونية لتحصين الجبهة الثقافية والمحافظة على الهوية الإسلامية للمجتمع الإسلامي، وتكوين المتخصصين الذين يجمعون بين الخبرة الفنية والتقنية وبين الخبرة العلمية والشرعية، لبيان صورة الإسلام الصحيح ونشر سماحة أحكامه وعدل تشريعاته، وردِّ عدوان المشكِّكين والمبطلين الذين ينشرون الضلالات ويثيرون الشبهات، لتحصين مقوِّمات الهوية ديناً ولغةً وتراثاً، وتعزيز الثقافة الرقمية التي يتحقق معها الأمن القومي الرقمي.

ومن النصوص التي نوردها في هذا المجال، قوله تعالى: **﴿فَلَوْلَا نَفَرَ مِنْ كُلِّ فِرْقَةٍ مِنْهُمْ طَائِفَةٌ لِيَتَفَقَّهُوا فِي الدِّينِ وَلِيُنْذِرُوا قَوْمَهُمْ إِذَا رَجَعُوا إِلَيْهِمْ لَعَلَّهُمْ يَحْذَرُونَ﴾** [التوبة:112] والآية على عمومها تشمل وجوب تهيئه المتخصصين في الفقه سواء كان حضورهم في الواقع أو في المواقع، وسواء كان الفقه في الدين وعلومه أو كان الفقه في الدنيا وعلومها.

وقوله تعالى: **﴿وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ ﴾**[الأنفال:60] وورود القوة مُنكَّرة في سياق الإثبات والأمر، يفيد عموم إعداد كلِّ قُوَّة بما في ذلك القوة الإلكترونية.

المحور الثالث

البعد المقاصدي وأثره في تعزيز السيادة الرقمية وتحديد نطاقها.

إن من أهم أولويات أي دولة ذات سيادة، العمل على حماية فضائها السيبراني وتحصين إقليمها الرقمي. وقد سبق وأن ذكرنا الإطار العام في المنظور الإسلامي لآليات المواجهة السيبرانية ضد تهديدات السيادة الرقمية، وهو إطار القواعد الفقهية.

ويساير إطار القواعد الفقهية إطارا آخر لا يقلّ أهمية عن هذا الإطار، وهو إطار مقاصد الشريعة الإسلامية.

ومن المعلوم أن محور مقاصد الشريعة يدور على قطبين اثنين: قطب المصالح وقطب المفاسد.

وكقاعدة عامة، فإن كلَّ ما يحقِّق للدولة مصلحة تتعزز بها سيادتها الرقمية، فإنه من الوسائل والطرق المشروعة، التي يتعين عليها إيجادها والعمل بمقتضاها.

وكلُّ ما كان مفوِّتا لهذا الغرض المقصود، تعيَّن صَدُّه ومواجهته.

غير أن ثمة إشكالات قد تُعَكِّر صَفْوَ هذا المبدأ العام، كتعارض بعض المصالح مع بعض، أو ترتب بعض المفاسد على تطبيق مبدأ السيادة، وهنا يأتي النظر المقاصدي أو الاجتهاد المقاصدي الذي يحدد للدولة في سبيل تعزيز سيادتها الرقمية نطاق تحركها لتعزيز مبدأ سيادتها الرقمية على وفق القاعدة السابقة -وهي قاعده المقاصدي أيضا-» لا ضرر ولا ضرار". ومن هذه الإشكالات:

1-انتهاك الخصوصية: فمن الحقوق الأساسية التي أجمعت عليها مختلف النظم والقوانين بما في ذلك الشريعة الإسلامية، الحق في الحياة الخاصة. وإن كان تمت خلاف في الفقه القانوني في تقرير طبيعة الحق في الحياة الخاصة، هل هو من الحقوق الشخصية أو من حقوق الملكية.

إلا أنه بشكل عام يُعدُّ واحدا من الحقوق المكفولة لجميع الأفراد. فتحريم التجسس: ﴿وَلَا تَجَسَّسُوا ﴾الحجرات:12] ٍ وتحريم النظر: «من اطلع في بيت قوم بغير إذنهم فقد حل لهم أن يفقأوا عينه». [1] وإيجاب الاستئذان قبل الدخول: ﴿يَاأَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا﴾ [النور:27]،

وكتمان السر: «إذا حدث الرجل بحديث ثم التفت، فهي أمانة».[2] «المجالس بالأمانات».[3] كلها شواهد على حماية الخصوصية. ومن أشكال الخصوصية، الخصوصية الرقمية.

لكن الإشكال المثار هو: هل من حق الدولة تعزيزا لسيادتها الرقمية، الاطلاع على حسابات الأفراد والمواطنين ومراقبتها، تحقيقا للمصلحة العامة وحفظاً لأمنها القومي.

وبالنظر إلى ما ورد من آثار وشواهد، يبدو أن المسألة لا تخلو من نزاع حولها. فقد وردت نصوص تنهى عن عموم التجسس سواء من قبل الحاكم أو من غيره، كما وردت نصوص تأمر بحسن الظن بالناس تعزيزا للمبدأ الشرعي:" الأصل في الناس البراءة". وكان أبو الدرداء يقول: كلمة نفع الله بها معاوية، سمعها من رسول الله صلى الله عليه وسلم الحديث: من تتبع عورات الناس يفسد الناس، أو كاد أن يفسد الناس" والقصة المشهورة التي تروى عن عمر رضي الله عنه أيضا: كان يتفقد أحوال الناس ليلًا، فوجد رجلًا يشرب الخمر في بيته. فاقتحم عمر البيت دون إذنٍ، وعندما واجه الرجل بخطئه، رد عليه الرجل قائلًا: "يا أمير المؤمنين، إن كنت قد عصيت الله في واحدة (شرب الخمر)، فقد عصيتَه في ثلاث:

دخلت بيتي بغير إذن. تجسست عليّ، وقد نهى الله عن التجسس. دخلت بغير سلام."[4]

---

[1] صحيح مسلم181/6برقم5693

[2] سنن أبي داوود418/4برقم4870

[3] المنذري. مختصر سنن أبي داود330/3برقم4702

[4] الخرائطي. مكارم الأخلاق ومعاليها ومحمود طرائقها. ص152 والقصة منكرة لا تصح عن عمر رضي الله عنه إسنادها ضعيه وفي متنها نكارة وعلل. والثابت عن عمر خلافه. عن المِسْوَرُ بن مَخْرَمَة عن عبد الرحمن بن عوف رضي الله عنه قال حرست مع عمر بن الخطاب رضي الله عنه المدينة ليلة إذ تنبت لنا سراج فمشينا نحوه حتى انتهينا إلى باب مجاف على قوم قد علت أصواتهم وكَثُر لغطهم فقال: أتدري بيت من هذا؟ قلت: لا أدري، قال: هذا بيت ربيعة بن أمية بن خلف وهم الآن شرب فما ترى؟ قلت أرانا قد

وهذه كلها شواهد تؤكد على وجوب احترام الخصوصية والحياة الخاصة للأفراد.

غير أنه مما يبرر إمكانية الدولة وحقها في مراقبة الحسابات الإلكترونية، بل والاطِّلاع عليها أيضا، هو النظر المصلحي والمقاصدي المبني على قاعدة: تقديم المصلحة العامة على المصلحة الخاصة" عند التعارض. لأن هذه الرقابة المسلطة على الحسابات الإلكترونية ليس دافعها نشر الفضائح ولا تتبع العورات ولا العدوان على الخصوصية، بل الدافع إليها حماية المجتمع وارساء النظام العام فيه. وإذا كان سائغا للحاكم أو للقاضي أن يقتطع جزءا من الممتلكات الخاصة لشق طريق أو لبناء سدٍّ تحقيقاً لمصلحة عامة، فلا ينبغي التوقف في جواز مراقبة الحسابات والاطِّلاع عليها لنفس الغرض المقصود.

ويمكن هنا التفريق بين الأفراد والمواطنين من حيث حالهم وعدالتهم. فمن كان مشتهراً منهم بالسوء والخيانة والإفساد والتحريض، أو له سوابق في الإضرار بالمصالح العامة للدولة او للأفراد، فلا حرج في مراقبتهم، بل واختراق حساباتهم. ومن التطبيقات الفقهية لقاعدة:" لا ضرر ولا ضرار"، أنه يجوز حبس المشهورين بالدعارة والفساد، حتى تظهر توبتهم، ولو لم يثبت عليهم جرم معين قضائيا، دفعا لشرهم، لأنهم قد يحتاطون ويتحفظون فيملون الأرض فساداً، دفعا لضررهم عن العباد.[1]

2-المعضلة الدلالية: وأعني بها تفسير المصطلحات وتحديد معناها السليم. فالتجسس مثلا الذي يتفق الجميع على تجريمه والمعاقبة عليه، قد يتم تفسيره بأنه كشف للحقائق وتوضيح لها وتنوير للرأي العام. فنشر بعض المعلومات والبيانات السرية، قد يؤدي إلى آثار مدمرة وعاقبة سيئة واضطرابات سياسية واجتماعية تحصل معها فوضى وقلق اجتماعي، في حين قد يتم تفسيرها بأنها من الحقائق التي يجب أن تواجه وتعلم وتتم معالجتها. ومصطلح الحرية مثلا، قد يؤخذ فيه بالمعنى المطلق، فتعتبر حينئذ الإساءة إلى الدين، أو إلى الرموز الدينية والوطنية، شكلا من أشكال الحرية، والعقوبة عليه لونا من ألوان الاستبداد والطغيان والإرهاب السياسي. وقضايا كثيرة تسببت في أزمات دبلوماسية وسياسية طاحنة سببها المعضلة الدلالية.

---

[1] أتينا ما نهانا الله عنه، قال الله عز وجل وَلاَ تَجَسَّسُوا وقد تجسسنا، قال فرجع وتركهم. إسناده صحيح رجاله كلهم ثقات أخرجه أبو بكر الخرائطي في مكارم الأخلاق. ص152. وانظر اللجنة الدائمة للبحوث العلمية والإفتاء بالمملكة العربية السعودية. فتوى 7066

إلا أن الفكاك من هذه المعضلة، هو تطبيق المقاصد العامة للشريعة. لأن من أهم المقاصد الشرعية، المقاصد الاجتماعية. فالمقصد العام من التشريع، هو حفظ نظام الأمة، وحفظ نظام الأمة يسترشد بقاعدة درأ المفاسد التي تقوّض هذا المقصد العام-حفظ نظام الأمة- والمعتبر في الحكم على الأمور، عواقبها ومآلاتها. والنظر في المآلات والعواقب من أعظم مسددات الاجتهاد المقاصدي ومرتكزات النظر المصلحي. وقد بين الشاطبي جوانب أهمية اعتبار المآل في الاجتهاد والتعامل مع الأمور والقضايا بشكل عام، فقال:" النظر في مآلات الأفعال معتبر مقصود شرعا كانت الأفعال موافقة أو مخالفة، وذلك أن المجتهد لا يحكم على فعل من الأفعال الصادرة عن المكلفين بالإقدام أو بالإحجام إلا بعد نظره إلى ما يؤول إليه ذلك الفعل، مشروعا لمصلحة فيه تستجلب، أو لمفسدة تدرأ، ولكن له مآل على خلاف ما قصد فيه، وقد يكون غير مشروع لمفسدة تنشأ عنه أو مصلحة تندفع به، ولكن له مآل على خلاف ذلك، فإذا أطلق القول في الأول بالمشروعية، فربما أدى استجلاب المصلحة3 فيه إلى المفسدة تساوي المصلحة أو تزيد عليها، فيكون هذا مانعا من إطلاق القول بالمشروعية وكذلك إذا أطلق القول في الثاني بعدم مشروعية ربما أدى استدفاع المفسدة إلى مفسدة تساوي أو تزيد، فلا يصح إطلاق القول بعدم المشروعية وهو مجال للمجتهد صعب المورد، إلا أنه عذب المذاق محمود الغب، جار على مقاصد الشريعة".[1]

[1] الشاطبي. الموافقات177/5

الخاتمة

لأبرز النتائج والتوصيات:

1-يعتبر البعد الرقمي أحد أهم الأبعاد المهمة في تشكيل مفهوم جديد للسيادة في العصر الحاضر، يرتبط به تحقيق الأمن القومي للدول من خلال قدرة الدول على التحكُّم في فضائها وإقليمها الرقمي.

2-لا يخرج التعريف الإجرائي للسيادة بما في ذلك السيادة الرقمية في الفكر الإسلامي عن مفهوم السلطة العليا الحاكمة ما دام الاتفاق على أن مصدر السلطة هو الشرع.

3-أهم التحديات التي تواجهها الدول في تحقيق سيادتها الرقمية، غياب الصفة القانونية والمعنوية لشبكة الإنترنت إضافة إلى انتشارها الواسع واللامحدود.

4-تعتبر وظائف الحكومة في الإسلام في إقامة الدين والدنيا، أحد أهم الجوانب التأصيلية لمبدأ السيادة الرقمية وتعزيزها في منظور الفقه الإسلامي.

5-أدَّت هيمنة الأجهزة الإلكترونية وبرامج الذكاء الاصطناعي إلى ظهور جرائم وتهديدات سيبرانية بدوافع متعددة مفوضة للسيادة الرقمية للدول.

6-تتوزع التهديدات السيبرانية والتحديات الرقمية على مستويات ثلاثة: الهوية والمكوَّن الثقافي، العدوان الحسي على النفس والأعراض والأموال، وأخيرا على مستوى التبعية وضعف الاستقلالية في المجال الرقمي.

7-العدوان الإلكتروني على الهوية الثقافية وعولمتها صورة من صور الهيمنة الثقافية والاختراق الثقافي، بناء على فكرة ثقافة غير محدودة.

8-من أهم القواعد الفقهية التي يمكن من خلالها نسج منظومة دفاع إلكترونية في المنظور الاسلامي قاعدة: " لا ضرر ولا ضرار"، وقاعدة: " تصرفات الحاكم على الرعية منوط بالمصلحة"، وقاعدة: " الوسائل لها أحكام المقاصد".

9-النظر المصلحي والاجتهاد والمقاصدي موازاة مع التقعيد الفقهي، يُشكِّلان الإطار العام لهيكل الدفاع الإلكتروني في المجال الرقمي.

10-من أهم الإشكالات التي تواجه النظر المقاصدي في أحقية الدولة في تعزيز سيادتها الرقمية، الحق في الخصوصية، والمعضلة الدلالية، ويعتبر الترجيح المقاصدي أهم الحلول المناسبة لها.

ومن التوصيات المهمة في هذا الإطار: العمل على إيجاد ميثاق إسلامي عن طريق صياغة تشريعية جامعة تضع أسسًا ومعايير إسلامية للتعامل مع الفضاء الرقمي، مع التركيز على الأخلاقيات، وحماية الحقوق، ومواجهة الجرائم السيبرانية، وتعزيز ثقافة المواطنة الرقمية.

قائمة المراجع

-القرآن الكريم.

-ابن السُّنِّي (ت: 364هـ)، عمل اليوم والليلة: سلوك النبي مع ربه عز وجل ومعاشرته مع العباد، تحقيق كوثر البرني، دار القبلة للثقافة الإسلامية ومؤسسة علوم القرآن، جدة / بيروت

-البخاري، محمد بن إسماعيل أبو عبد الله (ت: 256هـ)، الجامع الصحيح المختصر، تحقيق د. مصطفى ديب البغا، دار ابن كثير، اليمامة -بيروت، الطبعة الثالثة، 1407 هـ - 1987م.

-الخرائطي السامري، أبو بكر محمد بن جعفر بن محمد بن سهل بن شاكر (ت: 327هـ)، مكارم الأخلاق ومعاليها ومحمود طرائقها، تقديم وتحقيق أيمن عبد الجابر البحيري، دار الآفاق العربية، القاهرة، الطبعة الأولى، 1419 هـ -1999 م.

-الزحيلي، محمد مصطفى، القواعد الفقهية وتطبيقاتها في المذاهب الأربعة، دار الفكر، دمشق، الطبعة الأولى، 1427 هـ -2006 م.

-الشاطبي، إبراهيم بن موسى بن محمد اللخمي الغرناطي (ت: 790هـ)، الموافقات، تحقيق أبو عبيدة مشهور بن حسن آل سلمان، دار ابن عفان، الطبعة الأولى، 1417هـ/1997م.

-الشبل، عبد العزيز بن إبراهيم. (2012). الاعتداء الإلكتروني: دراسة فقهية. دار كنوز إشبيليا، الرياض.

-الصاوي، صلاح. (1992). نظرية السيادة وأثرها على شرعية الأنظمة الوضعية. دار طيبة.

-عبد الكريم، فتحي. (1984). الدولة والسيادة في الفقه الإسلامي: دراسة مقارنة. مكتبة وهبة.

-عمارة، محمد. (1999). مخاطر العولمة على الهوية الثقافية. دار نهضة مصر للطباعة والنشر والتوزيع.

-عودة، عبد القادر (ت: 1373هـ)، الإسلام وأوضاعنا السياسية، مؤسسة الرسالة للطباعة والنشر والتوزيع، بيروت -لبنان، 1401 هـ -1981 م.

-عودة، عبد القادر، التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي، دار الكاتب العربي، بيروت.

-الفاكهي، محمد بن إسحاق بن العباس المكي (ت: 272هـ)، أخبار مكة في قديم الدهر وحديثه، تحقيق د. عبد الملك عبد الله دهيش، دار خضر، بيروت، الطبعة الثانية، 1414هـ.

-الماوردي، أبو الحسن علي بن محمد. (450 هـ). الأحكام السلطانية. دار الحديث.

-محمد عابد الجابري. العولمة والهوية الثقافية. عشر أطروحات في كتاب (العرب والعولمة). مركز دراسات الوحدة العربية. بيروت. 1998م

-مرتضى الزبيدي، تاج العروس من جواهر القاموس، دار الفكر، بيروت، الطبعة الأولى، 1414هـ/1994م

-مسلم بن الحجاج القشيري النيسابوري (ت: 261هـ)، المسند الصحيح المختصر بنقل العدل عن العدل إلى رسول الله صلى الله عليه وسلم، تحقيق مجموعة من المحققين، دار الجيل، بيروت، مصورة من الطبعة التركية المطبوعة في إسطنبول سنة 1334 هـ.

-المنذري، عبد العظيم بن عبد القوي (ت: 656 هـ)، مختصر سنن أبي داود، تحقيق محمد صبحي بن حسن حلاق (أبو مصعب)، مكتبة المعارف للنشر والتوزيع، الرياض -المملكة العربية السعودية، الطبعة الأولى، 1431 هـ -2010 م.

-هوبز، توماس. (2011). اللفياثان: الأصول الطبيعية والسياسية لسلطة الدولة (ترجمة دينا حرب، بشرى صعب). دار الفارابي.

المقالات:

ذنون جاسم، فائز. (2015). "تأثير الإنترنت على مبدأ السيادة." مجلة كلية الحقوق بجامعة النهرين، 2، ص 331-348.

المواقع الإلكترونية:

-نصار، جمال. (2015). الهوية الثقافية وتحديات العولمة. مركز الجزيرة للدراسات. تم الاسترجاع من https://studies.aljazeera.net/ar/issues/2015/01/20151289524371594 8.html.

-اليحياوي، يحيى. "التبعية التكنولوجية الجديدة." الموقع الإلكتروني، 2024، elyahyaoui.org. تاريخ الزيارة: 2025/01/15 الساعة: 11:00.

المراجع باللغة الأجنبية:

-Bodin، J. (1986). Les Six Livres de la République. Librairie Arthème Fayard.

-Hiranyaprayoon، A.، et al. (2024). Exploring the vital role of facilitator organizations in supporting cancer patient care. Journal of Healthcare Management, 44(1), 1-10. https://doi.org/10.1007/s43999-024-00052-y

الفصل الثالث

تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني

Applications of artificial intelligence in the field of cybersecurity

1/ طالبة الدكتوراه خديجة رملي

جامعة أكلي محند أولحاج -البويرة – الجزائر-

Kh.remli@univ-bouira.dz

2/ سلسبيل دزيري

جامعة أكلي محند أولحاج -البويرة – الجزائر-

s.dziri@univ-bouira.dz

ملخص

تهدف هذه الدراسة إلى **استكشاف تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني،** وتحليل كيفية استخدامها لتحسين الحماية ضد التهديدات والهجمات الإلكترونية المتزايدة، كما تسعى إلى **مناقشة التحديات** التي تواجه استخدام الذكاء الاصطناعي في هذا المجال، وذلك من خلال المنهج الوصفي، حيث توصلنا في الأخير إلى مجموعة من النتائج أبرزها أن الذكاء الاصطناعي أسهم في تحسين القدرة على اكتشاف الهجمات المتقدمة والأنشطة غير الطبيعية بسرعة أكبر مقارنة بالأساليب التقليدية، كما تم التوصل إلى مجموعة من التوصيات التي يمكن أن تعزز فعالية الذكاء الاصطناعي في مجال الأمن السيبراني وتقليل المخاطر المرتبطة به، وأهمها، توفير **بيانات دقيقة وشاملة** لتدريب النماذج الذكية، مع ضمان تحديثها باستمرار لتواكب التهديدات الجديدة.

الكلمات المفتاحية: الذكاء الاصطناعي، الشبكات العصبية، الروبوتات، الخوارزميات المشفرة، الأمن السيبراني.

Abstract :

This study aims to explore the applications of artificial intelligence in the field of cybersecurity and analyze how it is used to improve protection against increasing threats and cyberattacks. It also seeks to discuss the challenges faced when using artificial intelligence in this field through the descriptive approach. Ultimately, we reached a set of conclusions, the most prominent of which is that artificial intelligence has contributed to improving the ability to detect advanced attacks and abnormal activities more quickly compared to traditional methods. Additionally, a set of recommendations was reached that could enhance the effectiveness of artificial intelligence in cybersecurity and reduce associated risks, the most important of which is providing accurate and comprehensive data to train intelligent models, while ensuring they are continuously updated to keep up with new threats.

Keywords: Artificial Intelligence, Neural Networks, Robotics, Encrypted Algorithms, Cybersecurity.

مقدمة

أصبح الذكاء الاصطناعي من الأدوات الأساسية في تعزيز أمن المعلومات وحمايتها في مواجهة التهديدات السيبرانية المتزايدة، وتطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني تتنوع وتشمل الكشف عن الهجمات المتقدمة، التحليل التنبؤي للتهديدات، وأتمتة استجابة الأنظمة، ومن أبرز استخدامات الذكاء الاصطناعي في هذا المجال، الكشف المبكر عن الهجمات، التنبؤ بالتهديدات، الاستجابة التلقائية، التحليل السلوكي، تعزيز الدفاعات ضد البرمجيات الخبيثة، حيث تساهم هذه التطبيقات في تحسين الاستجابة للتهديدات وتقليل زمن التفاعل مع الهجمات، مما يزيد من مستوى الأمان بشكل عام في البيئة الرقمية.

الإشكالية الرئيسية: من خلال ما سبق نصل إلى طرح التساؤل الرئيسي التالي:

ماهي مختلف تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني؟

الأسئلة الفرعية: يندرج تحت التساؤل الرئيسي مجموعة من التساؤلات الفرعية وهي كالتالي:

- ما المقصود بالذكاء الاصطناعي؟ وماهي بنيته الجوهرية؟
- فيما تتمثل تقنيات الذكاء الاصطناعي؟
- ماهي أبرز استخدامات الذكاء الاصطناعي؟
- فيما يتمثل الأمن السيبراني؟ وماهي مختلف التهديدات التي تواجهه؟
- ماهي أبعاد الأمن السيبراني؟
- ماهي استخدامات الذكاء الاصطناعي في مجال الأمن السيبراني؟ وماهي تحدياته؟

أهداف الدراسة: تسعى الدراسة التي بين أيدينا إلى تحقيق جملة من الأهداف وأهمها:

- الإلمام بمفهوم الذكاء الاصطناعي وبنيته الجوهرية.

- توضيح تقنيات الذكاء الاصطناعي.
- التطرق إلى أهم استخدامات الذكاء الاصطناعي.
- التعرف على الأمن السيبراني ومختلف التهديدات التي تواجهه.
- التعريج على أبعاد الأمن السيبراني.
- التعرف على استخدامات الذكاء الاصطناعي في مجال الأمن السيبراني وتحدياته.

أهمية الدراسة: إن دراسة تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني مهمة للغاية نظرا لتزايد التهديدات الإلكترونية وتطورها المستمر، وتبرز من خلال التصدي للهجمات المتقدمة، حيث يساعد الذكاء الاصطناعي في كشف الهجمات المتطورة التي يصعب رصدها بالطرق التقليدية، مما يساهم في حماية الأنظمة من تهديدات جديدة ومعقدة، وتحليل البيانات بسرعة وكفاءة، ويتيح الذكاء الاصطناعي تحليل كميات ضخمة من البيانات بسرعة، ما يمكنه من اكتشاف الأنماط المشبوهة في وقت مبكر، والاستجابة التلقائية، كما أنه من خلال أتمتة الاستجابة للهجمات، يمكن تقليل الزمن المستغرق في معالجة الحوادث وتحسين فعالية الدفاعات، تحسين الكفاءة البشري، ويعمل على تقليل العبء على فرق الأمن السيبراني البشرية، مما يسمح لهم بالتركيز على القضايا الأكثر تعقيدا، والتكيف مع التهديدات المتغيرة، كما يساعد الذكاء الاصطناعي في تحسين الأنظمة الأمنية بناء على البيانات والتهديدات الجديدة، مما يضمن الدفاع المستمر، وأيضا تساهم هذه الدراسة في تطوير أدوات وتقنيات أكثر فعالية للوقاية من الهجمات السيبرانية، وبالتالي تعزيز أمان المعلومات بشكل عام.

منهج الدراسة: في دراستنا هذه تم الاعتماد على المنهج الوصفي، الذي يعد أداة مهمة لدراسة مفهومي الذكاء الاصطناعي والأمن السيبراني، حيث يعتمد هذا المنهج على استعراض مختلف الأطر التصورية للذكاء الاصطناعي والأمن السيبراني، مع تحليل استخدامات الذكاء الاصطناعي في مجال الأمن السيبراني وكذا التحديات التي تواجهه.

المحور الأول

ماهية الذكاء الاصطناعي

عرف الذكاء الاصطناعي اهتماما كبيرا في العصر الحالي، وعليه سنتناول في هذا الصدد مفهوم الذكاء الاصطناعي وبنيته وأبرز تقنياه واستخداماته.

1-مفهوم الذكاء الاصطناعي

هناك تعريفات متعددة ونذكر منها:

يتكون مصطلح الذكاء الاصطناعي من كلمتين، الذكاء وتعني القدرة على الفهم وإدراك المفاهيم الجديدة، والاصطناعي فترتبط بالأشياء التي نتجت عن عناصر معينة على عكس الأشياء الطبيعية التي ظهرت نتيجة تدخل الإنسان.[1]

يعرف الذكاء الاصطناعي على أنه ذلك الفرع من علم الحاسوب الذي يهدف إلى فهم طبيعة الذكاء الإنساني عن طريق عمل برامج للحاسب الآلي قادرة على محاكاة السلوك الإنساني، فهو يهتم بالعمليات المعرفية التي يستعملها الإنسان في أداء الأعمال التي تعد ذكية، كالقدرة على فهم نص لغوي منطوق أو مكتوب أو لعب الشطرنج أوحل لغز ومسألة رياضية.[2]

ويشير الذكاء الاصطناعي إلى علم هندسة الآلات الذكية، وبصورة خاصة برامج الكمبيوتر حيث أنه يقوم على إنشاء أجهزة وبرامج حاسوبية قادرة على التفكير بالطريقة نفسها التي يعمل بها الدماغ البشري وتحاكي تصرفات البشر.[3]

---

[1] وفاء فواز المالكي، الذكاء الإصطناعي في تعزيز الإستراتيجيات التعليمية في التعليم العالي(مراجعة الأدبيات)، مجلة العلوم التربوية والنفسية، 7(5)، 2023، ص 96.

[2] حفيظة بلقاسمي ،رهانات الترجمة الآلية العصبية. المؤتمر العلمي الدولي حول الترجمة الآلية العصبية وتحديات الذكاء الإصطناعي يوم 26 ماي. برلين: إصدارات المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والإقتصادية، 2021 ،بلا تاريخ، ص 21.

[3] إبراهيم عباس الزهيري، و وآخرون، تطبيق الذكاء الإصطناعي في التعليم العالي بمصر في ضوء السياق الثقافي، مجلة العلوم التربوية- كلية التربية بقنا، 49(49)، 2021، ص 79.

من خلال ما سبق نستنتج أن الذكاء الاصطناعي هو مجمل البرامج والآلات التي تحاكي تفكير الأفراد ويمكن الانتفاع منها في مجالات واسعة كإيجاد الحلول للمشاكل المعقدة واتخاذ القرارات وتحليل البيانات الضخمة بسرعة ودقة عالية.

2-بنية الذكاء الاصطناعي

يمكن وصف الذكاء الاصطناعي على أنه نموذج لمعالجة البيانات فهو قادر على توليد أنظمة معالجة معلومات جيدة لحل مهام معينة، نلاحظ أن هذا الوصف يتم استيفاؤه من خلال المثال الأكثر شهرة وهو استغلال مجال حساب التفاضل والتكامل الرمزي في بناء برامج الذكاء الاصطناعي لأداء وظائف معينة، استنادا إلى ذلك يمكن اعتبار علم النفس الحسابي والفلسفة الحاسوبية والذكاء الآلي دعامات أساسية لبناء نماذج للذكاء الاصطناعي، ومع ذلك هناك طريقتان لبناء نماذج الذكاء الاصطناعي، تعرف الأولى باسم المقاربة الخالصة، أو الذكاء الاصطناعي من أعلى إلى أسفل، والتي يتم التعبير عن مبادئها في فرضية نيويل سيمون: "لا يمكن تنفيذ الإجراءات ذات المغزى إلا إذا كانت هناك آلية للحسابات الرمزية في نظام مادي ما، ومثل هذه الحسابات الرمزية بحد ذاتها شرط ضروري لوجود الذكاء في هذا النظام"، الاتجاه الأكثر تطورا ضمن هذا المنهج هو اتجاه الحوسبة الرمزية، استنادا إلى منطق المعالجة النحوية للرموز، والمبدأ الأساسي فيه هو أن المعرفة يتم تمثيلها من خلال هياكل الرموز ذات المعنى اللغوي، وكل رمز يمثل بعض الكيانات، سواء كانت مجردة أو ملموسة، والتي يناقشها النظام أو الوكيل الذكي، أو يراقبها أو يفكر فيها أو يعمل عليها، أما الطريقة الثانية التي حددها مارفن مينسكي فتسمى "النهج الصاعد"، أو "الذكاء الاصطناعي من أسفل إلى أعلى"، حيث يعتمد على افتراض أنه من الممكن محاكاة العمليات الطبيعية منخفضة المستوى التي تحدث في الدماغ الحي، ويجمع هذا الاتجاه بين تقنيات مختلفة مثل الشبكات العصبية الاصطناعية والحوسبة التطورية والحوسبة الحيوية، وفي الواقع الطريقتان المذكورتان أعلاه تشكلان أساس أي نهج لتطوير أنظمة الذكاء الاصطناعي.[1]

[1] وليد ورقلي، و مسعود بوخالفي، تأثير الذكاء الإصطناعي والمعرفة المالية على الشمول المالي:دراسة عينة من البلدان العربية . مجلة الميادين الإقتصادية، 06(01)، 2023، ص406.

3- تقنيات الذكاء الاصطناعي

تتضمن تقنيات الذكاء الاصطناعي العديد من الحقول الفرعية ومن بينها نجد:[1]

- **معالجة اللغة الطبيعية:** وهي تهدف إلى إنتاج أنظمة الحاسوب التي يمكنها فهم وترجمة اللغات الإنسانية والتواصل بها، باستخدام تقنيات التعلم الآلي والشبكات العصبية العميقة والتعلم العميق لتحسين قواعد معالجة اللغة الطبيعية؛

- **الشبكات العصبية:** وهي تحاكي عمل الخلايا العصبية في الدماغ وتستخدم في مهام التعرف على الصور والكلام ومعالجة اللغة الطبيعية واللعب؛

- **البراهين الرياضية:** وهي تسمح للحواسيب بحل المشاكل الرياضية واكتشاف مفاهيم رياضية جديدة؛

- **الخوارزميات الجينية:** هي نظم تحاكي تصرف الإنسان عندما يواجه مشكلات متكررة وتقوم باتخاذ القرار؛

- **الأنظمة المعتمدة على المعرفة:** وهي الأنظمة التي تقوم بترميز معرفة الخبراء البشريين بطريقة يمكن للحاسوب الاستدلال بها؛

- **الاستدلال القائم على الحالات:** وهي تحاكي كيفية استدلال البشر من الخبرة السابقة؛

- **الروبوتات:** وهي تركز على بناء روبوتات ذكية تتكيف مع بيئتها؛

- **تقنيات الرؤية:** وهي تركز على مهام مثل التعرف على الوجوه.

[1] Al-Qusi, A. J. Using of artificial intelligence applications for development of learning and educating process. 10 Scientific Conference 24-25 oct2009, 2010 ,Al-Mansour Journal, p. 40.

4-استخدامات الذكاء الاصطناعي

وتتمثل في الاستخدامات التالية:[1]

- **الرعاية الصحية:** يعد الذكاء الاصطناعي من أهم التقنيات التي تحدث ثورة في مجال الرعاية الصحية، إذ يساعد في تشخيص الأمراض بدقة أكبر من الأطباء البشريين في بعض الحالات، فتقنيات مثل تحليل الصور الطبية باستخدام الشبكات العصبية العميقة يمكنها اكتشاف الأمراض، مثل السرطان في مراحله المبكرة، بالإضافة الى ذلك يتم استخدام الذكاء الاصطناعي في تطوير أدوية جديدة من خلال تحليل التفاعلات الكيميائية، وتحديد الجزيئات الفعالة؛

- **التعليم:** يوفر الذكاء الاصطناعي تجارب تعليمية مخصصة تلبي احتياجات كل طالب على حدة، فمن خلال تحليل أنماط التعلم وأداء الطلاب، يمكن للأنظمة الذكية توفير مواد تعليمية مخصصة، وتقديم توصيات للمعلمين حول كيفية تحسين أساليب التدريس، بالإضافة إلى ذلك تستخدم تقنيات مثل الواقع المعزز والافتراضي، لتحسين تجربة التعلم وجعلها أكثر تفاعلية؛

- **الأعمال والتجارة:** يستخدم الذكاء الاصطناعي في تحسين العمليات التجارية، وإدارة الموارد بشكل أكثر كفاءة، حيث تساعد تقنيات التعلم الآلي في تحليل البيانات الكبيرة، لتقديم توقعات دقيقة حول الطلبات المستقبلية، وإدارة المخزون، بالإضافة إلى توفر روبوتات المحادثة المدعومة بالذكاء الاصطناعي خدمة عملاء فعالة وسريعة، ما يحسن من تجربه العميل ويقلل من التكاليف؛

- **المواصلات:** تعتبر السيارات ذاتية القيادة واحدة من أبرز تطبيقات الذكاء الاصطناعي، تعتمد هذه السيارات على تقنيات التعلم العميق وأجهزة الاستشعار المختلفة لفهم البيئة المحيطة، واتخاذ قرارات القيادة، وتعد السيارات ذاتية القيادة بتقليل الحوادث المرورية،

[1] علاء الدين حميدي. (10 7, 2024). الذكاء الإصطناعي .. الثورة القادمة في عالم التكنولوجيا. (شبكة الجزيرة الإعلامية) تاريخ الاسترداد 14 12, 2024، من الجزيرة: http://www.aljazeera.net

وجعل التنقل أكثر كفاءة وأمانا، وتستخدم تطبيقات الذكاء الاصطناعي في إدارة حركة المرور، وتحسين وسائل النقل العام؛

- **الحياة اليومية:** يستخدم الذكاء الاصطناعي في العديد من جوانب حياتنا اليومية بطرق قد لا نلاحظها، من خلال مساعدات الذكاء الاصطناعي مثل Siri و Alexa يمكننا التحكم في الأجهزة المنزلية، وإجراء المكالمات وإرسال الرسائل، كما تستخدم تقنيات التعلم الآلي في التوصيات على منصات البث مثل Netflix و Spotify، ما يساعدنا في اكتشاف محتوى جديد يناسب اهتماماتنا.

المحور الثاني

مدخل مفاهيمي حول الأمن السيبراني

سنتطرق من خلال هذا المحور إلى مفهوم الأمن السيبراني والتهديدات التي تعترضه إلى جانب أهدافه وأهميته وعرض أبرز أبعاده.

1-مفهوم الأمن السيبراني

يتكون مصطلح الأمن السيبراني من كلمتين هما الأمن، بمعنى زوال الخوف والسلامة والاطمئنان، وكلمة السيبراني المشتقة من كلمة Kybernetes بمعنى الشخص الذي يدير دفة السفينة أو المتحكم، أما مصطلح الأمن السيبراني فيعتبر أحد فروع العلوم التكنولوجية الذي يعنى بحماية الأنظمة والبرامج والشبكات من الهجمات الرقمية التخريبية والتي تهدف إلى الوصول غير المرخص إلى المعلومات الحساسة بغرض تغييرها أو تعطيلها أو إتلافها. [1]

يشير الأمن السيبراني إلى ممارسة الدفاع عن أجهزة الكمبيوتر والأجهزة المحمولة والأنظمة الالكترونية والشبكات والبيانات من الهجمات الخبيثة.[2]

كما يعكس الأمن السيبراني حسب الباحث Edward Amorso صاحب كتاب الأمن السيبراني مجموع الوسائل التي تحد من خطر الهجوم على البرمجيات والشبكات بواسطة وسائل وأدوات لمواجهة القرصنة وكشف الفيروسات الرقمية ووقفها وتوفير الاتصالات المشفرة والأمنة.[3]

---

[1] بوطبة عبد الله، بوستي توفيق، دور الأمن السيبراني في تعزيز الأمن الصحي للدول، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 09، العدد02، السنة 2024، ص708-709.

[2] أمينة بوخزر، و علي جقريف، أهمية اعتماد تقنية البلوك تشين في تعزيز الأمن السيبراني في القطاع المصرفي، مجلة البحوث في العلوم المالية والمحاسبية، 9(2)، (2024)، صفحة 387.

[3] وفاء مطروح، و ابتسام أنيس، تداعيات جائحة كوفيد 19 وتأثيره على تحقيق الأمن السيبراني في الجزائر، المجلة الدولية للاتصال الاجتماعي، 2(9)، (2022). صفحة 222.

2-تهديدات الأمن السيبراني

تتمثل أبرز التهديدات فيما يلي:[1]

- **البيانات غير المشفرة:** أحد التهديدات الشائعة التي تواجهها البنوك هو عندما تترك البيانات غير مشفرة ويستخدم المتسللون أو مجرمو الأنترنت البيانات على الفور مما يتسبب في مشكلات خطيرة ومنه يجب أن تكون جميع البيانات المخزنة على أجهزة الكمبيوتر في المؤسسات أو عبر الأنترنت مشفرة بالكامل مما يضمن أنه في حالة سرقة البيانات لا يتمكن المخترقون من استخدامها؛

- **البرامج الضارة:** تستخدم أجهزة الكمبيوتر والأجهزة المحمولة في الغالب لإجراء المعاملات الرقمية مما يستوجب تزويدها بالحماية، وتشكل البرامج الضارة خطرا كبيرا على البنوك عندما تتم المعاملات عبر الشبكات الالكترونية والأنترنت خاصة إذا كان جهاز المستخدم يحتوي على برامج ضارة مثبتة فيه دون أي حماية؛

- **خدمات الطرف الثالث:** تلجأ العديد من المؤسسات إلى الجهات الخارجية من البائعين وغيرهم بهدف خدمة عملائهم بشكل أفضل، وفي حال لم يكن لدى الجهات الخارجية إجراءات صارمة للأمن السيبراني تواجه المؤسسات مشاكل أمنية من خدمات الطرف الثالث؛

- **الانتحال:** يعد أحد أحدث أشكال التهديدات الالكترونية التي تواجهها البنوك حيث ينتحل مجرمو الأنترنت عنوان موقع المؤسسة على الويب URL بموقع ويب مشابه للموقع الأصلي ويعمل بالطريقة نفسها، وعندما يقوم المستخدم بإدخال بيانات تسجيل الدخول الخاصة به على الموقع المزيف يتم سرقة بيانات تسجيل الدخول من قبل هؤلاء المخترقين واستخدامها لاحقا وتتزايد حدة هذا التهديد مع استخدام تقنيات انتحال جديدة من قبل المخترقين؛

[1] جميلة جغل، و عادل زقرير، الأمن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي(التهديدات السيبرانية، آليات التحوط)، مجلة التنمية الاقتصادية، 8(1)، (2023) ، الصفحات 308-309.

- **التصيد الاحتيالي:** هو محاولة الحصول على معلومات حساسة مثل تفاصيل بطاقة الائتمان عن طريق التنكر ككيان جدير بالثقة في اتصال إلكتروني حيث تتطور عمليات التصيد الاحتيالي على الأنترنت بشكل مستمر.

3-أهداف الأمن السيبراني وأهميته

يهدف الأمن السيبراني إلى:[1]

- حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة أو التنقل، وإلى الحماية ضد تعطيل خدمة المستخدمين الشرعيين؛

- تحسين مستوى حماية المعلومات وضمان استمرارية تدفقها وتشغيلها؛

- ضمان انسيابية آمنة للمعلومات وانتقال مشروع، مصرح ومرخص للملفات والبيانات؛

- استرداد البيانات المسربة في أسرع وقت في حالة حدوث خرق للأنظمة الأمنية السيبرانية.

من خلال أهداف الأمن السيبراني يظهر جليا الأهمية الأمنية لحماية المعلومات ومصادرها والأنظمة المرتبطة بحفظها وصيانتها واسترجاعها، وهذا ما نلمسه في العناصر التالية:

- **السلامة:** أي سلامة البيانات والمعلومات وحمايتها من أي هجوم أو خرق أو قرصنة؛

- **السرية:** تكون كل المعطيات والبيانات والمعلومات في مأمن وغير مرخص أو مسموح لأي كان من الولج إليها؛

- **الجاهزية:** طالما أنها آمنة ومحمية فهي متاحة وجاهزة للاستعمال حسب الطلب والإتاحة.

---

[1] حياة حميدي، و نسيمة طايلب، مدخل مفاهيمي حول الأمن السيبيراني. مجلة مدار للدراسات الاتصالية الرقمية ، المجلد 02، العدد 02، 2022، ص08-10

فأهمية الأمن السيبراني تكمن في العديد من الفوائد والمميزات أهمها:

- التقليل من مخاطر التهديدات الأمنية والاختراقات المحتملة للبيانات الى جانب الحفاظ على سرية المعلومات؛

- إحلال الحماية الأمنية اللازمة للملفات الشخصية والحساسة لمنع الوصول غير المصرح إليها؛

- ضمان استمرارية عمل المؤسسات المؤمنة وتجنب تعطيل مصالحها المتصلة بالاستخدام السيبراني لشبكة الانترنت، مع تقليل وقت التوقف عن الخدمات الرقمية خاصة الحساسة منها.

4-أبعاد الأمن السيبراني

يشمل الأمن السيبراني أنظمة الأمن العسكرية والاقتصادية والاجتماعية والسياسية التي تهدف الى الحفاظ على الأمن من جميع التهديدات السيبرانية، كما يتم تضمين الأمن المتكامل الذي يعمل على الحفاظ على جوانب نظام الأمن السيبراني، ومن أهم ابعاد الأمن السيبراني نجد:[1]

- **البعد العسكري:** ويهدف الى الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يتيح تبادل وتدفق المعلومات والأوامر، وإنها فكرة لإنشاء ونشر شبكة للأنترنت والأهداف البعيدة، ولكنها أيضا نقطة ضعف، خاصة إذا كانت غير آمنة، ويمكن أن يؤدي تدمير قواعد البيانات العسكرية أو المساومة عليها الى تعطيل الاتصالات بين وحدات القيادة والوحدات العسكرية، فضلا عن إمكانية التحكم وفقدان السيطرة على بعض الأسلحة مثل الطائرات بدون طيار والصواريخ الموجهة والاقمار الصناعية.

[1] محمد مختار، الأمن السيبراني مفاهيم المستقبل، مجلة اتجاهات الأحداث، (02)،2015 ، ص 06.

- **البعد الاقتصادي:** نظرا لاستخدام أجهزة الكمبيوتر لتشغيل الصناعات وتنميتها ودفع الاقتصاد، ستصبح الانترنت أساس التجارة التمويل والمعاملات المالية، وكلها مرتبطة ببعضها البعض من خلال شبكات الكمبيوتر لتحقيق الأمن السيبراني خصوصا ما تعلق بالقطاع المالي.

- **البعد الاجتماعي:** يوجد أكثر من 4 مليارات مستخدم للأنترنت في جميع أنحاء العالم، منهم أكثر من 2,6 مليار يستخدمون مواقع الشبكات الاجتماعية، حيث مواقع التواصل الاجتماعي لديها أعلى تركيز للتفاعل البشري، تاركة الباب مفتوحا على مصراعيه لمشاركة الأفكار والتجارب الجيدة، لكنها في المقابل تفضح أخلاق الناس، وإن صعوبة الرقابة على محتوى الانترنت لا تعرض المجتمع للخطر فحسب، بل تعرض أيضا المعلومات الشخصية لأنشطة خارجية تطفلية، والتي يمكن أن تهدد السلم الاجتماعي للبلد نتيجة فقدان الأمن السيبراني الاجتماعي.

- **البعد السياسي:** بعيدا عن تسريبات الوثائق والامتيازات التي غالبا ما تؤدي الى أزمات دبلوماسية بين الدول، فإن التدخل السيبراني لروسيا في الانتخابات الأمريكية هو أهم دليل على الحاجة الى الأمن السيبراني وأهميته في البعد السياسي.

- **البعد القانوني:** يتطلب التطور التكنولوجي السريع الامتثال للقوانين القانونية من خلال تطوير الأطر والقوانين للأنشطة القانونية وغير القانونية في الفضاء السيبراني وأن الجرائم الإلكترونية هي في الغالب جرائم سيبرانية، وبعض البلدان ليس لديها إطار قانوني صارم للتعامل معها.

المحور الثالث

الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني

يحتوي هذا المحور على أبرز استخدامات الذكاء الاصطناعي في مجال الأمن السيبراني إلى جانب تحديات استخدام الذكاء الاصطناعي في مجال الأمن السيبراني.

1-استخدامات الذكاء الاصطناعي في مجال الأمن السيبراني

وفقا لتقرير Cap Gemini حول تطورات الأمن السيبراني، فإن أهم ميزة للذكاء الاصطناعي هي الأمن السيبراني، حيث تتعدد استخدامات ووظائف الذكاء الاصطناعي في الأمن السيبراني والتي نذكر منها ما يلي:

- **استخدام الذكاء الاصطناعي للتحقق من الأخبار**

هناك مجموعة من الأدوات مفتوحة المصدر المتاحة لاكتشاف التزييف العميق للأخبار والتي من بينها نجد ما يلي:[1] (الخاتم علي و وآخرون، 2024، صفحة 42)

- **Deep Lab Face:** هو برنامج شائع لإنشاء واكتشاف التزييف العميق للأخبار فهو يوفر أدوات لتدريب نماذج التعلم العميق لإنشاء مقاطع الفيديو التي تم التلاعب بها وتحديدها؛

- **Git Hub :** يستخدم للكشف عن التزييف العميق من خلال تعزيز التعلم الآلي والتعلم العميق ونقل تقنيات التعلم لتحسين الدقة، وهو يتضمن مجموعات بيانات وأوراق بحثية وموارد مختلفة لمواجهة التحدي المتمثل في تحديد المحتوى الذي تم التلاعب به؛

- **Py Torche :** توفر أدوات مفيدة لتحليل الوجه بغرض اكتشاف الخداع والتزييف العميق؛

[1] هاشم عبد الله الخاتم علي، و وآخرون، توظيف تقنيات الذكاء الاصطناعي في التحقق من المحتوى الاخباري بالتطبيق على عينة من الأخبار بموقع جمينة الاخباري. مجلة بحوث ودراسات في الميديا الجديدة، 5(3)، 2024، ص 42.

- **Facetorch :** يركز على اكتشاف التلاعب بالوجه بالفيديو من خلال مجموعة من الشبكات العصبية لمكافحة مختلف أشكال الغش والتزييف.

- **إثبات الجرائم السيبرانية باستخدام الشبكات العصبية**

تعد الشبكات العصبية آلية إلكترونية تحاكي الجوانب الهيكلية والوظيفية للشبكات العصبية الموجودة في النظم العصبية البيولوجية، وتؤتي نتائج كبيرة في حالات التنبؤ أو التصنيف أو التحكم في البيئات السيبرانية الحيوية والمعقدة، ومن تطبيقات استخدامها في إثبات الجرائم السيبرانية نجد ما يلي:[1]

- **شبكة Neuro Net:** وهي عبارة عن نظام شبكة عصبية يجمع بين المعلومات الموزعة ويعالجها ويثبت المخالفات السيبرانية، حيث يصدر تنبيهات وفي الوقت ذاته يبدأ بالتدابير المضادة فلقد أظهر الواقع العملي فعالية هذه الشبكة في إثبات ومكافحة جرائم هجمات حجب الخدمة، وقد تم تصميم معرفات هوية عصبية قائمة على الشبكات يمكنها على الفور إثبات وتصنيف مختلف الهجمات؛

- **شبكة IDS-NNM:** عبارة عن نظام لإثبات جرائم الاختراق الالكتروني باستخدام الشبكة العصبية المعتمدة على النمذجة، وقد أثبتت التجارب العملية فعاليتها في إثبات جميع محاولات الاقتحام في اتصالات الشبكة دون إعطاء أي تنبيهات خاطئة، كما تم استحداث أنظمة أخرى لإثبات جرائم الاختراق الالكتروني مع التركيز بشكل خاص على الأنظمة التي تستخدم شبكات عصبية اصطناعية لإثبات حركة المرور المشبوهة والتي قد تشكل جريمة؛

- **العميل المحقق الذكي:** هو عبارة عن قوى مستقلة يولدها الكمبيوتر وتتواصل مع بعضها البعض حيث يحدث تبادل للبيانات وتتعاون فيما بينها من أجل تنفيذ الاستجابات المناسبة في حالة وقوع أحداث غير متوقعة، حيث تعد هذه التقنية مناسبة لإثبات ومكافحة الهجمات الالكترونية نظرا لقابليتها على الانتقال والتكيف في البيئات التي تم نشرها فيها؛

[1] حمد عبد الله علي النيادي، الدليل السيبراني المستمد من الذكاء الاصطناعي، المجلة القانونية، 14(4)، (2022) ،ص1249-1254.

- **نظام المناعة الاصطناعية:** يتم توظيف نظام المناعة الاصطناعية لدعم الاستقرار في بيئة تتميز بالتغير المستمر، حيث يشتمل إثبات الاختراق الالكتروني المستند إلى المناعة الاصطناعية على تطور الخلايا المناعية (الاستنساخ والاختلاف) واكتشاف المضادات في وقت واحد، وينتج النظام المناعي الاصطناعي أجساما مضادة لمقاومة مسببات الجرائم كما يمكن إثبات هذه الجرائم بواسطة الخوارزمية الوراثية والمجموعات الضبابية.

كما نجد أيضا:[1]

- **التعامل مع كميات كبيرة من البيانات:** هناك الكثير من الأنشطة الجارية على خوادمنا، هذا يعني أنه يتم نقل كمية كبيرة من البيانات بين عملائنا ومنشآتنا وبين أجهزتنا وشبكاتنا كل يوم، وهذا يعني أن محللي الأمن السيبراني لا يمكنهم التحقق من كل شيء وبيانات عن المخاطر المحتملة، والذكاء الاصطناعي هو الخيار الأفضل لاكتشاف هذه التهديدات التي تمر عبر الأنشطة اليومية، بالإضافة إلى فحص كميات كبيرة من البيانات، يمكنه مراقبة حركة المرور تلقائيا وتحليل نشاط الخادم بدقة وتحديد المخاطر المحتملة في حرمة مرور المعلومات.

- **توقع التهديدات المستقبلية:** إن كمية البيانات التي تمر عبر محللي الأمن السيبراني تجعل من الصعب التنبؤ بالتهديدات المستقبلية، لكن الذكاء الاصطناعي يمكنه معالجة كميات كبيرة من البيانات في وقت واحد، مما يتيح الكشف المبكر عن الأنشطة الضارة، ويمكن أن يؤدي تحديد الإجراءات الوقائية والتهديدات المحتملة الى تقليل الوقت الضائع وإهدار الموظفين، ويساعد على البقاء يقظا من خلال اتخاذ خطوات لحماية المؤسسة.

- **تقليل وقت اكتشاف التهديد:** القدرة على اكتشاف التهديدات بسرعة أمر بالغ الأهمية، حيث أبلغ 42% 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، وأفادت 56 من المؤسسات أنها غارقة في ملف تعريف التهديد الذي يواجه

[1] حمد دحماني، الذكاء الإصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني والسياسي، المجلد 7، العدد2023،2، ص604-606.

المحللين السيبرانيين، وأفاد 32 %منهم بأنهم غير قادرين على التحقق بشكل فعال من التهديدات المحددة؛

- **التوفير في التكاليف:** تتأثر العديد من المؤسسات ماليا بانتهاكات البيانات كل عام، ولا يمكننا تجاهلها ولا يمكننا إيقاف المجرمين، حيث وجدت الدراسة فرقا بنسبة 80 % في توفير التكاليف للمنظمات التي تستخدم الذكاء الاصطناعي لأغراض الأمن السيبراني، 2,9 مليون دولار مقارنة ب 6,71 مليون دولار للمرافق التي لا تستخدم الخدمة؛

ولعل من أهم تقنيات الذكاء الاصطناعي التي لها تأثير فعال نجد Chat GPT ، وعلى الرغم من المخاوف بشأن مخاطر الذكاء الاصطناعي، هناك مزايا مهمة تجعل من Chat GPT أداة مفيدة لصناعة الأمن، واستخدام Chat GPT له فوائد عديدة في زيادة الإنتاجية، ومساعدة المهندسين، وتدريب الموظفين، وإنفاذ القانون، ومع ذلك فإنه يحلل بشكل نقدي المخاوف المشروعة بشأن التحيز العنصري، ونقص المقاييس التي تم التحقق من صحتها، واستغلال جرائم الانترنت، ونقاط الضعف والاستغلال، وقضايا الخصوصية، والهندسة الاجتماعية. والمعلومات المضللة، والحواجز التعليمية.

إن تطوير Chat GPT سيعمل على تحسين قدرة الصناعة على اكتشاف الهجمات الإلكترونية والاستجابة لها في الوقت الفعلي، وبالتالي تعزيز مرونة الأمن السيبراني بشكل عام، كما تبسط Chat GPT المهام كثيفة العمالة عن طريق تقليل إجهاد الانتباه، مما يسمح لموظفي الأمن بالتركيز على التفكير الاستراتيجي والتحليل، وتتضمن أيضا إمكانات Chat GPT ميزات تساعد الباحثين عن البرامج الضارة على أداء مهام معقدة مثل إنشاء التعليمات البرمجية ومقارنة العقود وتحليل عينة البرامج الضارة، بالإضافة الى ذلك تقوم بسد فجوة المعرفة الأمنية من خلال تسهيل تدريب الموظفين وتعليمهم حول الاحتيال والهندسة الاجتماعية وأمن كلمات المرور، بالإضافة الى ذلك قد تساعد Chat GPT جهات إنفاذ القانون في التحقيق والتنبؤ بالنشاط الإجرامي، ومساعدتهم على الاستجابة للتغيرات في تكتيكات وتقنيات الجرائم الإلكترونية، وعلى الرغم من الفوائد العديدة لاستخدام Chat GPT، تواجه فرق الأمن تحديا يتمثل في عدم وجود معايير موثوقة لتقييم سلامة أنظمة الذكاء الاصطناعي وأمانها

ومرونتها، لقد تم بالفعل تسليح Chat GPT من قبل مجرمي الانترنت واستخدموا لإنشاء وتوزيع إصدارات وتكتيكات متعددة من البرامج الضارة.

2-تحديات استخدام الذكاء الاصطناعي في مجال الأمن السيبراني

على الرغم من الفوائد المتعددة التي يحققها استخدام الذكاء الاصطناعي في مجال الأمن السيبراني إلا أن هناك عدة تحديات ومخاطر تواجه هذا الاستخدام وهي:[1]

- **التحيز في صنع القرار:** في حال استخدام أنظمة الذكاء الاصطناعي القائمة على مجموعات البيانات التي تحتوي على معلومات أو خوارزميات متحيزة في مجال الأمن السيبراني، فقد يؤدي الى قرارات تمييزية ضد جماعات أو أفراد معنيين وأن تكون لها عواقب وخيمة على المنظمة، وعلى سبيل المثال، إذا اتخذ الذكاء الاصطناعي قرارا قائم على المدخلات المتحيزة، فقد ينتج عن ذلك منع المستخدمين الشرعيين من الوصول الى أنظمة الشركة.
- **الافتقار الى القابلية للتفسير والشفافية:** تتسم الخوارزميات المستخدمة لاتخاذ قرارات بشأن التهديدات الأمنية بعدم الشفافية في كل الأوقات، وهو ما يصعب من تفسير قرارات الذكاء الاصطناعي السيئة ويفقد القدرة على تحسينها، وبالتالي يتأثر أمن المنظمة بالسلب.
- **الاستخدام الضار للخوارزميات:** على الرغم من أن خوارزميات الذكاء الاصطناعي تعمل على البحث في البيانات واكتشاف الأنماط بسرعة، إلا أن الجهات الضارة تستطيع استخدامها في الوصول الى المعلومات الحساسة أو مهاجمة البنية التحتية، كما يمكن للمهاجمين السيبرانيين أيضا الاستفادة من الذكاء الاصطناعي في شن هجمات أكثر تعقيدا من خلال التعلم من البيانات لفهم الأهداف ونقاط الضعف المحتملة بشكل أفضل.
- **إساءة استخدام الذكاء الاصطناعي:** قد يضر الذكاء الاصطناعي بالأمن السيبراني عندما يستخدم في أغراض ضارة مثل إنشاء أخبار مزيفة أو نشر دعاية سلبية.

[1] الذكاء الاصطناعي والامن السيبراني: العلاقة والفرق بينهما وتحدياتها، المؤسسة العامة للتدريب التقني والمهني، 5 جانفي، 2025، تاريخ الاسترداد 4 فيفري، 2025، من بكه: http://bakkah.com

- **انتهاك خصوصية البيانات:** هناك العديد من المخاوف المثارة بشأن خصوصية البيانات التي تعالجها وتحللها تطبيقات الذكاء الاصطناعي في الأمن، إذ أن تلك التطبيقات قادرة على التعرف على تلك البيانات، وهو ما يفرض ضرورة الامتثال للوائح الخصوصية من خلال الفحص القانوني قبل نشر أنظمة الذكاء الاصطناعي.

خاتمة

في الختام يمكن القول أن **تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني** من الأدوات الحديثة والمهمة التي تساعد في التصدي للتهديدات المتزايدة والمتطورة، وتحسين مستوى الحماية من الهجمات الإلكترونية، من خلال تقنيات مثل **التعلم الآلي و التعلم العميق،** حيث يستطيع الذكاء الاصطناعي الكشف المبكر عن الأنماط الشاذة، التنبؤ بالتهديدات المستقبلية، وأتمتة الاستجابة للأزمات الأمنية، ومع ذلك يواجه تطبيق الذكاء الاصطناعي في هذا المجال مجموعة من التحديات، مثل **محدودية البيانات والاعتماد على الخوارزميات الدقيقة،** إضافة إلى **المخاطر الأخلاقية** المتعلقة بالاستخدام الخاطئ للتكنولوجيا، كما أن هناك تحديات مرتبطة بـ**تكامل الذكاء الاصطناعي مع الأنظمة الحالية، و التهديدات الجديدة التي قد يتعرض لها الذكاء الاصطناعي نفسه** من قبل المهاجمين، وعلى الرغم من هذه التحديات تظل التطبيقات الذكية في الأمن السيبراني خيارا واعدا لتحسين مستوى الأمان، ويجب على المؤسسات الاستمرار في الاستثمار في البحث والتطوير لتخطي هذه العقبات والاستفادة الكاملة من إمكانيات الذكاء الاصطناعي في حماية البيانات والأنظمة الإلكترونية.

وقد تم التوصل إلى مجموعة من **النتائج** التي تبرز أهمية استخدام الذكاء الاصطناعي في مجال الأمن السيبراني، وأبرزها:

- **تحسين كشف التهديدات:** حيث أسهم الذكاء الاصطناعي في تحسين القدرة على اكتشاف الهجمات المتقدمة والأنشطة غير الطبيعية بسرعة أكبر مقارنة بالأساليب التقليدية.

- **استجابة أسرع للهجمات:** حيث من خلال الأتمتة، أصبح من الممكن استجابة الأنظمة للهجمات الإلكترونية بشكل أكثر سرعة وفعالية، مما يقلل من الأضرار الناتجة.

- **تحليل البيانات الضخمة:** حيث تمكن تقنيات الذكاء الاصطناعي من معالجة وتحليل كميات ضخمة من البيانات في وقت قصير، مما يعزز القدرة على التنبؤ بالهجمات المستقبلية.

- **تحسين استراتيجيات الدفاع**: حيث ساعد الذكاء الاصطناعي في تطوير استراتيجيات أمنية أكثر تطورا ومرونة، مما يساهم في تعزيز دفاعات الأنظمة ضد الهجمات المتزايدة التعقيد.

كما قد تم التوصل إلى مجموعة من **التوصيات** التي يمكن أن تعزز فعالية الذكاء الاصطناعي في مجال الأمن السيبراني وتقليل المخاطر المرتبطة به، مما يساهم في حماية الأنظمة من التهديدات الإلكترونية المستمرة والمتزايدة، والمتمثلة في:

- **تعزيز التدريب وتوفير البيانات عالية الجودة**: حيث يجب توفير **بيانات دقيقة وشاملة** لتدريب النماذج الذكية، مع ضمان تحديثها باستمرار لتواكب التهديدات الجديدة.

- **تحسين تقنيات الدفاع ضد الهجمات الموجهة للذكاء الاصطناعي**: حيث من المهم تطوير **استراتيجيات وتقنيات لحماية الذكاء الاصطناعي نفسه** من الهجمات التي تهدف إلى تضليل الخوارزميات مثل **الهجمات بالتضليل أو الهجمات على النماذج المدربة.**

- **تعزيز التعاون بين التقنيين والفرق الأمنية**: حيث يجب تعزيز التعاون بين فرق الأمن السيبراني ومطوري الذكاء الاصطناعي لضمان **دمج فعال** لتقنيات الذكاء الاصطناعي في نظم الأمان الحالية دون التأثير على أداء النظام.

- **مراعاة الجوانب الأخلاقية والخصوصية: حيث** يجب أن تلتزم المؤسسات بمعايير **الأخلاقيات والخصوصية** عند استخدام الذكاء الاصطناعي، مثل **حماية البيانات الشخصية** وتجنب استخدامها بشكل يضر بالحقوق الفردية.

- **الاستثمار في البحث والتطوير**: حيث يجب أن تستثمر المؤسسات في **البحث المستمر** لتحسين قدرات الذكاء الاصطناعي في مجالات مثل **التعلم الآلي العميق والتحليل السلوكي،** لتكون قادرة على التكيف مع الهجمات المتطورة.

- **تعزيز التدريب والتوعية البشرية**: حيث من الضروري **تدريب فرق الأمن السيبراني** على فهم كيفية عمل تقنيات الذكاء الاصطناعي وكيفية الاستفادة منها بشكل آمن، وكذلك على كيفية التعامل مع التحديات التي قد تظهر في تطبيقاتها.

قائمة المراجع

1-Al-Qusi, A. J. (2010). Using of artificial intelligence applications for development of learning and educating process. 10 Scientific Conference 24-25 oct2009 (p. 40). Al-Mansour Journal.

2- الذكاء الاصطناعي والأمن السيبراني: العلاقة والفرق بينهما وتحدياتهما. (5 جانفي, 2025). (المؤسسة العامة للتدريب التقني والمهني) تاريخ الاسترداد 4 فيفري, 2025، من بكه: http://bakkah.com

3- إبراهيم عباس الزهيري، و وآخرون، تطبيق الذكاء الإصطناعي في التعليم العالي بمصر في ضوء السياق الثقافي. مجلة العلوم التربوية-كلية التربية بقنا، 49(49)، السنة 2021، صفحة 79.

4- أمينة بوخزر، و علي جقريف، أهمية اعتماد تقنية البلوك تشين في تعزيز الأمن السيبراني في القطاع المصرفي، مجلة البحوث في العلوم المالية والمحاسبية، 9(2)،السنة 2024، صفحة 387.

5_ بوطبة عبد الله، بوستي توفيق، دور الأمن السيبراني في تعزيز الأمن الصحي للدول، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 09، العدد02، السنة 2024، ص708-709.

6- جميلة جغل، و عادل زقرير، الأمن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي(التهديدات السيبرانية، آليات التحوط). مجلة التنمية الاقتصادية، 8(1)، السنة 2023، الصفحات 308-309.

7- حفيظة بلقاسمي . (بلا تاريخ). رهانات الترجمة الآلية العصبية. المؤتمر العلمي الدولي حول الترجمة الآلية العصبية وتحديات الذكاء الإصطناعي، برلين: إصدارات المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والإقتصادية يوم 26 ماي 2021 (صفحة 21).

8- حمد دحماني، الذكاء الإصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني والسياسي، السابع(الثاني) 2023

9- حمد عبد الله علي النيادي،الدليل السيبراني المستمد من الذكاء الاصطناعي، المجلة القانونية، 14(4)، (2022)، صفحة 1249.

10- حياة حميدي، و نسيمة طايلب، مدخل مفاهيمي حول الأمن السيبيراني، مجلة مدار للدراسات الاتصالية الرقمية، 02،(02)، 2022 .

11- علاء الدين حميدي. (10 7, 2024). الذكاء الإصطناعي .. الثورة القادمة في عالم التكنولوجيا. (شبكة الجزيرة الإعلامية) تاريخ الاسترداد 14 12, 2024، من الجزيرة: http://www.aljazeera.net

12- محمد مختار، الأمن السيبراني مفاهيم المستقبل. مجلة اتجاهات الأحداث(02)، (2015).

13- هاشم عبد الله الخاتم علي، و وآخرون، توظيف تقنيات الذكاء الاصطناعي في التحقق من المحتوى الاخباري بالتطبيق على عينة من الأخبار بموقع جمينة الاخباري(نوفمبر 2023-أفريل 2024، مجلة بحوث ودراسات في الميديا الجديدة، 5(3)، (2024)، صفحة 42.

14- وفاء فواز المالكي، الذكاء الإصطناعي في تعزيز الإستراتيجيات التعليمية في التعليم العالي(مراجعة الأدبيات)،مجلة العلوم التربوية والنفسية، 7(5)، (2023)، صفحة 96.

15- وفاء مطروح، و ابتسام أنيس، تداعيات جائحة كوفيد 19 وتأثيره على تحقيق الأمن السيبراني في الجزائر، المجلة الدولية للاتصال الاجتماعي، 2(9)، (2022)، صفحة 222.

16- وليد ورقلي، و مسعود بوخالفي، تأثير الذكاء الإصطناعي والمعرفة المالية على الشمول المالي:دراسة عينة من البلدان العربية، مجلة الميادين الإقتصادية، 06(01)، (2023).

الفصل الرابع

دور الذكاء الاصطناعي في تعزيز الأمن السيبراني

الدكتورة فهيمة بلحمزي،

أستاذة محاضرة ب

كلية الحقوق والعلوم السياسية، جامعة مستغانم-الجزائر

fahima.belhamzi@univ-mosta.dz

الملخص

تُعد التهديدات السيبرانية من الظواهر الخطيرة التي تختلف بطبيعتها عن التهديدات التقليدية، حيث تمثل تحديات كبيرة لأمن الأفراد والدول .ومع التطور التكنولوجي وظهور الذكاء الاصطناعي كأحد الابتكارات القوية التي أثرت على مختلف المجالات، بما فيها مجال الأمن السيبراني، جاءت هذه الدراسة لتسليط الضوء على دور تكنولوجيا الذكاء الاصطناعي في تعزيز الأمن السيبراني .اعتمد البحث على المنهج الوصفي، وتوصل إلى ضرورة الإسراع في اعتماد تشريعات متخصصة تنظم الاستخدامات المختلفة لتكنولوجيا الذكاء الاصطناعي، بهدف حماية الخصوصية وتعزيز الأمن .كما أوصى بإنشاء هيئات متخصصة لمعالجة هذا الشأن .

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، الأمن، الفضاء السيبراني، تطبيقات الذكاء الاصطناعي.

Abstract

Cyber threats are considered dangerous phenomena that differ in nature from traditional threats, as they pose significant challenges to the security of individuals and nations. With technological advancements and the emergence of artificial intelligence (AI) as a powerful innovation influencing various fields, including cybersecurity, this study aims to highlight the role of AI technology in enhancing cybersecurity. The research relied on a descriptive approach and concluded that there is an urgent need to adopt specialized legislation to regulate the various uses of AI technology, with the aim of protecting privacy and enhancing security. The study also recommended the establishment of specialized bodies to address this issue.

Keywords: Artificial Intelligence, Cybersecurity, Security, Cyber Spacee, Artificial Intelligence Applications

المقدمة

تمثل تقنية الذكاء الاصطناعي إحدى إنجازات الثورة الصناعية الرابعة، نظرًا لاستخداماتها المتنوعة وانتشارها الواسع في مختلف مجالات الحياة .فقد أصبحت أداة رئيسية في ميادين الاقتصاد، الصناعة، الخدمات، القطاع العسكري والسياسي، بالإضافة إلى دورها الحيوي في تعزيز وتحسين الأمن السيبراني .ويعد هذا الأخير جزءًا لا يتجزأ من الأمن العام سواء على مستوى الفرد أو المجتمع، حيث يتم توظيف الذكاء الاصطناعي لتحسين أداء الأمن السيبراني داخل الدولة .يشير الذكاء الاصطناعي إلى تداخله العميق مع هذا المجال، فالنقطة المشتركة بينهما تكمن في أن جميع العمليات الأمنية تحدث ضمن إطار موحد وهو الفضاء السيبراني. ولكن يظل السؤال الرئيسي هو: ما مدى فعالية استخدام تقنية الذكاء الاصطناعي في تعزيز الأمن السيبراني؟ للإجابة عن هذا السؤال المحوري، لا بد من التطرق إلى مجموعة من الأسئلة الفرعية التي تشمل ما يلي، ما مفهوم تقنية الذكاء الاصطناعي وما هي مجالات استخدامها؟ ما المقصود بالأمن السيبراني وما أبعاده؟ كيف يمكن تطبيق تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني؟

المبحث الأول

مفهوم الذكاء الاصطناعي والأمن السيبراني

الأمن السيبراني يشير إلى حماية الأنظمة الإلكترونية والشبكات من التهديدات السيبرانية مثل الاختراقات، والهجمات الإلكترونية، والبرمجيات الخبيثة .يُعتبر الأمن السيبراني أمراً ضرورياً في عصرنا الحالي، نظراً للتزايد المستمر في استخدام التكنولوجيا والإنترنت في حياتنا اليومية .من ناحية أخرى، يعد الذكاء الاصطناعي مجالاً يُسهم في تطوير الأنظمة والبرامج من خلال محاكاة الذكاء البشري، ما يتيح حماية البيانات واتخاذ قرارات ذكية .يتم تطبيق الذكاء الاصطناعي في مجالات متنوعة تشمل التجارة الإلكترونية، والطب، والتعليم، وغيرها .في هذا المقال، نستعرض مفهوم المصطلحين وأهميتهما .في القسم الأول سنتناول مفهوم الذكاء الاصطناعي، بينما يخصص القسم الثاني لمناقشة الأمن السيبراني بتفصيل أكبر.

المطلب الأول

مفهوم الذكاء الاصطناعي

الذكاء الاصطناعي هو مجال يركز على تطوير أنظمة الكمبيوتر القادرة على أداء المهام التي تتطلب تفكيرًا ذكيًا وتحاكي السلوك البشري. يعد هذا التطور تقدمًا بارزًا في مجال التكنولوجيا، حيث يسمح للأنظمة الذكية بالتعلم والتكيف مع البيئة المحيطة والتفاعل معها بكفاءة .من خلال هذا السياق، سنتناول بعض التعريفات المتعلقة بالذكاء الاصطناعي ونستعرض أبرز المجالات التي يُستخدم فيها.

الفرع الأول: تعريف الذكاء الاصطناعي

تستعرض مراجعة الأدبيات حول موضوع الذكاء الاصطناعي العديد من التعريفات المتعلقة بمفهوم هذه التكنولوجيا، والتي لم يتم تطويرها فقط من قبل المنظمات والخبراء المختصين بهذا المجال، بل أيضًا من قبل المهتمين بتكنولوجيا المعلومات .تتناول بعض تعريفات[1] الذكاء

[1] خديجة محمد درار، اخلاقيات الذكاء الاصطناعي والروبوت، المجلة الدولية لعلوم المكتبات والمعلومات، المجلد 6، العدد3، ص272

الاصطناعي ارتباطه بعلوم الإدراك والسلوكيات المعرفية وغيرها من العمليات التي تتيح للأجهزة الحاسوبية أداء المهام بكفاءة مماثلة للقدرات البشرية، مع تمكين هذه الأجهزة من التفكير الذكي والمحاكاة العقلية .على سبيل المثال، يعَرِّف ريتش وكينج الذكاء الاصطناعي على أنه دراسة كيفية أداء الأجهزة الحاسوبية للمهام بشكل أكثر كفاءة من البشر .كما يُعَرّفه مجلس صناعة المعلومات بأنه "عبارة عن مجموعة تقنيات قادرة على التعلم والتكيف واستخدام المنطق وتنفيذ المهام بطرق مستوحاة من الفكر البشري ".الذكاء الاصطناعي يجمع بين العمليات المعرفية وآليات التنفيذ ويعتمد على خوارزميات تتعامل مع المشكلات التي تتطلب حلاً يتسم بالذكاء خارج النطاق التقليدي [1].يشير هذا المفهوم كذلك إلى قدرة الآلات مثل أجهزة الحاسوب على اكتساب الذكاء وتطبيق التفكير المنطقي بطريقة مشابهة لقدرة الإنسان في تفسير وتحليل كميات ضخمة من البيانات المكتوبة أو المنطوقة [2].ومع ذلك، هذه التعريفات ليست شاملة أو موحدة؛ إذ يوجد عدد لا يُحصى منها، وكل منها يعكس وجهة نظر مختلفة بناءً على مجال خبرة الفرد واهتماماته .وعلى الرغم من الاختلاف بين الباحثين بشأن إمكانات الذكاء الاصطناعي للوصول إلى مستوى العقل البشري بسبب الفجوات الجوهرية بين الاثنين، إلا أن الذكاء الاصطناعي أصبح بالفعل حقيقة واقعة في حياتنا العملية ويتم استخدامه بشكل يومي، مما يجعله جزءًا لا يتجزأ من تجربتنا التقنية والمجتمعية.

الفرع الثاني: مجالات استخدام الذكاء الاصطناعي

للذكاء الاصطناعي العديد من الاستخدامات التي يمكن تلخيصها في النقاط التالية:
يتم استخدام تقنية الذكاء الاصطناعي في مجالات خدمية متعددة، منها العسكرية، الصناعية، التقنية، المالية، الطبية، والتعليمية .وتتضمن تطبيقاته البارزة السيارات ذاتية القيادة، الطائرات بدون طيار، الروبوتات القادرة على العمل بشكل مستقل، وتشغيل الآلات المستخدمة في مختلف الصناعات .مثال على ذلك :العمل في بيئات معقدة مثل الكابلات داخل المفاعلات النووية، محطات الطاقة، المناطق تحت الأرض، واستكشاف المناجم، وهي مجالات يصعب فيها الاعتماد على الجهد البشري المباشر .تُستخدم عمليات المحاكاة الذكية على الحواسيب لدراسة

[1] حسن بن محمد حسن العمري، الذكاء الاصطناعي ودوره في العلاقات الدولية، المجلة العربية للنشر العلمي، العدد 29، 2021 على الرابط الالكتروني http//www.ajsp.net

[2] نرمين مجدي، الذكاء الاصطناعي وتعلم الآلة، سلسلة كتيبات تعريفية، العدد3 صندوق النقد العربي، ابو ظبي، الامارات 2020 على الرابط الالكتروني www.amf.org.ae

كيفية تعرف الدماغ البشري على الوجوه والأصوات المألوفة، معالجة الصور، استخراج البيانات الهامة منها، وتحسين القدرات المتعلقة بالذاكرة .كما تنطبق هذه التقنيات على تطوير الألعاب الإلكترونية، مثل ألعاب الشطرنج وألعاب الفيديو .تساعد الأجهزة الذكية في ممارسة المهارات الحركية والسيطرة على العمليات المعقدة وغير الخطية .تشمل هذه التطبيقات المهام الدقيقة مثل البحث في التصميم الصناعي أو التحكم في العمليات الصناعية.

يُستخدم الذكاء الاصطناعي لتعليم اللغة وفهم النصوص، سواء المكتوبة أو المنطوقة، كما يساهم في ترجمة اللغة بشكل فوري .تعتمد هذه التقنية على أجهزة كمبيوتر مبرمجة مسبقًا[1]، مثل تقنية Google، مع اتصال مباشر بالإنترنت .هذا التطور يجعلنا نُقر بأن الذكاء الاصطناعي يوفر مجموعة كبيرة من التطبيقات المتنوعة عبر قطاعات مختلفة. فهو يُستخدم في المجالات العسكرية والمالية والخدمية والصناعية .كما يمكن توظيفه في مجال التعليم من خلال منصات تعليمية وتطبيقات رقمية مخصصة .يوفر الذكاء الاصطناعي العديد من المزايا؛ على سبيل المثال، في المجال الطبي، يمكن أن يساعد الأطباء في تشخيص الأمراض وتوجيه العلاج بدقة أعلى .أما في قطاع التصنيع، فإنه يُسهم في تحسين عمليات الإنتاج وزيادة الكفاءة، حيث تستطيع الروبوتات المزودة بتقنيات الذكاء الاصطناعي إنجاز المهام الروتينية بدقة وسرعة كبيرتين .ومع ذلك، يواجه الذكاء الاصطناعي بعض التحديات والقيود، خاصة في المجالات التي تتطلب التفكير الإبداعي والحدس البشري.

المطلب الثاني

مفهوم الأمن السيبراني

في هذا المطلب، سيتم تسليط الضوء على مفهوم الفضاء السيبراني والجوانب المرتبطة به .يهدف ذلك إلى توضيح المفاهيم والمصطلحات المتعلقة به بشكل أقرب وأكثر شمولية .في الجزء الأول، سيتم التركيز على تعريف الفضاء السيبراني باعتباره المجال الذي تُنفذ فيه العمليات السيبرانية .أما في الجزء الثاني، فسيتم التطرق إلى التهديدات السيبرانية. وأخيرًا، سيُختتم الحديث بتناول مفهوم الأمن السيبراني وأبعاده المختلفة.

[1] نرمين مجدي، المرجع السابق، ص5

الفرع الأول: تعريف المجال السيبراني وتهديداته

لقد أصبح الفضاء السيبراني مجالًا جديدًا في العلاقات الدولية، حيث يتيح إنشاء قاعدة قوة جماعية تجمع بين الجهات الفاعلة الحكومية وغير الحكومية عبر الحدود .يُعَدُّ الفضاء السيبراني امتدادًا للنشاط البشري، بجانب الأدوار التي يؤديها البشر في المجالات الدولية الأخرى مثل البر، البحر، الجو، والفضاء .مصطلح" الحوكمة "يرتبط بوسائل الإعلام والتفاعل بين الإنسان والآلة. هذا المفهوم نابع من أعمال نوربرت فينر، الذي تناول فكرة التفاعل بين الإنسان والتكنولوجيا بما يؤدي إلى بناء بيئات اتصال مستدامة تُشكِّل النسيج الأساسي للفضاء السيبراني [1].أما من ناحية التعريف العسكري، فقد عرَّفت وزارة الدفاع الأمريكية الفضاء السيبراني بأنه "المنطقة العالمية داخل بيئة المعلومات، التي تتألف من شبكات مترابطة تتضمن البنى التحتية للبيانات والتكنولوجيا مثل الإنترنت، شبكات الاتصالات، الحوسبة، المعالجة، والتحكم ."هذه الشبكات تخدم الفضاء السيبراني كبعد رقمي للمعلومات، حيث البيئة تمثل بيئة افتراضية غير ملموسة [2].يغطي هذا المفهوم نطاقًا واسعًا من العمليات بما يشمل سرعة نقل البيانات والوصول إلى الشبكات .البيئة الإلكترونية تتعامل مع البيانات أثناء تدفقها عبر الشبكة، مما يُظهر التداخل العميق بين التكنولوجيا والبشرية في هذا المجال الجديد.

الفضاء السيبراني يعد عالماً افتراضياً يتألف من أنظمة الحاسوب، الشبكات، البرمجيات، البيانات، والمعلومات .يشمل هذا الفضاء كافة الأنشطة والعمليات التي ترتبط بالعالم الرقمي، مثل التواصل عبر الإنترنت، التجارة الإلكترونية، شبكات التواصل الاجتماعي، الخدمات المصرفية الإلكترونية، الخدمات الحكومية الرقمية وغيرها .مع التوسع المتزايد في استخدام التكنولوجيا والإنترنت في حياتنا اليومية، أصبح الفضاء السيبراني هدفاً للتحديات الأمنية والتهديدات السيبرانية .يتعرض هذا الفضاء للكثير من الهجمات، مثل القرصنة، البرامج الضارة، التصيد الاحتيالي، التجسس السيبراني، وغيرها من أساليب الاختراق والهجمات الإلكترونية.

---

[1] عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، مكتبة الاسكندرية وحدة الدراسات المستقبلية، 2016، ص7 ،8

[2] عادل عبد الصادق، نفس المرجع، ص11

التهديدات الاستراتيجية تنبع غالبًا من تضارب المصالح والأهداف الوطنية وتمحور حول زعزعة الاستقرار السياسي أو الاقتصادي أو الاجتماعي أو العسكري للدول .هذه التهديدات قد تؤدي إلى تدهور الحد الأدنى من الأمن القومي، ما يفرض ضغوطًا خارجية غير متوازنة قد تدفع الأطراف المعنية إلى اللجوء للقوة العسكرية، مما يعرض الأمن القومي لمخاطر كبيرة[1] .وفقًا لباري بوزان، التهديد يُعرَّف على أنه الحالة التي تتعرض فيها أراضي الدولة أو مصالحها للضرر أو العدوان، سواء كان ذلك باستخدام القوة الأيديولوجية أو ما يمتلكه طرف ضد آخر من موارد داخلية وخارجية [2].وينطبق هذا على التهديدات التي تواجهها الحكومات من خلال استغلال عناصر تحكم متنوعة سواء داخلية أو خارجية .أما التهديدات السيبرانية فتعود أصولها إلى مصطلح"Cyber" ، الذي يشير إلى كل ما يتعلق بأجهزة الكمبيوتر، تكنولوجيا المعلومات، والواقع الافتراضي. المصطلح مشتق من الكلمة اليونانية "Kybernetes"، والتي تعني القيادة أو التحكم. يرتبط هذا بشكل عام بإدارة الأنظمة سواء في الآلات أو الكائنات الحية بطريقة آلية [3].تشير التهديدات السيبرانية إلى استغلال تكنولوجيا المعلومات وأجهزة الكمبيوتر للإضرار بالبنية التحتية وتعطيل خطط مدروسة بعناية .يتضمن ذلك استخدام البريد الإلكتروني لاختراق مكاتب المراقبة أو شن هجمات لتدمير أنظمة الدفاع الجوي أو نظم المعلومات الهامة .كما تُعد هذه التهديدات خطرة على الأمن القومي والاجتماعي والاقتصادي دون أن يكون لها عواقب أخلاقية أو جسدية فورية [4].يمكن وصف التهديد السيبراني بأنه أي نشاط غير قانوني أو ضار يتم تنفيذه عبر الإنترنت أو شبكات الكمبيوتر . يشمل ذلك مجموعة واسعة من الأنشطة مثل القرصنة الإلكترونية، استخدام البرمجيات الخبيثة، الاحتيال السيبراني، سرقة الهوية، التجسس الإلكتروني، وتنفيذ هجمات موجهة على البنية التحتية للأنظمة الحساسة. هذه التهديدات لا تؤثر فقط على الأفراد، بل قد تمتد لجماعات ودول بأكملها عبر الفضاء الإلكتروني واستخدام تقنيات الاتصالات وتدفقات البيانات.

---

[1] احمد عبد الحليم، امن الخليج الى اين؟ اوراق الشرق الاوسط، 1992، ص30

[2] تيري ديبيل، استراتيجية الشؤون الخارجية، منطق الحكم الأمريكي، ترجمة وليد شحادة، دار الكتاب العربية، بيروت 2009، ص259

[3] www.en.oxfforddictionaires/definition/cyber

[4] ادريس عطية، مكانة الامن السيبراني في منظومة الامن الوطني الجزائري، مجلة مصداقية، جامعة العربي تبسي، المجلد 1، العدد 1، 2019 ص109

الفرع الثاني: المقصود بالأمن السيبراني

الأمن السيبراني يُعرف بأنه حماية الشبكات، أنظمة المعلومات، الأجهزة المتصلة بالإنترنت، والبيانات من التهديدات غير المصرح بها أو الانتهاكات التي قد تؤثر عليها .يتطلب الأمن السيبراني اتخاذ إجراءات وقائية واتباع معايير محددة تقلل من تأثير هذه التهديدات إلى الحد الأدنى .يتمحور الهدف الرئيسي حول منع الوصول غير المشروع وحماية الموارد الرقمية . وفقًا لتعريف ريتشارد كيميرير، يتعلق الأمن السيبراني بالإجراءات والتدابير التي تهدف إلى تقليل المخاطر الناجمة عن الهجمات على البرمجيات، الأجهزة الحاسوبية، أو عناصر التحكم . ويشمل ذلك استخدام الأدوات والوسائل المناسبة لضمان مستوى عالٍ من الحماية .يشمل الأمن السيبراني تطوير الموارد البشرية والمالية اللازمة لتكنولوجيا المعلومات والاتصالات، بهدف تقليل الأضرار والخسائر المحتملة وتحقيق الانتعاش في أسرع وقت ممكن عند وقوع أي حادث أمني .يعتمد تأثير الأضرار ومدى استعادتها على مدى حماية الأنشطة، الوظائف، القدرات، والمعلومات الموجودة ضمن الأنظمة من العناصر الضارة وسوء الاستخدام أو الاستغلال. يشمل الأمن السيبراني الأنظمة العسكرية والاقتصادية والاجتماعية والسياسية والإنسانية التي تهدف إلى حماية الأمن من التهديدات السيبرانية. يتضمن ذلك الأمن المتكامل الذي يعمل على الحفاظ على مختلف جوانب النظام السيبراني .ويمكن تناول الأمن السيبراني من عدة أبعاد رئيسية [1]:

البعد العسكري: يركز هذا البعد على ضمان قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، بما يتيح تبادل المعلومات والأوامر .ومع أن الشبكات العسكرية توفر أساسًا للتواصل الفعّال ونشر التقنيات مثل الطائرات بدون طيار والصواريخ الدقيقة، إلا أنها تشكل أيضًا نقطة ضعف إذا لم تكن مؤمنة بشكل كافٍ .أي هجوم على قواعد البيانات العسكرية أو التحكم في الأنظمة التقنية قد يؤدي إلى تعطيل الاتصالات بين القيادات والوحدات الميدانية، فضلًا عن افتقاد السيطرة على بعض المعدات العسكرية .

[1] لامية طالة، التهديدات والجرائم السيبرانية، تاثيرها على الامن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، المجلد 4، ال عدد2، 2020، ص61

البعد الاقتصادي :مع اعتماد الصناعات على أجهزة الكمبيوتر وتوسع الإنترنت كقاعدة للتجارة والمعاملات المالية، أصبح الأمن السيبراني الاقتصادي ضرورة بالغة .تتطلب الحماية في هذا المجال الحفاظ على أمان الشبكات المستخدمة خصوصًا في القطاع المالي، حيث يمكن أن يؤدي اختراقها إلى خسائر اقتصادية كبيرة .

البعد الاجتماعي: يُعد الإنترنت منصة تجمع أكثر من 4 مليارات مستخدم حول العالم، منهم ما يزيد على 6.2 مليار يستخدمون مواقع التواصل الاجتماعي .هذه المواقع تُعزز التفاعل البشري وتسمح بمشاركة الأفكار والتجارب، لكنها في الوقت نفسه تفتح الباب أمام المخاطر مثل كشف أخلاقيات وسلوك الأفراد وصعوبة مراقبة المحتوى .كما تسهم هذه الفجوات الأمنية في تعريض المعلومات الشخصية لجهات غير موثوقة، مما قد يهدد الاستقرار الاجتماعي .**البعد السياسي** :يبرز هذا البعد في أهمية الأمن السيبراني للحفاظ على استقرار العلاقات السياسية بين الدول. مثلًا، أثارت التدخلات السيبرانية الروسية في الانتخابات الأمريكية جدلًا واسعًا، ما يُظهر الحاجة الملحّة للأمن السيبراني لتعزيز الاستقرار السياسي ومنع الأزمات الدبلوماسية الناتجة عن تسريب الوثائق السرية أو الممارسات التطفلية .

البعد القانوني :مع التقدم التكنولوجي السريع، أصبح من الضروري تطوير أطر قانونية واضحة تنظم الأنشطة في الفضاء السيبراني .الجرائم الإلكترونية باتت تحديًا قانونيًا كبيرًا، وبعض البلدان لا تمتلك تشريعات صارمة للتعامل مع تلك الجرائم مما يُعرضها لمخاطر إضافية .

في المحصلة، يمثل الأمن السيبراني مجموعة من التدابير والإجراءات التي تتخذها الحكومات والشركات والأفراد لحماية الأنظمة والشبكات والبيانات الإلكترونية من التهديدات السيبرانية .يشمل ذلك حماية المعلومات الحساسة وتأمين الأنظمة والأجهزة الإلكترونية ضد محاولات التطفل والتخريب والتلاعب.

المبحث الثاني

وظائف الذكاء الاصطناعي في الأمن السيبراني

في هذا المبحث سوف دور الذكاء الاصطناعي في الأمن السيبراني كمطلب اول، وفي المطلب الثاني تم الاشارة فيه الى مختلف العوائق التي تحد من تطبيقات الذكاء الاصطناعي في الأمن السيبراني.

المطلب الأول

دور الذكاء الاصطناعي في تعزيز الأمن السيبراني

ان اهم خاصية للذكاء الاصطناعي هي الأمن السيبراني وهذا وفقا لتقرير Capgemini حول تطورات الأمن السيبراني، وعليه فان اهم وظائف الذكاء الاصطناعي تتمثل في حماية البيانات والتوقعات المستقبلية.

الفرع الأول: حماية البيانات

يمكن التعامل مع كميات كبيرة من البيانات بفضل تطور التقنيات الحديثة .يجري يوميًا نقل كميات هائلة من البيانات بين العملاء والمنشآت والأجهزة والشبكات المرتبطة بشبكاتنا وخوادمنا النشطة. مع هذا الحجم الهائل من البيانات، يصبح من الصعب على مختصي الأمن السيبراني رصد كل التفاصيل واكتشاف المخاطر المحتملة بشكل دقيق. هنا يبرز دور الذكاء الاصطناعي كخيار مثالي لاكتشاف التهديدات التي تتسلل خلال العمليات اليومية وفحص البيانات بكفاءة عالية .يمكن للذكاء الاصطناعي مراقبة حركة المرور على الشبكات، تحليل نشاط الخوادم بدقة، وتحديد المخاطر المحتملة لتحسين الأمن الشامل .تتعرض العديد من المؤسسات لخسائر مالية سنوية نتيجة خروقات البيانات[1]، وهو ما يجعل التصدي لهذه التهديدات أمرًا لا يمكن تجاهله أو تجنبه بالكامل .وفق الدراسات الحديثة، تمكنت المؤسسات التي تعتمد تقنيات الذكاء الاصطناعي من تخفيض تكاليف الأمن السيبراني بنسبة تصل إلى

[1] www.thkaa.sa

88٪، حيث تدفع المنشآت غير المستفيدة من هذه التقنيات حوالي 13 مليون دولار سنويًا مقارنة بـ 9.2مليون دولار للمؤسسات التي تعتمد عليها .من بين أدوات الذكاء الاصطناعي الفعالة يأتي ChatGPT، الذي يعتبر أداة ذات قيمة في مجال الأمن السيبراني على الرغم من وجود مخاوف مشروعة بشأن استخدامه. يقدم ChatGPT العديد من الفوائد مثل تعزيز الإنتاجية، دعم المهندسين، تدريب الموظفين والإسهام في تطبيق القوانين .ومع ذلك، فإن الأداة بحاجة إلى معالجة بعض الانتقادات التي تشمل التحيز العنصري، نقص المعايير للتحقق من البيانات، واستغلالها في جرائم الإنترنت وقضايا الخصوصية .على الرغم من هذه الجوانب السلبية، فإن تطوير ChatGPT يمكن أن يعزز قدرة الصناعة على اكتشاف الهجمات الإلكترونية والتعامل معها بشكل فوري وفعال، مما يعزز مرونة الأمن السيبراني عمومًا .الأداة تبسط الأعمال المعقدة وتسمح لموظفي الأمن بالتركيز على التفكير الاستراتيجي، كما تتيح للباحثين التعامل مع برامج ضارة بعمليات أكثر تعقيدًا كإنشاء التعليمات البرمجية وتحليل العينات الخبيثة ومقارنة العقود .علاوة على ذلك، يعمل ChatGPTعلى سد الفجوة المعرفية من خلال تدريب الموظفين ونشر الوعي حول الاحتيال والهندسة الاجتماعية ومخاطر البيانات . إضافة إلى هذه الفوائد، يمكن أن تدعم ChatGPTالفرق الأمنية وإنفاذ القانون في التحقيق وتتبع النشاط الإجرامي والتعامل مع التكتيكات المتغيرة للجرائم الإلكترونية [1].ومع ذلك، يظل التحدي الرئيسي أمام الفرق الأمنية هو غياب معايير موثوقة لتقييم سلامة أنظمة الذكاء الاصطناعي وأمانها ومرونتها .وقد شهد بالفعل استخدام ChatGPT من قبل مجرمي الإنترنت لتطوير أساليب وتكتيكات جديدة لنشر البرمجيات الضارة.

الفرع الثاني: التوقعات المستقبلية

كمية البيانات التي تمر عبر الحماية السيبرانية تجعل من الصعب التنبؤ بالتهديدات المستقبلية .ومع ذلك، فإن الذكاء الاصطناعي يتمتع بقدرة على معالجة كميات هائلة من البيانات في وقت قصير، مما يتيح الكشف المبكر عن الأنشطة الضارة .يمكن أن يسهم ذلك في تحديد التدابير الوقائية اللازمة والتهديدات المحتملة، وبالتالي تقليل الوقت الضائع على إدارة فريق العمل، ومساعدة المؤسسة على البقاء متيقظة من خلال اتخاذ خطوات استباقية لحمايتها .سرعة اكتشاف التهديدات تمثل أهمية قصوى، لا سيما أن 42%من المنظمات أبلغت عن زيادة في

[1] مزايا واهتمامات ChatGPTفي الامن السيبراني على المرقع الالكتروني www.tuxcare.com

التهديدات الحساسة للوقت .ومع بطء الإنسان في التعامل مع مثل هذه التهديدات بالطريقة المثلى، يستطيع الذكاء الاصطناعي فحص كميات هائلة من البيانات بشكل متزامن، مما يُسهل عملية الكشف عن التهديدات السيبرانية .على هذا النحو، أشارت 56%من المؤسسات إلى أنها تواجه صعوبات تتعلق بفرز وتحديد طبيعة التهديدات التي تعترض الدفاعات السيبرانية، فيما ذكر 23%أنهم غير قادرين على التحقق من التهديدات المحددة بشكل فعّال[1].

المطلب الثاني

العوائق التي تواجه الذكاء الاصطناعي في ضمان الأمن السيبراني

والتي تتمثل اساسا في عوائق بشرية واخرى مادية قد تجعل من دور الذكاء الاصطناعي في الأمن السيبراني محدد مما يستدعي مواجهتها والتصدي لها من خلال دراسة هذه التحديات ومحاولة ايجاد حلول لها.

الفرع الأول: التحديات البشرية والمادية

يعد دمج الذكاء الاصطناعي في الأمن السيبراني خطوة مليئة بالتحديات، خصوصًا مع الحواجز التي قد تعيق استخدام واعتماد هذه التقنية من قبل مجرمي الإنترنت بشكل متزايد . مع الأخذ بعين الاعتبار أن الذكاء الاصطناعي يعد صناعة ناشئة، يتوجب على المؤسسات استثمار مبالغ كبيرة من الأموال والوقت لتطوير أنظمة ذكاء اصطناعي ذات كفاءة عالية .يتطلب هذا الأمر تخصيص موارد هائلة في مجال الحوسبة وتوفير مراكز بيانات كبيرة، إلى جانب القدرة على صيانة هذه الأنظمة بشكل فعال .أصبح اعتماد الذكاء الاصطناعي ضمن أنظمة الأمن السيبراني أمرًا ضروريًا للمنظمات بهدف تجاوز العقبات الرئيسية التي تقف عائقًا أمام اعتماده واستمرارية نموه، مثل تحديات اكتساب الكفاءات البشرية المتخصصة، تعقيد تحليل البيانات، واستخدام الأدوات المناسبة المبنية على الذكاء الاصطناعي .وفقًا لشركة IBM، يُعد نقص الكفاءات أحد أبرز التحديات التي تعيق تبني الذكاء الاصطناعي وتطويره؛ إذ تواجه قرابة 37% من المؤسسات صعوبات في العثور على أفراد يمتلكون الخبرة والمعرفة اللازمة في هذا

[1] محمد مختار، الامن السيبراني مفاهيم المستقبل، مجلة اتجاهات الاحداث، العدد 2، 2015، ص6

المجال .يؤدي ذلك إلى نقص اصطناعي في الموارد البشرية، مما يزيد العبء على المؤسسات التي بدأت فعليًا في تطوير حلول تعتمد على الذكاء الاصطناعي[1].

تعقيد البيانات وافتقار المنظمات إلى الأدوات المناسبة يُعدّان من أبرز التحديات التي تواجهها المؤسسات في المراحل المتقدمة لاعتماد وتطوير الذكاء الاصطناعي .هذا بدوره يفتح المجال لاستخدام الذكاء الاصطناعي من قبل مجرمي الإنترنت، حيث يصبح سلاحًا ذا حدين : أداة وقائية قوية من جهة، وآلية هجومية فعالة من جهة أخرى .في الجوانب الأمنية، يمكن للذكاء الاصطناعي تحسين دقة وفعالية الهجمات السيبرانية، مما يعزز من خطورتها. على سبيل المثال، تُستخدم تقنيات الذكاء الاصطناعي في تحليل الأنظمة المعقدة واكتشاف الثغرات الموجودة فيها، وهي تقنية تُعرف باسم "التعتيم ."الغرض الأساسي من هذه التقنية هو تحديد نقاط الضعف التي يمكن استغلالها .استخدام الذكاء الاصطناعي في مثل هذه التقنيات يجعل الهجمات أكثر دقة وفعالية، مما يؤدي إلى تهديدات سيبرانية أكثر تدميرًا كالهجمات المرتبطة بالتصيد الاحتيالي .

أما بالنسبة للمنظمات التي تعتمد على الذكاء الاصطناعي في أنظمتها للأمن السيبراني، فإنها تحقق قدرة أكبر على اكتشاف التهديدات ومكافحتها بفضل قدرات الذكاء الاصطناعي على التعامل مع البيانات الضخمة وتحليل الأنماط والسلوكيات غير الطبيعية التي قد تشير إلى احتمال وقوع هجمات. ومع ذلك، فإن مجرمي الإنترنت يمتلكون ميزة غير محدودة بحدود استخدام التكنولوجيا، مما يزيد من قدرتهم على الاستغلال[2] .

في المجمل، دور الذكاء الاصطناعي في الأمن السيبراني يتمثل في الاستفادة من خوارزميات التعلم الآلي لتحسين كفاءة الأنظمة والشبكات في التصدي للتهديدات .من خلال هذه التقنيات، يمكن للمنظمات أن تعزز من قدرتها على حماية البيانات والمعلومات الحساسة ومواجهة أي مخاطر سيبرانية ناشئة.

[1] الذكاء الاصطناعي والامن السيبراني، دراسة فيما يخبئه المستقبل، مركز البيان للدراسات والتخطيط، على الرابط الالكتروني www.bayancentre.org

[2] انظر الرابط الالكتروني www.bayancentre.org

الفرع الثاني: سلبيات الذكاء الاصطناعي على الأمن السيبراني

لا شك أن الذكاء الاصطناعي يُعد أداة قوية لتعزيز الكفاءة وتحسين فعالية برامج الأمن السيبراني .ومع ذلك، فإن الإفراط في الاعتماد عليه قد يتحول سريعًا إلى نقطة ضعف . يجب على فرق الأمن السيبراني التحكم في رغبتها في السماح للذكاء الاصطناعي بالسيطرة الكاملة، مع الحرص على وضع ضوابط وتوازنات مناسبة، وإشراك العنصر البشري في اتخاذ القرارات الحاسمة .كما ينبغي توفير رؤية واضحة حول كيفية عمل أنظمة الذكاء الاصطناعي وآلية إنتاجها للقرارات .على الرغم من المزايا العديدة التي أتاحتها تقنيات الذكاء الاصطناعي في مختلف المجالات، إلا أنه لا يخلو من عيوب ومخاطر، منها[1]:

ارتفاع التكاليف: من أبرز العقبات التي تواجه اعتماد الذكاء الاصطناعي هو ارتفاع التكاليف اللازمة لإنشاء الأجهزة والأنظمة المعتمدة عليه .تتطلب هذه العملية بناء خوارزميات معقدة، واستخدام تقنيات حديثة، مما يؤدي إلى زيادة سريعة في التكاليف .يمثّل ذلك تحديًا كبيرًا للشركات الصغيرة ذات الموارد المحدودة، وحتى للشركات الكبرى التي تتكبد نفقات إضافية بسبب ضرورة تحديث الأجهزة والبرمجيات وصيانة الخوارزميات بشكل دوري.

زيادة البطالة: قد يتسبب انتشار الذكاء الاصطناعي في ارتفاع معدلات البطالة، حيث تعتمد المؤسسات بشكل متزايد على الأجهزة القادرة على تنفيذ المهام المعقدة باستمرارية، لتقوم بدور البديل عن الموظفين. هذا الاعتماد يهدد الوظائف التقليدية، مما يؤدي إلى تفاقم مشكلة البطالة في العديد من المجتمعات.

ضعف الإبداع على الرغم من القدرات الهائلة لأنظمة الذكاء الاصطناعي في التحليل والتنبؤ، إلا أنها تعاني من غياب الحس الإبداعي الذي يتميز به البشر .الأجهزة تعمل وفق برمجيات محددة مسبقًا ولا تستطيع الخروج عن نطاق هذه التعليمات أو ابتكار أفكار جديدة كما يفعل الإنسان.

اعتماد البيانات المكررة تمكّن الخوارزميات الأجهزة من تعلم أنماط جديدة عبر تحليل البيانات .ومع ذلك، إذا تعرضت الأجهزة لمجموعات بيانات مكررة، فقد تتوقف عن تحسين

[1] www.bakkah.com

أدائها أو تقدم نتائج غير دقيقة. للوصول إلى مستوى أعلى من الأداء، يضطر المطورون إلى تعديل الخوارزميات باستمرار لتلائم الظروف المتغيرة.

نقص التفكير الأخلاقي على الرغم من قدرة الذكاء الاصطناعي على تنفيذ المهام المتكررة بفعالية، إلا أنه يفتقر للقدرة على التفكير الأخلاقي أو إصدار أحكام مستنيرة مثل الإنسان . عندما تواجه الأنظمة حالة غير مبرمجة مسبقًا، قد تتعطل أو تقدم نتائج غير منطقية، مما قد يؤدي إلى عواقب غير متوقعة.

مخاطر الأمان والخصوصية إحدى أبرز القضايا المثارة حول استخدام الذكاء الاصطناعي هي المخاوف المتعلقة بالأمان والخصوصية. تعتمد هذه الأنظمة بشكل كبير على البيانات، مما يجعلها عرضة للوصول غير المصرح به أو إساءة الاستخدام، سواء عبر تسريب البيانات الحساسة أو التلاعب بالرأي العام باستخدام معلومات كاذبة.

زيادة الكسل بين الأفراد مع توسّع الأتمتة وتوافر المساعدين الرقميين، يميل عدد متزايد من الأشخاص إلى الاعتماد على الذكاء الاصطناعي لأداء المهام البسيطة مثل الحسابات أو حفظ المعلومات .هذا الاعتماد المفرط يهدد بزيادة الكسل وفقدان المهارات الأساسية التي كانت تعد جزءًا من النشاط البشري اليومي.

عدم القدرة على فهم المشاعر تعتمد أنظمة الذكاء الاصطناعي على نهج عقلاني وعملي للغاية دون أخذ المشاعر البشرية بعين الاعتبار. هذا يجعلها أقل كفاءة عند التعامل مع المجالات التي تتطلب الإقناع العاطفي أو فهم العلاقات الإنسانية .الموازنة بين استخدام الذكاء الاصطناعي والاعتماد على الخبرات البشرية تعتبر ضرورية لتحقيق الاستفادة القصوى وتجنب المخاطر المحتملة الناتجة عن هذه التقنية المتطورة.

الخاتمة

أصبح الفضاء الإلكتروني اليوم بيئة معلوماتية جديدة تستخدمها الأفراد والدول على نطاق واسع .تعتمد الدول بشكل كبير على شبكة الإنترنت لتأسيس قواعد بيانات متنوعة وتطوير خدمات وطنية مختلفة. ومع ذلك، فإن الفضاء الإلكتروني يظل مفتوحًا لجميع الدول دون استثناء، ما أدى إلى ظهور تهديدات متنامية، منها الهجمات السيبرانية، والجرائم الإلكترونية، والإرهاب السيبراني .تتنوع أشكال هذه التهديدات وتأخذ أبعادًا مختلفة، بما في ذلك الصراعات السيبرانية بين الدول، مما يؤثر بشكل كبير على التبادلات الدولية واستقرار الأمن. ومع ظهور تقنيات الذكاء الاصطناعي، التي تُعتبر من أبرز التطورات الحالية، سارعت دول عديدة إلى تبني هذه التقنيات لتعزيز أمنها السيبراني .لكن، وبالرغم من فوائدها الكبيرة، فإن هذه التكنولوجيا تتطلب وضع ضوابط وقوانين واضحة تنظم استخدامها بما يضمن التوازن بين الأمن والخصوصية .لذا، يجب على الدول تطوير الأطر القانونية اللازمة لاستخدام الذكاء الاصطناعي سواء على المستوى الإقليمي أو الدولي. وفي النهاية، يمكن القول إن الذكاء الاصطناعي يمثل تقدمًا ملموسًا في مجال التكنولوجيا مع العديد من الفوائد والتطبيقات المحتملة . ومع ذلك، ينبغي استخدامه بمسؤولية عالية مع التركيز على حماية الخصوصية والحد من الآثار السلبية التي قد تنجم عن إساءة استغلال هذه التقنيات. وبالإضافة إلى ذلك، يجب العمل على إيجاد آليات فعالة تضمن تحقيق الأمن السيبراني وخلق فضاء رقمي أكثر أمانًا للجميع.

قائمة المراجع

المقالات:

1- محمد مختار، الأمن السيبراني، مفاهيم المستقبل، مقال منضور في مجلة اتجاهات الاحداث، العدد 2 2015

2- لامية طالة، التهديدات والجرائم السيبرانية، تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مقال منشور في مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، المجلد 4، العدد2 2020

3- عادل عبد الصادق، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، مكتبة الاسكندرية، 2016

4- تيري ديبيل، استراتيجية الشؤون الخارجية، منطق الحكم الامريكي، ترجمة وليد شحادة، دار الكتاب العربية، بيروت 2019

المواقع الالكترونية

www.mandumah.com

www.ajsp.net

www.amf.org.ae

www.en.oxforddictionaires.com

www.thakaa.sa

www.tuxcare.com

www.bayancentre.org

www.bakkah.com

Chapter 05

Digital sovereignty in Algerian legislation

Mahcer Lotfi

Faculty of Law and Political Sciences, University of Tlemcen

lotfi.mahcer@univ-tlemcen.dz

Abstract:

The wave of change in the field of providing and communicating information has pushed all governments to shift towards electronic administration. The profound qualitative and quantitative transformations that the digital age is experiencing with all its horizons, and that the digital revolution "has begun to affect all aspects of life, especially the impact of the digital revolution on the sovereignty of states, and that the digital threat that has transcended the traditional concept of sovereignty has produced a new face of colonialism."

The continuity of countries today depends on their ability to protect their digital sovereignty from cyber security threats," and a cyber-defense strategy to establish a defense system that includes many technical and legal aspects.

The importance of digital transformation in Algeria and measuring its impact on human problems on the one hand and on activating development and enhancing its sustainability on the other hand. In this regard, we seek to compare the limits of the contribution of digital transformation in serving the public interest by reviewing the reasons for adopting digitization through the electronic administration mechanism.

Keywords: Digital sovereignty, Digital Transformation, Public Service, E-Government.

Introduction

The wave of change in the field of information delivery and communication has pushed all governments towards electronic management. Therefore, we find several developments driving the adoption of electronic management, including those related to government officials who are developing new methods to improve government work. This is to increase the efficiency of service delivery and sometimes in response to pressures from citizens, the business sector, or other parties related to government work.

And we find that in every country, there are real motivations that call for the transition to electronic governance. Considering other motivations. Depending on the economic and political situation of this country, the most important of these motivations are as follows.[1]

-The acceleration of scientific progress and technological development: With the spread of electronic culture and the advancement of communications, which have led to the interconnectedness of human societies through globalization trends towards a global village.

-The shift from traditional management styles to the new management thinking based on communication and information technology, understanding it from an administrative perspective that focuses on defining the organization's strategic goals and exploring

[1] Yves Guichet, Constitutional Law ; Ellipses, Paris, 1996.

The appropriate technologies capable of helping it achieve its goals.

-There are many reasons that have prompted many countries and organizations to hasten the implementation of e-governance in their management, including:
-The internet as a global network has made the world a small and homogeneous village.

- Globalization, which has been considered a driving force for many countries to improve their services and rise to global standards.

To obtain the global quality certification for its service in terms of citizen satisfaction on the other hand.

-The trend towards privatization has increased, as this trend has pushed the new world of countries towards privatizing their services.

-In addition to administrative procedures and complex operations and their impact on increasing business costs.

- The difficulty of providing circulating data to employees in the organization

-The necessity of achieving continuous communication among employees as the scope of work expands

It becomes clear to us that the primary reason for accepting the idea of electronic management, which is an alternative to

traditional management, is the necessity to respond to the requirements of both internal and external environments. The internal environment generates a lot of information and employee and worker records, which are difficult to control. Externally, due to numerous transactions with partners, suppliers, and others, there is an excess of information about them and a lack of control. Electronic management relies on computers in its various transactions, which contributes to controlling these aspects.

Based on the above, we pose the following question: To what extent does the internet affect state sovereignty?

1- Concept of Digital Sovereignty

1-1 The Concept of Classical Sovereignty

It seems there is no text to translate. Please provide the text you'd like me to translate. Sovereignty is the fundamental legal characteristic of the state. While the state shares with other entities the acquisition of legal personality, it alone possesses sovereignty. Meaning that it has the supreme authority that no other power or body can surpass, and this makes it superior to all others, considering itself as the supreme commanding authority. Therefore, state sovereignty simply means that it is the source of other authorities. Sovereignty is original and inherent to the state, distinguishing it from other political entities. Sovereignty is a single, indivisible unit, regardless of the number of public authorities, as these authorities do not share sovereignty but rather share jurisdiction.[1]

Sovereignty is original and inherent to the state, distinguishing it from other political groups. Sovereignty is a single unit that cannot be divided, no matter how many public authorities there are, because these authorities do not share sovereignty but rather share jurisdiction. The term "sovereignty" is derived from the Latin word "supraners," meaning "the highest." This concept was developed by the jurist Jean Bodin in his six books on the Republic in 1576.The

[1] Dominique Rousseau "the constitution or politics differently" Débat magazine, no. 64, March 1991, p. 183

word "sovereignty" is derived from the Latin word "supraners," meaning "the highest."

This concept was developed by the jurist Jean Bodin in his six books on the Republic in 1576.

The term "sovereignty" is derived from the Latin word "supraners," meaning "the highest." This concept was developed by the jurist Jean Bodin in his six books on the republic in 1576. Thus, the sovereign nature of state authority means its independence and lack of subordination to any other authority, enabling it to impose its binding will on individuals and entities without dispute. It also allows the state to exclusively organize the fundamental affairs of society, whether related to private or public relations, through the institutions created for this purpose.

So, the meaning of the sovereign nature of state authority is its independence and lack of subordination to any other authority, enabling it to impose its binding will on individuals and entities without dispute. It also allows it to take sole responsibility for organizing the fundamental affairs of society, whether related to private or public relations, through the institutions established for this purpose.[1]

So, the concept of the sovereign authority of the state refers to its independence and its lack of subordination to any other authority, enabling it to impose its binding will on individuals and entities

[1] Favoreu Louis "Constitutional Law: Law of the Constitution and Constitution of the Law," French Review of Constitutional Law, no. 1, 1990, p. 79

without dispute. It also allows the state to take sole responsibility for organizing the fundamental matters of society, whether they pertain to private or public relations, through the institutions established for this purpose. Consequently, sovereignty entails a set of consequences.

Consequently, sovereignty entails a set of outcomes, which are:

- The state is the only institution that holds an inherent authority not derived from any other authority that precedes or follows it.

- This sovereignty, represented by that authority, is a supreme sovereignty that is not surpassed by any other authority, neither within the state nor outside it.

- The state, as the owner of that sovereignty, is the one that determines and establishes its legal organization throughout its national territory, which includes moral principles and material rules, without being influenced by factors other than the requirements of national sovereignty.

- The state is the starting point and source of all authorities that arise from that political and legal organization.

- The state uniquely determines its competencies and the scope of its influence.

- The state, as a result of the above, monopolizes the manifestations of sovereignty that it exclusively holds, such as the

public force including the army and police, the minting of currency, and so on.

The state, as a result of the above, monopolizes the manifestations of sovereignty, such as the public force, the army, the police, the issuance of currency, and so on. Based on these results, it can be said that the state's enjoyment of sovereignty makes its authority original, supreme, unified, and indivisible.

Based on those results, it can be said that the state's enjoyment of sovereignty makes its authority an original, supreme, and indivisible one.

1- Forms and manifestations of sovereignty: Sovereignty is divided into legal and political forms, and it is practically manifested through various fields or aspects, both internally and externally, as well as regionally and personally.

A- Forms of sovereignty: The authority of the state is characterized by being legal and political sovereignty.

Legal sovereignty refers to the state's authority to issue legislation through its representatives, enforce it, and punish anyone who violates it. As for political sovereignty, it refers to the people in its political sense, who are credited with choosing the political officials who have the right to exercise legal sovereignty. Thus, it is the authority of the people to choose those who will be responsible for managing public affairs in the state.

B- Aspects of Sovereignty: Sovereignty has several fields or aspects, the most important of which are:

- Internal sovereignty and external sovereignty: Internal sovereignty refers to the supreme authority of the state exercised over individuals and entities within its territory. Accordingly, it can issue orders, legal rules, and general directives that have binding force and must be obeyed by individuals. It is also capable of performing all actions of particular importance to governance and politics, such as drafting the constitution, determining the system of government, imposing taxes, maintaining order, managing public facilities, minting currency, directly supervising the judiciary, monopolizing internal and external defense tasks, and undertaking the mission of maintaining security and public order... All these actions express sovereignty in its positive sense.

The state is subject only to its independent and singular will, due to the supremacy and elevation of its authority and the absence of any higher or parallel authority.

As for external sovereignty, it is the sovereignty exercised by the state in relation to other states, meaning the set of rights and powers it exercises in the international community, in its foreign relations, such as the right to conclude treaties and international agreements, the right to diplomatic representation and joining international organizations, the right to declare or end war, as well as the right to follow up on and protect the affairs of its nationals abroad. Thus, sovereignty in this sense is of a negative nature because

it does not impose specific actions on the state except for the restrictions imposed by international law and the treaties and agreements it has freely entered into.

However, a state's external sovereignty can be complete or incomplete. It is complete if the state is fully independent and not subject to another state, which is referred to as fully sovereign states. External sovereignty is considered incomplete if the state retains some aspects of its external sovereignty while losing others, due to its subordination to another state, such as protectorates and territories under mandate or trusteeship, which are referred to as partially sovereign states.

- Territorial sovereignty and personal sovereignty: Territorial sovereignty defines the state's exercise of its sovereignty within the boundaries of its territory, where it practices all aspects of sovereignty, including the authority to command and prohibit, impose penalties, and issue laws and regulations to be applied to everyone within its territory, regardless of their affiliation with its people. Therefore, territorial sovereignty is determined by the presence of individuals within its territory, whether they are citizens or foreigners, and as a result, the state has no authority over its citizens if they are outside its territory.

As for personal sovereignty, it is where the state defines the scope of its sovereignty over the individuals who make up its people and enjoy its nationality, whom it calls "citizens or subjects" and who hold its nationality. The state exercises personal sovereignty over its

citizens, whether they are within the state's territory or outside it in the territory of a foreign state. Accordingly, under this sovereignty, the state has the right to track its citizens in foreign countries, but it does not exercise this sovereignty over foreigners residing within its territory because they are not its citizens.

Digital sovereignty is considered one of the modern concepts in management science, resulting from many developments that contemporary societies have experienced since the transition to electronic work to improve public service and reduce material expenses by introducing modern technologies and means, including information systems. The system is defined in two ways: one is a concise definition, such as the following: a system is a set of elements that integrate with each other to achieve a specific goal. The expanded definition describes it as a set of interrelated components that work together to achieve a common goal. Inputs are accepted for systematic processes to produce outputs.

The definition of information is data that has the quality of credibility and is presented for a specific purpose or goal. Information is developed and elevated to the status of knowledge when used for comparison and evaluation of previous and specific results and for the purpose of communication. As for the information system, it is defined as a systematic way to store data and information about each user with the aim of assisting in planning, decision-making, and providing complete reports on every activity that serves the organization's goals.

Lucas defined it as a set of procedures, software, machines, installations, and methodologies necessary for data processing and retrieval, which are essential for managing the organization's activities.

As for the Human Resource Information System, it is defined as a system designed to perform a specific function within the organization's operations, specifically to manage human resources and primarily to provide the information needed by managers to make decisions related to the effectiveness and efficiency of human resource utilization, enhancing performance levels to fulfill their role in achieving organizational goals.

1-2 The concept of digital sovereignty

The concept of digital sovereignty and the changes occurring in the global system, along with new transformations in concepts and roles, have led to the emergence of new actors who now share the sovereignty of states. This is achieved through the creation of what is called soft power, which works to change concepts towards reality by overwhelming the system with a massive amount of information, making the ability to absorb it minimal. Therefore, one of the most significant challenges we face today in decision-making and achieving developmental goals is the ability to discern the truthfulness of information.

Among the topics related to the concept of "digital sovereignty" and "requirements for societal security and digital development," the lecture aims to "enable various national

institutions to benefit from studies conducted by several Algerian professors in the fields of cyber warfare and awareness plans, and to address various terms and meanings, as stated by the organizers of the scientific event."

It will work on this sensitive issue, which is experiencing significant developments and qualitative leaps in its aspects related to wars, influence, and espionage, with the aim of forming a scientific culture on how to use virtual domains and maintain vigilance against any attempts to breach or attack the institutions and resources of the nation.

This topic: "Based on regional and global contexts witnessing widespread dissemination of modern technologies, virtual spaces, and artificial intelligence, and their use to provoke crises and as a weapon."

And in the context of supporting the efforts of the state and various institutions to instill a cyber culture that contributes to enhancing Algerian national security.

Countries, economies, and societies have come under the threat of digital attacks. Sovereignty has taken on a digital face.

So, what does digital sovereignty mean? What are its pillars? What is its relationship with political and economic national sovereignty, and the security and stability of societies? And what is its position in the international competition for influence?

And technology has begun to be used to influence sovereignty, so the borders of virtual countries must be protected from internal concepts, especially those related to social media that need to be regulated because they represent fertile ground for promoting electronic campaigns that attempt to undermine the sovereignty of countries and manipulate and destabilize public opinion.

Digital sovereignty is "the ability of countries to operate in the electronic space and ensure that their rules are respected by various actors in the virtual world."

The virtual space and its interactions, along with modern technologies, are intensively used in wars and conflicts. The latest example was in Lebanon when the Zionist entity detonated communication devices in the hands of their owners, resulting in the deaths of many of them, in addition to exploiting the virtual space in psychological warfare.

The threat to sovereignty no longer comes only from massive armies and deadly weapons. It can also come from digital devices and programs that only need to manipulate symbols, numbers, and secret channels.

The concept of digital sovereignty is "linked to the sensitivity of data and electronic information and the importance of preserving them," and that "many countries face significant challenges in securing their cyberspace amid digital transformations."

Current threats "are not limited to military wars, but have extended to digital and software technologies that require adopting new strategies and approaches."

Cyber threats are considered a new face of colonialism and their impact on the sovereignty of nations, calling for the adoption of defense strategies based on developing infrastructure and investing in local human resources.

Algeria fully recognizes the importance of digital sovereignty and strives to enhance it through the national digital transformation strategy outlined by the President of the Republic, Mr. Abdelmadjid Tebboune, in order to build an inclusive digital economy, improve public services, and promote digital integration within the framework of protecting and securing personal data.

2- The Status of Digital Sovereignty in Algerian Legislation

He clarified in this regard that the Algerian legislator "established state control over its digital space as a confirmation of its sovereignty and an enhancement of the guarantee of the privacy and sanctity of its citizens and anyone present on its territory," referring to Law 07-18 related to the protection of natural persons in the field of processing personal data, which is considered "a constitutional mechanism for establishing the legal framework for the data processing system in our country, and addressing the repercussions of the rapid development of information and

communication technologies on private life, personal freedom, honor, and reputation."

And also Law No. 12-12 dated 14 Sha'ban 1430, corresponding to August 5, 2009, which includes specific rules for preventing and combating crimes related to information and communication technologies.

In this regard, he emphasized that the President of the Republic has given "special attention to protecting natural persons in the field of personal data processing" through "mechanisms for promoting and developing human rights and adapting care methods to technological advancements."

He mentioned that Algeria has worked on "keeping pace with technological advancements in media and communication by amending and enacting legislative texts that contribute to strengthening digital sovereignty, including the Electronic Communications Law, the Personal Data Protection Law, and the Cybercrime Law."

1-1 Law and Digital Sovereignty

Algerian legislation has addressed cybercrimes by issuing general and specific laws. The Algerian Constitution of 2016 also guaranteed the protection of fundamental rights and individual freedoms. These constitutional principles have been enshrined in practice through legislative texts included in the Penal Code and the Code of Criminal Procedure.

Criminal procedures that prohibit any violation of these rights.

The Algerian legislator addressed the criminalization of acts affecting computer systems, amending the Penal Code by Law No. 04-10 dated November 10, 2004, which modifies and supplements Ordinance No. 66-106 containing the Penal Code, under the title: "affecting automated data processing systems."

This section includes eight articles from Article 394 bis to Article 394 bis 7.

In this law, the local jurisdiction of the Public Prosecutor in the field of cybercrimes has been extended, according to Article 37, Paragraph 2 of the Code of Criminal Procedure (Order 15-02, 2015). Local jurisdiction extends if it concerns drug offenses, organized crime crossing national borders, crimes affecting automated data processing systems, money laundering, terrorism, crimes related to foreign exchange legislation, corruption, and smuggling (Ohaibia, 2018, p. 358).

The law also stipulates searches in Article 45, Paragraph 2 of the same amended law. Additionally, Article 65 bis 3, Paragraph 5 states that in cases of crimes affecting automated data processing systems, the competent Public Prosecutor can make technical arrangements without the subject's consent to capture, intercept, broadcast, and record speech made in private or confidential places, whether public or private.

Algeria sought to address the legal vacuum by strengthening its legislative system, especially since 2009, when Law No. 09-04 concerning the special rules for the prevention and combating of crimes related to information and communication technology was issued on August 5, 2009. (Law No. 09-04, 2009).

This law also contained 19 articles distributed over 6 chapters derived from international agreements.

International (Budapest Convention, 2001), and this law is in line with national legislation, especially those related to combating corruption, money laundering, and terrorism financing, as this law stipulates the establishment of The National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technology.

1-A Within the framework of Law 09-04

Digital transformation is considered one of the most important features of the current era, on one hand, and on the other hand, it makes it susceptible to risks such as hacking, exploitation, and espionage. Therefore, it has become urgent to study the aspects of criminal protection for this data within the framework of digital transformation and the spread of artificial intelligence technologies to ensure the security and safety of this data. Additionally, determining which data should be protected under criminal law is extremely difficult.

Because this data cannot be restricted due to the diversity and multiplicity of data types, the greatest difficulty lies in determining what can be published and generalized, and what is the opposite, and when it becomes criminal to do so the inability to establish a clear standard for distinguishing between authorized and protected information makes the picture unclear for all citizens.

According to the details and texts of Law 04-09[1], the first chapter included general provisions and clarified the purpose of the law is to establish specific rules to prevent and combat crimes related to information and communication technologies. This means forming the basis for the automated processing of data as stipulated in the Penal Code and any other crime that incites or facilitates its use in an information system, electronic communication system, or any other system, using the data mechanism being implemented. For a specific program, information programs are defined as any process of presenting facts, information, or concepts in a form ready for processing in an information system. The legislator also addressed the concept of electronic communications, which includes any transmission or reception of signals, writings, images, or sounds by electronic means.

or voices or different information by any electronic means. The legislator has limited the scope of this law in consideration of the

[1] Law No. 09-04 dated 14 Sha'ban 1430, corresponding to August 5, 2000. It includes specific rules for the prevention and combating of crimes related to information and communication technologies. Official Gazette No. 27, dated 16/08/2009.

laws that ensure the confidentiality of correspondence. And the freedom of societies in terms of the requirements of public order and the necessities of investigations or inquiries as outlined in the provisions of the Criminal Procedure Code[1]. The second chapter of the law addresses the subject of monitoring electronic communications and the cases in which electronic monitoring may be used to prevent acts considered terrorist, sabotage, or crimes affecting state security. In the event of information being available about a potential attack on an information system in a manner similar to that which threatens public order, national defense, or state institutions.

the national economy, within the framework of the law and with written permission from the competent judicial authority. Finally, the legislator clarified in Chapter Five the name of the authority and its competencies, as it is a national body for preventing and combating crimes related to information and communication technologies. It specifically undertakes the activation and coordination of operations to prevent and combat crimes linked to information and communication technology, and assist the judicial authorities.

[1] Code of Criminal Procedure. Order No. 155- 66 dated 18 Safar 1386 corresponding to 2, amended and supplemented by Law No. 13-23 dated August 5, 2023. Official Gazette No. 52.

Where the judicial police services are responsible for investigating crimes related to information and communication technologies[1].

2-2 Achieving digital sovereignty

Algeria has made tremendous efforts to reach the readiness of the National Digital Transformation Strategy project, which generally aims to change the digital management style and preserve the information and data of Algerians, especially in the field of investment in the financial and banking sector to realize the infrastructure axis. This was crowned with the signing, last April, of the deal related to the establishment of the Algerian National Center for Digital Services between the High Commission for Digitalization and the "Huawei Consortium" in the capital and Blida.

The project aims to achieve digital sovereignty and work on localizing national information by relying on a national information system that includes the national interoperability platform, which will connect sectoral information systems, as well as the national database and the national interactive portal for digital services that includes 40 digital public services for the benefit of citizens and institutions.

The government is currently making steady and serious strides towards digitizing all sectors, with a focus on the financial and banking sector, in line with the commitment of President

[1] According to the provisions of articles 12, 12, 15, 02, 02 of law 04-09. The previous source.

Abdelmadjid Tebboune, which states, "Achieving digital transformation to improve communication and generalize the use of information technology, especially in public facility administrations, and improving the governance of the economic sector, in line with global technological developments supported by digital transformation and artificial intelligence technology, such as the reliance on blockchain technology."[1]

Algeria is considered one of the Arab countries that work on preserving its digital sovereignty, at a time when there are individual actions and programs for each country, awaiting a unified stance in the field of communications and data security protection. This will emerge from the meeting in Saudi Arabia, where there will be a unified vision for protection and communications, and later a program to empower Gaza, Sudan, and Arab countries still in a state of war, including those that have lost their right to communications, internet, and high-speed data. At the same time, the Arab League is betting on Algeria's proposals in the field of infrastructure to achieve comprehensive and purposeful connectivity in the Arab region.

Algeria possesses several factors that make it competitive for the highest regional and international ranks. The political will from the President of the Republic, who has made the dissemination of modern communication technologies and the digitization of

[1] Al-Fatis, Muhammad bin Saeed, National Sovereignty in the Era of Virtual Geography, research published at the following link: /http://www.google.com/amp/s/.annabaa.org/arabic/informatics

government services one of the key pillars of his ambitious program to revive Algeria's economy, has been a significant contributor.

"In Algeria, we find no meaning in technology if it is not available to everyone regardless of social status or geographical location. What the country has achieved in terms of connecting to the fiber optic network and in terms of generalizing access for families, individuals, and institutions to fixed or mobile internet is evidence of this direction we believe in," he stated.
The first phase will also see the commissioning of the first national data center with all its components, including the infrastructure, interoperability platform, national public service database, interactive public service portal, and national cloud. During this period, 14 fully digital public services will be put into operation.

The second phase is expected to be enhanced by the commissioning of the second national data center with all its components and infrastructure, including the interoperability platform, the national public service database, the interactive public service portal, and the national cloud. This will occur three months after the first national data center becomes operational, launching 26 fully digital public services.

The implementation of these steps involves the creation of an infrastructure consisting of two national data centers that meet the approved standards, with the aim of hosting and centralizing national data within the national territory.
This project is the first of its kind in Algeria in terms of the set

objectives, its execution, scale, and the technologies used in its components.

The goal is to improve the transfer of skills and expertise in the field of executing such high-tech projects. Especially since some stages of its implementation will enable the involvement of digitalization actors and Algerian economic partners, allowing them to benefit from expertise in this field.

Algeria has made significant strides in the digital transformation process, which is expected to eliminate bureaucracy, adopt transparency in public administration, and strengthen the foundations of electronic governance, embodying the principle of digital national sovereignty.

These rapid steps are a manifestation of President Abdelmadjid Tebboune's commitment, number 25, which states "achieving a digital transformation to improve communication and generalize the use of information and communication technologies, especially in public service administrations, and improving the governance of the economic sector." In September, the President established the High Commission for Digitalization, which reflects—according to experts—the importance the President places on the process. In his evaluation of a presentation on digital transformation in Algeria during a cabinet meeting last Tuesday, the President of the Republic praised the "clarity of the vision for Algeria's digital direction," reminding that "the main goal of this massive project is to eliminate the bureaucracy that hinders projects, adopt

transparency in managing public affairs, and accurately determine the country's needs in all sectors."

The High Commission for Digitalization, a public institution of a special nature under the supervision of the Presidency of the Republic and endowed with legal personality and financial independence, is responsible for ensuring the monitoring and implementation of the national digitalization strategy.

It is also responsible for ensuring the alignment of the digitization plans of the relevant sectors with the national digitization strategy, evaluating the achievements of each sector, and proposing necessary corrections. Additionally, it undertakes the identification of priority projects and strategic investments, the mobilization of human resources, and the financial tools specific to them. It also proposes regulatory and legal tools and/or any technical solution to ensure the effectiveness and continuous improvement of the digital transformation axes, and suggests any measures that would enhance digital sovereignty and develop the national product.

In this context, the High Commission for Digitalization launched national workshops on preparing the national digital transformation strategy, where participants confirmed that the efforts of public authorities to establish a national strategy in this field would achieve digital sovereignty, which is an urgent need in today's world. In the same context, the Council of Ministers, which met the day before yesterday, approved the project to create a "base

for storing and protecting electronic data by the Chinese company Huawei."

The strategy is also expected to be reinforced by a specific law on digitalization, which the High Commissioner for Digitalization, Mariem Ben Mouloud, confirmed her body is currently preparing the draft of this text, highlighting that it will be ready during the first quarter of the next year as the regulatory framework for the field of digitalization.

These rapid steps are a manifestation of President Abdelmadjid Tebboune's commitment, number 25, which states "achieving a digital transformation to improve communication and generalize the use of information and communication technologies, especially in public service administrations, and improving the governance of the economic sector."

In September, the President established the High Commission for Digitalization, which reflects—according to experts—the importance the President places on the process.
In his evaluation of a presentation on digital transformation in Algeria during a cabinet meeting, the President of the Republic praised the "clarity of the vision for Algeria's digital direction," reminding that "the main goal of this massive project is to eliminate the bureaucracy that hinders projects, adopt transparency in managing public affairs, and accurately identify the country's needs in all sectors."

The High Commission for Digitalization, a public institution of a special nature under the supervision of the Presidency of the Republic and endowed with legal personality and financial independence, is responsible for ensuring the follow-up and implementation of the national digitalization strategy.

It is also responsible for ensuring the alignment of the digitization plans of the relevant sectors with the national digitization strategy, evaluating the achievements of each sector, and proposing the necessary corrections. Additionally, it undertakes the identification of priority projects and strategic investments, the mobilization of human resources, and the financial tools specific to them. It also proposes regulatory and legal tools and/or any technical solution to ensure the effectiveness and continuous improvement of the digital transformation axes, and suggests any measures that would enhance digital sovereignty and develop the national product. In this context, the High Commission for Digitalization launched national workshops on preparing the national digital transformation strategy, where participants confirmed that the efforts of public authorities to establish a national strategy in this field would achieve digital sovereignty, which is an urgent need in today's world. In the same context, the project to create a "base for storing and protecting electronic data by the Chinese company Huawei" was approved.

The strategy is also expected to be reinforced by a specific law on digitization, which the Minister of the High Commission for Digitization, Mariam Ben Mouloud, confirmed her agency is currently preparing the draft of this text, highlighting that it will be

ready during the first quarter of the next year as the regulatory framework for the field of digitization.

Ben Mouloud explained that "the ultimate goal of digitization lies in establishing a new model for managing administrations, bodies, and public and economic institutions by transitioning from traditional paper-based management to digital governance, which primarily relies on the extensive use of modern digital technologies to enhance transparency principles, strengthen the relationship between the administration and the citizen, and facilitate transactions and administrative procedures by ensuring the provision of high-quality, secure, and fast public services at the lowest cost."

Establishing this would achieve a synergy in human and material resources, rationalize state expenditures, reinforce the foundations of electronic governance, and embody the principle of digital national sovereignty.

Conclusion

In this article, we have demonstrated the importance of the principle of digital sovereignty and the path it has managed to carve over the past twenty years through various experiences of countries and transnational organizations that defend this principle. We have also demonstrated that digital sovereignty is built by taking into account the political, economic, technological, and legal realities of each country. The most important thing is to be aware of it and to outline a strategy for building digital sovereignty by mastering the country's technological trajectory and ensuring the weight of regulation in this area on the economy.

Digital sovereignty has become a vital issue in the era of advanced technology and digital transformation. With the increasing reliance on digital technologies in all aspects of life, the need to enhance the digital sovereignty of nations has emerged, ensuring governments' ability to protect their vital data, secure their digital infrastructure, and control the technologies used within their borders. Digital sovereignty is a fundamental element in achieving national, economic, and social security, and it imposes new challenges that require advanced strategies to achieve it the technical aspect of digital sovereignty relies on the ability of countries to develop and use local and independent technologies in sensitive areas such as cybersecurity, big data, and artificial intelligence. This requires the development of strong and resilient infrastructure, independence in providing key digital services, and the implementation of advanced cybersecurity standards.

We conclude by saying that The widespread global dissemination of information and communication technology, in addition to Other indicators that reflect the growth of e-commerce and civilian uses based on the information infrastructure, and its role in the economy, politics, and the functioning of governments and vital facilities, which has led to the erosion of the concept of state sovereignty as it was understood before technological innovations The new, especially the internet, which has transcended geographical boundaries, as countries, by entering the digital age and the internet in particular, have lost control over their sovereign space. This has led to the rising strategic importance of the digital domain. Consequently, it has been suffering from the increase in cyberattacks, privacy violations, and other risks that threaten the security and stability of the digital domain and its relation to trust in digital transactions. This has necessitated the importance of regional and international initiatives to regulate rights and duties in the digital domain and to utilize it in the field of development.

Bibliography

Yves Guichet, Constitutional Law; Ellipses, Paris, 1996.

Favoreu Louis "Constitutional Law: Law of the Constitution and Constitution of the Law," French Review of Constitutional Law, no. 1, 1990, p. 79

Souverainté numérique, assemblée nationale France, 2009.

Solange Ghernaouti-Hélie, comment lutter contre la cybercriminalité, Revue Pour la Science, 2010 n 391 Mai.

Kempf olivier, introduction a la cyber stratégie, economia, Paris 2015.

Christian, Pauline Türk, La souveraineté numérique : le concept, les enjeux, mare et martin droit public, 2018

Pauline Türk, Définition et enjeux de la souveraineté numérique, université Côte d'Azur, www.vie-publique.fr, publiée le 14/9/2020.

Pauline Türk, « L'autodétermination informationnelle : un droit fondamental émergent ? », Dalloz IP/IT, N° 11, page : 616, Nov 2020.

Code of Criminal Procedure. Order No. 155- 66 dated 18 Safar 1386 corresponding to 2, amended and supplemented by Law No. 13-23 dated August 5, 2023. Official Gazette No. 52.

Chapter 06

The Role of Artificial Intelligence in Enhancing Digital Sovereignty and Cybersecurity:

A Case Study of Algeria

دور الذكاء الاصطناعي في تعزيز السيادة الرقمية والأمن السيبراني: دراسة حالة الجزائر،

Dr. Abdelghani Hadjab (MCA) Mohamed Boudiaf University-M'sila (Algeria)

د. عبد الغني حجاب (أستاذ محاضر أ) جامعة محمد بوضياف بالمسيلة (الجزائر)

abdelghani.hadjab@univ-msila.dz

الملخص

أصبح الذكاء الاصطناعي (AI) أداة حاسمة في تعزيز السيادة الرقمية والأمن السيبراني، خاصة للدول التي تسعى لحماية بنيتها التحتية الرقمية من التهديدات المتطورة. تبحث هذه الدراسة دور الذكاء الاصطناعي في تعزيز الأمن السيبراني والاستقلالية الرقمية في الجزائر، مع التركيز على تطبيقاته في كشف التهديدات وحماية البيانات وتأمين البنى التحتية الحرجة. من خلال منهج دراسة الحالة، تقيّم الورقة الوضع الحالي للأمن السيبراني في الجزائر، وتحدد التحديات الرئيسية، وتستكشف كيف يمكن للحلول المدعومة بالذكاء الاصطناعي أن تقلل المخاطر مع تعزيز السيادة الرقمية الوطنية. تُظهر النتائج إمكانات الذكاء الاصطناعي في تحسين آليات الدفاع الاستباقي، وأتمتة الاستجابة للحوادث، وتقليل الاعتماد على التقنيات

الأجنبية في مجال الأمن السيبراني. وتختتم الدراسة بتوصيات سياساتية لدمج الذكاء الاصطناعي في الاستراتيجية الوطنية للأمن السيبراني في الجزائر لضمان المرونة والاكتفاء التكنولوجي.

الكلمات المفتاحية: الذكاء الاصطناعي (AI)، السيادة الرقمية، الأمن السيبراني، الجزائر، كشف التهديدات.

Abstract

Artificial Intelligence (AI) is increasingly becoming a pivotal tool in strengthening digital sovereignty and cybersecurity, particularly for nations seeking to safeguard their digital infrastructure against evolving threats. This study examines the role of AI in enhancing Algeria's cybersecurity framework and digital autonomy, focusing on its applications in threat detection, data protection, and critical infrastructure security. Through a case study approach, the paper evaluates Algeria's current cybersecurity landscape, identifies key challenges, and explores how AI-driven solutions can mitigate risks while reinforcing national digital sovereignty. The findings highlight the potential of AI in improving proactive defense mechanisms, automating incident response, and reducing dependency on foreign cybersecurity technologies. The study concludes with policy recommendations for integrating AI into Algeria's national cybersecurity strategy to ensure resilience and technological self-sufficiency.

Keywords: Artificial Intelligence (AI), Digital Sovereignty, Cybersecurity, Algeria, Threat Detection.

1. Introduction

The digital realm increasingly defines the contemporary global landscape, which has become indispensable for national security, economic prosperity, and the overall well-being of societies. Within this context, the concepts of digital sovereignty and cybersecurity have emerged as critical pillars for nations seeking to navigate the complexities and challenges of the digital age. Digital sovereignty, at its core, concerns the ability of a nation to exercise control over its digital infrastructure, data, and technological development, safeguarding its interests and the rights of its citizens. Cybersecurity, on the other hand, focuses on protecting digital assets and systems from a wide array of threats in cyberspace. The intersection of these two domains is becoming ever more crucial as nations strive to maintain autonomy and security in an increasingly interconnected world.

The advent of artificial intelligence (AI) represents a transformative force with the potential to significantly impact both digital sovereignty and cybersecurity. AI, with its advanced capabilities in data analysis, automation, and pattern recognition, offers new avenues for enhancing a nation's control over its digital resources and for bolstering its defenses against sophisticated cyber threats. However, the rise of AI also presents potential challenges, including concerns about data privacy, algorithmic bias, and the concentration of AI power in the hands of a few global entities. Consequently, the pursuit of what is increasingly termed "AI

sovereignty" has gained momentum, reflecting the desire of nations to maintain control over their AI development and deployment.

Nations today face a complex landscape of digital threats, ranging from sophisticated state-sponsored attacks aimed at critical infrastructure and sensitive data to the pervasive challenges of cybercrime, including ransomware, phishing, and identity theft. These threats can have significant consequences for national security, economic stability, and public trust. In this environment, the strategic application of AI in both enhancing digital sovereignty and strengthening cybersecurity capabilities is of paramount importance.

The central research question addressed in this article is: **What is the role of artificial intelligence in enhancing digital sovereignty and achieving cybersecurity, and how has Algeria specifically addressed these challenges?**

To answer this question, the **article aims** to: define digital sovereignty and cybersecurity from recent academic perspectives; analyze the potential of AI in strengthening the various components of digital sovereignty; examine the crucial role of AI in enhancing cybersecurity capabilities across detection, prevention, and response; present a detailed case study of Algeria's efforts in pursuing digital sovereignty and cybersecurity, with a particular focus on its adoption and development of AI; and finally, identify the key challenges and opportunities that Algeria faces in this evolving landscape.

The structure of this article will proceed as follows:

Section 2 will establish the conceptual framework by defining digital sovereignty and cybersecurity.

Sections 3 and **4** will analyze the synergistic role of AI in enhancing digital sovereignty. Section IV will explore AI as a cornerstone of modern cybersecurity.

Section 5 will present a detailed case study of Algeria's pursuit of digital sovereignty and cybersecurity.

Section 6 will discuss the challenges and opportunities for Algeria in this context.

Finally, **Section 7** will **conclude** with a summary of key findings and broader implications.

2. Conceptual Framework: Digital Sovereignty and Cybersecurity

The concept of digital sovereignty has garnered increasing attention in academic and policy circles as the digital realm becomes more central to state power and societal functioning. Recent academic definitions highlight various facets of this evolving idea. Digital sovereignty is broadly understood as the capacity of a country or region to exercise control over its digital infrastructure, data usage, and technological advancements without being unduly influenced by external forces. This encompasses the authority to make strategic decisions, create laws, and enforce them within the digital sphere. Some scholars define it as the ability to have control over one's digital destiny, encompassing the data, hardware, and software that a nation relies on and creates. This perspective emphasizes the importance of fostering homegrown tech industries, particularly where national security consequences are significant[1].

From a political economy standpoint, digital sovereignty can be seen as the manifestation of a political claim by a community to act as an autonomous agent in the digital realm. This understanding

[1] Sean Fleming, what is digital sovereignty, and how are countries approaching it? | World Economic Forum, Accessed May 9, 2025 https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

underscores that sovereignty is not merely about technological control but also about a conscious assertion of autonomy in the digital space[1]

Furthermore, digital sovereignty is increasingly viewed as encompassing the need to maintain and shape modes of freedom for individuals and groups within digitized societies. This perspective suggests that digital sovereignty should be normatively oriented towards vulnerability and freedom, remaining open to tensions and ambivalences in the digital environment[2].

The demand for digital sovereignty often involves an idea of greater autonomy, freedom of choice, co-determination, and control over "the digital". However, it is important to recognize that achieving complete self-sufficiency in all areas of the digital realm is neither possible nor sensible. Rather, the goal is often to create sufficient decision-making scope and reduce dependencies on potential hegemonic actors in the digital space. Ultimately, digital sovereignty can be understood as the power of a governing body to rule over itself in the digital realm, free from any interference by outside sources or bodies[3].

[1] Marília Maciel, Digital sovereignty: The end of the open internet as we know it? (Part 1) – Diplo Foundation, Accessed May 9, 2025 https://www.diplomacy.edu/blog/digital-sovereignty-the-end-of-the-open-internet-as-we-know-it-part-1/

[2] Braun, M., & Hummel, P. (2024). Is digital sovereignty normatively desirable? Information, Communication & Society, 1–14. https://doi.org/10.1080/1369118X.2024.2332624

[3] Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

Key components of digital sovereignty include data sovereignty, technological sovereignty, cybersecurity sovereignty, and legal sovereignty. Data sovereignty refers to the ability of a country or region to exercise full control over the data collected and processed within its territory, including establishing legal and regulatory frameworks for data protection and management. Technological sovereignty denotes the capacity to independently develop and manage a nation's technological infrastructure and resources, which is crucial for national security and innovation. Cybersecurity sovereignty ensures the protection of a nation's digital infrastructure and systems from cyber threats through the implementation of standards and incident management mechanisms. Finally, legal sovereignty refers to the ability to create and enforce a nation's own legal rules in the digital space, regulating online services and digital platforms[1]. These components highlight the multifaceted nature of digital sovereignty and the various dimensions that nations must address to assert their autonomy in the digital age.

Cybersecurity, as a crucial element of digital sovereignty, is defined in academic literature as the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyberattacks. Its primary aim is to reduce the risk of cyberattacks and to safeguard against the unauthorized exploitation of digital assets. Fundamentally, cybersecurity involves ensuring the confidentiality, integrity, and availability of information

[1] Hulkó G, Kálmán J and Lapsánszky A (2025) the politics of digital sovereignty and the European Union's legislation: navigating crises. Front. Polit. Sci. 7:1548562. doi: 10.3389/fpos.2025.1548562

in the digital realm[1]. Confidentiality entails keeping sensitive information private and accessible only to authorized individuals, often through methods like encryption and access controls. Integrity ensures that data has not been tampered with and remains accurate and complete throughout its lifecycle. Availability means keeping systems and data accessible to authorized users when needed, while protecting against disruptions such as cyberattacks.

A more comprehensive academic definition views cybersecurity as the collection and coordination of resources, including personnel, infrastructure, structures, and processes, to protect networks and cyber-enabled computer systems from events that compromise integrity and interfere with property rights[2]. This definition emphasizes the proactive and resource-intensive nature of cybersecurity in addressing present and emerging challenges in the digital environment. It is also understood as a multidisciplinary process that involves prevention, detection, and response to attacks[3]. This includes identifying potential vulnerabilities and instituting effective strategies to minimize the impact of possible threats[4].

[1] What is Cybersecurity? - CISA, Accessed May 9, 2025 https://www.cisa.gov/news-events/news/what-cybersecurity

[2] Francesco Schiliro, Towards a Contemporary Definition of Cybersecurity, arxiv.org, https://doi.org/10.48550/arXiv.2302.02274

[3] Cybersecurity - Glossary | CSRC - NIST Computer Security Resource Center, Accessed May 9, 2025 https://csrc.nist.gov/glossary/term/cybersecurity

[4] Francesco Schiliro, Towards a Contemporary Definition of Cybersecurity - ResearchGate, Accessed May 9, 2025 DOI:10.48550/arXiv.2302.02274DOI:10.48550/arXiv.2302.02274

Key principles and practices of cybersecurity include authentication, which verifies the identity of users trying to access systems; authorization, which determines what verified users can access; and the implementation of strong password practices, regular software updates, data backup strategies, and robust access control mechanisms. User education and awareness training are also critical components, as human error remains a leading cause of data breaches[1].

The relationship between digital sovereignty and cybersecurity is deeply intertwined. Cybersecurity is not merely a technical issue but a fundamental condition for achieving and maintaining digital sovereignty. A state's inability to effectively protect its digital infrastructure and data from cyber threats directly undermines its capacity to exercise control over its digital space and safeguard its national interests in the digital age. Conversely, a strong commitment to digital sovereignty provides the legal and policy framework for implementing and enforcing robust cybersecurity measures nationally[2]. Cyber incidents can strike at the very core of a nation's sovereignty by disrupting critical infrastructure, enabling the theft of intellectual property and state secrets, facilitating disinformation campaigns, and creating dominance by foreign ICT suppliers. Therefore, the pursuit of digital sovereignty inherently necessitates a

[1] What is Cyber Security? Definition & Best Practices - IT Governance, Accessed May 9, 2025 https://www.itgovernance.co.uk/what-is-cybersecurity

[2] Benjamin de Carvalho, Digital Sovereignty, Policy Brief, 2(2022), Accessed May 9, 2025. http://dx.doi.org/10.13140/RG.2.2.13315.27680

strong focus on establishing and maintaining a high level of cybersecurity[1].

Table 1: Academic Definitions of Digital Sovereignty

Definition
Ability to manage and regulate digital infrastructure, data, and technological development
Control over digital destiny, including data, hardware, and software
Capacity to control digital infrastructure, data use, and technological advancements without undue influence
A political community consciously understands itself as an autonomous agent in the digital realm
Maintaining and shaping modes of freedom for individuals and groups within digitized societies
More autonomy, freedom of choice, co-determination, and control over "the digital"
Power of a governing body to rule over itself in the digital realm, free from external interference

[1] Paul Timmers, Matthijs Punter, Claire Stolwijk, Cybersecurity and Digital sovereignty - Bridging the gaps, securitydelta.nl, Accessed May 9, 2025 https://securitydelta.nl/media/com_hsd/report/702/document/Whitepaper-digital-sovereignty.pdf

3. The Synergistic Role of Artificial Intelligence

Artificial intelligence offers a powerful suite of tools and capabilities that can significantly enhance various aspects of digital sovereignty, particularly in the realms of data, technology, and cybersecurity. By leveraging AI, nations can strengthen their control over their digital assets and reduce their reliance on external entities.

In the context of data sovereignty, AI provides advanced capabilities for enhanced data analysis and localization. AI-driven algorithms can be employed for robust data encryption and protection, ensuring that sensitive information remains secure within national borders. The concept of sovereign AI further underscores this, advocating for the development of AI models based on a country's own unique data, research, and intelligence. This approach allows nations to maintain greater control over the data used to train AI systems and the data generated by them, reducing the risk of foreign access or interference. The ability of AI to efficiently analyze large datasets can also help in identifying and managing sensitive national data, providing a deeper understanding of national resources and trends[1].

Technological sovereignty can also be significantly bolstered by the strategic application of AI. AI can facilitate the development of tailored technological solutions to address specific industrial and

[1] Niall McCarthy, Navigating Digital Sovereignty in the Age of AI - Planet Crust, Accessed May 9, 2025 https://www.planetcrust.com/decoding-digital-sovereignty-meaning-navigating-ai-era/?utm_campaign=blog

national needs, thereby reducing reliance on imported technologies[1]. By investing in national AI capabilities and infrastructure, countries can direct their technological future in alignment with their unique strategic priorities and cultural values[2]. The development of domestic AI capabilities aims to reduce dependence on foreign AI technologies, protecting nations from potential supply chain disruptions and reinforcing national sovereignty in critical technological domains[3]. This focus on homegrown innovation can stimulate domestic AI innovation, enhance national economic competitiveness, and create high-value jobs within the country[4].

While the role of AI in cybersecurity sovereignty will be explored in greater detail in the subsequent section, it is important to note here that AI is also playing an increasing role in legal sovereignty within the digital realm. AI-powered tools can assist in developing and enforcing legal rules in the digital space by monitoring compliance with data protection and AI governance

[1] Sanjay Misra, Petter Kvalvik, Bjørn Axel Gran, Kai Morgan Kjølerbakken, Aida Omerovic, Nadia Saad Noori, Book on Digital Sovereignty - IFE, Routledge, (Taylor & Francis Group), 2025, Accessed May 9, 2025 https://ife.no/en/research-fields/digital-sovereignty-artificial-intelligence-human-centric-ai-cybersecurity-digital-trust-icds-2024/

[2] Brian Letort, what is sovereign AI and why is it growing in importance? - Digital Realty, 2025, Accessed May 9, 2025 https://www.digitalrealty.com/resources/articles/what-is-sovereign-ai

[3] Muath Alduhishy, Sovereign AI: What it is, and 6 ways states are building it | World Economic Forum, 2024, Accessed May 9, 2025 https://www.weforum.org/stories/2024/04/sovereign-ai-what-is-ways-states-building/

[4] The Rise of Sovereign AI: National Strategies, Global Implications, Alphanome.AI, Accessed May 9, 2025 https://www.alphanome.ai/post/the-rise-of-sovereign-ai-national-strategies-global-implications

regulations. The ability of AI to analyze vast amounts of digital data can help in identifying potential violations of national laws, ensuring that online services and digital platforms operate within the established legal framework.

The concept of AI sovereignty has emerged as a critical subset of digital sovereignty, reflecting the growing understanding that control over AI development and deployment is essential for overall national autonomy in the digital age. Concerns about the increasing dominance of a small number of companies in the AI landscape have driven the need for nations to assert control over their use of AI through the development of national infrastructure and skills[1]. Pursuing AI sovereignty is seen as the latest and perhaps most crucial step in the ongoing quest for digital sovereignty, as AI continues its rapid spread into virtually every aspect of society, culture, and economy[2].

[1] Michael Webb, What is AI Sovereignty, and why does it matter for education? - Artificial intelligence, Accessed May 9, 2025 https://nationalcentreforai.jiscinvolve.org/wp/2024/08/02/what-is-ai-sovereignty-and-why-does-it-matter-for-education/

[2] Akash Kapur, From Digital Sovereignty to Digital Agency - New America, Accessed May 9, 2025 https://www.newamerica.org/planetary-politics/briefs/from-digital-sovereignty-to-digital-agency/

Table 2: Key Components of Digital Sovereignty and AI Enhancement

Component	Description	AI Enhancement
Data Sovereignty	Control over data collected and processed within a nation's borders	Enhanced data analysis and localization, AI-driven encryption and protection, Building AI on national data
Technological Sovereignty	Independent development and control of technological infrastructure	Developing tailored solutions, investing in national AI capabilities, reducing reliance on foreign AI
Cybersecurity Sovereignty	Protection of digital infrastructure from cyber threats	(Covered in Section IV)
Legal Sovereignty	Ability to create and enforce laws in the digital space	Developing and enforcing legal rules, Monitoring and enforcing data protection and AI governance

4. AI as a Cornerstone of Modern Cybersecurity

Artificial intelligence has become an indispensable component of modern cybersecurity strategies, offering significant enhancements across threat detection, prevention, and response. Its ability to process and analyze vast quantities of data at high speeds, identify complex patterns, and adapt to evolving threats makes it a crucial asset in defending against increasingly sophisticated cyberattacks.

In the domain of threat detection, AI excels at analyzing massive datasets from various sources, including network traffic, user behavior, and system logs, to identify patterns and anomalies that may indicate malicious activity. Machine learning algorithms, a key subset of AI, are particularly effective in performing behavioral analysis and anomaly detection, establishing baselines of normal activity and flagging any deviations that could signify a potential threat. AI systems can also monitor networks, endpoints, and applications in real-time, providing continuous vigilance against emerging threats. Furthermore, AI enables predictive analytics, allowing security teams to anticipate future threats based on the analysis of historical attack data and emerging trends[1]. This capability is vital for identifying new and complex threats, such as

[1] AI In Cybersecurity: Enhancing Threat Detection And Prevention, Boston Institute of Analytics, Accessed May 9, 2025 https://bostoninstituteofanalytics.org/blog/ai-in-cybersecurity-enhancing-threat-detection-and-prevention/

zero-day exploits and advanced persistent threats (APTs), which often evade traditional signature-based detection methods[1].

AI also plays a critical role in threat prevention. AI-powered threat hunting tools can proactively search for hidden threats within an organization's systems, identifying and neutralizing them before they can cause harm. Predictive analytics capabilities allow AI to identify vulnerabilities in systems and recommend necessary patches or security measures to prevent potential exploitation by attackers. AI enhances endpoint security by continuously monitoring activity on user devices and detecting and neutralizing threats directly at the endpoint, thus preventing breaches before they occur. Some organizations even use AI to simulate social engineering attacks, helping to identify potential vulnerabilities in human behavior and allowing for targeted training to improve overall security awareness[2].

The application of AI in threat response has revolutionized how organizations manage and mitigate cyber incidents. AI-driven systems can automate responses to certain types of attacks, enabling faster mitigation and reducing the potential for significant damage. AI-powered incident response systems can analyze security alerts in real-time, prioritize threats based on their severity, and automate workflows for investigating, containing, and eradicating attacks. This includes capabilities such as isolating affected systems and blocking

[1] What is AI in cybersecurity? EC-Council University, Accessed May 9, 2025 https://www.eccu.edu/blog/the-role-of-ai-in-cyber-security/

[2] AI and Cybersecurity: A New Era | Morgan Stanley, 2024, Accessed May 9, 2025 https://www.morganstanley.com/articles/ai-cybersecurity-new-era

malicious IP addresses automatically[1]. Moreover, AI-driven threat intelligence provides security teams with a deeper understanding of attack trends, allowing them to proactively adapt their security measures and stay ahead of emerging threats[2].

Machine learning (ML) is a fundamental component of many AI applications in cybersecurity. Supervised learning involves training ML models on labeled datasets of known benign and malicious samples, enabling them to predict whether new, unseen samples are malicious. Unsupervised learning, on the other hand, allows ML algorithms to analyze unlabeled data and discover hidden structures, relationships, and patterns, which can be invaluable for uncovering new attack patterns and anomalies. Reinforcement learning, a third type of ML, involves training models through trial and error, rewarding correct actions and penalizing incorrect ones, which can be particularly useful for identifying innovative ways to solve complex cybersecurity problems. Machine learning also enables the rapid processing and synthesis of large volumes of security data, allowing security teams to operationalize intelligence from various sources in near real-time[3]. Through continuous learning from

[1] AI-Powered Incident Response: Revolutionizing Threat Detection and Mitigation - Cyble, Accessed May 9, 2025 https://cyble.com/knowledge-hub/ai-powered-incident-response/

[2] Courtney Goodman, AI in Cybersecurity: Transforming Threat Detection and Prevention - Balbix, 2025, Accessed May 9, 2025 https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

[3] Lucia Stanham, Machine Learning (ML) in Cybersecurity: Use Cases - CrowdStrike, 2023, Accessed May 9, 2025 https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/machine-learning/

evolving data, ML models can improve their accuracy over time, reduce false positives, and adapt to the ever-changing threat landscape[1].

5. Algeria's Pursuit of Digital Sovereignty and Cybersecurity

Algeria has recognized the increasing importance of the digital realm for its national development and has embarked on a comprehensive digital transformation strategy. The government has placed a significant focus on improving the nation's digital infrastructure, regulatory frameworks, and the provision of digital services to its citizens. A key objective of this strategy is to position Algeria as a leading digital hub in the region by the year 2029, fostering an ecosystem where technology drives economic growth, innovation flourishes, and global partnerships thrive. Digital sovereignty has been identified as a central pillar in achieving this vision, with the government expressing a clear commitment to strengthening Algeria's control over its digital destiny[2].

In line with its digital sovereignty goals, Algeria has undertaken several significant cybersecurity initiatives. In 2020, the government established the National Council for Information Systems Security (CNSSI). Operating within the Ministry of

[1] What Is Machine Learning in Cybersecurity? | The University of Tulsa, 2024, Accessed May 9, 2025 https://online.utulsa.edu/blog/what-is-machine-learning-cybersecurity/

[2] Connected Algeria accelerates the nation's transition towards a competitive, digitally-driven economy., Accessed May 9, 2025 https://www.connectedalgeria.dz/about

National Defense, the CNSSI is responsible for developing the national strategy for information systems security. The government also created the Agency for Information Systems Security, tasked with implementing and enforcing the policies and strategies approved by the CNSSI. Furthermore, Algeria has put in place laws related to data protection and cybercrime, including Law No. 07-18 on the protection of natural persons in the processing of personal data[1]. The National Information Security Repository (NISR), published in 2020, provides a set of recommendations, best practices, guidelines, and controls to improve the security of information systems for individuals and companies, aligning with various international standards[2]. Efforts to strengthen national cybersecurity agencies and overall strategies are ongoing, as Algeria aims to build a more secure digital landscape[3].

Algeria has also recognized the strategic importance of artificial intelligence for its digital sovereignty and has taken proactive steps to build capabilities in this field. In 2023, the government established an AI Council, jointly under the Ministry of Higher Education and Scientific Research and the Ministry of Knowledge Economy,

[1] Hana Saada, "Algeria Aims to Enhance its Digital Sovereignty," Says Head of National Authority for the Protection of Personal Data - Dzair Tube, 2024, Accessed May 9, 2025 https://www.dzair-tube.dz/en/algeria-aims-to-enhance-its-digital-sovereignty-says-head-of-national-authority-for-the-protection-of-personal-data/

[2] Abdeldjalil Fortas, Cybersecurity and governance | The State of Software Engineering in Algeria, 2025, Accessed May 9, 2025 https://state-of-algeria.dev/docs/insights/cybersecurity/

[3] Algeria's Cybersecurity Journey: A Nation on the Rise! - EKSec, 2024, Accessed May 9, 2025 https://eksec.net/algerias-cybersecurity-journey-a-nation-on-the-rise/

Startups, and Micro-Enterprises. The nation has also adopted a National Artificial Intelligence Strategy, aiming to improve Algerian skills in AI through education, training, and research, and to leverage AI as a development tool across various socio-economic sectors. This strategy focuses on key areas such as scientific research, creating a supportive environment for AI development, building local expertise, and assisting startups in providing AI-powered solutions[1]. To support these efforts, Algérie Télécom, the state-owned telecom company, announced the launch of an investment fund dedicated to startups specializing in AI, cybersecurity, and robotics[2]. The government also emphasizes the importance of aligning AI strategies with national priorities, including cybersecurity, recognizing the potential of AI to enhance the nation's digital defenses.

[1] Benjamin FLAUX, Algeria Unveils AI Strategy to Boost Digital Transformation - Ecofin Agency, 2024, Accessed May 9, 2025 https://www.ecofinagency.com/public-management/1012-46241-algeria-unveils-ai-strategy-to-boost-digital-transformation

[2] Algeria earmarks $11 million to support AI, cybersecurity startups - Techpression, Accessed May 9, 2025 https://techpressionmedia.com/algeria-earmarks-11m-to-support-ai/

Table 3: Algeria's Digital Sovereignty and Cybersecurity Initiatives

Initiative	Description
National Council for Information Systems Security (CNSSI)	Develops national strategy for information systems security.
Agency for Information Systems Security	Implements and enforces cybersecurity policies and strategies.
Law No. 07-18 on the protection of natural persons in the processing of personal data	Establishes legal framework for data protection.
National Information Security Repository (NISR)	Provides guidelines and best practices for information security.
AI Council	Scientific advisory body for AI strategy and policy.
National Artificial Intelligence Strategy	Aims to improve AI skills and leverage AI for socio-economic development.
Investment fund for AI, cybersecurity, and robotics startups	Supports the growth of the tech ecosystem in these key areas.

6. Challenges and Opportunities for Algeria

Despite the progress made, Algeria faces several challenges in its pursuit of digital sovereignty and robust cybersecurity. The regulatory environment in Algeria has been described as slow to adapt to rapidly evolving international digital trends, which can hinder the growth of the digital economy and the adoption of new technologies. Gaps in digital infrastructure persist, particularly in rural areas where access to high-speed broadband remains limited, creating a digital divide within the country. Enhancing digital skills and awareness among a broader segment of the population is also crucial for maximizing the benefits of digital transformation and improving overall cybersecurity posture[1].

Balancing the need for stringent data protection regulations, which are essential for digital sovereignty, with the need to foster an environment conducive to the development and deployment of AI technologies presents another challenge. Additionally, Algeria's reliance on imported hardware and software for its digital infrastructure could potentially create vulnerabilities and undermine its digital sovereignty in the long term[2].

[1] Hadia Beghoura, Algeria - Digital Economy - International Trade Administration, 2024, Accessed May 9, 2025 https://www.trade.gov/country-commercial-guides/algeria-digital-economy

[2] Algeria earmarks $11 million to support AI, cybersecurity startups - Techpression, Accessed May 9, 2025 https://techpressionmedia.com/algeria-earmarks-11m-to-support-ai/

However, Algeria also has significant opportunities to further advance its digital sovereignty and cybersecurity goals. The strong commitment and strategic focus on digital transformation at the highest levels of government provide a solid foundation for continued progress. The government's proactive investments in AI and cybersecurity startups and the development of national digital infrastructure are likely to yield positive results in the coming years. The establishment of key institutions such as the AI Council and the CNSSI demonstrates a forward-thinking approach to governance and coordination in these critical areas[1]. With its strategic location and growing digital capabilities, Algeria has the potential to emerge as a regional leader in digital transformation, setting an example for other nations in the Middle East and North Africa. Furthermore, by strategically leveraging AI to enhance its cybersecurity capabilities, Algeria can better protect its critical infrastructure, sensitive data, and national interests in the increasingly complex digital landscape[2].

[1] Maria Buza, Sherif Taha, DPA Digital Digest: Algeria [2025 Edition], Digital Policy Alert, 2025, Accessed May 9, 2025 https://digitalpolicyalert.org/digest/dpa-digital-digest-algeria

[2] Driving Innovation in AI for a Smarter Algeria, aicouncil, Accessed May 9, 2025 https://aicouncil.dz/

7. Conclusion

The analysis presented in this article underscores the critical and increasingly intertwined roles of artificial intelligence, digital sovereignty, and cybersecurity in the contemporary global context. AI offers powerful tools for enhancing a nation's control over its digital assets and for strengthening its defenses against the growing spectrum of cyber threats. Digital sovereignty provides the overarching framework for nations to assert their autonomy in the digital realm, while cybersecurity serves as the essential foundation for ensuring the security and resilience of digital infrastructures and data.

Algeria's journey towards digital transformation highlights the nation's commitment to embracing the opportunities and addressing the challenges of the digital age. The establishment of national strategies and institutions focused on digital sovereignty, cybersecurity, and artificial intelligence demonstrates a proactive approach to building a secure and autonomous digital future. While challenges related to infrastructure, regulation, and skills development remain, Algeria's strategic investments and policy initiatives, particularly in the realm of AI, position it for potential leadership in the region's digital evolution.

The experiences of Algeria offer valuable lessons for other developing nations seeking to strengthen their digital sovereignty and cybersecurity in the age of AI. A holistic and strategic approach that integrates AI into national digital frameworks, addresses specific

national challenges, and leverages unique opportunities is crucial for success. As the digital landscape continues to evolve at a rapid pace, the ongoing commitment to innovation, adaptation, and international collaboration will be essential for all nations striving to secure their digital future.

References :

1. Abdeldjalil Fortas, Cybersecurity and governance | The State of Software Engineering in Algeria, 2025, Accessed May 9, 2025 https://state-of-algeria.dev/docs/insights/cybersecurity/

2. AI and Cybersecurity: A New Era | Morgan Stanley, 2024, Accessed May 9, 2025 https://www.morganstanley.com/articles/ai-cybersecurity-new-era

3. AI In Cybersecurity: Enhancing Threat Detection And Prevention, Boston Institute of Analytics, Accessed May 9, 2025 https://bostoninstituteofanalytics.org/blog/ai-in-cybersecurity-enhancing-threat-detection-and-prevention/

4. AI-Powered Incident Response: Revolutionizing Threat Detection and Mitigation - Cyble, Accessed May 9, 2025 https://cyble.com/knowledge-hub/ai-powered-incident-response/

5. Akash Kapur, From Digital Sovereignty to Digital Agency - New America, Accessed May 9, 2025 https://www.newamerica.org/planetary-politics/briefs/from-digital-sovereignty-to-digital-agency/

6. Algeria earmarks $11 million to support AI, cybersecurity startups - Techpression, Accessed May 9, 2025

https://techpressionmedia.com/algeria-earmarks-11m-to-support-ai/

7. Algeria earmarks $11 million to support AI, cybersecurity startups - Techpression, Accessed May 9, 2025 https://techpressionmedia.com/algeria-earmarks-11m-to-support-ai/

8. Algeria's Cybersecurity Journey: A Nation on the Rise! - EKSec, 2024, Accessed May 9, 2025 https://eksec.net/algerias-cybersecurity-journey-a-nation-on-the-rise/

9. Benjamin de Carvalho, Digital Sovereignty, Policy Brief, 2(2022), Accessed May 9, 2025. http://dx.doi.org/10.13140/RG.2.2.13315.27680

10. Benjamin FLAUX, Algeria Unveils AI Strategy to Boost Digital Transformation - Ecofin Agency, 2024, Accessed May 9, 2025 https://www.ecofinagency.com/public-management/1012-46241-algeria-unveils-ai-strategy-to-boost-digital-transformation

11. Braun, M., & Hummel, P. (2024). Is digital sovereignty normatively desirable? Information, Communication & Society, 1–14. https://doi.org/10.1080/1369118X.2024.2332624

12. Brian Letort, What is sovereign AI and why is it growing in importance? - Digital Realty, 2025, Accessed May 9, 2025

https://www.digitalrealty.com/resources/articles/what-is-sovereign-ai

13. Connected Algeria accelerates the nation's transition towards a competitive, digitally-driven economy., Accessed May 9, 2025 https://www.connectedalgeria.dz/about

14. Courtney Goodman, AI in Cybersecurity: Transforming Threat Detection and Prevention - Balbix, 2025, Accessed May 9, 2025 https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

15. Cybersecurity - Glossary | CSRC - NIST Computer Security Resource Center, Accessed May 9, 2025 https://csrc.nist.gov/glossary/term/cybersecurity

16. Driving Innovation in AI for a Smarter Algeria, aicouncil, Accessed May 9, 2025 https://aicouncil.dz/

17. Francesco Schiliro, Towards a Contemporary Definition of Cybersecurity, arxiv.org, https://doi.org/10.48550/arXiv.2302.02274

18. Francesco Schiliro, Towards a Contemporary Definition of Cybersecurity - ResearchGate, Accessed May 9, 2025 DOI:10.48550/arXiv.2302.02274DOI:10.48550/arXiv.2302.02274

19. Hadia Beghoura, Algeria - Digital Economy - International Trade Administration, 2024, Accessed May 9, 2025

https://www.trade.gov/country-commercial-guides/algeria-digital-economy

20. Hana Saada, "Algeria Aims to Enhance its Digital Sovereignty," Says Head of National Authority for the Protection of Personal Data - Dzair Tube, 2024, Accessed May 9, 2025 https://www.dzair-tube.dz/en/algeria-aims-to-enhance-its-digital-sovereignty-says-head-of-national-authority-for-the-protection-of-personal-data/

21. Hulkó G, Kálmán J and Lapsánszky A (2025) The politics of digital sovereignty and the European Union's legislation: navigating crises. Front. Polit. Sci. 7:1548562. doi: 10.3389/fpos.2025.1548562

22. Lucia Stanham, Machine Learning (ML) in Cybersecurity: Use Cases - CrowdStrike, 2023, Accessed May 9, 2025 https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/machine-learning/

23. Maria Buza, Sherif Taha, DPA Digital Digest: Algeria [2025 Edition], Digital Policy Alert, 2025, Accessed May 9, 2025 https://digitalpolicyalert.org/digest/dpa-digital-digest-algeria

24. Marília Maciel, Digital sovereignty: The end of the open internet as we know it? (Part 1) - DiploFoundation, Accessed May 9, 2025 https://www.diplomacy.edu/blog/digital-sovereignty-the-end-of-the-open-internet-as-we-know-it-part-1/

25. Michael Webb, What is AI Sovereignty, and why does it matter for education? - Artificial intelligence, Accessed May 9, 2025 https://nationalcentreforai.jiscinvolve.org/wp/2024/08/02/what-is-ai-sovereignty-and-why-does-it-matter-for-education/

26. Muath Alduhishy, Sovereign AI: What it is, and 6 ways states are building it | World Economic Forum, 2024, Accessed May 9, 2025 https://www.weforum.org/stories/2024/04/sovereign-ai-what-is-ways-states-building/

27. Niall McCarthy, Navigating Digital Sovereignty in the Age of AI - Planet Crust, Accessed May 9, 2025 https://www.planetcrust.com/decoding-digital-sovereignty-meaning-navigating-ai-era/?utm_campaign=blog

28. Paul Timmers, Matthijs Punter, Claire Stolwijk, Cybersecurity and Digital sovereignty - Bridging the gaps, securitydelta.nl, Accessed May 9, 2025 https://securitydelta.nl/media/com_hsd/report/702/document/Whitepaper-digital-sovereignty.pdf

29. Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

30. Sanjay Misra, Petter Kvalvik, Bjørn Axel Gran, Kai Morgan Kjølerbakken, Aida Omerovic, Nadia Saad Noori,Sanjay Misra, Petter Kvalvik, Bjørn Axel Gran, Kai Morgan Kjølerbakken, Aida Omerovic, Nadia Saad Noori, Book on Digital Sovereignty - IFE, Routledge, (Taylor & Francis

Group), 2025, Accessed May 9, 2025 https://ife.no/en/research-fields/digital-sovereignty-artificial-intelligence-human-centric-ai-cybersecurity-digital-trust-icds-2024/

31. Sean Fleming, What is digital sovereignty, and how are countries approaching it? | World Economic Forum, Accessed May 9, 2025 https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

32. The Rise of Sovereign AI: National Strategies, Global Implications, Alphanome.AI, Accessed May 9, 2025 https://www.alphanome.ai/post/the-rise-of-sovereign-ai-national-strategies-global-implications

33. What is AI in cybersecurity? EC-Council University, Accessed May 9, 2025 https://www.eccu.edu/blog/the-role-of-ai-in-cyber-security/

34. What is Cyber Security? Definition & Best Practices - IT Governance, Accessed May 9, 2025 https://www.itgovernance.co.uk/what-is-cybersecurity

35. What is Cybersecurity? - CISA, Accessed May 9, 2025 https://www.cisa.gov/news-events/news/what-cybersecurity

36. What Is Machine Learning in Cybersecurity? | The University of Tulsa, 2024, Accessed May 9, 2025

https://online.utulsa.edu/blog/what-is-machine-learning-cybersecurity/

الفصل السابع

الذكاء الاصطناعي آلية لتطوير الأمن السيبراني،

طالب الدكتوراه عبد الحق عبد النور

a.abdennour@cu-maghnia.dz

المخبر المتوسطي للدراسات القانونية

الدكتور عمر حماس

أستاذ محاضر قسم أ -المركز الجامعي مغنية

o.hammas@cu-maghnia.dz

المخبر المتوسطي للدراسات القانونية

الملخص:

يلعب الأمن السيبراني المدعوم بالذكاء الاصطناعي دور بالغا جراء استخدام الدول لمختلف تقنياته في محاربة والتصدي لمختلف التهديدات التكنولوجية التي قد تقع وتمس أمن المجالات الحيوية للدول وخاصة تلك المتعلقة بالمجال الأمني والاقتصادي للدول ،وبالمجال الاجتماعي المتعلق بأفرادها وخاصة في مجال الصحة في ظل الاعتماد على الروبوتات الطبية وكذا الحواسيب ،كل هذا شكل تحديات قانونية أخلاقية وجب بيانها وإثرائها من خلال إحداث قوانين وقواعد تكون ضوابط شرعية لاستخدم الذكاء الاصطناعي استخداما ايجابيا ،وبعيد عن الاستخدام السيئ له والذي قد يمس بحرمة وخصوصية الدول وأفرادها.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، الحماية التقنية الذكية، الحق في الخصوصية.

Abstract:

Cybersecurity powered by artificial intelligence plays a significant role as countries use various AI technologies to combat and counter various technological threats that may occur and affect the security of vital sectors of countries, especially those related to the security and economic sectors of countries, and the social sector related to their individuals, especially in the field of health in light of the reliance on medical robots and computers. All of this poses legal and ethical challenges that must be clarified and enriched by creating laws and regulations that serve as legitimate controls for the positive use of artificial intelligence, and avoiding its misuse, which may violate the sanctity and privacy of countries and their individuals.

Keywords :

Artificial intelligence, cybersecurity, smart technology protection, right to privacy.

مقدمة

يشكل الذكاء الاصطناعي في الأمن السيبراني سلاح ذو حدين على حسب الاستخدام سواء كان ايجابيا أو سلبيا فأضحى اليوم ما يعرف بالذكاء الاصطناعي السيبراني ،أو الأمن السيبراني المدعوم بالذكاء الاصطناعي ،وكما هو معلوم أن اليوم العالم أصبح منفتحا على بعضه من خلال مختلف المجالات وخاصة المجال الأمني والاقتصادي والاجتماعي في ظل توسع وانتشار الانترنت واستخدام الشبكة العنكبوتية وهو ما ساهم في تبادل مختلف المعلومات والبيانات بمختلف أشكالها وأنواعها ،فالدول وخاصة المتقدمة وفي ظل الصراع القائم والمستمر فيما بينها عملت على استغلال تكنولوجية الذكية في الأمن السيبراني في حمايتها منظوماتها المختلفة والتصدي لمختلف الهجمات ،وبالمقابل وفي ذات الوقت استغلت التكنولوجية الذكية في الأمن السيبراني في تنفيذ هجمات على الدول المتصارعة معها ،فالحرب اليوم حرب تكنولوجية بامتياز رغم وجود مواثيق دولية واتفاقيات وتشريعات تقضي بأخلقة استخدام الذكاء الاصطناعي في مختلف المجالات وخاصة المجال الأمني والمتعلق بخصوصية الأفراد وبياناتهم ،فالدول اليوم تسعى لإيجاد أرضية حقيقية تبنى عليها مختلف الثوابت الأخلاقية والتشريعية لتوظيف الذكاء الاصطناعي السيبراني فيما تقتضيه الضرورة الأمنية ودون المساس بحرمة وأمن الدول ومختلف بياناتهم وبيانات أفرادهم ،وهذه المنطلقات جاءت إشكالية الورقة البحثية كالتالي:

فيما تتجسد وتتمثل التطبيقات والتأثيرات بين الذكاء الاصطناعي والأمن السيبراني؟

للإجابة على هذه الإشكالية تم اتباع المنهج الوصفي لعرض مختلف المفاهيم المستحدثة والمنهج التحليلي للوقوف على النصوص القانونية المنظمة والمؤطرة للمواضيع ذات الصلة بالذكاء الاصطناعي السيبراني، وعليه تمت عنونة المبحث الأول مظاهر تطبيقات الذكاء الاصطناعي في الأمن السيبراني وعنون المبحث الثاني **الإطار** القانوني للحماية التقنية الإدارية الذكية في الأمن السيبراني.

المبحث الأول

مظاهر تطبيقات الذكاء الاصطناعي في الأمن السيبراني

بين الذكاء الاصطناعي والأمن السيبراني علاقة تأثير وتأثر وعلاقة تكامل تكنولوجي ذكي من خلال تنوع تطبيقات ومظاهر الذكاء الاصطناعي في الأمن السيبراني، كما تجلت تأثيرات الأمن السيبراني الذكي في مختلف المجالات الاقتصادية والاجتماعية والأمنية، كل هذا سيتم التعرض له من خلال عنون المطلب الأول التطبيقات التقنية الذكية في الأمن السيبراني وعنونة المطلب الثاني مظاهر تطبيقات الذكاء الاصطناعي في الأمن السيبراني.

المطلب الأول

التطبيقات التقنية الذكية في الأمن السيبراني

تساهم اليوم تقنيات الذكاء الاصطناعي المختلفة في التأثير على الأمن السيبراني وهو ما تجسد في مختلف المظاهر المختلفة والمتعددة، كما تجسد التأثير القوي والخطير للذكاء الاصطناعي السيبراني في المجال الأمني، كله هذه التأثيرات والتطبيقات التقنية سيتم بيانها من خلال عنونة الفرع الأول التأثيرات التقنية بين الذكاء الاصطناعي والأمن السيبراني، وعنوان الفرع الثاني التطبيقات الأمنية للذكاء الاصطناعي في الأمن السيبراني.

الفرع الأول: التأثيرات التقنية بين الذكاء الاصطناعي والأمن السيبراني:

يتخوف العالم اليوم من زيادة الهجوم السيبراني ،ولهذا تعد حماية سلامة البيانات من الهجمات الالكترونية أهمية بالغة عند تشغيل البيانات لخوارزميات الذكاء الاصطناعي ،فلذلك فهو يتجاوز الآمان في سياق عروض القيمة المستندة إلى الذكاء الاصطناعي نوع الهجمات الالكترونية وهو ما يسمى تعلم الآلة العدائي [1]،فيستغل هذا النوع من الهجمات قيود تصميم الشبكة العصبية ،المستخدمة في العديد من خوارزميات الذكاء الاصطناعي، حيث يمكن

[1] Jordi Canals ،Franz Heukamp،ترجمة طه محمد احمد يوسف ،مستقبل الإدارة في عالم الذكاء الاصطناعي ،در حميثرا للنشر ،القاهرة مصر ،الطبعة الأولى ، 2022،ص 309.

للمتسلل الخصم الضار التلاعب ببيانات إدخال الخاصة بخوارزمية الذكاء الاصطناعي ،إما في مرحلة التدريب أو التشغيل لخداع الأنظمة في رؤية شيء ما أو الاستماع إليه لخرق نظام الآمان بالكامل ،وقد يحدث هجوم وقت التدريب في مرحلة بناء نموذج تعلم الآلة باستخدام البيانات الضارة ،ويستخدم هجوم وقت الاستدلال المدخلات التي تم توليفها بشكل خاص والتي تؤثر على النموذج[1] ،فتكامل عدد من تقنيات الذكاء الاصطناعي مثل تنقيب البيانات والشبكات العصبية الذكية والمنطق الضبابي والأنظمة الخبيرة ،مع الإجراءات التقليدية والطرق الإحصائية قد تساعد في تحليل البيانات المخزنة لتدعم عمليات إدارة أمن المعلومات واكتشاف عمليات التلاعب والتجسس ،وتحسن هذه التقنيات قدرة أنظمة إدارة امن المعلومات من ربط وتحليل الأحداث الناتجة من أنواع مختلفة من الأدوات الحديثة المستخدمة في إدارة الشبكات ومراقبتها ،حيث يمكن الاستعانة بتقنيات الذكاء الاصطناعي والأنظمة الخبيرة في مواجهة الجرائم الالكترونية التي تهدد اقتصاد دول عديدة[2] ،كما يستخدم الذكاء الاصطناعي لتطوير أنظمة الأمن السيبراني التي تكشف وتتعامل مع الهجمات الالكترونية في الوقت الفعلي ،فالأنظمة المدعومة بالذكاء الاصطناعي يمكنها اكتشاف البرمجيات الخبيثة والهجمات كهجمات **DDoS**بشكل أسرع وأدق[3]

الفرع الثاني: التطبيقات الأمنية للذكاء الاصطناعي في الأمن السيبراني

تمكن الشبكات الآلية والتعلم الآلي الجهات الاجرامية من شن هجمات الكترونية ضخمة ولكنها مصممة لإحداث تأثير على العمليات المجتمعية دون استخدام موارد كبيرة أو مهارات متطورة أو أعداد كبيرة من المنفذين [4]، سيتطلب تهديد الهجمات السيبرانية المدعومة من الذكاء الاصطناعي الاستثمار في الدفاع السيبراني المدعوم من الذكاء الاصطناعي ،فان الأمن السيبراني للمنتجات الجديدة المدعومة من الذكاء الاصطناعي كالسيارات بدون سائق هي

---

[1] Jordi Canals، Franz Heukamp،ترجمة طه محمد احمد يوسف المرجع نفسه ،ص310،309.

[22] إسلام ديب، محمد شوقي العناني، الذكاء الاصطناعي ودوره في مكافحة الفساد، دار النهضة العربية للنشر والتوزيع، القاهرة مصر، الطبعة الأولى ،2022، ص 15.

[3] احمد مصطفى مندور، الذكاء الاصطناعي بين الأمن والعدالة، سلاح العصر لمكافحة الجريمة، دار النهضة العربية للنشر والتوزيع، القاهرة مصر، الطبعة الاولى ،46،2025.

[4] ممدوح عبد الحميد عبد المطلب، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، دار النهضة العربية للنشر والتوزيع القاهرة مصر، الطبعة الأولى ،2020، ص 9.

مصدر قلق متزايد ،أيضا هناك نوع آخر من التهديدات وهي الطائرات ذاتية التحكم **Drones**،حيث يمكن تزويد هذه الطائرات بدون طيار ذاتية التحكم بملامح الوجه واستخدامها في الاغتيالات والتجسس[1]،فقد فحص تقرير صادر سنة 2018 التهديدات المتعلقة بإساءة استخدام الذكاء الاصطناعي لأغراض الاجرامية قد حدد منها ثلاث فئات رئيسية ،أولها التهديدات المرتبطة بالأمن القومي ثم التهديدات المرتبطة بالأمن المادي ،وثالثا لتهديدات المتعلقة بالأمن السياسي[2] ،فالأمن السيبراني مزيج من العمليات والتقنيات الممارسة ،والهدف من حماية البرامج والتطبيقات والشبكات وأجهزة الكمبيوتر والبيانات من الهجوم ،ويشمل الأمن السيبراني المادي للبرامج والتطبيقات والشبكات وأجهزة الكمبيوتر ،وامن غير مادي أو معنوي يتعلق بالبيانات والمعلومات من أي هجوم وأضرار متعمدة وسرقة المعلومات والتحكم في الوصول الصحيح للأجهزة والتطبيقات والشبكات لحمايتها من الضرر الذي قد يحدث عبر الشبكات [3]، ويتم إثبات الجرائم السيبرانية باستخدام الشبكات العصبية من خلال شبكة **NeuroNet**وهي عبارة عن نظام شبكة عصبية يجمع المعلومات الموزعة ويعالجها، وتثبت المخالفات السيبرانية وتصدر تنبيهات وفي الوقت ذاته بل تبدأ التدابير المضادة[4] ، أيضا هناك شبكة **IDS-NNM** وهو عبارة عن نظام تم استحداثه سنة 2009وذلك لإثبات جرائم الاختراق الالكتروني باستخدام الشبكة العصبية المعتمدة على النمذجة ، وقد أثبتت فعاليتها التجارب العلمية في إثبات جميع محاولات الاقتحام في اتصالات الشبكة دون إعطاء أي تنبيهات خاطئة ،أيضا وفي ذات السنة واستنادا إلى الانتشار الخلفي للشبكات العصبية تم تقديم طريقة هجينة لإثبات وتصفية البريد المزعج[5] ،أيضا من بين وسائل إثبات الجرائم السيبرانية العميل المحقق الذكي ،وهو عبارة عن قوة مستقلة يولدها الكمبيوتر وتتواصل مع بعضها البعض ،حيث يحدث تبادل للبيانات وتتعاون فيما بينها من اجل تنفيذ الاستجابات

---

[1] ممدوح عبد الحميد عبد المطلب المرجع نفسه، ص 10

[2] محمد سعود كمال عبد الحي، انعكاسات الذكاء الاصطناعي على القانون الجنائي، دار الفكر الجامعي، الإسكندرية مصر، الطبعة الأولى ،2025، ص 35.

[3] شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 1 ،2022، ص298.

[4] حمد عبد الله علي مطر النيادي، الدليل السيبراني المستمد من الذكاء الاصطناعي، المجلة القانونية المجلد 14، العدد 4 ،2022، ص 1249.

[5] حمد عبد الله علي مطر النيادي، المرجع نفسه، ص 1250،1249.

المناسبة في حالة وقوع أحداث غير متوقعة ،وتعد هذه التقنية مناسبة لإثبات ومكافحة الهجمات الالكترونية ونظرا لقابليتها والقدرة على التكييف في البيئات التي يتم نشرها فيها. [1]

المطلب الثاني

مظاهر تطبيقات الذكاء الاصطناعي في الأمن السيبراني

لا يخلو مجال من المجالات وخاصة تلك الحساسة إلا وكانت عرضة لمختلف الهجمات والتهديدات السيبرانية، وهو ما داعي الدول الى توظيف واستغلال الذكاء الاصطناعي السيبراني في مختلف المجالات لتوفير امن سيبراني ذكي كامل، وتحقيق أمان وحماية للمنظومة الداخلية للدولة، وعليه سيتم عرض جانب من تطبيقات الأمن السيبراني الذكي من خلال عنونة الفرع الأول تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني الاجتماعي

الفرع الأول: تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني الاجتماعي

تشكل الجوانب الاجتماعية والمتمثلة في كل من الجانب التعليمي والصحي أهمية بالغة، حيث مسها الأمن السيبراني لأهميته في الحياة الاجتماعية للأفراد، فحماية خصوصية والأفراد وبياناتهم وأهمية الأمن السيبراني اقتضى توفير آليات تكون كحماية من مختلف التهديدات والهجمات السيبرانية وهو ما سيتم التطرق إليه بالتفصيل كما يلي:

أولا: تطبيقات الذكاء الاصطناعي في الأمن السيبراني التعليمي:

تجلى اليوم بما يعرف بضمان أمن سيبراني حتمي ينبغي تحقيقه المدارس والجامعات ،فالأهداف والأهمية التي يكتسيها توظيف الأمن السيبراني المدعوم بالذكاء الاصطناعي في الجامعات هو ما تسعى إليه مختلف الدول المتقدمة والنامية ،وكذا الدول العربية ،فاليوم المملكة العربية السعودية خاضت تجربة في هذا المجال ،حيث أجرت تجربة البحث للتحقق من صحة الفروض في الجامعات السعودية ،وقد أدى عدم وضع سياسات لأمن المعلومات إلى زيادة المخاطر التي يتعرض لها الطلاب وأعضاء هيئة التدريس والإداريين بالجامعات السعودية ،كما

[1] حمد عبد الله علي مطر النيادي، المرجع نفسه، ص 1251.

تعمل الجامعات السعودية إلى ضبط الأمن ألمعلوماتي والحد من مخاطر الاختراق الالكتروني ،كما يمثل تطبيق الذكاء الاصطناعي مدخل لتطوير صناعة القرار في الجامعات السعودية[1] .

ثانيا: تطبيقات الذكاء الاصطناعي في الأمن السيبراني الصحي:

أيضا في القطاع الصحي هو الأخر فان تقنيات الذكاء الاصطناعي فيه تساعد في جمع البيانات حول صحة الأفراد ،وهو ما يمكن من خلاله أن تؤدي هذه البيانات إذا تم تسريبها أو استغلالها بشكل غير قانوني إلى تهديد الصحة الشخصية وتعرض الأفراد للخطر[2] ، فالتطور الكبير في مجال الحاسوب الآلي وظهور الانترنت واستخدامها في جمع وتخزين معلومات الأشخاص لأغراض متعددة سمح لجمع كم هائل من البيانات الشخصية وحفظها في الحاسوب الآلي ،وقد ساهمت الانترنت في نشر هذه المعلومات والبيانات كالحالة الصحية والمحفوظة في موقع تخزين الحاسوب الآلي ،حيث يتم تبادل هذه المعلومات مع الحواسيب المتزامنة مع بعضها البعض وبالتالي فهذا خرق للخصوصية[3]

الفرع الثاني: تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني الاقتصادي

يعد الاقتصاد العمود الفقري لأي دولة، فبتطور اقتصادها تضمن سيادتها وقوتها، وفي ظل الصراع التكنولوجي الذكي تسعى مختلف الدول لضرب بعضها البعض من خلال مختلف الهجمات التي قد تقع على مجالات المنظومة الاقتصادية هدف إسقاط اقتصادياتها بعضها، للتفصيل سيتم عرض تطبيقات الأمن السيبراني الذكي في المجال الاقتصادي كما يلي

أولا: تطبيقات الذكاء الاصطناعي في الأمن السيبراني التسويقي:

تعتمد اليوم كبرى الشركات العالمية في تسويق منتجاتها على تقنيات الذكاء الاصطناعي لما يقدمه من امتيازات وأرباح مالية كبيرة ،هذه المزايا والامتيازات كانت محل أطماع جماعة الهكر ، وعليه فان دقة التسويق بالذكاء الاصطناعي تعتمد على مدى جودة تدريب النماذج

---

[1] جيهان سعد محمد الخضري، هدى جبريل علي سلامي، نعمة ناصر مدبش كليبي، الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية دراسة مقارنة، مجلة تطوير الأداء الجامعي، المجلد 12، العدد 1،2020، ص225.

[2] احمد مصطفى مندور المرجع نفسه، ص58.

[3] حامد عدنان عكال رشيد، الحماية المدنية للحق في الخصوصية من تأثير الذكاء الاصطناعي، مجلة الحقوق، العدد 48، ص 363.

وهوما يتطلب تدريب النموذج استخدام مجموعات بيانات ضخمة ،ولتي يمكن للقراصنة الوصول إليها عن طريق الهندسة العكسية لأنظمة الذكاء الاصطناعي[1] ،ويلجا المتسللون الهكر Hackersأدوات متقدمة لاكتشاف نقاط الضعف واختراقها في أمان أنظمة الشركات ،ولتجنب هذه الهجمات ستحتاج حلول الذكاء الاصطناعي للتنفيذ في مجال الأمن السيبراني ،مما يساعد في ردع المتسللين عن الوصول إلى البيانات المستخدمة في التدريب النموذجي ومعالجتها[2]

ثانيا: تطبيقات الذكاء الاصطناعي في الأمن السيبراني المصرفي:

يتجلى اليوم ما يعرف بالابتزاز السيبراني ،فمع تطور التقنيات الحديثة ،وانتشار أسواق المعلومات فتحت مجالا خصبا لجرائم الحاسبات ،حيث أصبح كثيرا من اقتصاد الانترنت يدور حول الإعلانات ،وجزء من هذه الإعلانات يستهدف استخدام قواعد بيانات المعلومات الشخصية ،ومن الأمثلة على ذلك سرقة بطاقات الائتمان فمن السهل سرقة أرقام بطاقات الائتمان التي يتم استخدامها للشراء عبر الانترنت أو اختراق قواعد بيانات المتاجر والمواقع التي يتم الشراء منها والاستيلاء على هذه الأرقام[3]،أيضا هناك قواعد بيانات المعلومات ،فعند الشراء على شبكة الانترنت تقوم بعض المواقع بتسجيل أرقام بطاقات الائتمان في قواعد البيانات الشخصية الخاصة بها ،لسهولة الشراء في المرات المقبلة ما يجعلها هدف سهلا لكثير من المجرمين الذين يمكن اختراق مواقع هذه الشركات ولحصول على بيانات المتعاملين[4] ،أيضا يتم جمع معلومات اقتصادية استخبارية ويتحقق هذا من خلال اختراق قواعد البيانات المالية والمصرفية وقواعد بيانات الشركات والبنوك وجمع المعلومات التي قد تؤثر على الأمن الوطني للدول ،وكذلك من خلال التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى[5]

---

[1] علاء محمد ساعي، الذكاء الاصطناعي افاقه وتطبيقاته في مجال الإدارة الحديثة، دار مؤسسة رسلان للطباعة والنشر والتوزيع، 2024، ص 101.

[2] علاء محمد ساعي، المرجع نفسه، ص 101.

[3] علي احمد إبراهيم، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الالكترونية، المجلة القانونية المجلد 9، العدد8، 2021، ص 2823.

[4] علي احمد إبراهيم، المرجع نفسه، ص 2824.

[5] شريفة كلاع، المرجع نفسه، ص303

المبحث الثاني

الإطار الأمني والقانوني للحماية التقنية الإدارية الذكية في الأمن السيبراني

تتنوع الجوانب القانونية للحماية التقنية الذكية في الأمن السيبراني من خلال عدة مظاهرها أهمها مصير المسؤولية القانونية للذكاء الاصطناعي في حماية الخصوصية ،وكذا التأطير التشريعي الدول للذكاء الاصطناعي في محال حماية الخصوصية وإيجاد قانوني أخلاقي للذكاء الاصطناعي بشكل جلي ،وبالتالي تحقيق حماية قانونية كاملة من خلال التشريع بقوانين وكذا بيان المسؤولية القانونية للآثار المترتبة عن الذكاء الاصطناعي وعليه جاء المطلب الأول معنونا بالمسؤولية القانونية للذكاء الاصطناعي و حماية الخصوصية، عنوان المطلب الثاني التشريعات الدولية وحماية الخصوصية.

المطلب الأول

المسؤولية القانونية والأمن القانوني للذكاء الاصطناعي وحماية الخصوصية

أثار تحديد الأساس القانوني للذكاء الاصطناعي في حماية الخصوصية إشكالات عديدة وخصوصا في ظل استخدام الروبوتات الطبية وكذا الحواسيب وما تحمله من تخزين للمعلومات ومختلف البيانات المتعلقة بالحالة الصحية للأفراد وكذا مختلف البيانات الأخرى كالحالة الاجتماعية الخاصة بهم، وعليه جاء الفرع الأول معنونا أثر المسؤولية القانونية للذكاء الاصطناعي في حماية الخصوصية وجاء الفرع الثاني معنونا ب الأمن القانوني للذكاء الاصطناعي وحماية الخصوصية.

الفرع الأول: المسؤولية القانونية للذكاء الاصطناعي في حماية الخصوصية

ساهم اليوم استخدام التطبيقات الذكية للذكاء الاصطناعي في مختلف المجالات إلى زيادة الأضرار المتولدة عنه كاستخدام الروبوتات الطبية في المجال الطبي، أو استخدام الطائرات ذاتية القيادة ذات الأغراض الأمنية ،وهو ما دفع بالفقهاء والقانونية للبحث عن الشخص المسؤول القانوني عن ما تحدثه هذه التقنيات ،خصوصا مع عندما تكون تعمل هذه الآلات الذكية من تلقاء نفسه ،وهو ما زاد من تعقيد الأمر في تحديد المسؤولية ،فالفقهاء والقانونية وتبعا للتساؤلات العديدة المطروحة حول إمكانية إسقاط المسؤولية القانونية على أساس قواعد الحراسة أو على أساس المنتجات المعيبة:

أولا: قيام المسؤولية القانونية للذكاء الاصطناعي على أساس أحكام الحراسة:

تطبيق أحكام الحراسة على أنظمة الذكاء الاصطناعي ،فمختلف التشريعات تتفق على أن أحكام الحراسة والتي تقوم على انه الحارس يكون مسؤولا عن الأضرار الناتجة عن الشيء الذي هو تحت سلطته الفعلية ،فالبرغم من أن أجهزة الذكاء الاصطناعي لها نوع من الاستقلالية وتجنب الأخطاء إلا أن الحارس لها يتحمل مسؤولية هذا الأضرار التي تنشا عنها وهو ما ذهب إلى تطبيقه المشرع العراقي في مادته 231 من القانون المدني العراقي[1] ،وهناك جانب آخر من الرأي ذهب إلى فكرة تطبيق الحراسة الرقمية على الذكاء الاصطناعي ،فاعتبار الذكاء الاصطناعي شخصية قانونية مستقلة وجب العمل بفكرة الحارس الافتراضي ،حيث يتم التمييز ضمن أجهزة التي تعمل بتطبيقات الذكاء الاصطناعي بين خوارزميات الذكاء الاصطناعي وبرمجته الدقيقة وبين العقل الصناعي او محرك الذكاء وهو الجزء المسؤول عن عمل تطبيقات الذكاء الاصطناعي الذي يوصف بأنه العقل الذي يتخذ القرارات ومن ثم ينفذها الهيكل المادي[2] .

[1] حامد عدنان عكال رشيد، المرجع نفسه، ص366.

[2] محامد عدنان عكال رشيد، لمرجع نفسه، ص366. 367.

ثانيا: قيام المسؤولية القانونية للذكاء الاصطناعي على أساس المنتج:

أما عن أساس قيام المسؤولية القانونية للذكاء الاصطناعي على أساس المنتج، فيكون هذا راجع لعيب في الإنتاج أو التصنيع، ولتحقق المسؤولية وجب البحث عن مدى علاقة منتج الذكاء الاصطناعي بالأضرار التي حصلت، فلقيام مسؤولية المنتج أو المصنع عن أضرار الذكاء الاصطناعي يتطلب توافر شروط والمتمثلة في وجود عيب في الآلة او الروبوت، وان يكون الضرر الذي أصاب المتضرر بفعل الذكاء الاصطناعي، وان يكون الآلة أو الروبوت مطروحا للتداول، وجود العلاقة السببية [1].

فالظاهر يبدو لنا انه لا علاقة بين المسؤولية القانونية عن أضرار تطبيقات الذكاء الاصطناعي والقائمة على أساس الحراسة أو المنتج والحق في الخصوصية والتي تمس بحقوق الإنسان ،لكن التطبيق الواقعي لهذه لأنظمة الذكاء الاصطناعي المادية والمعنوية خصوصا في المجال الطبي والاقتصادي والأمني أدى إلى المساس بحق الخصوصية التي تقتضيها المواثيق الدولية لما تحمله هذه الأجهزة كالروبوتات أو أجهزة الحاسوب من أسرار خاصة بالأشخاص أو بالدول والتي قد تكون في يوم امن الأيام ظاهرة للعيان والعالم ،وهو ما اقتضى ضبطها تشريعيا وقانونيا داخليا وخارجيا ،وهو ما يحقق امن سيبراني في مختلف المجالات.

الفرع الثاني: الأمن الرقمي القانوني للذكاء الاصطناعي وحماية الخصوصية

أولا: الأمن الرقمي للذكاء الاصطناعي وحماية الخصوصية

الأمن الرقمي ،وما يصطلح عليه أيضا بالأمن الالكتروني ،والمقصود به هو الحفاظ على الأعمال المعلوماتية والتقنية للجهات الداخلية والخارجية من التهديدات الداخلية والخارجية مع الحفاظ على سرية المعلومات للمحافظة على سلامتها ويتم عن طريق استراتيجيات يتحكم فيها عدة أشخاص ،وفق إجراءات تقنية وقانونية وفق الاختصاص المعمول [2]،ومن البيانات التي استخدمتها الدول في هذا الجانب ومنها من يستخدم لمراقبة حركة مرور شبكة المعلومات عن طريق إجراء تحليلات البيانات الضخمة واكتشاف سلوك المستخدم غير القانوني عن

[1] حامد عدنان عكال رشيد، المرجع نفسه، ص367. 368..

[2] محمد حمدي عبد العليم علام، المرجع نفسه، ص170.

طريق تسجيل الدخول إلى مواقع الويب ذات الرموز غير المعتمدة ،ويتم الحفاظ على الأمن الرقمي من خلال أربعة اتمات والمتمثلة في أتمتة هجمات الهندسة الاجتماعية حيث يتم هذا باستهداف الضحايا عبر الانترنت باستخدام المعلومات لإنشاء برامج ضارة مخصصة تلقائيا في مواقع الويب ورسائل البريد الالكتروني والروابط التي من المحتمل النقر عليها أو يرسلونها من عناوين تنتحل صفة جهة اتصالهم الحقيقية ،ويتم باستخدام ملف أسلوب الكتابة الذي يحاكي تلك الاتصالات مع تطور الذكاء الاصطناعي [1]،أما ثاني أتمتة وهي أتمتة اكتشاف الثغرات الأمنية من خلال دراسة الأنماط التاريخية باستخدام الثغرات الأمنية في الكود لتسريع اكتشاف الثغرات وإنشاء كود لاستغلالها ثم التحكم في البيانات وهذا يشكل غاية في الخطورة على الأمن الرقمي للدول ،وبالسيطرة عليه سيؤدي إلى زعزعة النظام العام الالكتروني ،وثالث أتمتة وهي أتمتة أكثر تطورا للقرصنة ،حيث يتم استخدام الذكاء الاصطناعي بشكل مستقل أو بالتنسيق مع البشر لتحسين اختيار الهدف وتحديد الأولويات والتهرب من الاكتشاف والإبداع نتيجة للتكنولوجيا المتقدمة للمجرمين ،حيث تصبح قادرة على استغلال الثغرات الأمنية في الأنظمة لفترة طويلة ،وتبدو الأدوات لمكافحة القرصنة أكثر تقدما باستخدام الذكاء الاصطناعي وأفضل بكثير مقارنة بما كان ممكنا لمكافحتها بالوسائل التقليدية لتطوير الخدمة البشرية في الإدارة عن طريق محاكاة الإنسان في الخدمة بطريقة متقدمة لمحاربة هذه الظاهرة حفاظا على مراقبة التهديدات الأمنية والتحكم في إدارتها الأمنية [2]،أما عن رابع أتمتة وهي أتمتة مهام الخدمة في الجرائم الالكترونية الجنائية ،فيستخدم مجرمو الانترنت تقنيات الذكاء الاصطناعي لأتمتة المهام المختلفة كمسار لهجومهم ،مثل معالجة المدفوعات أو الحوار مع ضحايا برامج الفدية ،لهذا سارعت دول عديدة لعقد مؤتمرات من اجل التعامل معها وتم تطوير العديد من البرامج القائمة على أنظمة الذكاء الاصطناعي لمكافحتها ووقفها قبل حدوثها [3].

[1] محمد حمدي عبد العليم علام، المرجع نفسه، ص172.

[2] Miles Brundage. the malicious use of artificial intelligence forecasting prevention and mitigation futur of humanity institute university of oxford centre for the study of existential risk university of Cambridge center for a new American security electronic frontier foundation openai February 2018.p25

[3] Miles Brundage. the malicious use of artificial intiligence forecasting prevention op cit .p62.

ثانيا: الأمن القانوني للذكاء الاصطناعي وحماية الخصوصية

يتجسد الأمن القانوني للذكاء الاصطناعي في حماية الخصوصية من خلال عدة إجراءات شرطية استباقية ،ففي ظل توسع الأنشطة الاجرامية واعتمادها على الذكاء الاصطناعي من خلال القرصنة والابتزاز وسرقة الكترونية وغيرها ،وهو ما حتم على الأجهزة الأمنية اعتماد على الذكاء الاصطناعي لمواجهة الجرائم الالكترونية ،وعليه فيمكن للأجهزة الأمنية من أن تطور قدراتها من خلال استخدام تقنيات الذكاء الاصطناعي والتي من بينها ،الشرطة الاستباقية حيث يتم ردع العمل الإجرامي من خلال العمل الاستباقي الشرطي بتحليلات البيانات ،ومن أهم الإجراءات المساعدة في ذلك تبني الأجهزة الأمنية لأنظمة التخزين السحابي [1]،أيضا اعتماد الشرطة الرقمية والذي يعني تطوير أجهزة الشرطة بهدف الاستفادة من التقنيات الحديثة كالاستفادة من الوفرة في الأدلة الرقمية ،كذلك يجب الاعتماد على تقنيات الذكاء الاصطناعي لتصبح أكثر فعالية في جمع المعلومات عن المجرمين وتحليل البيانات لاستخدام تلك المعلومات للمساعدة في سرعة وفاعلية اتخاذ القرار[2] ،دائما وفي إطار مواجهة الجرائم الالكترونية اعتماد التحقيق الرقمي بحيث لابد من أن تحول الحكومة بكاملها إلى حكومة رقمية ،وأولى الخطوات أن يتم تفعيل الهوية الرقمية ،حيث أن وجود هوية لمستخدم الانترنت يبرز بقوة الكثير من الحلول التي ممكن أن تقدمها قوات الأمن لمنع الجريمة والكشف عن مرتكبيها[3] ،فصناع القرار في الولايات المتحدة الأمريكية ،دول الاتحاد الأوربي ،روسيا ،الصين ،الهند وغيرها من الدول ،يصنفون مسائل الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية ،إضافة إلى إعلان أكثر من 130 دولة حول العالم عن تخصيص أقسام وسياسات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني[4] .

[1] علي احمد إبراهيم، المرجع نفسه، ص 2824.

[2] علي احمد إبراهيم، المرجع نفسه، ص 2824. 2825.

[3] علي احمد إبراهيم، المرجع نفسه، ص. 2825.

[4] شريفة كلاع، المرجع نفسه، ص 298.

المطلب الثاني

التشريعات الدولية وحماية الخصوصية

في ظل الاعتماد الحتمي والضروري على الذكاء الاصطناعي في مختلف المجالات الحيوية للدول وما افرزه من أثار ايجابية وسلبية ، أدى إلى طرح هذا إشكاليات قانونية عدة ومن خلاله سعت الدول وخاصة تلك المتقدمة إلى الموازنة بين العمل بالذكاء الاصطناعي وحتمية وتنظيمه و أخلقته خصوصا في السنوات الأخيرة ،وهو ما تجسد فعلا من خلال شرعت فيه الدول المتقدمة خاصة الدول الأوربية وكذا الولايات المتحدة الأمريكية وهو ما سيتم التعرض إليه من خلال عنون الفرع الأول النظام التشريعي الأوربي للذكاء الاصطناعي في حماية الخصوصية ،وعنون الفرع الثاني النظام التشريعي الأمريكي للذكاء الاصطناعي في حماية الخصوصية

الفرع الأول: النظام التشريعي الأوربي للذكاء الاصطناعي في حماية الخصوصية

في ظل الانتشار الواسع لاستخدام الذكاء الاصطناعي في مختلف المجالات ومنه اعتماد أنظمته على البيانات الخاصة هذه البيانات دفعت مختلف التشريعات للتسريع في إرساء قواعد قانونية الغاية منها حمايتها من مختلف المخاطر والتهديدات التي قد تتعرض لها، وهو فعلا ما قام به الاتحاد الأوربي ،حيث اتخذ هذا الأخير خطوات جادة في سبيل تحقيق الحماية عن طريق اللائحة العامة لحماية البيانات حيث دخلت حيز التنفيذ سنة 2018،وقد تضمنت العديد من الحقوق لصاحب البيانات بعرض الحد من الآثار المترتبة على استخدام أنظمة الذكاء الاصطناعي ،فقد أرست مجموعة من الضمانات لحماية خصوصية صاحب البيانات كالموافقة الصريحة لأصحاب البيانات على معالجة بياناتهم الشخصية[1] ،الأسانيد القانونية في هذا ،ما جاء في المادة 22 فقرته 3 من اللائحة العامة لحماية البيانات على انه "بخصوص حماية المعالجة الآلية للبيانات يجب على مراقب البيانات اتخاذ التدابير المناسبة التي تحول دون المساس بحقوق وحريات أصحاب البيانات ومصالحهم المشروعة "،كما أوجبت المادة 13 و14 من ذات اللائحة

[1] احمد مصطفي الفقي، توظيف خوارزميات الذكاء الاصطناعي في نظام العدالة الجنائية بين الفرص والتحديات، مجلة القانون والتكنولوجيا كلية القانون الجامعة البريطانية، مصر، المجلد 3، العدد 2،2023، ص 608،609.

على مراقبي البيانات ضرورة إخطار أصحاب البيانات الشخصية بالمعالجة الخوارزمية لبياناتهم ،كما نصت المادة 15 على حقهم في الوصول البيانات الشخصية مدة لمعالجة الخوارزمية للبيانات[1] ،أيضا التوجيه الأوربي رقم 2016/2/680 ووفقا لنص المادة 11منه فانه تحظر القرارات المؤتمتة التي تنتج آثار قانونية على صاحب البيانات أو تؤثر عليه بشكل كبير ،مالم يكن مصرحا بذلك من قبل الاتحاد ا والدول الأعضاء[2]،وفي ابريل 2021 أصدرت المفوضية الأوربية قانون الذكاء الاصطناعي والغاية منه تنظيم استخدام الذكاء الاصطناعي في مختلف المجالات بما في ذلك القانون ،ويركز هذا القانون تحديد معايير الأمان والسلامة[3]،كما قام المشرع البريطاني فقد تم تعيين لجنة مختارة حول الذكاء الاصطناعي سنة 2017 للنظر في الآثار الاقتصادية والاجتماعية والأخلاقية في مجال الذكاء الاصطناعي[4] ، كما قام أيضا المركز الوطني للأمن السيبراني البريطاني بإصدار إرشادات حول الأمان الذكي باستخدام أدوات لمساعدة المستخدمين على فهم الاعتبارات عند استخدام أمان الذكاء الاصطناعي الجاهز للأدوات ،وكذا توجيه أولئك الين يسعون إلى بناء أدوات أمان داخلية للذكاء الاصطناعي ويوفر من المعلومات الكثيرة حول كيفية تحديد الاحتياجات والتعامل مع البيانات ،وتحقيق أقصى استفادة من الذكاء الاصطناعي للمساعدة في تحديد ما إذا كان حل الذكاء الاصطناعي هو نهج جيد لمشكلة معينة ومجموعة من الاحتياجات[5]، التي تساعد على فك شفرات الاختراق الغير شرعي للبيانات المتاحة على الشبكة ،فلهذا فالحفاظ على امن المعلومات الرقمية من صلاحيات الحكومات للحفاظ على تهديدات الأمن الرقمي سواء الداخلية أو الخارجية والحفاظ على السيادة والأمن القومي[6].

[1] احمد مصطفي الفقي، المرجع نفسه، ص609.

[2] احمد مصطفي الفقي، المرجع نفسه، ص609.

[3] أيمن احمد راشد، احمد محمد أمين، العدالة الذكية دور الذكاء الاصطناعي في المحاماة والقضاء، دار مصر للنشر والتوزيع، الطبعة الأولى ،2024، ص 123.

[4] عبد الوهاب محمد عبد الوهاب السادة، الذكاء الاصطناعي وتأثيره على العدالة الروبوت قاضيا ومحاميا، دار الفكر الجامعي، الإسكندرية مصر، الطبعة الأولى،2025، ص179.

[5] محمد حمدي عبد العليم علام الاستراتيجية القانونية للذكاء الاصطناعي وتطبيقاته، دور المعرفة للنشر والتوزيع ،2024، ص170.

[6] محمد حمدي عبد العليم علام، المرجع نفسه، ص171.

الفرع الثاني: النظام التشريعي الأمريكي للذكاء الاصطناعي في حماية الخصوصية

أصدرت الولايات المتحدة الأمريكية في سنة 2017، قانون مستقبل الذكاء الاصطناعي وآفاقه في العالم وهو أول قانون يتمحور حول نظم الذكاء الاصطناعي[1]، أيضا هناك قوانين قانون الخصوصية في كاليفورنيا **CCPA**والذي يتناول حماية البيانات الشخصية في الأنظمة الذكية[2] .

إن الغاية من الأخذ نظام التشريعي الأوربي والأمريكي كنموذج، هو التطور الحاصل في هذه الدول في مجال الذكاء الاصطناعي، بالإضافة إلى هذه فهم من الدول التي تسعى إلى إيجاد إطار قانوني وتشريعي لضبط هذه التقنية الذكية ذات التأثيرات الخطيرة والتي قد تمس بخصوصية الأفراد خاصة.

[1] عبد الوهاب محمد عبد الوهاب السادة المرجع نفسه، ص179.

[2] أيمن احمد راشد، احمد محمد أمين المرجع نفسه، ص124.

خاتمة

تحصيلا لما جاء في الورقة البحثية فان الذكاء الاصطناعي في الأمن السيبراني شكل أهمية بالغة فتبنته الدول وخاصة المتقدمة في منظوماتها المختلفة في سبيل تحقيق آمنا وحماية من مختلف التهديدات والهجمات التي قد تقع، وقد تم التوصل إلى النتائج التالية:

أولا: بين الذكاء الاصطناعي والأمن السيبراني علاقة تكنولوجية تكاملية ذكية، يتجلى من خلالها تطبيقات وتأثيرات للذكاء الاصطناعي في الأمن السيبراني.

ثانيا: لا يخلو مجال من مجال الحيوية للدول إلا وقد مسه تطبيق من تطبيقات الأمن السيبراني الذكي لأهمية هذه المجالات.

ثالثا: تجلى التأطير والتنظيم القانوني للذكاء الاصطناعي واستخداماته في مختلف المجالات وهو ما أدى إلى المساس بالخصوصية خصوصا في السنوات الأخيرة.

رابعا: أهمية الأمن السيبراني دفع بالدول إلى إدخالها في منظومتها التربوية والتعليمية والتطرق إلى الأهداف والغايات المرجوة منه.

ومن خلال هذه النتائج تم التوصل إلى التوصيات التالية:

أولا: حتمية تطوير المنظومة الأمنية الداخلية والمتعلقة بالأمن السيبراني الذكي لما له من أهمية في بالغة في إرساء قواعد حماية وأمان في مختلف المجالات.

ثانيا: ضرورة فتح مدراس جهوية في محال الأمن السيبراني والذكاء الاصطناعي لتقديم أفضل تكوين لأكبر عدد من المتمدرسين في هذا المجال.

ثالثا: إدخال الأمن السيبراني والذكاء الاصطناعي كمقياس تعليمي في المنظومة التربوية خاصة في ظل التطور التكنولوجي الحاصل.

رابعا: إرساء قواعد تشريعية قانونية حمائية من مختلف التهديدات والهجمات السيبرانية والاستخدام السيئ للذكاء الاصطناعي خاصة في مجال الخصوصية.

قائمة المراجع

الكتب:

01-Franz Heukamp،Jordi **Canals ، ترجمة** طه محمد احمد يوسف، مستقبل الإدارة في عالم الذكاء الاصطناعي، دار حميثرا للنشر، القاهرة مصر، الطبعة الأولى، 2022.

02-إسلام ديب، محمد شوقي العناني، الذكاء الاصطناعي ودوره في مكافحة الفساد، دار النهضة العربية للنشر والتوزيع، القاهرة مصر، الطبعة الأولى ،2022، ص 15.

03-احمد مصطفى مندور، الذكاء الاصطناعي بين الأمن والعدالة، سلاح العصر لمكافحة الجريمة، دار النهضة العربية للنشر والتوزيع، القاهرة مصر، الطبعة الأولى ،46،2025.

04-ممدوح عبد الحميد عبد المطلب، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، دار النهضة العربية للنشر والتوزيع القاهرة مصر، الطبعة الأولى ،2020.

05-عبد الوهاب محمد عبد الوهاب السادة، الذكاء الاصطناعي وتأثيره على العدالة الروبوت قاضيا ومحاميا، دار الفكر الجامعي، الإسكندرية مصر، الطبعة الأولى،2025.

06-أيمن احمد راشد، احمد محمد أمين، العدالة الذكية دور الذكاء الاصطناعي في المحاماة والقضاء، دار مصر للنشر والتوزيع، الطبعة الأولى ،2024.

07-علاء محمد ساعي، الذكاء الاصطناعي افاقه وتطبيقاته في مجال الإدارة الحديثة، دار مؤسسة رسلان للطباعة والنشر والتوزيع، 2024.

08-محمد سعود كمال عبد الحي، انعكاسات الذكاء الاصطناعي على القانون الجنائي، دار الفكر الجامعي، الإسكندرية مصر، الطبعة الأولى.2025.

09-محمد حمدي عبد العليم علام، الاستراتيجية القانونية للذكاء الاصطناعي وتطبيقاته، دور المعرفة للنشر والتوزيع ،2024.

المجلات:

01-حمد عبد الله علي مطر النيادي، الدليل السيبراني المستمد من الذكاء الاصطناعي، المجلة القانونية المجلد 14، العدد 4 ،2022.

02-جيهان سعد محمد الخضري، هدى جبريل علي سلامي، نعمة ناصر مدبش كليبي، الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية دراسة مقارنة، مجلة تطوير الأداء الجامعي، المجلد 12، ال عدد1 ،2020.

03-حامد عدنان عكال رشيد، الحماية المدنية للحق في الخصوصية من تأثير الذكاء الاصطناعي، مجلة الحقوق، العدد 48

04-علي احمد إبراهيم، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الالكترونية، المجلة القانونية المجلد 9، العدد 8، 2021.

05-احمد مصطفي الفقي، توظيف خوارزميات الذكاء الاصطناعي في نظام العدالة الجنائية بين الفرص والتحديات، مجلة القانون والتكنولوجيا كلية القانون الجامعة البريطانية، مصر، المجلد 3، العدد 2، .2023.

06-شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 1 ،2022،

07-Miles Brundage. The malicious use of artificial intelligence forecasting prevention and mitigation futur of humanity Institute University of oxford centre for the study of existential risk university of Cambridge center for a new American security electronic frontier foundation openai February 2018.

الفصل الثامن

السيادة الوطنية للدول في ظل التهديدات السيبـــرانية

-دراسة حول إعادة دلالة مفهوم سيادة وستفاليا-

الدكتورة بوزيد عويشة

أستاذ(ة) محاضر(ة) الصنف (أ)

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

جامعة أبوبكر بلقاي / تلمسان

البريد الالكتروني: awichabouzid@yahoo.fr

ملخص

في الحقيقة يعتمد مفهوم السيادة السيبرانية في مفهومه ومضامينه إلى حد كبير على مضمون السيادة الوطنية التقليدية ولذلك غالبا ما ينظر إليه على أنه امتداد للسيادة ضمن مفهومها التقليدي الوستفالي ولعل ثورة المعلومات التي ميزت هذا العصر هي من سرع لظهور مفهوم كهذا، فعلى الرغم من أهمية تدفق المعلومات وسهولة وسرعة انتشارها إلا أن هذا الأمر خلق نوع من الارباك للدول وباقي الفواعل الأخرى في العلاقات الدولية كالأفراد والمنظمات وجماعات المصالح... إلخ، فالأمن اليوم لم يعد مقتصرا على سلامة الدولة جغرافيا ضمن حدودها بل أصبح مفهوما واسعا شاملا لجميع الأبعاد ولعل الحدود السيبرانية التي أضحت عرضة للتهديدات أهم دليل على ذلك.

سنحاول من خلال هذه الدراسة تسليط الضوء على ثلاث نقاط أساسية تتعلق بتحول مفهوم السيادة من الإطار الوستفالي إلى السيادة الرقمية، وبعدها سنركز على معالجة

نقطة مهمة تتعلق بأهم تجليات ومظاهر اختراق السيادة الوطنية للدول في ظل هاته المتغيرات الجديدة، وفي الأخير سنوضح أهم الجرائم المعلوماتية مركزين على جريمة التجسس الاقتصادي الالكتروني وسبل وآليات الحد منها هي وباقي الجرائم على المستوى الدولي.

الكلمات المفتاحية

السيادة، معاهدة وستفاليا، السيادة الرقمية، ثورة المعلومات، الجرائم الالكترونية، التجسس الالكتروني الاقتصادي.

Abstract

In fact, the concept of cyber sovereignty, in its concept and implications, relies largely on the traditional concept of national sovereignty. Therefore, it is often viewed as an extension of sovereignty within its traditional Westphalian concept. Perhaps the information revolution that characterized this era is what accelerated the emergence of such a concept. Despite the importance of the flow of information and the ease and speed of its dissemination, this has created a kind of confusion for states and other actors in international relations, such as individuals, organizations, interest groups, etc. Security today is no longer limited to the geographical integrity of the state within its borders. Rather, it has become a broad concept encompassing all dimensions. Perhaps the most important evidence of this is the cyber borders, which have become vulnerable to threats. Through this study, we will attempt to shed light on three key points related to the shift in the concept of sovereignty from the Westphalian framework to digital sovereignty. We will then focus on addressing a crucial point related to the most significant manifestations and manifestations of the breach of national

sovereignty in light of these new variables. Finally, we will highlight the most important cybercrimes, focusing on the crime of electronic economic espionage and the means and mechanisms for combating it, along with other crimes, at the international level.

Key words

Sovereignty, Treaty of Westphalia, digital sovereignty, information revolution, cybercrime, economic cyber espionage.

مقدمة

تعد السيادة الوطنية إحدى الركائز الأساسية التي قامت عليها الدولة الحديثة في إطار معاهدة **وستفاليا** عام **1648** حيث مثلت تلك المعاهدة نقطة تحول في رسم معالم النظام الدولي من خلال إقرار مبدأ السيادة المطلقة للدول داخل حدودها الجغرافية ومنع التدخل في شؤونها الداخلية غير أن التحولات التكنولوجية المتسارعة وفي مقدمتها الثورة الرقمية قد أفرزت تحديات غير مسبوقة لهذا المفهوم الكلاسيكي التقليدي وفي مقدمتها التهديدات السيبرانية.

فالفضاء السيبراني بخصائصه الفريدة من لا مركزية وتجاوز للحدود المادية قد أصبح مسرحا جديدا للمواجهات بين الدول والجهات الفاعلة من غير الدول وقد أضحى الأمن السبيراني من أولويات الأمن القومي للدول خاصة مع تزايد الهجمات الرقمية التي تستهدف البنى التحتية والمؤسسات الحكومية والأنظمة الاقتصادية وحتى العمليات السياسية وعلى اختلاف طبيعتها.

في هذا السياق تبرز الحاجة الملحة إلى إعادة قراءة مفهوم السيادة الوطنية في ظل هذه التحديات السيبرانية إعادة دلالته بما يتماشى مع متطلبات العصر الرقمي.

الإشكالية

بالاعتماد على ما سبق قمنا بصياغة إشكالية الدراسة على النحو التالي:

هل مازالت سيادة وستفاليا قادرة على الاستجابة لتحديات القرن الحادي والعشرين أم أننا أمام ضرورة بلورة نموذج سيادي جديد يدمج بين السيادة المادية والسيادة الرقمية؟ وهل تعتبر ثورة المعلومات وجه جديد لأوجه الهيمنة والسيطرة على الشعوب المغلوبة على أمرها؟

الفرضية

1- السيادة الرقمية هي امتداد للسيادة بمفهومها التقليدي الوستفالي

2- تعتبر ثورة المعلومات وما صاحبها من تهديدات آلية من آليات الضغط على الوحدات السياسية الأضعف ضمن النظام الدولي.

أولا-تعريف مفهوم السيادة

لقد حظي موضوع السيادة بدراسات مستفيضة وعميقة اعتبارا بأن موضوع السيادة يمثل أهم مواضيع القانون الدولي، ولعل أبرز ما اختلف حوله الفقهاء والمتخصصين في ميدان القانون الدولي هو تحديد المفهوم العام لهذا المصطلح، لكن صعوبة التحليل والتنقيب حول الموضوع لا توحي بعدم وجود الكثير من المحاولات والاسهامات العلمية التي استطاعت حقا الاقتراب ولو بدرجة متوسطة من المفهوم الجامع المانع لمصطلح السيادة[1].

استخدم "**جون بودان**" الفقيه الفرنسي تعبير السيادة أول مرة قاصدا به السلطة السياسية، لكن هذا الاعتقاد اختلف حوله بعد ذلك الباحثون فمنهم من يرى أن السلطة السياسية شيء يختلف تماما في مضامينه عن السيادة، وفي المقابل نجد فئة أخرى تؤيد رأي الفقيه "**جون بودان**" حول هذا الموضوع.[2]

لقد قام الأستاذ الباحث "**دي مالبرغ كاري**" مفهوما عاما حول السيادة مفاده أن:

"السيادة تمثل صفة أو هي إحدى خصائص السلطة العامة التي بموجبها بلا ترضى بأي حال من الأحوال وجود سلطة أخرى فوقها"، وبالتالي فإن الأستاذ "**كاري دي مالبرغ**" يجعل من مفهوم السيادة مفهوما سلبيا يتمثل في إنكار كل مقاومة أو قيود على السلطة العامة

إذن السيادة ميزة خاصة بالسلطة العامة فالسيادة تظفي على السلطة العامة صفة المحرك الأساسي في الدولة بمعنى هي التي تختص بجميع الصلاحيات العليا في البلاد وبالتالي لا مجال لغيرها من السلطات، من هنا نستنتج بأن الأستاذ الباحث ركز في تعريفه هذا على المفهوم السلبي للسيادة لأنه اذا ما بحثنا في واقعنا نلمس جيدا بأن السيادة تبقى مجرد صورة من صور الهيبة التي تؤكد استقلالية الدول على المستويين المحلي الداخلي والعالمي الدولي، بلكن عمليا نلاحظ العكس نظرا لبروز ظاهرة الاعتماد المتبادل بين الوحدات الدولية وعلى كافة الأصعدة والميادين الحياتية.

---

[1] - ادريس بوكرا، الوجيز في القانون الدستوري والمؤسسات السياسية، القاهرة: دار الكتاب الحديث، 2003، ص، 21.

[2] - يحيى الجمل، الأنظمة السياسية المعاصرة، بيروت: دار النهضة للطباعة والنشر، د.س.ن، ص: 41.

انطلق الأستاذ "**إيزمان**" في تعريفه للسيادة من الدولة معتبرا أن هاته الأخيرة عبارة عن تشخيص قانوني للأمة، فحسب رأيه الذي يجعل من الامة دولة هو توافر السلطة العامة التي تتميز بعقل وإرادات هذه الامة فلا توجد فوقها سلطة تخضع لها فاعتمادا على هاته المعطيات استنتج الباحث "**إيزمان**" أن السلطة العليا في المجتمع السياسي هي التي لا نوازيها أو تناظرها سلطة أخرى فهس حسب هذا المنطق تمثل السلطة التقديرية المطلقة[1].

لقد اتفق الفقه السياسي على أن الذي يميز الدولة عن غيرها من التنظيمات والجماعات الأخرى هو خاصية السيادة التي كما سبق وأن أسلفنا الذكر تتصف بها السلطة العامة في البلاد والتي طبعا تعد سلطة قاهرة على تنظيم وفرض توجيهاتها دون الخضوع لضغط خارجي من غيها لا داخليا ولا خارجيا[2].

بعض الفقهاء السياسيين اعتبروا أن السيادة تشير إلى:

"القوة القادرة على تحقيق الوحدة السياسية للدولة الدائمة غير المؤقتة التي لا تقبل التجزئة ولا التفويض والتي لا مجال للمسؤولية عنها أمام سلطة أخرى"[3].

اعتمادا على ما سبق تشير السيادة إلى عدم التبعية بجميع اشكالها ولها عنصران:

العنصر الأول يتميز بالخصوصية الإيجابية حيث يتمثل في القدرة فوق العادية للبشر لفرض السلطة، أما العنصر الثاني فيتميز بالسلبية كونه يبدو في الصفة التي تعطي لصاحب السيادة الصلاحيات المخولة لعدم تبعيته في أي شيء لطرف آخر وإن كان ذلك لا يتلاءم والواقع[4].

---

[1] - سعيد بوشعير، القانون الدستوري والنظم السياسية المقارنة، ج.1، ط.و، الجزائر: ديوان المطبوعات الجامعية، 2002، ص: 99.

[2] - محمد نصر مهنا، علم السياسة، القاهرة: دار غريب للطباعة والنشر والتوزيع، د.ت.ن، ص: 290.

[3] - المرجع نفسه، ص: 291.

[4] - سعيد بوشعير، مرجع سبق ذكره، ص: 100.

تحليل هذين العنصرين المتعلقين بالسيادة يبرز لنا أن السيادة لها وجهان مختلفان تماما الأول إيجابي أما الثاني فهو سلبي.

فمثلا إذا ما عدنا إلى نظرية العقد الاجتماعي التي تفترض أن قيام الدولة القومية ونشأتها هو نتاج عقد قائم بين الحاكم والمحكومين (الشعب) فأي إخلال أو نقض لعهود قطعها الحكام على أنفسهم عند تولي زمام الحكم يؤدي إلى إعادة النظر في هذه العلاقة التعاقدية وذلك باتخاذ أجزاء تغيير الحاكم[1].

المثال المدرج يفسر لنا حقا وجها السيادة السلبي والايجابي، فالوجه الإيجابي يتحقق عند الحد الذي يصبح فيه الحاكم الممثل للدولة خادما لشعبه مسؤولا مكلفا وليس مشرفا بالمسؤولية والسلطة الموكلة إليه، اما الوجه السلبي للسيادة يتجلى عند قيام الحاكم بأعمال التعسف واضطهاد الشعب وإخراجه من دائرة الحكم التي يعتبر المواطن الطرف الرئيسي الفاعل فيها أكثر من غيره.

ثانيا-تطور السيادة من المفهوم التقليدي الوستفالي إلى المفهوم الرقمي السيبراني

تعتبر السيادة مفهوم ذو طبيعة قانونية وسياسية في آن واحد برز بشكل كبير مع بروز الدولة القومية بمفهومها الحديث، فأصبحت السيادة مطلبا ضروريا لا بد من ترسيخه عمليا ليميز الدولة المستقلة سياسيا واقتصاديا، وسنحاول من خلال هذا العنصر الكشف عن مضمون النشأة التاريخية لمبدأ السيادة.

شهد مفهوم السيادة تطورا كبيرا منذ بداية القرن السادس عشر **16** ففي البداية تميزت بمفهومها المطلق بمعنى حرية الدولة حرية تامة في إدارة وتسيير شؤونها الخاصة بالبيئة المحلية والدولية، لكن هذا الوضع لم يبق كذلك مع بروز مجموعة من المتغيرات التي أفرزت تراجعا ملحوظا في مدى تطبيق هذا المبدأ على المستوى العملي، خصوصا على مظهره

[1] خليل مجدي، التدخل الأجنبي والتدخل الدولي، الحوار المتمدن، على الرابط الالكتروني: https://www.ahewar.org/débat/show.artK

الخارجي وذلك بسبب تعارض هذا المظهر الخارجي للسيادة مع باقي سيادات الدول الأخرى، ومع ذلك رفضت الدولة رفضا تاما مطلقا المساس بهذه الخاصية التي تميزت بقداستها منذ زمن بعيد، وبالتالي رفض أي تدخل أجنبي أيا كان نمطه والمستهدف لشؤونها الداخلية وسلامة إقليمها[1].

فمفهوم السيادة كغيره من المفاهيم لم يكن وليد لحظة أو نتاج لظرف معين بل جاء كنتيجة حتمية لتراكم مجموعة هائلة من المتغيرات المتعلقة أساسا بالتطور الحاصر في أشكال الدول وأنماط حكوماتها، ذلك طبعا عن طريق تطور الحضارات والتقدم الحاصل في المطالبة المستمرة الدائمة بالحرية والمشاركة في غمار الحكم[2].

ما يهمنا في هذا الإطار هو البحث عن موقع هذه القضية في تاريخنا الإسلامي أولا بنوع من التلخيص والتدقيق، ثم حصر أهم ما يتعلق بشأنها في الفكر الغربي.

1- السيادة في الشريعة الإسلامية:

نستهل تحليل هذا العنصر من البحث اعتمادا على ة الآية 59 من سورة النساء:

"يا أيها الذين آمنوا أطيعوا الله وأطيعوا الرسول وأولي الأمر منكم فإن تنازعتم في شيء فردوه إلى الله والرسول إن كنتم تؤمنون بالله واليوم الآخر ذلك خير وأحسن تأويلا"[3].

انطلاقا من الآية الكريمة نستنتج بأن السيادة مبدأ وارد في الشريعة الإسلامية وهي تخص الله تعالى، فحكم التشريع يعود له وحده سبحانه وتعالى وان السيادة المقصودة هنا متمثلة في شريعة كتاب الله القران الكريم والسنة النبوية الشريفة فالدولة تستند في حكمها عبر

[1] - عبد القادر بوراس، التدخل الدولي الإنساني وتراجع مبدأ السيادة الوطنية، دار الجامعة الجديدة، 2009، ص: 19.

[2] -عبد الله حسن العايد، انعكاسات العولمة على السيادة الوطنية، ط.1، عمان: دار كنوز المعرفة العلمية للنشر والتوزيع، 2009، ص: 52.

[3] - سورة النساء، القرآن الكريم، الآية 59.

السيادة المخولة لها نمن خلال التزامها بالأحكام الشرعية وتنفيذها لها في الواقع العملي وبالطبع فان هذا الحق السيادي يرافقه حق مراقبة الأمة للسلطة الحاكمة وبالتالي محاسبتها على افعالها.[1]

تكمن الفكرة الرئيسية هنا في أن السيادة سلطة تخص الله سبحانه وتعالى، لكن الله عندما جعل خلفاء له في الأرض قدم لهم كيفيات وأنماط تسيير شؤونهم انطلاقا من مبايعة حاكم يتولى أمورهم الدينية والدنيوية استنادا إلى قواعد الدسين الإسلامي المقدمة من خلال القرآن الكريم والسنة النبوية الشريفة.

2- السيادة في الفكر الغربي:

عموما نستطيع التركيز في هذا السياق على الفكرة القائلة بأن السيادة ظهرت كنتيجة لما يعرف بالعقد الاجتماعي، فمنطقيا وانطلاقا من هذا الاعتقاد فإن السيادة في هذه الحالة تصبح للجماعة المكونة للعقد أي لمجموع الأفراد المكونين للأمة، ولعل الآراء التي تبناها "**جون جاك روسو**" في كتابه "**العقد الاجتماعي**" دليل قاطع على هذا الطرح[2].

وإذا ما بحثنا في أصل هذه الفكرة نجد أنها تعود في أصولها عند بعض الكتاب أبرزهم "**سوارز**" و "**بلارمان**" فقد أكدا بأن السيادة لا يمكن بأي حال من الأحوال أن تنتمي لشخص واحد ومحدد بل هي مسألة تتعلق بجميع الأشخاص على اختلافهم، كما أن آراء كل من "**توماس هوبز**" و"**جون لوك**" من نفس آراء "**جون جاك روسو**" الذي أسهم حقا في إعطاء الدلالة الأوضح والأدق حول موضوع السيادة الشعبية.

وإلى جانب هؤلاء الرواد المؤيدين لفكرة السيادة الشعبية نلمح بأن "فيليب بوت" قد صرح عام **1480** بأن السيادة هبي في الواقع سيادة في يد جميع الافراد[3].

السيادة كقاعدة دولية ظهرت منذ سنة **1468** في إطار نصوص معاهدة وستفاليا والتي أكدت بكل وضوح أن الدولة لها شؤون متعلقة بالبيئة الداخلية لنظامها السياسي وأخرى

---

[1] - إبراهيم نعيم الظاهر، إدارة الدولة والنظام السياسي الدولي، ط.1، الأردن: عالم الكتب الحديث للنشر والتوزيع، 2010، ص: 67.

[2] - إدريس بوكرا، المرجع السابق الذكر، ص: 129.

[3] - المرجع نفسه، ص: 130.

متعلقة بالبيئة الخارجية، كما أبرزت المعاهدة ضرورة عدم التدخل في تلك الشؤون من قبل الكيانات الأخرى فالمبدأ إجباري لا بد من الالتزام به في علاقات الدول ببعضها البعض .

هناك اتجاه فكري سائد يؤكد بأن السيادة بمفهومها المعاصر تعود إلى القرن السادس عشر **16** وأول من استخدمها هو الفقيه الفرنسي "**جون بودان**" حيث عمل بعها في النظام الفرنسي، ثم اهتم "**توماس هوبز**" بالاصطلاح مع بدايات القرن 17 ليتواصل ذيوعه فتردد على الالسنة في الولايات المتحدة الأمريكية بعد استقلالها عام **1776** ومع هذا الاقبال على المفهوم أصبح محوريا في دساتير بعض الدول وعلى إثر كل هذا أخذ المفهوم يتطور بتسارع فبعد ارتباطه بالأمير الحاكم في وقت ما تطور المبدأ ليرتبط بالشعب الصاحب الفعلي للسلطة[1].

على الرغم من أن المفكر "**جان بودان**" نظر لمفهوم السيادة الوطنية إلا أن إسهاماته لم ترتق بفكرة السيادة إلى التطلعات الديمقراطية المرغوبة، وللإشارة فإن هذا المفهوم ظل سائدا كدلالة على السلطة المطلقة التي تعلو على القانون والأفراد كما انها اعتبرت صمام آمال نحو القضاء على سيطرة البابا والامبراطور والتحرر من النظم الاستبدادية والاقطاعية[2].

ما تجدر إليه الإشارة ها هنا هو أن فلاسفة عصر التنوير ورواد النظرية العقدية (**العقد الاجتماعي**) كان لهم الفضل الكبير في حدوث ثورات جاءت من أجل الحد من استبداد الطبقات الأرستقراطية ومصالح الملوك وبالفعل تم ذلك بنجاح حين اتحدت الطبقة البورجوازية مع الطبقات الشعبية من أجل الإطاحة بحكم الملوك، وبالتالي سادت فكرة السيادة الشعبية وأصبحت تحجز مكانها ضمن الدساتير الوطنية للدول لتصبح عبارة عن سلوكيات وأفعال[3] وهذا ما تكرس أكثر في عهد الديمقراطية والترسيخ الديمقراطي الذي كفل للمواطن حق حكم نفسه بنفسه.

وبعد كل هذا ومع دخول العالم في مرحلة جديدة من تاريخه ألا وهي مرحلة العولمة بأبعادها الاقتصادية الاجتماعية الثقافية عرف مفهوم السيادة تحولا ملموسا وواضحا وهذا من

---

[1] - المرجع نفسه، المكان نفسه.

[2] - سمير حمياز، "إشكالية السيادة الوطنية في ظل المتغيرات في ظل المتغيرات الدولية الراهنة"، في دورية: الآداب والعلوم الاجتماعية، العدد: 1، 2017، ص:03.

[3] - المرجع نفسه، المكان نفسه.

جعل من هذه الأخيرة تتنحى من مضمونها الوستفالي، وهنا برزت السيادة الرقمية كسمة جديدة من سمات السيادة الوطنية.

اعتمادا على كل ما تم عرضه نستنتج بأن السيادة مفهوما شهد تطورا ملحوظا عبر العصور حيث بدأ بالمعنى التقليدي الذي ظهر بعد معاهدة وستفاليا عام **1648** والتي أكدت على مبدأ سيادة الدولة الكاملة على أراضيها واستقلالها في اتخاذ قراراتها دون تدخل خارجي، وقد ظل هذا المفهوم سائدا لقرون طويلة معتمدا على الحدود الجغرافية والسلطة السياسية والعسكرية إلا أن السيادة بعد أن خرجت من صفتها السابقة إلى حلة جديدة مواكبة لعصر العولمة وظهور ما يسمى بالتحديات العابرة للحدود مثل حقوق الإنسان و التدخلات الإنسانية والاتفاقيات الدولية، مما أدى إلى ظهور ما يعرف بالسيادة المقيدة ومع دخول العالم إلى العصر الرقمي ظهر مفهوم جديد يعرف ب السيادة الرقمية وهو يشير إلى قدرة الدولة على التحكم في بياناتها الرقمية والبنية التحتية السيبرانية والتكنولوجيا المستخدمة داخل حدودها الالكترونية حيت لم تعد السيطرة الجغرافية كافية بل أصبحت السيطرة على تدفق المعلومات وحماية الفضاء الالكتروني وتنظيم استخدام البيانات أمورا أساسية لحفظ استقلال الدول وقد تبنت دول مثل الصين، والولايات المتحدة الامريكية والاتحاد الأوروبي سياسات مختلفة لتعزيز سيادتها الرقمية سواء عبر التشريعات التنظيمية، أو البنية التحتية الرقمية المستقلة أو الأنظمة الرقابية الالكترونية.

ثالثا-تجليات اختراق السيادة في عصر المعلوماتية

رأى "**فرنسيس فوكوياما**" في كتابه "**نهاية التاريخ**" و"**الرجل الأخير**" أن هناك أربع تأثيرات واضحة لثورة المعلومات وتكنولوجيا الاتصال على الحياة الإنسانية في العالم كله، أول تلك الآثار تتمثل في دعم آليات التحول الديمقراطي وبالتالي جعل النظم المتسلطة في خانة ضعف وهذا سيكون تقريبا في جل أنحاء العالم، ناهيك عن حدوث تراجع كبير في سيادة الدول من خلال إضعاف السلطة المركزية وجعلها مقسمة على فئات متعددة، كما اعتبر "**فرنسيس فوكوياما**" بأنه من خلال المتغيرات التي سوف تحدث في العالم هو تحول مفهوم القوة

من خلال مضامينها وكيفيات ممارستها وأثرها، وفي الأخير أكد بأن المنظمات القوية سوف تتفتت على شكل وحدات صغيرة[1].

وبالفعل كل ما تنبأ به المنظر "**فرنسيس فوكوياما**" نحن نعيشه اليوم في عالمنا المعاصر المعولم، الذي لم يعد في إطاره أثر للعامل الجغرافي حين أصبحت عملية انتقال الأفكار والأفراد والبضائع تتم بصورة في لمح البصر وبسرعة فائقة التصور، ولهذا سميت هاته المرحلة ثورة المعلومات هذه الأخير التي أثرت على الدولة التي كانت تمثل الفاعل الرئيسي في العلاقات الدولية كما أن ثورة المعلومات يسرت انتقال وانتشار المعلومة في أوساط مختلف الأفراد ومن بيئة إلى بيئة، هذا ما زاد من إضعاف دور الدولة في التأثير على عقول وقيم مواطنيها اعتبارا بأن هؤلاء المواطنين أصبحوا على دراية تامة بما يجري داخل بيئة النظام السياسي الداخلية، وعند هذا الحد برزت جماعات ومؤسسات أخرى تنافس الدولة في القيام بالأدوار المنوطة إليها وهنا تحولت السيادة لتصبح محل جدل كبير[2].

ما يمكن الإشارة إليه ها هنا كنقطة مهمة يجب عدم إغفالها هو أن الاعلام والديمقراطية وجهان لعملة واحدة فالديمقراطية هي من تضمن للإعلام حريته، وهذا الأخير هو من يدافع عنها ويعمل على دعمها واستمرارها فالهدف الأسمى المشترك بينهما يتمثل في حفظ كرامة الفرد والجماعة وصوتها من جميع أشكال الاعتداء، ولعل هذا الأمر كان سببا رئيسيا نحو الالحاح والاحتياج للديمقراطية، وفي المقابل – وكما ذكرنا سابقا – هناك تداول رقمي للمعلومات فات السيطرة والتحكم وبهذا التقى الشقان معا حيث مهدت وعبدت التكنولوجيا الطريق لمختلف الممارسات الديمقراطية، وبالتالي ظهور ما يعرف بالديمقراطية الرقمية[3]، التي تم تعريفها على النحو التالي:

"هي توظيف أدوات تكنولوجيا المعلومات والاتصالات الرقمية المعلوماتية في توليد وجمع وتصنيف وتحليل ومعالجة ونقل وتداول كل البيانات والمعلومات والمعارف المتعلقة بممارسة

---

[1] - مصطفى سحاري، "السيادة الوطنية للدول في ظل ثورة المعلومات"، في مجلة: المعيار، المجلد: 10، العدد: 4، ديسمبر 2019، ص: 52.

[2] - المرجع نفسه، ص: 53.

[3] - حكيم سياب، الاعلام الآلي والقانون، ط.1، عمان: دار وائل للنشر والتوزيع، 2014، ص -ص: 115 – 116.

قيم الديمقراطية وآلياتها المختلفة بغض النظر عن نوع هذه الديمقراطية وقالبها الفكري ومدى انتشارها وذيوعها، ومستوى نضجها، وسلامة مقاصدها وفعاليتها في تحقيق أهداف مجتمعها"[1].

هذا التعريف يوحي لنا في مضامينه أن الديمقراطية الرقمية لا تحل محل الديمقراطية التي عهدناها وعرفناها وعايشناها بل هي مجرد وسيلة من وسائل ممارسة الأفعال الديمقراطية فعلى الرغم من تأثير الديمقراطية والرقمية وسطوتها وقدرتها على التغيير يجب أن تحافظ على مكانتها الحقيقية المتمثلة في خدمتها للمجال التي تدخله[2].

إذن على الرغم من عديد المزايا التي ذكرناها سلفا والمتعلقة بأهمية ثورة المعلومات خاصة فيما يتعلق بالحد من تسلط الأنظمة المستبدة وتنوير الرأي العام المحلي والعالمي وجعل الأفراد على دراية تامة بما يجري ويدور من أحداث حولهم من خلال سرعة الحصول على المعلومات وانتشارها بشكل كبير، إلا أن هاته الثورة أثرت سلبا على سيادة الدول من خلال العديد من المظاهر وفي مقدمتها الجريمة المعلوماتية.

إذن ما معنى الجريمة المعلوماتية؟

تعرف على أنها:

"كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها"[3].

"كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة باعتبارها من المصالح المتطورة التي تمتد مظلة قانون العقوبات لحمايتها"[4].

لقد تبنى مؤتمر الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين مؤخرا تعريفا شاملا جامعا لها مفاده أن:

---

[1] - نقلا عن: المرجع نفسه، ص: 117.

[2] - المرجع نفسه، المكان نفسه.

[3] - نقلا عن: أمينة حمشاشي، "ماهية الجريمة المعلوماتية"، في: دورية دراسات وأبحاث، العدد: 1، 209، ص: 452.

[4] - نقلا عن، المرجع نفسه، ص: 451.

"هي أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية او داخل نظام الحاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"[1].

من خلال هذه التعريفات المذكورة أعلاه نلمس جيدا بأن الجريمة المعلوماتية من أخطر الجرائم التي أصبحت تهدد أمن الفرد، الدولة والمجتمع ككل، ولهذا سننتقل إلى توضيح أهم وأخطر الجرائم التي ساهمت في ظهورها التكنولوجيا العالية ألا وهي "**الجوسسة الاقتصادية الالكترونية**" إذن ما معنى الجوسسة الاقتصادية الالكترونية؟ وكيف ساهمت في اختراق سيادة الدول؟

1- تعريف الجوسسة الاقتصادية الالكترونية:

يقصد بجريمة الجوسسة الاقتصادية الالكترونية سرقة الأسرار التجارية بغرض الحصول على معلومات دقيقة وحساسة والتي تمكن من تحقيق ميزة تنافسية ومنافع تجارية أو حتى تحطيم الخصم وإرباكه وإلحاق الخسائر به[2].

وغالبا ما تحدث عملية التجسس الاقتصادي من خلال الاعتماد على شخص من المنظمة أو المؤسسة المراد اختراقها، كما يمكن حصول ذلك عن طريق استغلال الثغرات التي عادة ما توجد في الأنظمة المعلوماتية المستخدمة في أعمال الشركات والمؤسسات الاقتصادية[3].

إذن التجسس الاقتصادي يعتبر نمطا من أنماط الجريمة المعلوماتية والتي يعاقب عليها القانون لأنه يقوم على خاصية اختراق أمن وسلامة الافراد، المؤسسات وحتى الدول وفيما يلي سنعالج نقطة أخرى تتعلق بمدى تأثير جريمة الجوسسة الاقتصادية الالكترونية على أمن وسيادة الدول.

---

[1] - نقلا عن: المرجع نفسه، المكان نفسه.

[2] - الموسوعة، "التجسس الاقتصادي. سرقة الاسرار التجارية لتدمير المنافسين"، على الرابط الالكتروني: https://www.algazeera.net/encyclopedia/2022/8/1/ ، تاريخ الدخول: 2025/05/12، ساعة الدخول: 23:23.

[3] - المرجع نفسه.

2- تأثير جريمة الجوسسة الاقتصادية الالكترونية على أمن وسيادة الدول:

تهدف جريمة الجوسسة الاقتصادية الالكترونية إلى ما يلي:

– زعزعة أمن الدول والحكومات، حيث تصبح هذه الأخيرة في حالة قلق دائم ومستمر بشأن معلوماتها الاقتصادية السرية وتصبح محل مساومة في شكل اقتصادي أو سياسي أو عسكري من قبل الهاكرز أو المتجسسين[1].

– تعتبر جريمة الجوسسة الاقتصادية مدخلا من مداخل تدمير اقتصاديات الدول وعلى اختلاف طبيعتها في حال عدم امتلاك هذه الأخيرة لنظام أمنى معلوماتي قويا وفعالا، فهي تؤثر في غالب الأحيان على المداخيل المالية للدول[2].

– بإمكان المتجسس الاقتصادي الالكتروني سواء كان فرد أو دولة أو حكومة أن يستغل فئة المواطنين الفقراء الذي يعيشون في كنف دولة متخلفة سائرة في طريق النمو من خلال استدراج هذه الفئة واغرائها بالمال وما شابه مقابل زعزعة استقرار النظام ونشر أفكار توحي بعدم شرعيته من خلال إمكانية القيام بانقلابات عسكرية ، وقد اعتبر في هذا السياق المتحدث باسم "**الكرملين" الروسي ديمتري بيسكوف**" أن مجموعة "**البريكس**" تعتبر أن التجسس الالكتروني هو عبارة عن إرهاب وتهديد أمني يهدد سلامة الفرد، الدولة والمجتمع ككل، إذن جريمة الجوسسة الاقتصادية تؤثر بشكل كبير على الأمن الدولي فاليوم توسع مفهوم الأمن ولم يعد يقتصر على تلك الصفة التقليدية بل ظهرت مفاهيم جديدة بخصوصه وعلى رأسها الأمن السيبراني أو ما يسمى بالأمن المعلوماتي[3].

إذن تمثل الجوسسة الالكترونية الاقتصادية واحدة من بين أخطر التهديدات الأمنية التي تهدد سلامة الفرد، الدولة والمجتمع وهذا إن دل على شيء إنما يدل على أن مظاهر السيطرة تغيرت في عالم اليوم هذا العالم المعولم، فقديما مثل الاستعمار التقليدي والحروب المسلحة والنزاعات المسلحة آليات مباشرة للضغط والهيمنة، أما اليوم وبحكم الثورة المعلوماتية

---

[1] - خواص نصيرة، "الجوسسة الاقتصادية الالكترونية، الوجه الجديد للجرائم المعلوماتية الماسة بأمن الدولة"، في مرجع: كوثر مازوني، الجريمة المعلوماتية أعمال ندوة وطنية، ط.1، الجزائر: منشورات دار الخلدونية، 2022، ص: 150.

[2] - المرجع نفسه، ص: 151.

[3] - المرجع نفسه، المكان نفسه.

والتكنولوجيا تغيرت أساليب السيطرة على الشعوب المغلوبة على أمرها فظهرت جرائم المعلوماتية، ولعل من بين أبرزها – إضافة للتي ذكرناها سابقا- نجد التدخل في الشؤون السياسية بطريقة غير مباشرة من خلال التواصل مع أفراد عبر شبكات التواصل الاجتماعي الافتراضية لبث التفرقة وزعزعة أمن الدولة والنظام ، كذلك انتهاك الخصوصية الوطنية والتحكم في تدفق المعلومات، وهذا ما تقوم به بعض الشركات الأجنبية من خلال احتكارها للبنية التحتية للاتصالات والمنصات الرقمية.

تأسيسا على ما سبق نستطيع القول بأن ثورة المعلومات نعمة ونقمة في الوقت ذاته بحكم أنها نقلة نوعية في تاريخ العلم والمعرفة وفرت مزايا عديدة للأفراد والمجتمعات والدول، لكن في المقابل الكثير من جزم بأنها آليات هيمنة وسيطرة نستطيع أن نطلق عليها تسمية الاستعمار المقنع الغير مباشر بحكم أنها تمثل آلية من آليات اختراق السيادة الوطنية نظرا لتراجع فاعلية العامل الجغرافي وظهور تحدي الحدود السيبرانية.

رابعا-آليات التصدي لعمليات اختراق أمن وسيادة الدول

قبل الشروع في ذكر آليات وسبل مواجهة تحديات اختراق أمن وسيادة الدول لا بد من أن ننطلق من فكرة أساسية مفادها أن السيادة الوطنية بمفهومها التقليدي تعبر عن عدم التدخل في شؤون الدولة الداخلية، وبالتالي فإن الدولة تمارس سيادتها المطلقة على اقليمها وحدها.

فسيادة الدول تعني بشكل عام حرية الدولة في التصرف داخل اقليمها وخارجه لكن بشرط لا بد من أحذه بعين الاعتبار ألا وهو الأطر القانونية المبينة من خلال قواعد القانون الدولي العام العرفية والاتفاقية[1].

في غالب الأحيان نعتبر السيادة سلطة الدولة العليا التي لا تخضع لسلطة أعلى منها على المستوى الخارجي، كما أنها لا تخضع داخليا إلى سلطة أخرى منافسة لها -أو بالأحرى - منافية لمبادئها وقيمها الأيديولوجية فهي في الواقع مجموعة من الممارسات قد تكون مطلقة لا

[1] - نغم إسحاق زيا، القانون الدولي الإنساني والقانون الدولي لحقوق الانسان، الإسكندرية: دار المطبوعات الجامعية، 2009، ص: 62.

تحدها حدود أو نسبية تقيدها قواعد القانون الطبيعي، لكن السيادة تبقى مقيدة بإرادة الدولة نفسها أو بالقانون الدولي الذي يعبر بحد ذاته عن تلك الإرادة[1].

مبدأ السيادة وكما هو معلوم ينجر عنه منطقيا واجب عدم التدخل في الشؤون الداخلية للدول هذا الالتزام المكرس في المادة الثانية من الفقرة السابعة لميثاق الأمم المتحدة، لذا نجد أن الدول في الغالب كثيرا ما تمسكت بالاختصاص الشخصي وحقها الكامل في تنفيذ القوانين على إقليمها عبر سلطاتها التشريعية والتنفيذية فاعتمادا على هذا الطرح نستطيع القول والتسليم بأن العائق الرئيسي لتطبيق حقوق الانسان ووضع أحكامها حق التطبيق يكمن في السيادة[2]

وعلى الرغم من تكريس هذا المبدأ عمليا في الكثير من الحالات والمناسبات إلا أنه تجدر بنا الإشارة بأن الفترة التي أعقبت الحربين العالميتين الأولى والثانية أدت إلى ضرورة تكثيف الجهود دوليا نحو حماية حقوق الانسان وعدم المساس بها بأي شكل من الأشكال فبرزت مفاهيم أخرى منافية إلى حد كبير للسيادة وفي مقدمتها نجد التدخل الإنساني من أجل حماية الفئات المستضعفة، وهذا ما جعل من السيادة تتقلص وتتغير في مفهومها نحو تكريس قضية النسبية، ناهيك عن بروز ظاهرة العولمة وما أفرزته من آثار جعلت من الدولة فاعلا ليس رئيسيا في العلاقات الدولية بل برزت العديد من الفواعل التي أضحت تنافس هاته الدولة، وكذلك وكمرحلة جديدة من مراحل العولمة دخل العالم في حقبة جديدة هي حقبة تفجر المعلومة وانتشارها بشكل سهل، مرن وسريع وهذا بدوره ما أنتج إشكاليات عديدة تتعلق بآليات حماية سيادة الدولة في ظل هذه المتغيرات فبرز مفهوم جديد ألا وهو السيادة الرقمية للدول. والتي أصبحت مهددة من قبل مجموعة من الأفراد والمنظمات واللوبيات، وفيما يلي سننتقل إلى عرض أهم السبل والآليات التي بإمكانها ليس القضاء على التهديدات وإنما الحد منها.

[1] - الأمين شريط، حق السيادة القائمة على الثروات الطبيعية، الجزائر: ديوان المطبوعات الجامعية، د.س.ن، ص: 17.
[2] - محمد بسلطان، مبادئ القانون الدولي العام، ج.2، الجزائر، دار الغرب للنشر والتوزيع، 2002، ص 282.

وبما أننا ركزنا في بحثنا هذا على واحد من بين أنماط الجرائم المعلوماتية الأكثر تهديدا لأمن الدول والممثلة في الجوسسة الالكترونية الاقتصادية سنحاول تبيان مجموعة من الآليات ذات الطابع الدولي التي استحدثت بغرض حماية أمن الدول سندرجها في النقاط التالية:

– لقد سعت الجهود الدولية في العديد من المناسبات نحو مكافحة الجريمة المعلوماتية وفي مقدمتها جريمة التجسس الاقتصادي الالكتروني، ولهذا قامت في العام **2001** بإبرام اتفاقية بودابست والمتعلقة بمكافحة هذا النوع من الجرائم المعلوماتية.

– من أجل حماية الفرد الدول والمجتمعات على حد سواء وجب تسريع عملية تنسيق الجهود الدولية والتعاون المشترك من خلال تبادل المعلومات وتعقب الهاكرز المتجسسين، ناهيك عن الدور المهم لشرطة الأنتربول الدولية وما يمكن أن تحققه من مزايا حول هذا الخصوص.

– ضرورة العمل نحو تعزيز مسألة التعاون الإقليمي في مجال الأمن خاصة بالنسبة لدول قارة افريقيا من خلال المنظمات الخاصة وفي مقدمتها الأفريبول.

– يعتبر التعاون القضائي واحد من أهم السبل التي بإمكانها الحد من هذه الجرائم ولهذا وجب على الدول أن تتبنى اتفاقيات قضائية ثنائية ومتعددة الأطراف لاستلام وتسليم المجرمين المخترقين الكترونيا، ونشر أوامر بالقبض على المبحوثين دوليا[1].

إضافة إلى تكثيف الجهود الدولية الرامية إلى مكافحة الجريمة المعلوماتية بصفة عامة والتجسس الالكتروني الاقتصادي يجب تقنين تشريعات وطنية للحد منها، كما يجب على تلك التشريعات من أن تحدد نمط الجريمة أولا، وتقوم بضبط عناصرها ثانيا، وتحد من الآثار الناتجة عن عملية مكافحتها ثالثا.

رأى الدكتور "**منصور رحماني**" بخصوص هذه المسألة:

"لا ينسب النجاح إلى أي تشريع فيما وضع لأجله إلا إذا تحققت فيه أربعة عناصر، أولها أن يؤدي الغرض الذي وضع من أجله، وثانيها أن يتم ذلك في أقل زمن، وثالثها أن يكون

[1] - المرجع نفسه، ص: 153-

ذلك الغرض قد تحقق بأقل ما يمكن من التكاليف، وآخرها ألا تكون سلبياته أكثر من إيجابياته فإذا انعدم عنصر واحد من هذه العناصر لم يكن التشريع ناجحا ولا فعالا فيما وضع من أجله، وفي موضوع مكافحة الجريمة فإن النجاح مرهون بالتقليل من نسبها في زمن قياسي، مع اجتناب التكاليف الباهظة والإفرازات السلبية التي تخلفها عملية المكافحة"[1].

من خلال رأي الدكتور "**منصور رحماني**" نلمح جيدا بأن الرشادة والعقلانية أساس وضع التشريعات المتعلقة بالحد من الجريمة المعلوماتية وقد فسر ذلك من خلال تركيزه على مسألة الجهد، الوقت والتكاليف، وبالرجوع إلى آثار تلك التشريعات أكد على ضرورة طغيان الآثار الإيجابية أكثر من السلبية حتى يتسنى تحقيق الغرض الذي جاء من أجله.

وفي نفس السياق نستطيع القول بأن الآليات التقنية لمكافحة الجريمة الإلكترونية* أو ما يعرف بأمن المعلومات تعتبر حلا أمثلا في هذه الحالة ولعل أبرز تلك الآليات نجد ضرورة تفعيل برامج الحماية ضد البرامج الخبيثة والممثلة في الفيروسات المدمرة، أيضا لا بد من فصل الشبكات الداخلية عن شبكة الأنترنيت، إضافة إلى ضرورة استخدام تكنولوجيا كشف أجهزة التجسس الالكترونية وانشاء مراكز خاصة بمكافحة التجسس الالكتروني وتكوين هاكرز خاص بمكافحة الاختراقات.

[1] - نقلا عن: حكيم سياب، المرجع السابق الذكر، ص: 135.

* للمزيد من المعلومات والتفاصيل حول الآليات التقنية لمكافحة الجريمة الإلكترونية راجع في ذلك: محمد عطا أحمد عبد العزيز، آليات منظمات مكافحة الجرائم الالكترونية وتحقيق الأمن الاجتماعي"، في: مجلة الخدمة الاجتماعية، المجلد: 62، العدد: 6، 2019.

الخاتمة

في ظل التهديدات السيبرانية المتزايدة والمستمرة في عصرنا الحالي شهد مفهوم السيادة الوطنية للدول تحولا نوعيا يستدعي إعادة النظر في المفهوم التقليدي للسيادة كما أقرته معاهدة وستفاليا سنة **1648**، فبينما كانت السيادة تفهم سابقا على أنها حق مطلق للدولة في إدارة شؤونها الداخلية دون أي تدخل خارجي، فإن الفضاء السيبراني بطبيعته اللامركزية والعابرة للحدود قد فرض واقعا جديدا يضعف من قدرة الدولة على احتكار القوة والسيطرة داخل حدودها.

لقد باتت التهديدات الرقمية مثل التجسس الالكتروني والهجمات السيبرانية وحروب المعلومات تشكل تحديا مباشرا للسيادة التقليدية، إذ أصبح بالإمكان التأثير على البنية التحتية الحيوية والمؤسسات السياسية، وحتى الأمن المجتمعي دون الحاجة إلى تدخل عسكري مباشر أو عبور الحدود الجغرافية.

وعليه فإن إعادة دلالة مفهوم السيادة اليوم يتطلب ادماج عناصر جديدة تتعلق بالسيادة الرقمية، والقدرة على الدفاع السيبراني وضمان أمن البيانات والمجالات الافتراضية، وهذا يتطلب تعاونا دوليا لإرساء قواعد قانونية وأخلاقية تحكم الفضاء السيبراني مع الحفاظ على خصوصية السيادة الوطنية ضمن توازن دقيق بين الأمن والانفتاح الرقمي.

من هنا فإن التحدي الأكبر اليوم أمام الدول ليس فقط حماية حدودها الرقمية بل أيضا تطوير مفهوم السيادة عصري قادر على التكيف مع طبيعة التهديدات السيبرانية التي لم تعد تعترف بحدود وستفاليا الجغرافية.

قائمة المراجع

أولا-المصادر

القرآن الكريم.

ثانيا-الكتب

1. إسحاق زيا، نغم، القانون الدولي الإنساني والقانون الدولي لحقوق الانسان، الإسكندرية: دار المطبوعات الجامعية، 2009.

2. بوكرا، ادريس، الوجيز في القانون الدستوري والمؤسسات السياسية، القاهرة: دار الكتاب الحديث، 2003.

3. بسلطان، محمد، مبادئ القانون الدولي العام، ج.2، الجزائر، دار الغرب للنشر والتوزيع، 2002.

4. بوراس، عبد القادر، التدخل الدولي الإنساني وتراجع مبدأ السيادة الوطنية، دار الجامعة الجديدة، 2009.

5. بوشعير، سعيد، القانون الدستوري والنظم السياسية المقارنة، ج.1، ط.5، الجزائر: ديوان المطبوعات الجامعية، 2002.

6. الجمل، يحيى، الأنظمة السياسية المعاصرة، بيروت: دار النهضة للطباعة والنشر، د.س.ن.

7. حسن عبد الله، انعكاسات العولمة على السيادة الوطنية، ط.1، عمان: دار كنوز المعرفة العلمية للنشر والتوزيع، 2009.

8. مازوني، كوثر، الجريمة المعلوماتية أعمال ندوة وطنية، ط.1، الجزائر: منشورات دار الخلدونية، 2022.

9. مسعد، عبد الرحمن زيدان، تدخل الأمم المتحدة في النزاعات المسلحة غير ذات الطابع الدولي، ط.2، مصر: دار الكتب القانونية، 2008.

10. نعيم الظاهر، إبراهيم، إدارة الدولة والنظام السياسي الدولي، ط.1، الأردن: عالم الكتب الحديث للنشر والتوزيع، 2010.

11. نصر مهنا، محمد، علم السياسة، القاهرة: دار غريب للطباعة والنشر والتوزيع، د.ت.ن.

12. سياب، حكيم، الاعلام الآلي والقانون، ط.1، عمان: دار وائل للنشر والتوزيع، 2014.

13. شريط، الأمين، حق السيادة القائمة على الثروات الطبيعية، الجزائر: ديوان المطبوعات الجامعية، د.س.ن.

ثالثا-الدوريات

1. أحمد عبد العزيز، محمد عطا، آليات منظمات مكافحة الجرائم الالكترونية وتحقيق الأمن الاجتماعي"، في: مجلة الخدمة الاجتماعية، المجلد: 62، العدد: 6، 2019.

2. حمياز، سمير، "إشكالية السيادة الوطنية في ظل المتغيرات في ظل المتغيرات الدولية الراهنة"، في دورية: الآداب والعلوم الاجتماعية، العدد: 1، 2017.

3. حمشاشي، أمينة، "ماهية الجريمة المعلوماتية"، في: دورية دراسات وأبحاث، العدد: 1، 209.

4. سحاري، مصطفى، "السيادة الوطنية للدول في ظل ثورة المعلومات"، في مجلة: المعيار، المجلد: 10، العدد: 4، ديسمبر 2019.

المواد العلمية الالكترونية:

1. مجدي، خليل، التدخل الأجنبي والتدخل الدولي، الحوار المتمدن، على الرابط الالكتروني: https://www.ahewar.org/débat/show.artK، تاريخ الدخول: 2012/12/10، على الساعة: 21:10.

2. الموسوعة، "التجسس الاقتصادي. سرقة الاسرار التجارية لتدمير المنافسين"، على الرابط الالكتروني:

3. https://www.algazeera.net/encyclopedia/2022/8/1/ ، تاريخ الدخول : 2025/05/12، ساعة الدخول : 23:23.

الباب الثاني

آليات وتحديات الذكاء الاصطناعي في إطار تعزيز السيادة الرقمية وتحقيق الأمن السيبراني

Chapter 01

Artificial Intelligence and its Applications to Enhance Cybersecurity

الذكاء الاصطناعي وتطبيقاته في سبيل تعزيز الأمن السيبراني

Dr. Belbey ikram

Lecturer A, Faculty of law and political sciences, University of Mostaganem, Algeria

Laboratory of human rights and public freedoms

ikram.belbey@univ-mosta.dz

Abstract

This study aims to identify the role of artificial intelligence and its applications in enhancing cybersecurity and protection from cyber threats; It concluded that artificial intelligence technologies are essential tools in the future of information security, as they help provide solutions to the increasing problems with the increase in cyber threats and the complexity of attackers' methods, as with the increase in electronic attacks on institutions and companies in recent years, it became clear that the current approach to cybersecurity suffers from a chronic weakness in the ability to combat electronic threats; which requires the intervention of artificial intelligence with its technologies and applications to solve these problems.

Keywords: Artificial intelligence; Cybersecurity; Applications; Expert systems; Smart weapons.

الملخص:

تهدف هذه الدراسة إلى تحديد دور الذكاء الاصطناعي وتطبيقاته في تعزيز الأمن السيبراني والحماية من التهديدات السيبرانية؛ وخلصت إلى أن تقنيات الذكاء الاصطناعي هي أدوات أساسية في مستقبل أمن المعلومات، حيث تساعد في تقديم حلول للمشكلات المتزايدة مع زيادة التهديدات السيبرانية وتعقد أساليب المهاجمين، حيث أنه مع تزايد الهجمات الالكترونية على المؤسسات والشركات خلال الأعوام الماضية، بدا واضحا أن النهج الحالي للأمن السيبراني يعاني ضعفا مزمنا في القدرة على مكافحة التهديدات الالكترونية؛ مما يستدعي تدخل الذكاء الاصطناعي بتقنياته وتطبيقاته لحل تلك المشكلات.

الكلمات المفتاحية: ذكاء اصطناعي؛ أمن سيبراني؛ تطبيقات؛ النظم الخبيرة؛ الأسلحة الذكية.

Introduction:

In recent years, we have witnessed rapid developments in the field of technology, and among these amazing developments were the progress in the fields of artificial intelligence and cybersecurity.

These two technologies have radically transformed the way we deal with data, information, and communication over the Internet. Since the emergence of the Internet and the emergence of electronic and information technology at the dawn of the third millennium, societies have changed rapidly and radically, as the increasing importance of knowledge, along with globalization and the implications of technological development in the era of the Fourth Industrial Revolution, have created a completely different world.

This is because this Fourth Industrial Revolution, which differs from previous revolutions in its intensity, complexity, and scope, is based in essence on a new technological phenomenon called digital transformation, i.e. the integration of technology that includes the Internet of Things, cloud computing, big data analytics, and artificial intelligence, and thus businesses and societies have found themselves facing unprecedented opportunities and challenges.

However, these challenges have become more severe with the explosion in the circulation and spread of information and data. This data has become necessary for societies and organizations to protect according to many mechanisms. Reliance on cybersecurity has emerged to protect information and prevent access to sensitive data.

It has become imperative to employ artificial intelligence to achieve cybersecurity, due to the increasing reliance of computer systems on the Internet and wireless networks to store and exchange information[1].

The objectives of the study are to identify artificial intelligence and its uses, as well as cybersecurity and its dimensions; in addition to the necessity of knowing the impact of artificial intelligence and its applications on cybersecurity.

As for the importance of this research, it is highlighted by explaining the concept of both artificial intelligence and cybersecurity. It is also expected that this study and its results will help those interested in information and security to identify and understand risks, in addition to a future outlook on this topic, especially with regard to the context of artificial intelligence in the security field, as artificial intelligence overlaps with cybersecurity, and the common denominator between them lies in the fact that all operations occur in one common space, which is cyberspace.

The problem of this study lies in determining the extent of the effectiveness of artificial intelligence in protecting and enhancing cybersecurity? Have these applications contributed to solving the problem of cyber threats? What are the proposed solutions to activate cyber artificial intelligence?

We will answer this problem according to the following two sections:

[1] Khalil Saidi and Marzouq Bin Mahdi, Artificial Intelligence as an Inevitable Trend in Protecting Cybersecurity, Journal of Studies in Human Rights, Volume 6, Issue 1, 2022. P. 26.

Section One

The Concept of Artificial Intelligence and Its Importance in the Field of Cybersecurity

The concept of both artificial intelligence and cybersecurity will be addressed, as well as highlighting the importance of using artificial intelligence in the field of cybersecurity, according to the following two requirements:

A: The concept of artificial intelligence and cybersecurity

In this requirement, we will address the various concepts under study, as follows:

1: The concept of artificial intelligence

The term AI coined in 1956 can be defined as a system ability to correctly interpret to learn from external data and to Leverage the Learning to achieve specific objectives truth flexible adaptation[1]. Artificial intelligence, abbreviated as (AI), is a branch of computer science, and one of the basic pillars on which the technology industry is based in the current era. The term artificial intelligence (AI) refers to systems or devices that simulate human intelligence to perform

[1] Mohiuddin Ahmed and others, explainable artificial intelligence for cybersecurity, springer nature Switzerland, 2022. P 2.

tasks and that can improve themselves based on the information they collect[1].

Despite the importance of artificial intelligence in the world of technology, there is no comprehensive and agreed-upon definition of artificial intelligence, as it is more of a field than a concept that can be easily defined. The approved definitions of artificial intelligence have varied according to the specialization in which it developed. Artificial intelligence is derived from fields other than computer science; such as psychology, neuroscience, cognitive science, philosophy, linguistics, probability, and logic. Accordingly, artificial intelligence as a cognitive field can be divided into many subfields that overlap greatly, such as machine learning and robotics, then neural networks and vision, as well as natural language processing and speech processing[2].

As for the great jurists, Alin Turing defined it as "the ability to act as if a human being is acting by trying to deceive the interrogator and appear as if a human being is answering the questions posed by the interrogator."

John McMarthy defined it as "the science and engineering of making intelligent machines, especially", and in contrast, Kurzweil, one of the most famous researchers in the field of artificial

[1] Balasal Bint Nabi Yasmine and Amroush Al-Hussein, Artificial Intelligence and Its Role in Achieving Sustainable Development, Journal of Legal and Economic Studies, Volume 5, Issue 1, 2022. P. 1155.

[2] Andersen, L, Human Rights in the Age of Artificial Intelligence, November 2018. P8. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf.

intelligence, defines it as "the art of making machines capable of performing operations that require intelligence as humans do"[1].

From all of the above, artificial intelligence can be defined as "a means of controlling a computer or robot by a program that thinks in the same way as intelligent humans think."

This means that artificial intelligence is one of the modern computer sciences that seeks advanced methods for programming it to perform tasks and conclusions similar to the methods attributed to human intelligence, by understanding the complex mental processes that the human mind performs while thinking and translating them into equivalent mathematical processes that increase the computer's ability to solve complex processes. However, this does not mean at all that we are now facing intelligent machines that think with the same concept of human intelligence and thinking, or that we are facing a machine that has engaged in a type of perception or feeling similar to the level of human perception and feeling[2].

In fact, through studies, it becomes clear that artificial intelligence has a special nature as it mimics human intelligence, and this is evident through several characteristics and features[3], the most

[1] Amir Farag, Civil and Criminal Liability Provisions for Operating Artificial Intelligence Robots for the Damages They Cause, University Publications House, Alexandria, 2023. p. 25.

[2] Mustafa Abu Mandour Musa Issa, the Adequacy of General Rules of Civil Liability in Compensating for Artificial Intelligence Damages: An Analytical and Comparative Study, Damietta Law Journal for Legal and Economic Studies, Issue 5, January 2022. pp. 214-215.

[3] In addition to the above, some characteristics of artificial intelligence can be added as follows:

important of which is its ability to learn and perceive, and thus its independence in making some decisions. Artificial intelligence is also characterized by accuracy and speed in some tasks[1].

Although it is difficult to limit the importance of artificial intelligence, especially due to the continuous and rapid development in artificial intelligence, it can be referred to in some points as follows:

- Artificial intelligence contributes to preserving the accumulated human experiences by transferring them to smart machines;

- It enables humans to use human language in dealing with machines instead of computer programming languages, which makes the use of machines available to all segments of society, after dealing

- Artificial intelligence is used to solve problems presented in the absence of complete information.
- The ability to think, perceive, and achieve quick and effective results and conclusions.
- The ability to discover knowledge and apply it within the available capabilities.
- The ability to learn and understand from previous experiences and expertise.
- The ability to use old experiences and employ them in new situations better and faster.
- The ability to use trial and error to explore controversial matters, while increasing the ability to respond quickly to new and different situations and circumstances, and difficult and complex cases.
- The ability to develop, innovate, understand and perceive visible matters.
- The ability to provide important information to support immediate decisions.

See: Ammar Yasser Al-Babli, The Role of Artificial Intelligence Systems in Predicting Crime, Police Thought Journal, Volume 28, Issue 110, July 2019. p. 146.

[1] Belbey Ikram, Artificial Intelligence in International Law: A Study of the Concept, Frameworks and Applications, Legal Book Foundation and Ibn al-Nadim for Publishing and Distribution, Algeria, 2024. p. 39.

with advanced machines was the preserve of specialists and those with experience;

- Artificial intelligence plays an important role in many sensitive fields such as helping to diagnose diseases and prescribe medications, legal and professional consultations, interactive education, security and military fields, and other fields;

- Smart systems contribute to the fields in which decisions are made, as these systems enjoy independence, accuracy and objectivity, and therefore their decisions are far from error, bias, racism, prejudice, or even external or personal interference;

- The application of artificial intelligence will contribute to achieving the goals of sustainable development; Goal 7 (Affordable and Clean Energy), Goal 13 (Climate Action), Goal 14 (Life Below Water) and Goal 15 (Life on Land)[1].

— Artificial intelligence is already helping to build sustainable smart cities.

— Artificial intelligence can help people with disabilities or special needs in many ways, and artificial intelligence is best used in translating from text to voice and from voice to text, thus it can help

[1] Ahmed Al-Saleh Saba'a and others, Implementing the Artificial Intelligence Strategy at the International Level (The United Arab Emirates as a Model), Al-Mayadeen Economic Journal, Volume 1, Issue 1, 2018. p. 34.

people with visual impairments or hearing impairments in using information and communication technology.

— Smart machines reduce a lot of risks and psychological pressures on humans, and make them focus on more important things, by employing these machines to do hard and dangerous work, explore unknown places, and participate in rescue operations during natural disasters, and they have an effective role in fields that include many complex details, which require exhausting mental focus and continuous mental presence, and sensitive and quick decisions that do not tolerate delay and error, such as quick security decisions.

— Understanding and analyzing data and information that is rapidly growing[1].

2: The concept of cybersecurity

The term cybersecurity is new, as its emergence was linked to the technological revolution. The definitions of this term have differed according to the nature of countries, as well as the strategy they adopt in providing it.

We provide some of these definitions as follows: Letho Marti and Neittaanmaki Pekka define it as: "A set of measures taken to defend against computer hacker attacks and their consequences, and includes implementing the required countermeasures.

[1] Balbey Ikram, previous reference, p. 48.

Edward Amorso defines it as: "It is the means that can reduce the risk of attack on computers or networks, including the tools and means used to confront hackers."[1].

Cybersecurity can be defined as a combination of processes involved in saving an individual's or organization's data online and offline. Cybersecurity is defined as: "the security of networks, information systems, data and devices connected to the Internet", and therefore relates to the preventive measures and standards that must be taken and adhered to in order to confront threats and prevent violations or unauthorized access, to reduce their impact.

It is also defined as: "measures to reduce the risk of attacks on programs, computers or controls, including the means and tools used".

Cybersecurity, based on its objectives, is an activity that ensures the protection of human and financial resources related to information and communications technology, and the possibility of reducing losses and damages that lead to the realization of risks and threats, and perhaps the expansion can be restored as quickly as possible. The extent to which the wheels of production do not stop, and the damage does not turn into a loss, depends on whether the activities, functions, capabilities or information contained in

[1] Ben Adeed Samia, Cybersecurity and Information Security Risks and the Development of Technical Knowledge on Information Systems Protection Programs, Journal of Information Security and Digitization of the Higher Education and Scientific Research Sector, p. 6.

information and communications systems are protected from malicious elements or use or misunderstanding or misuse[1].

It is worth noting that cybersecurity is a term used to describe the capabilities of a country, organization or company to protect against viral attacks. There are many tools that have been used, as we have previously explained, to assess the status of cybersecurity. - An example of this tool - is the Global Cybersecurity Index of the International Telecommunication Union. It is a capacity building tool that assesses countries' commitment to cybersecurity and identifies their capabilities and areas for improvement. The cybersecurity status of countries can be assessed based on their development in the five pillars (legal, technical, regulatory, capacity building and cooperation)[2].

Cybersecurity has several features, the most important of which are:

- Cybersecurity is not a one-time course of action; rather, it is an ongoing process and contains innovative defense mechanisms as it confronts threats to systems, networks, etc.

- It works to create a secure cyber ecosystem and establish a reliable system.

[1] Mohamed Dahmani, Artificial Intelligence as a Mechanism to Enhance Cybersecurity, Journal of Legal and Political Thought, Volume 7, Issue 2, 2023. p. 603.

[2] Khaled Dhaher Abdullah Jaber Al-Suhail Al-Mutairi, The Role of Criminal Legislation in Protecting Cybersecurity in the Gulf Cooperation Council Countries, Journal of Legal and Jurisprudential Research, Issue 38, 2022. P. 987.

- It carries out a preemptive control process with the aim of searching for risks, working to solve them, and closing loopholes.

- It works on subsequent defense, which is represented by the rule of returning the situation to what it was.

- It provides the feature of alerting to the presence of an error or misuse of networks that expose data and information to danger from within institutions; and also covering external risks and monitoring threats.

As for the dimensions of cybersecurity, they can be summarized as follows:

Military dimensions: Cybersecurity plays an important role in the process of exchanging important information between military institutions electronically and virtually without hacking this communication, which is positively reflected in achieving the military objectives of countries.

Political dimensions: Cybersecurity plays an important role in political life, as this role has increased in light of citizens' reliance on social networking sites in their daily lives and modern technologies, as cybersecurity has a role in parliamentary election campaigns, electronic protests, and others.

Economic and social dimensions: The economic dimension is related to two main areas, the first: the information and communications technology industry, which includes the development and production of devices and software, and the

second: e-commerce by opening a free market on the Internet, and one of the most famous examples is providing electronic wallet services.

The cybersecurity market can also grow at the GCC level by relying on purchasing cybersecurity products and services from technologies related to protecting devices and detecting cyber threats.

The social dimension is related to the frequency of communication between individuals through blogs, email and social networking sites, which constitutes what can be called the cross-border and transnational audience or the virtual world audience, and therefore it is necessary to secure these networks and sites. However, on the contrary, it may expose the morals of societies to danger and cause a threat to the social peace of countries.

The social dimension is also linked to scientific, cultural, and service fields, as it allows access to remote areas and specific groups, such as the elderly, the sick, and others with special needs. In addition to the role it can play in exchanging information during times of humanitarian crises and disasters, the social dimensions do not stop at providing citizens with reassurance in their daily lives and benefiting from the energies of information and communication technologies in developing their various activities, but rather extend beyond that to maintaining the essential values in society: such as belonging and beliefs.

Legal dimensions: The revolution in information, communications and technology in general has resulted in modern

patterns of behavior that constitute violations that entail criminal and civil liability. This has also resulted in the imposition of modern legislative frameworks for crimes committed against cyberspace to keep pace with these rapid developments in technology and to activate the foundations of joint international cooperation to combat cybercrime.

One of the most prominent legal practices in the field of cybersecurity is guaranteeing some rights in this field, the most important of which are: the right to access the information network, and the new forms related to the use of information and communications technology, such as the right to create electronic blogs and the right to own cultural programs[1].

B: The importance of using artificial intelligence in the field of cybersecurity

The benefits and importance of using artificial intelligence-powered cybersecurity tools and systems are as follows:

1: Technological progress and cybersecurity challenges

As technology advances, the challenges facing cybersecurity have increased. While the digital age provides great advantages and opportunities, it also opens the door to new risks. Individuals, companies and governments face threats from cybercriminals,

[1] Khaled Zahir Abdullah Jaber Al-Suhail Al-Mutairi, the previous reference, pp. 1006-1009.

hackers and cyber breaches, so protecting systems and data requires the use of advanced technologies, such as artificial intelligence.

2: Uses of artificial intelligence in protecting systems and data

Artificial intelligence plays a crucial role in protecting systems and data from increasing threats in the world of cybersecurity, and among some of the main uses of artificial intelligence in this field we find:

— **Threat detection**: AI can recognize the behavior pattern of cyber attacks and detect potential threats before they occur, helping to take preventive measures.

— **Data analysis**: AI uses deep learning and advanced analysis techniques to understand cyber data and identify patterns and anomalies that may indicate attacks.

— **Enhanced response:** Thanks to AI, a faster and more effective response to breaches and attacks can be developed by detecting and inferring attacks and taking the right measures.

— **Improving network and information security:** AI can improve data classification and encryption, monitor data leaks, and enhance network security in general[1].

[1] Mohamed Gomaa Mohamed El Sayed, Artificial Intelligence and Cybersecurity Technology, Beni Suef University website, at the link: https://www.bsu.edu.eg/Backend/Uploads/PDF/Conference/Artificial%20Intelligence%20and%20Cybersecurity%20Technology.pdf

— **Accelerating detection and response times**: When companies integrate AI with cybersecurity, they ensure rapid detection and response to security threats, as AI scans the entire system and identifies threats early, facilitating security tasks.

— **Combating malicious bots**: There are many bots that are used in malicious activities such as spreading malware and stealing data, and AI has the ability to identify, recognize, and block patterns of these bots.

— **Securing authentication**: AI provides many tools such as fingerprint scanners and facial recognition, which are required to secure authentication during login attempts on sites that contain sensitive information and require an additional layer of security for protection. These tools help detect fraudulent login attempts and cyberattacks aimed at stealing data.

— **Improving accuracy and efficiency**: AI-based cybersecurity systems provide better accuracy and efficiency compared to traditional security solutions, and AI algorithms have the ability to recognize patterns that the human eye cannot detect, which increases the accuracy of detecting malicious activities.[1].

[1] Artificial Intelligence and Cybersecurity: The Relationship, Differences and Challenges Between Them, on Bakkah website, at the link: https://bakkah.com/ar/knowledge-center/الذكاء-الاصطناعي-السيبراني

Section Two

Applications of Artificial Intelligence in the Field of Cybersecurity

Artificial intelligence technologies are essential tools in the future of information security, as they help provide solutions to growing problems. With the increase in cyber threats and the complexity of attackers' methods, the use of systems that learn from data becomes essential. Deep learning algorithms and computer vision are solutions that can help organizations detect and prevent threats before any damage occurs.

This requires expanding the applications of these technologies and integrating them with existing systems to enhance organizations' ability to confront threats. Research in artificial intelligence is expected to continue to develop better tools to confront cyber attacks, which requires government and private institutions to invest in these areas.

Cybersecurity leaders should enhance their strategies by understanding how to use artificial intelligence effectively, and research efforts should be directed towards creating algorithms to analyze past data to predict future threats, which helps secure work environments. Studies show that integrating artificial intelligence into cybersecurity can improve efficiency and security.

However, the ethical and legal challenges related to the use of artificial intelligence in cybersecurity should be taken into account.

This use raises issues around privacy and information security, as algorithms may lead to biases that affect security decisions, so it is necessary to take measures to manage the associated risks and frameworks should be developed to improve the ethical and security use of this technology and balancing the benefits and risks is important to ensure the integrity of information and promote a culture of security[1].

A: Using artificial intelligence to detect cyber threats

Artificial intelligence is used to detect threats and other potential malicious activities. Traditional systems cannot keep up with the huge number of malware being created. Artificial intelligence intervenes and addresses this problem.

The cybersecurity company teaches artificial intelligence systems to detect viruses and malware using complex algorithms so that the artificial intelligence can run pattern recognition in the programs. Artificial intelligence systems are also trained to identify even the smallest behaviors of ransomware attacks and malware before they enter the system and then isolate them from this system; They can also use predictive functions that exceed the speed of traditional methods, as systems that operate on artificial intelligence open the possibility of natural language processing that automatically

[1] Alaa Abdel Khaleq Hussein and others, Cybersecurity: Principles and Practices to Ensure Information Integrity, Dar Al-Sard for Printing, Publishing and Distribution, Baghdad, Iraq, First Edition, 2024. P. 122.

collects information by activation through articles, news and studies about cyber threats.

This information can provide insight into severe cases, cyber attacks and prevention strategies. This allows cybersecurity companies to stay up to date on the latest risks and timeframes and build responsive strategies to keep organizations protected. AI can also be used to increase network awareness. It can scan for phishing by simulating clicks on email links and analyzing word choice and grammar.

It can monitor network connections for the intended installation of malware, command and control communications, and the presence of suspicious packages. Furthermore, virus detection has been changed from an exclusively signature-based framework that was plagued by issues of reaction time, efficiency, and storage requirements to a behavioral analysis framework that can distinguish unmarked malware and previously unidentified threats[1].

B: Expert systems and smart cyber weapons

Among the applications of artificial intelligence that have shown their fruits in the field of cyber security, we find smart cyber expert systems and smart weapons to confront cyber threats, and they will be studied in the following two sections:

[1] Omar Yasser Al-Babli, Artificial Intelligence in the Face of Confronting Rumors and Terrorist Financing Crimes in the Cyber Environment: Implications and Ways to Confront, Publications of the Arab Administrative Development Organization, Egypt, 2023. pp. 221-222.

1: Smart cyber expert systems

Expert systems are a computer system that simulates human expertise and knowledge in a specific field. Expert systems in artificial intelligence are based on a set of cognitive rules that define the relationships between concepts and ideas in the specific field.

Expert systems are characterized by their ability to analyze information related to the specific problem, identify available and appropriate options for the solution, and recommend the best possible solutions. Therefore, expert systems can be used in a wide range of fields, such as medicine, engineering, commerce, finance, marketing, education, and others[1].

It can be defined as follows: Expert systems are intelligent programs that contain a lot of knowledge and experience possessed by an expert or several experts in one of the fields of knowledge. They use the laws of thinking, logic, common sense, and others, to reach results based on previous knowledge stored in the knowledge base[2].

The great progress in these technologies raises security concerns, including the use of counter-technologies by hackers and the creation of unexpected cyber threats, by attacking entire

[1] Mohammed Alarda, Expert Systems in Artificial Intelligence: Definition and Applications in Reality, Website: Al-Munawwarah, at the link: https://mohammedalarda.com/النظم-الخبيرة-في-الذكاء-الاصطناعي/

[2] Khaled Nasser Al-Sayed, Origins of Artificial Intelligence, Al-Rashd Library Publishers, Kingdom of Saudi Arabia, 2004. p. 189 and following.

networks at a much faster rate that smart cyber expert systems cannot counter.

The relationship between artificial intelligence and cyber security is highlighted in these systems, through self-learning algorithms in countering cyber threats that monitor data entering and exiting networks, isolating strange data, and being prepared to react to sudden cyber threats. Artificial intelligence technology, like machine learning and natural language processing, enables analysts to respond to threats with greater confidence and speed.

Among the most important challenges facing smart cyber expert systems with cyber security are:

- The development of countless applications in which artificial intelligence can be used maliciously by hackers, posing potential security threats, the emergence of new attacks through the use of artificial intelligence systems to accomplish tasks that may be unexpected by terrorist and criminal entities, exploiting the weaknesses of artificial intelligence cyber systems,

- Carrying out cyber attacks using drones containing advanced weapons systems that lead to hacking systems and network sites that are difficult to confront.

- Using threats related to hacking cyber databases, with the aim of accessing privacy, social and political manipulation, and shaping a trend of public opinion.

- The lack of close cooperation between policymakers and legislators with technical researchers to investigate, prevent, and mitigate potential malicious uses of artificial intelligence technologies.

- The lack of practices in research fields with more mature methods and methodologies to address the expected threats of dual-use applications of artificial intelligence cyber and everything related to information security.

Therefore, cyber expert systems can be used in the future to improve the response to sudden cyber threats, and therefore we must take into consideration before starting to develop the cyber expert system, the development of alternative solutions to any security problem so that the expert system is capable of them, in order to confront various threats and challenges.

The requirements for developing the cyber expert system are necessary to make the expert system successful in achieving its goals, and future cyber expert system projects do not start on their own, but sometimes start because there is an urgent need for them, In the end, cyber expert systems can be considered as transferring the expertise of specialists in the field of cyber security to the computer, which means the direct intervention of the human mind in the computer's mind in confronting cyber threats[1].

[1] Alaa Abdel Razzaq Al-Salmi, Introduction to Cyber Artificial Intelligence, Publications of the Arab Administrative Development Organization of the League of Arab States, Egypt, Second Edition, 2024. pp. 148-150.

2: Smart Weapons to Counter Cyber Threats

With the increasing size and complexity of cyber attacks, artificial intelligence helps security operations analysts confront threats, through the smart technologies included in cyber expert systems, that the role of smart weapons that use artificial intelligence technology is focused on helping to detect threats and other malicious activities because traditional systems cannot maintain the absolute number of malware created every month.

Therefore, the cybersecurity company strives to provide defensive smart weapons to protect against threats, through the learning feature that artificial intelligence is characterized by to detect malware and viruses, as well as vulnerabilities in networks and systems, by using complex algorithms that implement sample identification in artificial intelligence programs that automatically collect information through case studies, articles and cyber threats.

Thus, it provides insight into cyber attacks, prevention strategies, and methods of confronting them; The effective role of smart weapons through the cybersecurity system will help achieve a number of sustainable development goals set by the United Nations, including:

- Improving the management of equipment use and maintenance and expanding access to information related to economic interaction between private and public institutions

- Making information and communications technology available to all in a safe and transparent manner, providing great potential to accelerate human progress, bridge the digital divide and develop knowledge societies, as well as scientific and technological innovation in various fields, such as medicine and energy.

- Building trust and providing security in the use of information and communications technologies for sustainable development will be a special priority in light of the growing challenges.

Finally, it can be said that smart cyber weapons, also based on artificial intelligence, protect cybersecurity from attacks, but sometimes they can be detected by criminals. They can be used to pose serious threats to cyberspace, and therefore it is necessary to give an effective role to defensive smart weapons, through a number of tasks that can be given to these weapons in order to confront these threats.

Indeed, when applying these tasks, they gave great results in practice. For example, vulnerabilities were revealed in various areas through abnormal user behavior and other possible anomalies, through which an information breach was detected and dealt with[1].

[1] Alaa Abdel Razzaq Al-Salami, previous reference, pp. 187-189.

Conclusion

Through the above, and through our study of artificial intelligence and its role in enhancing cybersecurity, we have reached a set of results that we follow with the necessary recommendations.

Results:

- Artificial intelligence is an ally of cybersecurity programs, so it has become important to protect electronic security and benefit from artificial intelligence in enhancing it by building smart software specifically for this purpose.

- Cyber expert systems are a new concept that is little used at the present time, and it is expected to be used more widely in the future due to the serious threats to which the cyberspace is exposed.

- Artificial intelligence technologies related to cybersecurity are developing very rapidly and have become relied upon in various fields, especially in security systems.

Recommendations:

- The need to enhance the cyber infrastructure by companies, in order to enable the application of advanced technologies such as artificial intelligence.

- A legal and ethical framework must be developed that ensures the use of artificial intelligence in cybersecurity in a responsible and balanced manner.

- Institutions must work to address future challenges and expected developments to stay on top of cybersecurity technology.

— Explore new AI technologies to improve cyber data analysis and faster response to threats.

— Analyze emerging security challenges associated with new applications of AI in cybersecurity.

References:

Books:

Andersen, L, Human Rights in the Age of Artificial Intelligence, November 2018.

Amir Farag, Civil and Criminal Liability Provisions for Operating Robots with Artificial Intelligence for the Damages They Cause, Dar Al-Matbouat Al-Jami'ah, Alexandria, 2023.

Alaa Abdel Razzaq Al-Salmi, Introduction to Cyber Artificial Intelligence, Publications of the Arab Organization for Administrative Development of the League of Arab States, Egypt, Second Edition, 2024.

Belbey Ikram, Artificial Intelligence in International Law: A Study of the Concept, Frameworks and Applications, Legal Book Foundation and Ibn Al-Nadim for Publishing and Distribution, Algeria, 2024.

Khaled Nasser Al-Sayed, Origins of Artificial Intelligence, Al-Rashd Library Publishers, Kingdom of Saudi Arabia, 2004.

Mohiuddin Ahmed and others, explainable artificial intelligence for cybersecurity, springer nature switzerland, 2022.

Omar Yasser Al-Babli, Artificial Intelligence in the Face of Confronting Rumors and Terrorist Financing Crimes in the Cyber Environment: Implications and Ways to Confront, Publications of

the Arab Organization for Administrative Development, Egypt, 2023.

Articles:

Ammar Yasser Al-Babli, The Role of Artificial Intelligence Systems in Predicting Crime, Journal of Police Thought, Volume 28, Issue 110, July 2019.

Ahmed Al-Saleh Saba'a and others, Applying the Artificial Intelligence Strategy at the International Level (The United Arab Emirates as a Model), Journal of Economic Fields, Volume 1, Issue 1, 2018.

Balsal Bint Nabi Yasmine and Amroush Al-Hussein, Artificial Intelligence and its Role in Achieving Sustainable Development, Journal of Legal and Economic Studies, Volume 5, Issue 1, 2022.

Ben Adeed Samia, Security Risks Cyber and Information and the Development of Technical Knowledge on Protection Programs for Information Systems, Journal of Information Security and Digitization of the Higher Education and Scientific Research Sector, no publication year.

Khaled Dhaher Abdullah Jaber Al-Suhail Al-Mutairi, The Role of Penal Legislation in Protecting Cybersecurity in the Gulf Cooperation Council Countries, Journal of Legal and Jurisprudential Research, Issue 38, 2022.

Khalil Saidi and Marzouq Bin Mahdi, Artificial Intelligence as an Inevitable Trend in Protecting Cybersecurity, Journal of Human Rights Studies, Volume 6, Issue 1, 2022.

Mustafa Abu Mandour Musa Issa, The Adequacy of General Rules of Civil Liability in Compensating for Artificial Intelligence Damages: A Comparative Analytical Study, Damietta Law Journal for Legal and Economic Studies, Issue 5, January 2022.

Mohamed Dahmani, Artificial Intelligence as a Mechanism to Enhance Cybersecurity, Journal of Legal and Political Thought, Volume 7, Issue 2, 2023.

Websites:

https://www.bsu.edu.eg/Backend/Uploads/PDF/Conferenceالذكاء/percentage20الأمن20percentageوتكنولوجيا20percentageالاصطناعي20percentage.السيبرانيPDF

https://bakkah.com/ar/knowledge-center/الذكاء-الاصطناعي-السيبراني

https://mohammedalarda.com/النظم-الخبيرة-في-الذكاء-الاصطناعي/

الفصل الثاني

الذكاء الاصطناعي ودوره في تعزيز الأمن السيبراني

الدكتور بن عوالي علي

أستاذ محاضر (أ)

كلية الحقوق والعلوم السياسية-جامعة مستغانم

ali.benaouali@univ-mosta.dz

ملخص

تهدف هذه الدراسة إلى بيان مصطلح الذكاء الاصطناعي، ودوره في تعزيز الأمن السيبراني، حيث أخذ الذكاء الاصطناعي صدارة الاهتمام والدراسة في القرن الواحد والعشرين، حيث أحدث ثورة في شتَّى المجلات، وفرض هذا الذكاء الاصطناعي وجوده ودراسته، واستخدامه، باعتباره عاملاً أساسيًا في شتَّى مجالات البحث والابتكار، وتحقيق الأمن السيبراني.

ومن المجالات تطبيقات الذكاء الاصطناعي وأبرزها استخدامه في تحسين الأمن السيبراني، وبيان التحديات التي تواجه تطبيق الذكاء الاصطناعي في الأمن السيبراني،

وتوصلت هذه الدراسة إلى نتائج عدة منها أن تقنيات الذكاء الاصطناعي تساهم في تحسين الأمن السيبراني بطريقة فعالة وناجعة، وذلك عبر التنبؤ بالتهديدات والاستجابة السريعة لها، كما وصلت إلى أنه أصبح من الضروري إلى تكوين نخبة من الموارد البشرية وتأهيلهم في كيفية استخدام تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني بشكل فعال وناجع، وهذا ما قامت به الدولة الجزائرية، لما لهذا التخصص من أهمية بالغة.

الكلمات المفتاحية: الذكاء الاصطناعي، البحث، الابتكار، تقنيات الذكاء الاصطناعي، الأمن السيبراني، الحرب السيبرانية.

Summary:

This study aims to explore the concept of Artificial intelligence, (Ai) and its role in enhancing cyber security.

Al has taken the forefront of interest and research in twenty-first century, revolutionizing various.

Its existence, study, and application have become fundamental to innovation across multiple sectors, including cyber security.

The applications of Artificial intelligence, particularly its use in improving cyber security, present both opportunities and challenges.

One of the key findings of this study is that Al techniques significantly contribute to improving cyber security in effective and efficient manner, particularly through threat prediction and rapid response.

This highlights the need to form an elite group of human resources, trained in how to effectively and efficiently apply Al techniques in the field of cyber security.

The Algerian government, recognizing the importance of this specialization, has already under taken initiatives to address this need.

Keywords: Artificial intelligence, and research, innovation, Al techniques, cyber security, cyber war.

مقدمة

يعيش العالم اليوم في عصر يموج بالتقنيات المبتكرة والتطورات السريعة، وقد أطلق على هذا العصر "الثورة الرقمية" أو "الثورة الصناعية الرابعة" التي تتميز باختلافها عن الثورات الصناعية السابقة، كما أنها تتميز بتكامل التكنولوجيا الرقمية والعلوم الفيزيائية، مما يجعلها مرتبطة بالعديد من الصناعات والقطاعات.

حيث يُعدُّ الذكاء الاصطناعي أهم مخرجات الثورة الصناعية الرابعة وعاملا أساسيًا من هذه الثورة، نظرا لتنوع استخداماته في جميع العديد من القطاعات، منها تحسين الأمن السيبراني، وحماية القطاع العسكري، وقطاع الصحة، والتعليم، وغيرها، حيث أضحى هذا المجال جزءا أساسيا من حياتنا اليومية وأصبح يزداد الاهتمام به واستخدامه تبعا للتقدم المستمر للتكنولوجيا وزيادة قدرات الذكاء الاصطناعي.

إشكالية الدراسة

وبدأت ملامح ما يسمَّى بالمجتمع الخامس (The Fifth community) أو "مجتمع ما بعد المعلومات" تلوح في الأفق في نظر أهل الاختصاص، وعلماء الاستشراف والتنبؤ، وهذا المجتمع الخامس تندمج فيه المعلومة والآلة مع عقل الإنسان، ولأجل مسايرة ذلك أعادت الدول تسطير استراتيجيات جديدة تتلاءم مع الثورة التكنولوجيا العظيمة التي غزت هذا العصر بتقنياتها الباهرة، حتى تحافظ على استقرارها، وتحمي مجتمعها، واقتصادها، وأمنها، ولمواجهة المخاطر التي تهدد مصالحها في كل وقت وحين.

وقد أزال عصر الذكاء الاصطناعي المفهوم التقليدي للقوة الذي كان يعتمد أساسًا على القدرات العسكرية، والاقتصادية، (Hard Power) لتصبح القوة اليوم في يد من يملك التكنولوجيا الحديثة المتطورة المتمثلة في حسن استخدام الذكاء الاصطناعي ومواجهة الأمن السيبراني، أو ما يُسمَّى بالقوة السيبرانية (power Cyber) الذي فرض نفس كمفهوم جديد في العلاقات الدولية، وفقا لقاعدة: "من يملك المعلومة يملك القوة" وتتمثل المعلومة هنا في حسن استخدام الذكاء الاصطناعي وحسن استعماله لحماية مصالحه من هجمات السيبرانية التي

يشنها المجرمون الالكترونيون، أو العدو الالكتروني، حيث انتقل العدو من مواقعه التقليدية الظاهرة للعيان إلى المواقع الالكترونية التي يصعب كشفها واكتشافها، "الحروب الالكترونية".

الإشكالية

وتأسيسًا على ما سبق ذكره تتمحور الإشكالية الرئيسة للورقة البحثية حول ما ماهية الذكاء الاصطناعي؟ وما دوره في تعزيز الأمن السيبراني؟

ويندرج ضمن هذا التساؤل الرئيسي مجموعة من الأسئلة الفرعية على النحو التالي:

ما مفهوم الذكاء الاصطناعي؟

وما هي أنواع الذكاء الاصطناعي؟

ما هي مختلف مجالات الذكاء الاصطناعي؟

وما هو الأمن السيبراني؟ وما هي علاقته بالذكاء الاصطناعي

أهداف الدراسة

تهدف هذه الدراسة إلى التعرف على الذكاء الاصطناعي وبيان أهم مميزاته، ذلك كونه من أكثر المواضيع التي نالت الحيز الأكبر من الاهتمام في السنوات الأخيرة الماضية، كما تهدف هذه الدراسة إلى إبراز أنواع الذكاء الاصطناعي والتعرف على مختلف مجالاته التي شملت شتى ميادين الحياة، إضافة إلى بيان الأمن السيبراني، وعلاقته بالذكاء الاصطناعي.

منهج الدراسة

وللإجابة على الإشكالية السابقة اعتمدنا على المنهج الوصفي، باعتباره المنهج المناسب للدراسة حيث تطرقنا من خلال هذه الورقة البحثية الى مفهوم الذكاء الاصطناعي وأنواعه وأهم مجالاته، وإلى مفهوم الأمن السيبراني، وعلاقته بالذكاء الاصطناعي.

خطة الدراسة

تم تقسيم الورقة البحثية محورين أساسيين: المحور الأول: ماهية الذكاء الاصطناعي وأنوعه، ومجالات استخدامه، والمحور الثاني: مفهوم الأمن السيبراني وعلاقته بالذكاء الاصطناعي.

المحور الأول

ماهية الذكاء الاصطناعي وأنواعه ومجالاته

الذكاء الاصطناعي هو أحد علوم الحاسوب يهدف الى تطوير أنظمة وبرامج قادرة على محاكاة الذكاء البشري، أي لها القدرة على التفكير بطريقة تشبه طريقة تفكير البشر.

أولا: مفهوم الذكاء الاصطناعي

عبارة الذكاء الاصطناعي مركبة من كلمتين، أي يتكون من كلمتين:

الأولى: هي الذكاء والتي تعني القدرة على المعرفة والفهم والتفكير، والفطنة، والتَّحْليلِ والاِسْتِنْتاجِ، والتركيب.

والكلمة الثانية: هي الاصطناعي من الفعل اصطنع يصطنع اصطناعًا، وأصل هذه الكلمة ثلاثي وهو فعل صنع، أي جذر الكلمة، لكن لَمَّا كان يفيد الطلب وبذل الجهد بإعمال العقل، وإجهاده باستعمال العصف الذهني لتوليد الأفكار، زيد بألف والتاء التي تفيد الزيادة والطلب، وبذل الجهد، أصل الكلمة: صنع يصنع صُنعًا ومنه قوله تعالى: ﴿صُنْعَ اللهِ الَّذِي أَتْقَنَ كُلَّ شَيْءٍ إِنَّهُ خَبِيرٌ بِمَا تَعْمَلُونَ﴾[1] وذلك على وزن فعل يفعل فعلاً، ثم زيد وأضيف لهذا الفعل الثلاثي ألف، وتاء، فصار "اصطنع" على وزن افتعل خماسي، واستبدلت تاء الفعل بالطاء، لأن الصد من حروف الاستعلاء، والتاء من حروف الاستفال، ومن طبيعة الحال الضعيف يلجأ إلى القوي ويعتمد عليه، استُبدلت التاء طاء حتَّى تناسب الصاد التي قبلها، فصار اصطنع، ومما هو أنَّ "كل زيادة في المبنى تفيد زيادة في المعنى" ففعل اصطنع يفيد بذل الجهد والطاقة، وغير ذلك مما يدل على المشقة والحركة.

ومما ينبغي الإشارة إليه في هاته الكلمة أن حرف الصاد والطاء تفيد الاستعلاء والقوة والامتلاك، وهذا ما يقوم بها الذكاء الاصطناعي بالفعل، حيث صارت الدول التي تستخدم هذا العلم تملك القوة والمنعة في كل المجالات الاقتصادية، والعسكرية، والاجتماعية،

1- سورة النمل، الآية: 88.

والصحية، والسياسية، حيث لها القوة العلمية الكاملة لحماية نفسها من الهجمات السيبرانية، والحروب الالكترونية.

وعبارة أو اسم اصطناعي أيضًا منسوب إلى كلمة صناعة واصطناع، وهو كل ما كان مصنوعا وغير طبيعي، فيُقال القمر الاصطناعي، وهو جهاز يطلق عن طريق صاروخ في الفضاء خارج إطار الجاذبية الأرضية في مدار معين حول الأرض، يحمل أجهزة ومعدات علمية لاستخدامات متنوعة قد تكون للبحث العلمي، أو الطب، أو الأرصاد الجوية، أو لدراسة ظواهر بيئية أو فضائية معينة، أو قد يكون لأغراض تجسسيه وغيرها.

وفي مجال الطب يقولون: تنفس اصطناعي، وهو استخدام وسائل معينة صنعها الإنسان لمساعدة المرضى على التنفس واستنشاق الهواء، أو الأوكسيجين.

ومن ثَمَّ فإن كلمة اصطناعي تقابلها كلمة طبيعي، وتعني كل ما صنعته يد الإنسان بغرض محاكاة أمور طبيعية لتحقيق أهداف وغايات معينة[1].

أمَّا تعريفه اصطلاحًا: فله تعريفات عدة منها:

عرفه جون مكارثي وهو أول من حدد مصطلح الذكاء الاصطناعي بأنه" وسيلة لصنع جهاز كمبيوتر، أو روبوت يتم التحكم فيه عن طريق الكمبيوتر، أو برنامج يفكر بذكاء وبنفس الطريقة التي يفكر بها البشر الاذكياء، ويتم تحقيق الذكاء الاصطناعي من خلال دراسة كيف يفكر الدماغ البشري، وكيف يتعلم البشر ويقررون ويعملون أثناء محاولة حل مشكلة ما، ثم استخدام نتائج هذه الدراسة كأساس لتطوير برامج وأنظمة ذكية.

كما بأنه: "جزء من علم الكمبيوتر يهدف الى تصميم أنظمة كمبيوتر ذكية، بمعنى أنها تعطي نفس الخصائص التي نعرفها باستخدام الذكاء في السلوك الإنساني.

1- ميمي جمال، الذكاء الاصطناعي في الجزائر، بين المخاطر والمساهمة في تحقيق الأمن السيبراني، مجلة المعيار المجلد 15، العدد 02، ديسمبر 2024، ص 371-372.

أو هو قدرة الآلة[1] على محاكاة أو مضاهاة العقل البشري، وهو أيضا محاولة جعل الآلة تسابق وتتعدى قدرات العقل البشري، من خلال توظيف مجموعة خوارزميات تعمل على جهاز حاسوب(كومبيوتر)[2].

ولا يعتبر جهازًا بديلاً عن العقل البشري الذي صنعه الخالق الذي أتقن كلَّ شيء صنعًا.

وعُرِّف أيضا بأنه: "علم الحاسبات الذي يهتم بأنظمة الحاسوب التي تمتلك خصائص مرتبطة بالذكاء البشري والقدرة على اتخاذ القرارات بدرجة مشابهة إلى حد ما للسلوك البشري في مختلف المجالات.

وأنظمة الذكاء الاصطناعي هي تلك الأنظمة المهتمة بتطوير الحاسوب ليقوم بالمهام التي تتطلب ذكاء بشريا من خلال جعل الآلات تقوم بأعمال تعتمد على الذكاء البشري في أدائها في الواقع.

أو هو قدرة الآلة على محاكاة طريقة عمل العقل البشري، مثل قدرته على التفكير، والاستكشاف، وإثبات النظريات الرياضية المعقدة، ومهم أخرى متعددة، غير أنه لم يصل إلى مجاراة العقل البشري لحد الآن[3].

وبصفة عامة يمكن تعريف الذكاء الاصطناعي بأنه " مجموعة الجهود المبذولة لتطوير نظم المعلومات المحوسبة بطريقة تستطيع أن تتصرف فيها وتفكر بأسلوب مماثل لتفكير البشر، هذه النظم تستطيع أن تتعلم اللغات الطبيعية، وإنجاز مهام فعلية بتنسيق متكامل، أو

1- المقصود بالآلة: فالآلة تعتبر فرعًا من فروع الذكاء الاصطناعي الذي يُشير إلى منح الآلات القدرة على التعلم، واتخاذ القرار بالاعتماد على نفسها دون الحاجة إلى برمجتها من قبل الإنسان، بحيث يمكنها التعلم من الإجراءات السابقة، وتخزين البيانات للاستفادة منها والتحسين من أدائها في أي عمل مستقبلي، ويتم ذلك عن طريق استخدام برامج يتم تصميمها لتوليد الأفكار من خلال البيانات التي تُعرض عليها، وتطبيقها على عمليات مثل اتخاذ القرارات، والتعرف على الأصوات، أو حتى التنبؤ بالمستقبل. نرمين مجدي، الذكاء الاصطناعي وتعلم الآلة، سلسلة كتيبات تعريفية، ال عدد03، صندوق النقد العربي، أبو ظبي، الإمارات العربية المتحدة، 2020، ص6.

2- لحمر هيبة، التحول إلى الذكاء الاصطناعي بين المخاوف والتطلعات-التجربة الإماراتية نموذجا، مجلة الاقتصاد والتنمية، المجلد 09العدد02، 2021، ص9.

3- ميمي جمال، الذكاء الاصطناعي في الجزائر، بين المخاطر والمساهمة في تحقيق الأمن السيبراني، المرجع السابق، ص 372.

باستخدام صور وأشكال إدراكية لترشيد السلوك المادي، كما تستطيع في نفس الوقت تخزين الخبرات والمعارف الإنسانية المتراكمة واستخدامها في عملية اتخاذ القرارات.

وما يلاحظ من خلال التعريفات السابقة: أنه لا يوجد تعريف جامع وشامل للذكاء الاصطناعي، حيث إن بعض التعريفات ركزت على تشبيه الذكاء الاصطناعي بالذكاء البشري، وأخرى ركزت على الهدف من الذكاء الاصطناعي، وبعضها الآخر ركز على تصرف الذكاء الاصطناعي كالإنسان، إلا أنَّ جميع التعريفات السابقة تدور حول فكرة واحدة وهي قدرة الآلة على التصرف مثل البشر.

وأهمُّ ما يميز الذكاء الاصطناعي أنَّ لديه القدرةَ على تنظيم واستغلال ما تعلَّمه، مع إمكانية تحليله للغات وفهم الأصوات، وتصنيفها، وحل المشكلات العويصة، وكذلك شرح المناهج الدراسية، وتقييم الطلبة، والإجابة على مختلف الأسئلة، والاستفسارات المطروحة، وغير ذلك من القدرات التي تمَّ برمجته عليها[1].

حيث إنه من خلال أنظمة مبرمجة بدقة عالية تستخدم تقنيات قادرة على جمع البيانات، واستخدامها للتنبؤ أو لتقديم توصيات، أو حتى اتخاذ القرارات بمستويات متفاوتة من التحكم الذاتي، واختيار أفضل إجراء ممكن لتحقيق الأهداف المرجو تحقيقها[2].

والذكاء الاصطناعي فرع قائم بذاته من فروع علوم الحاسبات، علم يجعل الآلات وكأنها تفكر مثل البشر، في محاولة لمحاكاة القدرات الذهنية للإنسان، كالتعلم، والاستنباط ورد الفعل على وضعيات معينة أو وضعيات جديدة.

1- هناء رزق محمد، أنظمة الذكاء الاصطناعي ومستقبل التعلُّم، مجلة دراسات في التعليم الجامعي، العدد52، 2021، ص 573-573.

2- عبد الله بن شرف الغامدي، الذكاء الاصطناعي للتنفيذيين، سلسلة الأدلة الإرشادية، الهيئة السعودية للبيانات والذكاء الاصطناعي، ص8.

ومن ثَمَّ فإنَّ الذكاء الاصطناعي لا يعدو أن يكون فرعًا من فروع علوم الحاسوب، مجاله محاكاة السلوك الذكي في أجهزة الكومبيوتر أو الحاسوب، بحيث تصير هذه الآلة قادرة على تقليد السلوك الإنساني الذكي[1].

حيث إنَّ الذكاء الاصطناعي باعتباره هو فرعًا من فروع علوم الحاسوب فهو يركز على تصميم وتطوير أنظمة، وبرامج قادرة على تنفيذ مهام تشبه الذكاء البشري، ويَستخدم في هذا المجال تقنيات وأدوات متطورة تعتمد على القدرات الحسابية العالية للحواسيب، وتكنولوجيا المعلومات، لإنشاء نماذج تتفاعل وتتعلَّم وتتخذ قرارات بشكل مشابه للقرارات التي يتخذها البشر، ويشمل فروع الذكاء الاصطناعي تصنيف الصور، والأصوات، والترجمة الآلية، وكذلك التخطيط، والاستنتاج، حيث يُعد الذكاء الاصطناعي من أعظم الابتكارات التكنولوجية الحديثة، وأشدِّها أهمِّية، ويُستخدم على نطاق واسع في مجالات مثل الروبوتات وتحليل البيانات الضخمة وتطوير تطبيقات الذكاء الاصطناعي لمختلف الصناعات[2].

وتأسيسًا على ما سبق يمكن القول: إنَّ الذكاء الاصطناعي (Artificial Intelligence AI) هو أحد أوسع الفروع في علوم الكومبيوتر، مجاله إنتاج الآلات الذكية ذات القدرة على القيام بالعديد من العمليات والمهام التي هي في الأصل من اختصاص العقل البشري وذلك بالاعتماد على برمجيات وأنظمة متطورة.

ثانيا: أنواع الذكاء الاصطناعي

يمكن تصنيف الذكاء الاصطناعي على حسب القدرات التي يتمتع بها إلى ثلاثة أنواع مختلفة وهي:

1-الذكاء الاصطناعي المحدود أو الضيق: حيث يُعتبر الذكاء الاصطناعي المحدود أو الضيق ((Weak AI or Narrow AI أحدَ أنواع الذكاء الاصطناعي التي تستطيع القيام بمهام مُحددة وواضحة، كالسيارات ذاتيّة القيادة، أو حتى برامج التعرُّف على الكلام، أو

1- هاشم ناصر الدين محمود سويدان، الحماية القانونية للمصنفات الناشئة عن برامج الذكاء الاصطناعي، مجلة قبس للدراسات الإنسانية والاجتماعية، المجلد 07، العدد 02، 2023، ص380.

2- حسن نايف مبارك الحجرف، دور الذكاء الاصطناعي في تعزيز الأمن السيبراني، رؤى نظرية، 2024، ص 14075.

الصور، أو لعبة الشطرنج الموجودة على الأجهزة الذكية، ويُعتبر هذا النوع من الذكاء الاصطناعي أكثر الأنواع شيوعا وتوافرًا في هذا العصر.

2- الذكاء الاصطناعي العام: (General AI)، وهذا النوع الذي يحاكي العقل البشري، ويُمكن أن يعمل بقدرة تُشابه قدرة الإنسان من حيث التفكير، إذ يُركز على جعل الآلة قادرة على التفكير والتخطيط من تلقاء نفسها، وبشكل مُشابه للتفكير البشري، وبدأت ملامح هذا النوع تلوحُ في الأفق، حيث بدأ التركيز عليه في مجالات شتَّى، ولا يزال يحتاج للكثير من الجهد والبحث لتطويره وتحويله إلى واقع حقيقي، وتعد طريقة الشبكة العصبيّة الاصطناعيّة (Artificial Neural Network) من أهمّ طرق دراسة الذكاء الاصطناعي العام، إذ تُعنى بإنتاج نظام شبكات عصبيّة للآلة مُشابهة لتلك الي يحتويها العقل البشري[1].

3- الذكاء الاصطناعي الفائق: يُعتبر الذكاء الاصطناعي الفائق(Super AI)، النوع الذي قد يفوق مستوى الذكاء البشري في بعض العمليات، أو الأعمال من حيث مدة إنجازها، وهذا التفوق ليس مطلقًا، وإنما في بعض العمليات، حيث قامت بعض الدول بالاعتماد على تقنيات الذكاء الاصطناعي لتشغيل الروبوتات التي تعمل مكان الشرطة.

وقد أكَّدت بعض الدراسة الحديثة أن العقل البشري لا يزال متفوقاً وأكثر كفاءة من الذكاء الاصطناعي، حيث تشير الأبحاث التي أجرتها جامعة أكسفورد في بريطانيا، إلى أن العقول البشرية تعمل بطريقة أسرع ومختلفة جذرياً عن خوارزميات التعلم الآلي، وفقاً لصحيفة "التليغراف البريطانية"[2]

ومن الناحية النظرية يمكن أن يتفوق الذكاء الاصطناعي على البشر بالفعل، إلا أن ذلك يحتاج إلى عدة عقود حتى يستطيع اكتساب الأدوات والتعلم عمومًا مع إمكانية القيام ببعض الوظائف والمهارات التي يستطيعها البشر خلال وقت قريب؛ بما في ذلك ترجمة اللغات، وكتابة المقالات المدرسية، وكتابة الكتب[3]، لكن هذا ليس مطلقا.

1- خليل سعيدي، مرزوق بن محمدي، الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبراني، مجلة دراسات في حقوق الانسان، المجلد06، العدد01، 2022، ص28.

2- دراسة العقل البشري يتفوق على الذكاء الاصطناعي بالتفكير الذكي والمرن/ https://aawsat.com

3- هل يمكن للذكاء الاصطناعي أن يتفوق على العقل البشري/ https://www.google.com/search?

حيث إن هناك العديد من العقبات التي تواجه الذكاء الاصطناعي وتعرقل تطوره بالشكل المطلوب، ومن أبرز هذه العقبات ما يأتي:

-**القدرة على التكيّف:** يستطيع البشر التكيف مع الكثير من المهات بسرعة كبيرة في غضون دقائق، من خلال بعض المعارف الجديدة، وأما الذكاء الاصطناعي، فإنه يحتاج إلى وقت طويل حتى يتمكن من التكيف.

- **الأخطاء الفادحة:** في معظم الأحيان ترتكب أنظمة الذكاء الاصطناعي أخطاءً فادحة عند الخطأ، وربما تقوم بتلبية طلبات مختلفة تمامًا ومغايرة لما يأمر به المستخدم.

- **الحاجة إلى التعلم من جديد عند تغيير القواعد:** ربما يتمكّن البشر من التعامل مع الأشياء بسهولة عند تغيير قاعدة من القواعد، وأما الذكاء الاصطناعي؛ فإنها يحتاج إلى إعادة تعلم القواعد من جديد[1].

ثالثا: مجال استخدام الذكاء الاصطناعي

للذكاء الاصطناعي العديد من المجالات التي يمكن استخدامه فيها، ويمكن ذكر بعض هذه المجالات فيما يلي:

1-تُستخدم تقنية الذكاء الاصطناعي في مجالات خدماتية مختلفة، كالقطاع العسكري، والصناعي، والتقني، والمالي، والاقتصادي، والطبي، والتعليمي، وتشمل التطبيقات المهمة لهذه التقنية السيارات ذات القيادة الذاتية، والطائرات بدون طيار، وتقنيات استخدام الروبوتات للعمل بشكل مستقل، وتُشغَّل الآلات المستخدمة في مهام عدة ومختلفة، مثل العمل في المفاعيل النووية، ومحطات الطاقة، وإصلاح الكابلات ومدِّها تحت الأرض وفي البحار، واكتشاف المناجم بشتَّى أنواعها، وغير ذلك من المهام التي تحل محل الاستخدام البشري[2].

1- هل يمكن أن يتفوق الذكاء الاصطناعي على البشر / https://misbar.com/qna/2023/10/19

2- محمد دحماني، الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني والسياسي، المجلد 07، العدد 02، ص 600.

2-يمكن استخدام الذكاء الاصطناعي في معرفة عمليات المحاكاة الذكية الحاسوبية لدراسة كيفية التعرف الدماغ البشري على الوجوه، والأصوات المألوفة، ويعالج الصور، ويستخرج البيانات المفيدة منها، وكيفية تحسين الذاكرة.

3-من مجالات الذكاء الاصطناعي إمكانية ممارسة المهارات الحركية والتحكم اللفظي وغير الخطي من استعمال الأجهزة الذكية التي تقوم بأداء المهام العقلية مثل القيام بالتصميم الصناعي، والتحكم في العمليات، واتخاذ القرارات وغير ذلك.

4-إمكانية استخدام الذكاء الاصطناعي لتعلم اللغة، والفهم التلقائي للغة المكتوبة والمقروءة، وترجمة اللغات بإجابات مبرمجة مسبقا، حيث يتم جمع العديد من عمليات البحث في "google"على أجهزة الكومبيوتر المتصلة بالأنترنت[1].

وخلاصة القول في كيفية عمل الذكاء الاصطناعي؟

إنَّ أسس عمل الذكاء الاصطناعي ترتكز على استيعاب كمية كبيرة من البيانات المصنفة، وتحليلها بحثاً عن الأنماط والارتباط بين بعضها البعض، للتوصل إلى تنبؤات بالحالات والاحتمالات المستقبلية، عبر استخدام التعلُّم الآلي والبرامج المتخصصة لكتابة وتدريب الخوارزميات، ما يسمح بتغذية روبوت الدردشة بأمثلة نصية حتى يستطيع الإجابة عن أسئلة المستخدمين وإنشاء تبادلات واقعية معهم، والتعرف على الصور وإنشاء موسيقى ووسائط أخرى متعددة واقعية، وتتلخص خطوات عمل الذكاء الاصطناعي في أربع خطوات أساسية هي:

- التعلم لإنشاء القواعد وتحويلها لمعلومات قابلة للتنفيذ وفقاً لبرمجة الذكاء الاصطناعي.

- المنطق الذكي الذي يركز على اختيار الخوارزمية الصحيحة للوصول إلى النتيجة المرجوة، أو المستهدفة.

1- نرمين مجدي، الذكاء الاصطناعي وتعلم الآلة، سلسلة كتيبات تعريفية، العدد03، صندوق النقد العربي، أبو ظبي، الإمارات العربية المتحدة، 2020، ص ص8-18.

- التصحيح الذاتي لضبط الخوارزميات بشكل مستمر والتأكد منها لتحقيق أكثر النتائج دقة.

- الإبداع بالاعتماد على القواعد والإحصائيات والتقنيات التكنولوجية لإنشاء وسائط متعددة وحديثة.

المحور الثاني

مفهوم الأمن السيبراني وعلاقته بالذكاء الاصطناعي

أصبحت القطاعات المرقمنة بأنواعها المختلفة والمتعددة مهددة من قبل القرصنة الإلكترونية، وذلك بسبب التطور التكنولوجي الهائل، مما جعلها تنتشر في جميع المؤسسات في الوقت الحالي، لهذا أصبحت الحاجة إلى تخصصات إلكترونية جديدة، والتي يكون من شأنها توفير الحماية الكافية للأنظمة التقنية، والأجهزة الحديثة المستخدمة في حياتنا، مثل تخصص الأمن السيبراني.

أولا: مفهوم الأمن السيبراني[1]

إن عبارة الأمن السيبراني مركبة من كلمتين، أي يتكون من كلمتين:

الأولى: كلمة الأمن: الأمان والأمانة بمعنى واحد وهو الشعور بالطمأنينة، والراحة والاستقرار النفسي والقلبي والعلقي، والأسري والاجتماعي، وقد أَمِنْتُ فأنا آمن، وأَمَّنت غيري فهو آمن ومطمئنٌّ من قِبلي، والأمن ضدُّ الخوف، والرعب، والأمانة ضدُّ الخيانة[2].

وفي هذا المجال يقول رسول الله صلى الله عليه وسلم: "من أصبح منكم آمنا في سربه معافى في جسده عنده قوت يومه، فكأنما حيزت له الدنيا"[3]

فمعنى الأمن هو إحساس الفرد، أو الجماعة، أو المجتمع، أو الدولة بالطمأنينة، والاستقرار/ وانتشار الثقة والمحبة، وعدم وجود خيانة بين الأفراد لبعضهم البعض، واستئصال

1- بداية الأمن السيبراني، ظهر مع نهاية الحرب الباردة، وظهور مصطلح حرب الإنترنت أو الحرب السيبرانية، وتطور مع ثورة الإنترنت وأنظمة الحاسوب، وصار وسيلة أمنية وحربية دولية أساسية، ويسمى أيضا أمن الكمبيوتر، وهو عبارة عن سيلة أساسية وضرورية لحماية البرمجيات وأجهزة الحاسوب والشبكات، وهو مجموعة من الإجراءات المتخذة لمواجهة الهجمات والاختراقات السيبرانية وما ينتج عنها من أخطار. ينظر: لأمن السيبراني مفهومه وتاريخه/ https://www.aljazeera.net/encyclopedia/2024/9/19 يوم 29/ 12/ 2024 على الساعة 15:00

2- ابن منظور، لسان العرب، دار المعارف، باب الهمزة، ص 140.

3- أبو عيسى الترمذي، جامع الترمذي، بيت الأفكار الدولية، رقم الحديث 2346، ص 385.

الفساد مع إزالة كل ما يعكر أو يهدد الاستقرار والعيش في هدوء، أ ويمس بمقتضيات النفس والجسم، لضمان القدرة على الاستمرار في الحياة بأمن وسلام.

وما شُرِّعت القوانين والتدابير إلا من أجل تحقيق الحماية اللازمة للإنسان في نفسه، وماله، وعرضه.

وللأمن أنواع عدّة نذكر منها :الأمن الاجتماعي، الأمن الاقتصادي، الأمن السياسي، الأمن العسكري، الأمن البيئي، الأمن الغذائي، الآمن السيبراني، وقد ذُكر أصل أمن هذه الأنواع كلِّها في قوله تعالى:﴿ أطمعهم من جوع وآمنهم من خوف ﴾[1]

الثانية: السيبراني: تُكتب سيبراني، بدون ياء بعد الباء، وسيبراني بإضافة الياء بعد الباء، وسيبيراني بيائين قبل وبعد الباء، ويقصد بهذه الكلمة الفضاء السيبراني، وهي صفة لكل ما هو مرتبط بتقنية المعلومات

والحاسوب، أو الكومبيوتر، ويعني أيضا فضاء الإنترنت أو العالم الافتراضي[2].

فعبارة السيبرانية جاءت من كلمة "cyber" والتي تعني أي شيء يتعلق بأجهزة الكومبيوتر وتكنولوجيا المعلومات، والواقع الافتراضي.

والتهديدات السيبرانية تعني استغلال أجهزة الكومبيوتر وتكنولوجيا المعلومات لتخريب البنية التحتية الاستخباراتية للعدو، وتدميرها، وكذلك تعطيل شبكات الدفاع الجوي وفقًا لخطط مدروسة بعناية فائقة الدقة، واستخدام البريد الالكتروني، ومكاتب المراقبة التابعة لرئيس الدولة، فإنَّ التهديد السيبراني، أو الهجوم السيبراني يمثل تهديدًا لأمن القومي للدول، والأمن الاجتماعي، والاقتصادي[3].

1- سورة قريش، الآية 4.

2- إسلام فوزي، الآمن السيبراني، الأبعاد الاجتماعية والقانونية، تحليل سوسيولوجي، المجلة الاجتماعية القومية، المجلد 56، العدد 02، 2019، ص 103.

3- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، جامعة العربي تبسي، المجلد01، العدد 01، 2019، ص 108.

ومن ثَم فإنَّ الأمر جد خطير؛ إذ كشفت دراسة حديثة في مجال تكنولوجيا المعلومات عن أنَّ الجرائم السيبرانية كلَّفت دول العالم ما قارب من ستة (06) تريليونات دولار عام 2021 وهذا ضعف المبلغ في عام 2015، فهذه التكاليف سببها الأضرار، والآثار الكثيرة التي تُخلفها الجرائم السيبرانية، منها سرقة البيانات، أو تخريبها، وسرقة الأموال، وفقد الإنتاجية، وسرقة الملكية الفكرية، والاختلاس، والاحتيال، و إحداث الاختلالات التجارية بسبب القرصنة، والتحقيق الجنائي، واختراق الأنظمة، والإضرار بالسمعة، أضف إلى ذلك أن بعض المجموعات السيبرانية قد تكون مدعومة ومدفوعة من قبل جهات معينة، أو حتى من بعض الدول كما هو ملاحظ في قضية الذباب الذي يأتينا من الجارة الغربية، لأغراض التشويش، أو الهجوم، او الاستخباراتية[1].

أمَّا تعريفه اصطلاحًا: فله تعريفات عدة منها:

يُعرَّف الأمن السيبراني على أنه مجموعة من الإجراءات القانونية، والتقنية، والفنية، والتي باتخاذها يتم تأمين الموارد الاجتماعية، والموارد البشرية، والاقتصادية، والعسكرية، المرتبطة بشبكات الاتصال ونقل المعلومات (الأنترنت) ودفع كل الأخطار الناجمة عن تسلل أو اقتحام أو سرقة أو عبث أو قرصنة، وكل استغلال غير مرخص وغير مشروع لتلك المعلومات، وهي الأفعال التي من شأنها أن تسبب أضرارًا بمصالح الدولة، أو الأفراد[2].

أو أنها تلك الإجراءات والتدابير والتقنيات والأدوات المستحدثة والمستخدمة قصد حماية أمن وسلامة الشبكات والبرامج والبيانات المرتبطة بالحواسيب والأجهزة، ووقايتها من كل ولوج، أو من الهجمات المختلفة والمتنوعة، أو من محاولات الإتلاف، أو من محاولات الوصول غير المصرّح به أو غير المرغوب فيه، ويشمل ذلك حماية كل من الأجهزة والبيانات[3].

كما يُعرَّف الأمن السيبراني بأنه الحماية لشبكات الاتصالات وأنظمة المعلومات والبيانات، بما في ذلك الأجهزة

1- إسلام فوزي، الأمن السيبراني الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي، ص 101.

2- ميمي جمال، الذكاء الاصطناعي في الجزائر، بين المخاطر والمساهمة في تحقيق الأمن السيبراني، المرجع السابق، ص 373.

3- مني عبد الله السمحان، متطلبات تحقيق الآمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية بالمنصورة، المجلد 111، العدد01، 2020، ص 7.

المتصلة بالإنترنت، حيث يتعلق الأمن السيبراني بالتدابير الوقائية والمعايير التي يجب اتباعها والامتثال لها لمواجهة التهديدات، والحد من الانتهاكات، أو الوصول غير المصرح به[1].

وحسب الاتحاد الدولي للاتصالات فالأمن السيبراني هو "مجموعة من الأدوات والسياسات والمفاهيم الأمنية، والتحفظات الأمنية والمبادئ التوجيهية، ونهج إدارة المخاطر والإجراءات والتدريب، وغيرها من الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المؤسسات والمستعملين من المخاطر الأمنية ذات الصلة في البيئة السيبرانية."

وعرَّفه وكالة الأمن السيبراني وأمن البنية التحتية الأميركية "سي آيا إس إيه" بأنه "فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به، أو الاستخدام الإجرامي، ويمثل ممارسة ضمان سرية المعلومات وسلامتها وتوافرها."

وتعرفه الموسوعة البريطانية بأنه "حماية نظم الحوسبة والمعلومات من الأضرار والسرقة والاستخدام غير المصرح به."

وتعرفه شركة "كاسبر سكاي" الدولية الخاصة للأمن السيبراني بأنه "أشكال الدفاع عن الحواسيب والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الخبيثة، ويعرف أيضا بأمن تكنولوجيا المعلومات أو الأمن الإلكتروني للمعلومات"[2]

ومن الناحية العلمية والإجرائية فإن الأمن السيبراني يشكل جدار تصدٍّ ودفاعي لكل ما يمكن أن تتعرض له شبكات الاتصال ونقل المعلومات عبر الإنترنت، من مخاطر أو أفعال سيّئة غير مشروعة تضرّ بمصالح البلاد والعباد.

1- العتيبي، عبد الرحمن بجاد شارع، دور الأمن السيبراني في تحقيق رؤية 2030، رسالة ماجستير، جامعة نايف العربية للعوم الأمنية، 2020.

2- لأمن السيبراني مفهومه وتاريخه/ https://www.aljazeera.net/encyclopedia/2024/9/19يوم 2024/12/29 على الساعة: 15:25.

فهو يُعنى بحماية شبكات الإنترنت وأجهزة الكومبيوتر من خطر الاختراق، ويعمل على الحفاظ على المعلومات التي تحتويها تلك الأجهزة من السرقة، ويحاول أيضا التصدي للهجمات المتكررة، المعلومة منها والمجهولة على البرمجيات لتعطيلها من خلال وسائل متعددة كالفيروسات والبرامج المدمجة.

وعليه فإن الكلام يدور حول عالم افتراضي رقمي بامتياز، يعتمد على وسائل الاتصال الحديثة والإنترنت

والحواسيب لتحويل أو تبادل أو تخزين المعلومات في استثمار قوي ومباشر للتطور التكنولوجي والذكاء

الاصطناعي، حيث به يتم إدارة الكثير من الآمور التي تتعلق بالمعلومات والمعاملات والاقتصاد أو ما يتعلق

بالحياة المدنية أو العسكرية أوغرها من المجالات الكثيرة والمتنوعة.

ثانيا: أبعاد الأمن السيبراني

يتضمن الأمن السيبراني أنظمة الأمن العسكري، والاقتصادي، والاجتماعي، والسياسي، والإنساني، التي تهدف إلى الحفاظ على الاستقرار، والأمان من جميع التهديدات السيبرانية، يتضمن الأمن المتكامل الجوانب التي تسهم في تعزيز نظام الأمن السيبراني، وتُعد من أهم أبعاده[1]، نذكر منها:

1-البعد العسكري:

يهدف الأمن السيبراني إلى الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يسهل تبادل المعلومات والأوامر، حيث تطرح فكرة إنشاء ونشر شبكة للإنترنت والأهداف البعيدة، ولكنها تُعد نقطة ضعف، خاصة إذا لم تكن آمنة، يمكن أن يؤدي تدمير قواعد البيانات العسكرية أو قرصنة بياناتها ومعلوماتها، أو تعطيل

1- مختار محمد، الأمن السيبراني مفاهيم المستقبل، مجلة اتجاهات الأحداث، 2023، ص 6-7.

الاتصالات بين وحدات القيادة والوحدات العسكرية، بالإضافة إلى خطر فقدان السيطرة على بعض الأسلحة مثل الطائرات بدون طيار أي ذات القيادة الذاتية، والصواريخ الموجهة والأقمار الصناعية.

2-البعد الاقتصادي:

نظرًا لاستخدام أجهزة الكمبيوتر في تشغيل الصناعات وتطويرها ودفع عجلة الاقتصاد إلى الأمام بزيادة الإنتاج وتنويعه باستخدام التكنولوجيا الحديثة والمتطورة في ذلك، ستكون الإنترنت أساساً للتجارة والتمويل والمعاملات المالية، حيث ترتبط جميعها ببعضها البعض من خلال شبكات الكمبيوتر لضمان الأمن السيبراني.

حيث إن البعد الاقتصادي للأمن السيبراني يعكس التأثير السلبي الذي يمكن أن يحدثه التهديد السيبراني على النظام الاقتصادي، ويبرز أهمية اتخاذ التدابير اللازمة لحماية الأنظمة والشبكات والبيانات من الهجمات السيبرانية.

3-البعد الاجتماعي:

يوجد أكثر من أربعة (4) مليار مستخدم للإنترنت حول العالم، حيث يستخدم أكثر من مليارين وستمائة (2.6) شخص مواقع الشبكات الاجتماعية، وتتمتع مواقع التواصل الاجتماعي بأعلى معدلات التفاعل البشري، مما يتيح فرصاً كبيرة لمشاركة الأفكار، والتجارب الناجحة، لكنها في المقابل تكشف أيضاً عن أخلاقيات الأفراد، فصعوبة الرقابة على محتوى الإنترنت ليست مجرد خطر على المجتمعات، بل تعرض أيضاً المعلومات الشخصية لاستخدامات غير مشروعة من جهات خارجية، والغزو الثقافي الرقمي، والابتزاز، والتنمر الالكترونيين، كل ذلك يهدد السلم الاجتماعي في البلدان، نتيجة فقدان الأمن السيبراني الاجتماعي[1].

1- إسلام فوزى، الأمن السيبرانى، الأبعاد الاجتماعية والقانونية تحليل سوسيولوجى، ص 109.

4-البعد السياسي:

هناك العديد من الأمثلة التي تؤكد أهمية البعد السياسي للأمن السيبراني، مثل تسريب الوثائق الحساسة المختلفة التي تسبب مشكلات جسيمة على المستوى الداخلي والخارجي للدولة، وتؤثر بصفة صريحة على العلاقات الدولية، مثلا أزمة الخليج بين قطر ودول الخليج الأخرى في 5 يونيو 2017، كانت الشرارة هي الاختراق الذي تعرضت له وكالة الأنباء القطرية في 23 ماي 2017. ومثل ما فعلت روسيا عن طريق الهجمات السيبرانية في الانتخابات الأمريكية.

كما لا يمكن إنكار دور شبكات التواصل الاجتماعي في المشهد السياسي، فهي تستخدم في حملات الانتخابات والتظاهرات الافتراضية والحركات الاحتجاجية الإلكترونية، كما لا يمكن إنكار دور هذه الشبكات في قيام ثورات الربيع العربي أواخر 2010 بالإضافة إلى ذلك، تستغل العديد من الحكومات هذه المنصات لترويج سياساتها.

وفي سياق آخر، يجب ألا نغفل عن استخدام الجماعات الإرهابية لتلك المواقع، لتجنيد أعضاء جدد وجمع التمويل لعملياتها والترويج لأفكارها التخريبية، تعد هذه المنصات وسيلة للتواصل بين الأفراد والجماعات الإرهابية، وهذا يؤكد الحاجة الملحة إلى الأمن السيبراني، وأهميته لجميع الدول في بعدها السياسي.

وبالتالي، يجب أن تعمل الدول على حماية أمنها من التهديدات والمخاطر التي تنطوي عليها شبكة الإنترنت.

5-البعد القانوني:

تتمثل المخاطر القانونية، بشكل أساسي، في غياب الإطارين التشريعي، والتنظيمي المناسبين للتعامل مع نتائج الأعمال القانونية وغير القانونية منها، والتي تتم في الفضاء السيبراني، ويتطلب النشاط الاقتصادي، والتجاري وغيرهما تحديدًا واضحًا، للواجبات والحقوق، فمستخدمو هذه التقنيات، عبر الفضاء السيبراني بحاجة إلى إطار قانوني وتنظيمي يؤمّن حماية استخدامهم، ففي حالة غياب الأطر التشريعية، والتنظيمية تصبح الجرائم السيبرانية خطرًا حقيقيًّا على العمليات المعلوماتية المتعلقة بحقوق الإنسان الدولية، وتؤدي إلى أضرار اقتصادية،

واجتماعية وسياسية خطيرة، فتأطير مخاطر الأمن السيبراني وفق الأطر القانونية والتنظيمية وطنيا ودوليا يهدف إلى حماية الأصول المعلوماتية، والتقنية وفقًا للسياسات والإجراءات المتبعة.

ولمسايرة هذا التطور التكنولوجي السريع والخطير في نفس الوقت ينبغي على المنظومة التشريعية والتنظيمية المسارعة في وضع النصوص القانونية والتنظيمية لتأطير هذه التكنولوجيا بشتَّى أنواعها وأهدافها، حيث تسطيع هذه التشريعات التعامل مع جميع الأنشطة القانونية وغير القانونية على الإنترنت، باعتبار أنَّ الجرائم الإلكترونية في الغالب جرائم سيبرانية، وقد كثرت وتنوعت وتشعَّبت، ولمواجهتها ومحاربتها لا بدَّ من إيجاد تشريع صارم، وفعَّال للتعامل مع هذه الجرائم الالكترونية، سواء أكانت وطنية محلية، أم عابرة للحدود منطلقة من دول أخرى[1].

ثالثا: علاقة الأمن السيبراني بالذكاء الاصطناعي:

تتجلَّى وظائف استخدام الذكاء الاصطناعي في تحسين الأمن السيبراني من خلال التطبيقات التالية[2].

1-التعامل مع البيانات الضخمة

حيث يتم تنفيذ العديد من الأنشطة عبر الأنترنت، مما يعني نقل كميات كبيرة من البيانات بين العملاء والبنية التحتية يوميًا، تظهر هذه العملياتُ التحديات التي يواجهها محللو الأمن السيبراني في التحقق من كل شيء وتقييم مخاطر محتملة، يُعتبر الذكاء الاصطناعي الخيار الأمثل لاكتشاف هذه التهديدات التي تنشأ خلال الأنشطة اليومية، بفضل قدرته على مراقبة حركة المرور، وتحليل نشاط الخادم بدقة وتحديد المخاطر المحتملة بشكل تلقائي.

1- إسلام فوزى، الأمن السيبرانى، الأبعاد الاجتماعية والقانونية تحليل سوسيولوجى، ص 115.

2- حداوي، وآخرون، القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في المنظمات- دراسة تحليلية لآراء عينة من العاملين في المصارف الأهلية في النجف الأشرف .مجلة العلوم الإنسانية والطبيعية، 2023.

2-توقع التهديدات المستقبلية

تعتبر كمية البيانات التي يتعامل معها محللو الأمن السيبراني تحديًا في التنبؤ بالتهديدات المستقبلية، إلا أن الذكاء الاصطناعي يستطيع معالجة حجم كبير من البيانات في وقت واحد، مما يمكّن من الكشف المبكر عن الأنشطة الضارة، بفضل تحديد التهديدات المحتملة والإجراءات الوقائية في الحين باستخدام الذكاء الاصطناعي، حيث الذكاء الاصطناعي يكون دائما على استعداد ويقظة لأي تهديد محتمل، واتخاذ الإجراءات اللازمة لحماية البيانات أو التعاملات أو غير ذلك مما يحتاج إلى القواية والحماية.

3-سرعة اكتشاف التهديد في وقت وجيز

يعتبر اكتشاف التهديدات بسرعة أمرًا حيويًا ومهمًا للغاية، حيث أبلغت 42% من المؤسسات عن زيادة في التهديدات الحساسة للوقت، وفي الوقت نفسه يمكن للذكاء الاصطناعي فحص كميات هائلة من البيانات في وقت واحد للكشف عن التهديدات السيبرانية، مما يعزز الأمن بشكل كبير. وبحسب استطلاع، أفاد 56% من المؤسسات بأنها تعاني من ضغط شديد بسبب تحليل تهديدات يشغل المحللين السيبرانيين، وأبلغ 23% منهم أنهم غير قادرين على التحقق من التهديدات بشكل فعال.

د. التقليل من التكاليف

يعاني العديد من المؤسسات من تأثيرات مالية جسيمة نتيجة انتهاكات البيانات كل عام، وهذا أمر لا يمكن تجاهله أو التوقف عن مواجهة المجرمين، وفقًا للدراسات التي توضح الفروقات الكبيرة في توفير التكاليف بنسبة 80% للمؤسسات التي تعتمد على تقنيات الذكاء الاصطناعي في أمنها السيبراني، حيث يتم تقديم خدمات بتكلفة 2.9 مليون دولار مقابل 6.71 مليون دولار لمن لا يستخدمون هذه التقنيات.

من بين التقنيات البارزة في مجال الذكاء الاصطناعي، نجد " Chat GPT "وعلى الرغم من المخاوف المتعلقة بالتحديات مثل التحيز العنصري ونقص المعايير الموثوقة، إلا أن لهذه التقنية فوائد هامة في ساحة أمن المعلومات، حيث تساهم في زيادة الإنتاجية، ومساعدة المهندسين، وتدريب الموظفين، وتعزيز تطبيق القانون، كما أن تطور تقنية " Chat GPT

" يعمل على تعزيز قدرة الصناعة على كشف واستجابة الهجمات الإلكترونية في الوقت الفعلي، مما يعزز مرونة الأمن السيبراني بشكل عام، كما تساعد تقنية " Chat GPT " أيضًا الباحثين على مكافحة البرمجيات الضارة وتحليلها، وتسد الفجوات في المعرفة الأمنية، وتسهل تدريب الموظفين حول الأمن السيبراني، وعلى الرغم من التحديات التي قد تواجه استخدام تقنية Chat GPT ، فإنه يمثل خطوة هامة نحو تحسين الأمان والمرونة في الأنظمة التي تعتمد على الذكاء الاصطناعي[1].

1- حسن نايف مبارك الحجرف، دور الذكاء الاصطناعي في تعزيز الأمن السيبراني، رؤى نظرية، ص 14085.

الخاتمة

وفي خاتمة هذه الدراسة يمكن الخروج ببعض النتائج والتوصيات المستخلصة من هذه الورقة البحثية

أولا: النتائج:

1-يمثل الذكاء الاصطناعي تقدُّمًا هائلاً في مجال التكنولوجيا، وله فوائد وتطبيقات كثيرة، وهو سيف ذو حدين، ولذلك يجب استخدامه بشكل مسؤول وفقًا للقوانين والأخلاقيات، وإلا أدَّى إلى كوارث هائلة.

2-يجب التركيز على حماية الخصوصية، والعمل على جعل الذكاء الاصطناعي فضاءً رقميا أكثر أمانًا، ووسيلة فعَّالة في خدمة الأمن السيبراني لحماية مصالح الدولة، ومؤسساتها العامة والخاصة.

3-يجب فرض العقوبات على سوء استخدام الذكاء الاصطناعي وتعزيز الأمن السيبراني

4-تطبيقات الذكاء الاصطناعي مهمة جدا في الحفاظ على خصوصيا رواد ومستخدمي مختلف المنصات في البيئة الرقمية الحديثة.

5-أوضحت الدراسة أن هناك حاجة لتطوير إطار قانوني وأخلاقي يضمن استخدام التكنولوجيا بشكل مسؤول وفعَّال داخل المؤسسات والمنظمات.

6-بناءً على النتائج المحققة، يجب على الجهات المعنية الاستثمار في تعزيز البنية التحتية، وتطوير السياسات والإجراءات اللازمة من أجل تطبيق الذكاء الاصطناعي بشكل فعَّال في مجال الأمن السيبراني.

7-الاتفاق الدولي لمواجهة الحروب السيبرانية، نظرًا لخطورة الوضع أبدت بعض الدول استعدادها لخوض مثل هذه الحروب، حيث أنشأت جيوشا سيبرانية، في حين عقدت دول أخرى اتفاقيات سياسية وعسكرية لمواجهة هذه الحروب، مثلا لقد توصَّلت الولايات المتحدة

الأمريكية والصين سنة 1015 لاتفاق خاص بالحروب السيبرانية، يقضي بعدم شنّ أي هجوم سيبراني بين الدولتين على البنية التحية وشركات القطاع الخاص في حالة السلم.

8-يجب على الدولة الجزائرية أن تولي أهمية كبيرة للذكاء الاصطناعي لتوفير الأمن السيبراني لجميع مؤسساتها العامة والخاصة، ومصالحها، باعتباره وسيلة فعَّالة وناجعة لمواجهة أي تهديد سيبراني داخلي أو خارجي.

9-رعاية الكفاءات الوطنية التي أثبتت قدراتها في مجال الذكاء الاصطناعي، والتبني بالرعاية والتمويل

الجدّيين الأفكار الواردة في مذكرات تخرّج طلبة التكنولوجيا ونظم المعلوماتية والذكاء الاصطناعي.

10-العمل على تكوين الكفاءات البشرية في مجال الذكاء الاصطناعي لمواجهة التهديدات السيبرانية الداخلية والخارجية من أجل حماية مصالحها.

ثانيا: التوصيات

1-تعزيز البنية التحتية السيبرانية: يجب على المؤسسات والمنظمات العمل في تطبيق التقنيات المتقدمة مثل الذكاء الاصطناعي في تحسين البنية التحتية حماية لمصالحها من الهجمات السيبرانية.

2-تدريب وتأهيل الموارد البشرية: ينبغي تعزيز التدريب والتأهيل للمتخصصين في مجال الأمن السيبراني لفهم

واستخدام التقنيات الحديثة بشكل فعاَّل.

3-يجب تطوير الإطار القانوني، والتنظيمي، والأخلاقي من أجل ضمان استخدام الذكاء الاصطناعي في الأمن السيبراني بطريقة مسؤولة ومتوازنة.

4-إنشاء معاهد متخصصة تعني بالتكوين في تكنولوجيا الذكاء الاصطناعي تستقبل نخبة الطلبة في العلوم والرياضيات والفيزياء.

5-تشجيع وتعزيز الشراكة مع وزارة التعليم العالي والبحث العلمي ورعاية الطاقات الشابة التي تزخر بها، مع تبنّي مشاريع الذكاء الاصطناعي خاصة تلك التي تعزز الأمن السيبراني.

قائمة المصادروالمراجع

القرآن الكريم

السنة النبوية

1-ميمي جمال، الذكاء الاصطناعي في الجزائر، بين المخاطر والمساهمة في تحقيق الأمن السيبراني، مجلة المعيار المجلد 15، العدد 02، ديسمبر 2024.

2-سلسلة كتيبات تعريفية، العدد03، صندوق النقد العربي، أبو ظبي، الإمارات العربية المتحدة، 2020.

3-لحمر هيبة، التحول إلى الذكاء الاصطناعي بين المخاوف والتطلعات-التجربة الإماراتية نموذجا، مجلة الاقتصاد والتنمية، المجلد 09العدد02، 2021.

4-هناء رزق محمد، أنظمة الذكاء الاصطناعي ومستقبل التعلُّم، مجلة دراسات في التعليم الجامعي، العدد52، 2021.

5-عبد الله بن شرف الغامدي، الذكاء الاصطناعي للتنفيذيين، سلسلة الأدلة الإرشادية، الهيئة السعودية للبيانات والذكاء الاصطناعي.

6-هاشم ناصر الدين محمود سويدان، الحماية القانونية للمصنفات الناشئة عن برامج الذكاء الاصطناعي، مجلة قبس للدراسات الإنسانية والاجتماعية، المجلد 07، العدد 02، 2023.

7-حسن نايف مبارك الحجرف، دور الذكاء الاصطناعي في تعزيز الأمن السيبراني، رؤى نظرية، 2024.

8-خليل سعيدي، مرزوق بن مهدي، الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبراني، مجلة دراسات في حقوق الانسان، المجلد06، العدد01، 2022.

9-محمد دحماني، الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني والسياسي، المجلد 07، العدد 02.

10-نرمين مجدي، الذكاء الاصطناعي وتعلم الآلة، سلسلة كتيبات تعريفية، العدد03، صندوق النقد العربي، أبو ظبي، الإمارات العربية المتحدة، 2020.

11- ابن منظور، لسان العرب، دار المعارف، باب الهمزة، ص 140.

12-إسلام فوزي، الأمن السيبراني، الأبعاد الاجتماعية والقانونية، تحليل سوسيولوجي، المجلة الاجتماعية القومية، المجلد 56، العدد 02، 2019.

13-إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، جامعة العربي تبسي، المجلد01، العدد 01، 2019.

14-**إسلام** فوزي، الأمن السيبراني الأبعاد الاجتماعية والقانونية تحليل سوسيولوجى، ص 101.

15-مني عبد الله السمحان، متطلبات تحقيق الآمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية بالمنصورة، المجلد 111، العدد01، 2020.

17- العتيبي، عبدالرحمن بجاد شارع، دور الأمن السيبراني في تحقيق رؤية 2030، رسالة ماجستير، جامعة نايف العربية للعوم الأمنية، 2020.

18- مختار محمد، الأمن السيبراني مفاهيم المستقبل، مجلة اتجاهات الأحداث، 2023.

19-إسلام فوزي، الأمن السيبراني، الأبعاد الاجتماعية والقانونية تحليل سوسيولوجى.

19-حداوي، وآخرون، القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في المنظمات-دراسة تحليلية لآراء

20-حسن نايف مبارك الحجرف، دور الذكاء الاصطناعي في تعزيز الأمن السيبراني، رؤى نظرية.

21-دراسة العقل البشري يتفوق على الذكاء الاصطناعي بالتفكير الذكي والمرن/

https://aawsat.com

22-هل يمكن للذكاء الاصطناعي أن يتفوق على العقل البشري/

https://www.google.com/search

23-هل يمكن أن يتفوق الذكاء الاصطناعي على البشر/

https://misbar.com/qna/2023/10/19

21-الأمن السيبراني مفهومه وتاريخه**19/9/2024//**

https://www.aljazeera.net/encyclopedia

22-لأمن السيبراني مفهومه وتاريخه19/9/2024//

https://www.aljazeera.net/encyclopedia

Chapter 03

Protecting Digital Sovereignty in the Context of Contemporary Cybersecurity Challenges

حماية السيادة الرقمية في إطار التحديات الأمنية السيبرانية المعاصرة

Dr. Benguettat Khadidja

Doctor of Law, Lecturer A, Faculty of Law and Political Sciences,

University of Mostaganem, Algeria

Dr. Latroche Amina

Doctor of Law, Lecturer A, Faculty of Law and Political Sciences,

University of Mostaganem,, Algeria

Abstract:

This research addresses the topic of "Digital Sovereignty and its Protection within the Framework of Cybersecurity," discussing the importance of digital sovereignty as a right for nations to control their digital space and protect their data and national interests amidst rapid technological changes. The cyberspace has become a complex field facing increasing threats, from cyber-attacks to espionage, necessitating the enhancement of international legal frameworks that

protect digital sovereignty. Different nations have varying perspectives on managing cyberspace; some, like China and Russia, adopt a strict policy for controlling the internet, whereas others, such as the United States, reject this concept, considering cyberspace as public property. The study also presents an international approach to enhancing legal protection for digital sovereignty, focusing on the 2001 Budapest Convention, which is the first international legal framework for combating cybercrimes. The situation calls for strengthening international cooperation and achieving a balance between protecting digital sovereignty and individual rights, contributing to enhanced cybersecurity and the protection of national interests in the digital age.

Keywords: Digital Sovereignty, Cybersecurity, Digital Space, Cyber Crimes, Budapest Convention.

ملخص:

يتناول هذا البحث موضوع "السيادة الرقمية وحمايتها في إطار الأمن السيبراني"، حيث يناقش أهمية السيادة الرقمية كحق للدول في السيطرة على فضائها الرقمي وحماية بياناتها ومصالحها الوطنية في ظل التحولات التكنولوجية المتسارعة. وقد أصبح الفضاء السيبراني ميدانًا معقدًا يواجه تهديدات متزايدة، من هجمات إلكترونية إلى تجسس إلكتروني، مما يستدعي تعزيز الأطر القانونية الدولية التي تحمي السيادة الرقمية، حيث تختلف رؤية الدول حول كيفية إدارة الفضاء السيبراني، إذ نجد بعض الدول تتبنى سياسة صارمة للسيطرة على الإنترنت، مثل الصين وروسيا، بينما ترفض دول أخرى مثل الولايات المتحدة هذا المفهوم، معتبرة أن الفضاء الرقمي هو ملكية عامة. كما يعرض البحث المقاربة الدولية لتعزيز الحماية القانونية للسيادة

الرقمية، مع التركيز على اتفاقية بودابست لعام 2001 التي تعتبر الإطار القانوني الدولي الأول لمكافحة الجرائم السيبرانية. إن الوضع يستدعي تعزيز التعاون الدولي وتحقيق توازن بين حماية السيادة الرقمية وحقوق الأفراد، مما يساهم في تعزيز الأمن السيبراني وحماية مصالح الدول في العصر الرقمي.

الكلمة المفتاحية: السيادة الرقمية، الأمن السيبراني، الفضاء الرقمي، الجرائم السيبرانية، اتفاقية

Introduction:

Digital surveillance for protecting national security is a sovereign domain, long considered by states to be a reserved area almost impervious to any form of regulation. There is no binding regulation on digital surveillance on a global scale, despite an unprecedented global awareness of the extent of intervention by public and private digital entities in fundamental rights. This awareness has hastened the inclusion of this activity within the scope of legitimate oversight. The term "digital sovereignty" has been in use since 2012 during the World Conference on International Telecommunications, particularly by Russia and China, who have demanded the restoration of their "sovereign rights" over network management and the establishment of an international treaty to better share responsibilities.

Digital sovereignty has become one of the most prominent issues facing nations both nationally and internationally. The concept refers to the right of states to independently control their digital space and manage their electronic resources, including data and digital infrastructure. However, this right is increasingly threatened by cyber assaults, such as hacking, electronic espionage, and attacks targeting critical infrastructure.

The importance of this topic stems from the growing role of digital space in achieving national security and sovereignty, as well as its direct impact on data protection and the continuity of essential services. Its significance is also evident in the urgent need to establish effective legal and regulatory frameworks to protect states from digital attacks and to enhance international cooperation to address shared challenges in this field.

This research aims to highlight the concept of digital sovereignty and identify forms of assaults on it, while reviewing the international mechanisms available for its protection, and the role of the United Nations in enhancing this protection. It also seeks to provide practical recommendations that contribute to achieving a balance between protecting digital sovereignty and international cooperation.

The fundamental problem of this research stems from the following question:

How can the legal and political protection of digital sovereignty be enhanced in the face of increasing challenges posed by the digital space?

This research relies on the descriptive analytical approach to understand the concept of digital sovereignty and analyze forms of

assaults on it, in addition to the legal approach to study the relevant international mechanisms.

To answer the posed problem, the first section will discuss the nature of digital sovereignty, followed by an international approach to preserving digital sovereignty in the second section.

1. The Nature of Digital Sovereignty

Digital sovereignty is a modern concept associated with the rapid technological developments the world has witnessed in recent decades. This term reflects the state's ability to exercise its authority and control over cyberspace, which includes data, digital infrastructure, and information flows within and beyond its borders. Digital sovereignty aims to protect national interests in the digital environment and ensure the technological resources are utilized in a way that serves national security and economic development. Although digital sovereignty is an extension of traditional sovereignty, it raises numerous legal and political challenges, especially given the transboundary nature of digital space, necessitating the adaptation of traditional concepts to the new digital reality.

1.1 The Concept of Digital Sovereignty

In the context of rapid digital transformation, the concept of digital sovereignty has emerged as a fundamental tool for enhancing

state control over its digital resources and protecting its cyberspace. This concept refers to the right of states to manage their data and control the digital infrastructure within their national borders, ensuring their security and independence in the digital world.

1.1.1 Definition of Digital Sovereignty

The concept of sovereignty is linked to the Treaty of Westphalia of 1648, which established the principle of state sovereignty over its territories and the management of its internal affairs without external interference. This principle is a fundamental foundation of modern international law and has garnered significant attention from scholars of international law and political researchers[1]. Definitions of sovereignty vary depending on intellectual starting points and the circumstances surrounding the emergence of the concept of sovereignty. The English word "Sovereignty" is derived from the Latin word "Superanus," which means "supreme" or "highest." Jean Bodin (1530-1596) was the first to use this term in his book "The Six Books of the Republic," where he presented the first comprehensive theory about sovereignty[2]. John Austin (1790-1859), a pioneer of the classical theory, formulated the theory of sovereignty on the basis that the state is a legal system

1- Ali Sadiq Abu Haif, "Public International Law," Knowledge Establishment, Alexandria, 1995, p. 35.

2- Al-Sadiq Al-Sheibani, "The Crisis of Contemporary Democracy," Al-Shorouk Press, Cairo, n.d., p. 50.

embodied in a supreme authority acting as the ultimate source of power[1]. The principle of sovereignty is a fundamental pillar upon which the theory of the state depends, and thus the term sovereignty is synonymous with the term state in international politics. There is no sovereignty without a state, and a state cannot exist without sovereignty.

In the international system, the concept of "sovereignty" has undergone a significant transformation from being absolute to relative, due to ongoing global changes. One of the most notable developments that contributed to this shift is cyberspace, which posed a challenge to the traditional concept of sovereignty in international law. This challenge is one of the most significant indicators of the need to reconsider concepts of control and management, as cyberspace has added a new dimension to international interactions, requiring a reassessment of sovereignty mechanisms in this field[2].

The idea of "digital sovereignty" emerged in the early 2000s. In 2011, Pierre Bellanger, the head of "Skyrock," made an initial attempt to define this concept: "Digital sovereignty is the control of our present and our destiny as they appear and are directed through

1- Abdel Wahab Al-Kayyali, "Political Encyclopedia," Vol. 2, 2nd edition, Arab Institute for Publishing and Distribution, Beirut, 1996, p. 163.

2- Indira Araji, "Power in Cyberspace; A Modern Era of Challenge and Response," Dar Mirza, Beirut, 2019, pp. 83-86.

the use of technology and information networks[1]." Therefore, achieving digital sovereignty has become a common goal among companies, public entities, and recently, Internet users, whether they are citizens or consumers[2].

Digital sovereignty was defined as "the state's extension of its control and jurisdiction over the digital space represented by the Internet[3]." It was also defined as "a legal technical domain characterized by state, corporate, and individual claims to control it, meaning the subjection of cyberspace to the interests and values of the state, thereby enabling the latter to control its cyberspace to ensure it follows the same rules, standards, and considerations present in society[4]." In its 2019 report, the Senate's Commission of Inquiry on Digital Sovereignty defined digital sovereignty as: "The state's ability to act in cyberspace (...) which is a necessary condition to maintain our values, (...) including, on one hand, the autonomous

---

1- Pierre Bellanger, "On Sovereignty in General and Digital Sovereignty in Particular," Les Échos, August 30, 2011 (archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm). Accessed on: September 18, 2024.

2- Nicolas Colin and Henri Verdier, "Digital Sovereignty: The Industrial Path," paristechreview.com, June 30, 2014 (www.paristechreview.com/2014/06/30/souverainete-numerique). Accessed on: September 16, 2024.

3- Mohamed Saadi, "The Impact of Emerging Technology on Public International Law," Dar Al-Jamea Al-Jadida, Egypt, 2014, p. 240.

4- Marwa Zein El-Abidin Saad, "The Impact of the Changing Concept of Sovereignty on Judicial Jurisdiction in Cybercrimes," International Journal of Jurisprudence, Judiciary, and Legislation, Judges Club of Egypt, Egypt, Volume 3, Issue 3, October 2022, p. 703.

capability to assess, make decisions, and act in cyberspace, and on the other hand, control over our networks, electronic communications, and data[1]."

Thus, cyber sovereignty refers to the ability of states to control the electronic space that includes digital infrastructure and data within their borders or that affect their security and interests. Countries like China are embracing their cyber sovereignty by allocating substantial resources to the electronics industry and controlling this space, as the concept of cyber sovereignty relates to national control of electronic space serving the state's political, economic, security, and cultural interests.

1.1.2 Forms of Assault on the Digital Sovereignty of States

An assault on digital sovereignty refers to the violations that states endure in their ability to manage and protect their digital data and information. There are various forms of assaults on the digital sovereignty of states, among the most prominent are:

A. Cyber Attack

This involves the use of electromagnetic energy or anti-radiation weapons to attack individuals and facilities with the goal of

[1]- Inria Institute, "Digital Sovereignty: What Role for Research?", in: https://www.inria.fr/fr/souverainete-numerique-role-recherche, March 29, 2021. Accessed on: September 18, 2024.

weakening the enemy's combat capability and reducing their effective use of the electromagnetic spectrum. These attacks include jamming and electromagnetic deception. Typically, the losses resulting from a cyber-attack led to substantial material damages, unlike traditional warfare, which involves human casualties[1]. Examples of cyber-attacks include disrupting logistical support systems to reduce support for enemy forces and decrease their effectiveness, and controlling power generation systems.

B. Cyber Espionage as a Violation of Digital Sovereignty

Cyber espionage is one of the most crucial preliminary stages of cyber warfare operations and is defined as the unauthorized interception of communication systems, networks, and data with the intent of obtaining and manipulating information. Cyber espionage is among the first forms of threats that affect national security and pose a risk to the interests of states and individuals[2]. It refers to deliberate attempts to penetrate computer systems and websites of a rival state or adversary to steal confidential information. This type of espionage aims to acquire a vast database related to military, political, security, economic, and industrial systems and secrets. These

1- Mohamed Atef Imam Ibrahim, "Cyberspace and Its Impact on National Security of States: The Case of Cyber Warfare," Research Studies, Arab Democratic Center, April 23, 2022, HTTPS://DEMOCRATICAC.DE/?P=81775. Accessed on: September 10, 2024.

2- Karim Raqouli and Lakhdar Nouioua, "Mediterranean Cybersecurity Between Reality and Security Stakes." Tabna Journal of Academic Scientific Studies. Volume 2, Issue 2, 2019, p. 74.

operations rely entirely on modern technological communication and networking systems within states[1].

In the current era, espionage has transcended military and warfare scopes to include various fields such as economics, technology, politics, and industry. Although military espionage still holds significant importance and is considered one of the most dangerous types of espionage, the nature of the information required today has changed significantly. In the past, secret information revolved around the size of armies and their equipment, and such information was considered extremely important. Now, this data is more widely available, published in newspapers and media, and the maps showing troop distributions in conflict zones are openly discussed. Modern espionage focuses more on precise and advanced information, such as modern military technology, strategic economic data, and knowledge related to scientific and industrial developments. This change reflects the significant transformations in the concept of national security and the importance of information in the digital age[2].

---

[1]- Sharifa Klaa, "Cybersecurity and the Challenges of Espionage and Cyber Breaches for States Across Cyberspace," Journal of Law and Humanities, University of Djelfa, Volume 15, Issue 1, 2022, p. 295.

[2]- Samia Bouchoucha, Haya Salmani, "Electronic Espionage and Methods of Combating It," Journal of Social Sciences and Humanities, University of Tebessa, Volume 16, Issue 1, 2023, p. 54.

C. Cyber Intrusions

Cyber intrusions involve breaching systems to obtain intelligence information about a state or organization. It is a system or program designed to exploit the opponent's data and damage it, as well as to disrupt their computer system, with the goal of gaining superiority in security, military, and political domains. This process occurs at multiple levels, whether individual, institutional, or state-level. Cyber intrusions take various forms, but ultimately aim to access and seize critical information from the adversary, using computer systems that target the information infrastructure of the intended entity[1].

D. Attacks on Critical Infrastructure

Denial-of-service attacks might seem to cause relatively minor damage in the cyberspace of states, but they can lead to significant financial costs and losses if the service disruption continues for an entire week. If the attacks target infrastructure, the real-world losses can be tremendous, especially when industrial operations and the administrative systems associated with them are targeted. For example, a group of hackers could manipulate systems related to

[1]- Ali Mohamed Mahmoud, "Cyber Space Wars and Their Relation to Fifth Generation Wars," Dar Al Maaref, Egypt, 2020, pp. 55-56.

energy, such as oil and gas pipelines, fuel production plants, and power generation stations[1].

Regardless of the exact number of electronic activities and operations targeting critical infrastructure, many actual incidents have occurred that justify increasing concern about securing this infrastructure, which has become increasingly interconnected. For example, in early 2020, cybercrime attacks targeting Brno University Hospital in the Czech Republic forced the hospital to suspend scheduled surgical operations and redirect patients to other nearby facilities. In another incident four years prior, the Ukrainian electricity distribution company reported a network outage lasting several hours due to a cyberattack targeting computers and Supervisory Control and Data Acquisition (SCADA) systems, causing a power outage affecting about 225,000 customers[2].

E. Cyber Hacking

Hacking involves unauthorized access to other people's devices and their electronic networks, aiming to compromise the confidentiality and privacy of individuals or to impact the integrity

[1]- Nour El-Din Hamed Ali Ibrahim, "Cyberspace: Concepts and Dimensions," Scientific Journal of Research and Commercial Studies, Helwan University, Volume 38, Issue 2, 2024, pp. 737-738.

[2]- Lee, Robert M., Michael J. Assante & Tim Conway, 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid," SANS & E-ISAC, March 18. As of October 21, 2020: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, Accessed on: September 01, 2024.

of content by altering or destroying it[1]. Hacking does not just target the personal information of citizens; it goes further by exposing state security secrets and breaching the websites of governmental institutions and the emails of some world leaders, especially those from countries that have experienced civil wars. The last decade has witnessed unprecedented leaks characterized by secrecy and detailed information about targeted international figures, aimed at overthrowing them or creating problems and disturbances within the countries they belong to[2].

F. Attacks on Military Systems

These target weapon control systems, satellites, or military communication systems to disrupt warfare operations. Attacks on military and governmental operations typically involve targeting systems on a daily basis, often as a fundamental part of espionage. These attacks aim either to obtain weapon designs, access confidential information, understand the enemy's thinking during a war, or learn about military plans and troop positioning. Therefore, any network connected to the Internet is vulnerable to attacks, and even those not connected are not necessarily safe from danger. Governments and militaries rely on these networks during

1- Leila Baouni, "Threats in Cyberspace and Their Reflections on Digital Sovereignty: Cyber Piracy as a Model," Strategia Journal, Military Institute for Documentation, Evaluation, and Reception, Volume 8, Issue 2, 2021, p. 9.

2- ibid, p. 18.

peacetime, but this does not mean that relying on them in wartime is safe. In fact, the advantage of advanced military technology for modern armies can turn into a disaster if it is subjected to cyberattacks that lead to its disruption[1].

These are some examples that reflect the different forms of cyber warfare, which rely on digital technologies to impact states and organizations. These forms pose a real challenge to digital sovereignty and require an effective response from governments to enhance cybersecurity and protect sensitive data and information.

1.2 The Issue of Recognizing States' Sovereignty over Their Digital Space

Political scholars differ on the impact of cybersecurity on state sovereignty. Daniel Lambach believes that cyberspace has enhanced state sovereignty through what is known as "electronic sovereignty" or "data sovereignty," which refers to the imposition of national sovereignty in cyberspace, meaning the formation of areas with national sovereignty in this space. This concept relies on the theory of practice and the dual concepts of relocalization, also known as "territorial ontology."

The ways in which actors (such as states) exercise control over cyberspace include cutting off the internet during times of political

[1]- Nour El-Din Hamed Ali Ibrahim, op. cit., p. 737.

crisis, controlling codes and algorithms through artificial intelligence technologies, and imposing strict censorship on content, as is the case in Turkey and Thailand. Additionally, states resort to national hacking or imposing "data localization" laws that prevent data from being transferred across borders, as in the cases of Russia and China, reflecting a regular display of state power.

There are many tools available for states seeking to re-establish their national territories in cyberspace, such as blocking Internet Protocol (IP) and monitoring keywords to track discussions on sensitive topics, and blocking access to websites considered subversive[1]. These measures have been implemented in several countries, such as the "Great Firewall" in China and the strict government internet control systems in North Korea. However, some believe that cybersecurity poses a threat to state sovereignty due to hacking operations and cyberattacks, such as shadow broker attacks and electronic vulnerabilities that cross state borders.

The issue of recognizing digital sovereignty for states arises from the negative stances adopted by some countries. Not all countries have yet recognized digital sovereignty in cyberspace, as policies and practices vary from one country to another. Some countries, like the United States, consider cyberspace to be a part of

[1]- Daniel Lambach, "The Territorialization of Cyberspace," International Studies Review, Vol. 22, Issue 3, September 2020, pp. 482–506.

the global commons, and therefore sovereignty cannot be transferred to this space. On the other hand, other countries have a different vision, believing that control is necessary to limit the impacts of cyberspace and its reflections on state security[1]. China adopts a strong policy to control cyberspace, reflecting its concept of digital sovereignty. The European Union focuses on data protection through the General Data Protection Regulation (GDPR) and considers data as part of national sovereignty. These countries realize that cyberspace can affect their national security, prompting them to take stricter measures to control information and infrastructure, and to enact various laws for data protection and cybersecurity, reflecting their views on digital sovereignty. These legislations sometimes lead to legal conflicts between countries, especially regarding cross-border data exchange.

Despite the increasing need for international cooperation to face global cybersecurity challenges, this cooperation can be complicated due to differences in national policies. Countries have sought to control and assert their jurisdiction over the internet by regulating their electronic space, aiming to preserve it. These efforts reflect the determination of states to combat actions that threaten the trust, integrity, and security of their virtual community, especially with the increasing cyberattacks.

[1]- Indira Araji, op. cit., p. 112.

2. The International Approach to Preserving Digital Sovereignty

Sovereignty is a fundamental principle of international law, as widely accepted in the 1928 international arbitration decision regarding the Island of Palmas. In this context, numerous statements from the United Nations, NATO, the Organization for Security and Co-operation in Europe, the European Union, as well as most countries individually, affirm that international law applies to cyberspace. Accordingly, offensive cyber operations that violate state sovereignty are considered explicit violations of international law, resulting in "international responsibility[1]."

2.1 Enhancing International Legal Protection for Cybersecurity

The 2001 Budapest Convention, also known as the Cybercrime Convention, is the first international treaty aimed at combating cybercrimes by providing a common legal framework for member states to regulate and coordinate their efforts against crimes occurring over the internet. Signed in Budapest, Hungary, on November 23, 2001, and effective from July 1, 2004, the convention calls for the harmonization of national legislations related to cybercrime, defining crimes such as unauthorized access to computer

[1]- Marwa Zein El-Abidin Saad, op. cit, p. 707.

systems, cyber fraud, data assault, and infringement of intellectual property rights. The convention also includes measures to enhance international cooperation among member states to facilitate the exchange of information and assist in cross-border investigations and legal actions[1].

The Budapest Convention plays an important role in enhancing digital sovereignty by providing an international legal framework to address cybercrimes. However, there are challenges related to digital sovereignty within the context of this convention. On one hand, the convention contributes to the protection of digital sovereignty of states by providing legal and procedural tools that help combat cybercrimes that may threaten their digital security. The convention enables states to update their legislations and practices to align with technological advancements and enhances international cooperation in combating transnational cybercrimes.

On the other hand, there is sometimes debate about the impact of this convention on the digital sovereignty of states, as the commitment to information exchange and cooperation with other countries may pose challenges related to the protection of national data and privacy rights. Some countries may see this convention as

1- Suleiman Qataf, Abdel Halim Bougrien, "The Substantive Legal Mechanisms to Combat Cybercrime under the Budapest Convention and Algerian Legislation," Academic Journal of Legal and Political Research, University of Laghouat, Volume 6, Issue 1, 2022, pp. 337, 339.

a restriction on their digital sovereignty, especially if it requires them to cooperate on issues related to their national security or sensitive information.

Thus, it can be said that the Budapest Convention represents an important step in enhancing digital sovereignty by protecting cyberspace from crimes, but it also poses challenges associated with balancing international cooperation and protecting national sovereignty.

2.2 The United Nations' Intervention to Protect Digital Sovereignty

The United Nations plays an increasingly important role in protecting the digital sovereignty of nations through various efforts to enhance cybersecurity and address digital threats. These efforts include several axes, most notably:

2.2.1 Enhancing International Legal Frameworks

Interest in addressing activities that infringe digital sovereignty at the United Nations level began during the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Havana, Cuba, from August 27 to September 7, 1990. At this congress, the General Assembly adopted a resolution concerning legislation related to cybercrime. This conference was followed by many activities aimed at strengthening the defense of

state digital sovereignty. In 1994, efforts in this field intensified, and in 2005, during the Eleventh United Nations Congress on Crime Prevention and Criminal Justice held in Bangkok, Thailand, the United Nations adopted a declaration calling for the unification and coordination of legislation related to combating cybercrime. This declaration reflects the organization's commitment to addressing threats to state sovereignty in cyberspace[1].

The United Nations works to develop policies and legal frameworks to enhance digital sovereignty, including the Open-ended Working Group it established in 2018 to address cybersecurity issues. This group aims to build international concepts about the laws and standards that govern the digital space.

2.2.2 Maintaining Peace and Security in Cyberspace

Reviewing many examples of cyberattacks that used cyber weapons for offensive or defensive purposes, such as the attacks on Estonia in 2007, the Natanz reactor in 2010, Deir ez-Zor in 2010, and Georgia in 2015, it is clear that their impact and implications on international peace and security are equivalent to those used in cases

1- Ahmed Shehirt, Murad Qreibiz, "Challenges of the Internet to State Sovereignty (Digital Sovereignty)," Journal of Legal and Economic Research, University Centre Aflou, Volume 5, Issue 1, 2022, p. 315.

of aggression or traditional wars[1]. Therefore, the United Nations, through institutions such as the International Security Council, addresses digital threats that may threaten international peace and security, such as cyberattacks targeting critical infrastructure. In 2021, several resolutions were adopted to encourage countries to enhance cybersecurity measures.

2.2.3 Combating Cybercrimes to Preserve Digital Sovereignty

The United Nations seeks to establish a comprehensive framework to confront this type of crime. In this context, it has presented a set of substantive and procedural rules to address these crimes, as was evident at the Twelfth United Nations Congress on Crime Prevention and Criminal Justice held in Salvador, Brazil, from April 12 to 16, 2008. Item 40 of the conference report emphasized the importance of building national capacities to combat cybercrime, including the stages of prevention, detection, investigation, and prosecution of offenders, and enhancing security in cyberspace. Item 42 of the report highlighted the importance of coordination among countries in the field of combating cybercrime. The focus was on the necessity of exchanging information about national legislations,

[1]- Widad Bou Talleb, Manal Boukorou, "The Struggle of Cyberspace and Its Impact on International Peace and Security – New Threats and Challenges and Ways to Confront Them," Journal of Legal and Social Sciences, University of Djelfa, Volume 7, Issue 4, 2022, p. 816.

enhancing cooperation and technical assistance, studying national experiences, and also the legal procedures related to cybercrimes[1].

Overall, the United Nations' efforts aim to enhance international cooperation in protecting the digital sovereignty of states, with a focus on security, privacy protection, and human rights in cyberspace. The United Nations, through programs like the United Nations Development Program, also seeks to build the technical capacities of states, especially developing countries, to help them develop strong cybersecurity defenses and protect their infrastructure from cyberattacks.

[1]- Amal Yebdi, "United Nations Efforts in Combating Cybercrime," Journal of Research in Law and Political Science, University of Tiaret, Volume 8, Issue 1, 2022, pp. 308, 308.

Conclusion

In conclusion, it can be said that digital sovereignty represents one of the significant challenges that nations face in the modern era. The importance of digital sovereignty is growing in the context of rapid technological development and increasing reliance on the digital space in various aspects of life, including the economy, politics, and security. This makes maintaining digital sovereignty a fundamental element in the age of information and technology. Nations are working to enhance their strategies to ensure that they can protect their digital interests and secure the rights of their citizens in the digital space. This requires coordination between national and international policies to achieve a secure and prosperous digital environment.

The study has reached the following conclusions:

- The digital sovereignty of states faces many threats, where a state may attempt to hack or disrupt the cyberspace of another state in order to undermine its digital sovereignty.

- States that possess strong digital sovereignty are better able to protect themselves from cyberattacks and specifically to prevent foreign control or interference in their digital systems.

- The lack of legal regulation for cyberattacks is the biggest challenge facing cyberspace, despite the existence of international will at the level of negotiations and United Nations resolutions. However, this will is not effectively implemented, especially by the major powers dominant in this field.

- There is an urgent need to develop international legal mechanisms to regulate the digital space and protect states from digital assaults.

The study concludes with the following recommendations:

- Every country should adopt comprehensive national strategies that include plans for responding to cyber emergencies, in addition to establishing a legal framework that regulates data collection and protection, focusing on protecting the rights of individuals and government bodies.

- It is essential to enhance cooperation among countries in the field of information and resource exchange about cyber threats, such as sharing data about attacks and their methods, which enhances the ability of states to confront these threats and preserve digital sovereignty.

— Modern technologies should be adopted for detecting and analyzing cyber threats, enhancing the ability of states to quickly respond to attacks and accurately identify their sources.

— It is important to enact effective international legislation to protect the digital space and enhance the ability of states to maintain their sovereignty in this field.

— Awareness of the importance of protecting personal data and privacy should be enhanced, as increasing awareness can be a key factor in strengthening digital sovereignty.

الفصل الرابع

تحديات استخدام تطبيقات الذكاء الاصطناعي في تحسين التقنيات المرتبطة بالأمن السيبراني

"دراسة تحليلية من منظور قانوني"

Challenges of Using Artificial Intelligence Applications to Improve Technologies Related to Cybersecurity "An Analytical Study from a Legal Perspective"

الأستاذ الدكتور: صدّام فيصل كوكز المحمدي

أستاذ القانون الخاص/ كلية القانون – جامعة الفلوجة/ العراق

البريد الإلكتروني: saddam.faisal@uofallujah.edu,iq

الملخص

أصبحت التقنيات الخاصة بالأمن السيبراني، تقنيات ذكية، معتمدة بصورة كبيرة على نظم الذكاء الاصطناعي، سواء في تكوين تلك التقنيات أو تشغيلها أو الأساليب والأنماط التي تعمل بموجبها، لكن هذا التطوير بات يخفي وراءه تحديات ومخاطر، لا يكون التغلّب عليها تقنياً فقط، وإنّما يكون ذلك بالمواجهة القانونية أيضاً، سواء بالاعتماد على الأنظمة القانونية القائمة، أو باستحداث نظم قانونية جديدة تتلاءم والتطور الحاصل في مجال الذكاء الاصطناعي.

لذا فإنَّ الهدف من هذه الدراسة، هو استكشاف التحديات المرتبطة باستخدام التطبيقات التقنية القائمة على الذكاء الاصطناعي، والتي يمكن أن تعرّض الأمن السيبراني للخطر، لذلك تستعرض هذه الدراسة، دور نظم الذكاء الاصطناعي في تطوير تطبيقات الأمن السيبراني، وتقترح الأساليب الفاعلية للاستفادة من تقنيات الذكاء الاصطناعي، لمواجهة

التهديدات والثغرات التي يواجهها العاملون في مجال الأمن السيبراني، وتبين في ذات الوقت التحديات التي تواجه استخدام تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني.

الكلمات المفتاحية:

الذكاء الاصطناعي، الأمن السيبراني، التهديدات السيبرانية، انتهاك الخصوصية، الهجمات السيبرانية.

Abstract

Cybersecurity technologies have become smart technologies that rely heavily on artificial intelligence systems, whether in the formation of these technologies, their operation, or the methods and patterns by which they operate. However, this development now hides behind it challenges and risks that cannot be overcome only technically, but also through legal confrontation, whether by relying on existing legal systems or by creating new legal systems that are compatible with the development taking place in the field of artificial intelligence. Therefore, the aim of this study is to explore the challenges associated with the use of technical applications based on artificial intelligence, which can expose cybersecurity to danger. Therefore, this study reviews the role of artificial intelligence systems in developing cybersecurity applications, and suggests effective methods for benefiting from artificial intelligence technologies to confront the threats and vulnerabilities faced by cybersecurity workers, while at the same time showing the challenges facing the use of artificial intelligence technologies in the field of cybersecurity.

Keywords : Artificial Intelligence, Cyber Security, Cyber Threats, Privacy Infringement, Cyber Attacks.

مُقَدِّمَة

تمهيد وتقسيم:

أثَّرت التكنولوجيا المرتبطة بنظم الذكاء الاصطناعي بشكل كبير وفعّال في مجال الأمن السيبراني، خصوصاً بعد أن امتد انتشار استخدام تطبيقات الذكاء الاصطناعي في مختلف المجالات الحياتية، وهذا التأثير رافقته بعض الميزات، كما كانت له بعض السلبيات، خصوصاً في مجال الأمن السيبراني، حيث أنَّ ما نشهده اليوم من التقدم التكنولوجي، وانتشار الأتمتة الإلكترونية للنظم الإدارية والمالية والأمنية على المستويين الوطني والدولي، أصبح سمة بارزة للقرن الحادي والعشرين، حيث نلحظ فيه ميلاً متزايداً نحو اللجوء إلى تكنولوجيا الذكاء الاصطناعي (AI :Artificial Intelligence)، واستخدام التطبيقات المتصلة به، في مجالات حياتية متنوعة، ومنها مجال الأمن السيبراني، وهو ما يظهر بشكل واضح في التوسع الهائل في القدرات الحاسوبية، والعمل المستمر على التكامل الشامل في الشبكات التي تربط المشتركين بها بواسطة الأجهزة الذكية، والتطور السريع للأعمال التجارية الإلكترونية، والتحوّل إلى رقمنة البيانات والمعلومات، بما يؤكد على إمكانات التنفيذ الفعال للنظم الإدارية والمالية والأمنية، المرتكزة على أنظمة الذكاء الاصطناعي.

والمقصود من مصطلح الأمن السيبراني (Cybersecurity)، بشكل عام هو: إرشادات أمن الإنترنت،[1] فهو: أيُّ ممارسةٍ لحماية الأنظمة المتصلة بشبكة الإنترنت، بما في ذلك الأجهزة والبرامج والبيانات، من الهجمات السيبرانية أو التلف أو الوصول غير المصرَّح به للدُّخلاء، وهذا الممارسات تكون عادة بصورة مجموعة من العمليات والتقنيات والضوابط المصمَّمة لحماية الأنظمة والشبكات والبيانات من التهديدات السيبرانية.[2]

والغاية من عمليات الأمن السيبراني، تتحدد في الحماية من المخاطر السيبرانية، والعمل على إبقائها عند مستوى مقبول، من خلال حماية أكبر عدد ممكن من الأصول الرقمية، حيث لا يقتصر دمج الأمن السيبراني بالذكاء الاصطناعي، على تأمين البيئة الرقمية، بل يشمل أيضاً

---

1. According to the ISO/IEC 27032:2023(en Cybersecurity—Guidelines for Internet security).

2. ISO/IEC. Cybersecurity — guidelines for internet security. https://standards.iteh.ai/catalog/standards/sist/2d12469a-69be-4365-88bb-05df3b0212d 2023.

تحديد قيمة الأصول المهددة، وتحديد موقع التهديد، ثم تحديد أولويات الإجراءات الحمائية، لبناء إطار دفاعي متعمّق يضمن استمرارية الخدمة.[1]

والسبب الدافع إلى هذه الدراسة، هو أنّنا نعيش عصر الابتكارات المرتبطة بنظم الذكاء الاصطناعي، ومن ثمَّ فإنَّ المخاوف بشأن أمن ورفاهية المجتمع البشري، تتزايد وعلى نحو مستمر، وذلك لإتّساع نطاق التطبيقات التي تستند إلى أنظمة الذكاء الاصطناعي، حيث هذه الدراسة تسلّط الضوء على مسائل مهمّة، تتجلّى في تحديد نقاط الضعف الكامنة في أنظمة الأمن السيبراني المعتمدة على تقنيات الذكاء الاصطناعي، وتبيّن فرص استخدام تطبيقات الذكاء الاصطناعي الناجحة، وسبل مواجهة التحديات التي تواجه تطبيق نظم الذكاء الاصطناعي في مجال الأمن السيبراني.

وجدير بالذكر هنا، أنَّ أهمية البحث في هذه الدراسة تظهر على المستويين العلمي والعلمي، في مجال التطوير والتحسين في التقنيات المستخدمة في مجال الأمن السيبراني، قد ازدادت أهميّته بشكل كبير اليوم، خصوصاً في ظل تزايد الهجمات السيبرانية التي أصبحت تستهدف البنى التحتية الحساسة للدول والمؤسسات بشكل متكرر، خصوصاً في الدول التي أضحت تعتمد على أتمتة أنظمتها الإدارية المحاسبية والمالية والاقتصادية وحتى القانونية، فضلاً عن أنشطتها العسكرية والأمنية، وكذلك نظم إمدادات المياه، والمنشآت البتروكيماوية، ومحطات الطاقة النووية، وأنظمة البنية التحتية للنقل، وانظمة إدارة انقطاع التيار الكهربائي، وغير ذلك من المجالات الحيوية، والتي بات المساس بها وتخريب البيانات الحساسة الخاصة بها هدفاً للمهاجمين والمتسللين.[2]

وممّا يزيد في إدراك أهمّية هذا الموضوع، هو ما اوصت اللجنة الكهروتقينة الدولية (IEC Comission International Electrotechnical)، ببناء أنظمة سيبرانية مرنة،

---

1. International Electrotechnical Commission. Iec — cyber security. https://drive.google.com/file/d/1j0z2tmiajq5ff8ZfDPEwbHHIFXBwJIV5/view?usp=shari (2022).

2. Tomas Pl˙eta, Manuela Tvaronavi˘cien˙e, Silvia Della Casa, and Konstantin Agafonov. Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases. Insights into regional development. Vilnius: Entrepreneurship and Sustainability Center, 2020, vol. 2, no. 3. 2020.

تتجاوز الكثير من التعقيدات والضعف، من خلال تقنيات ذكية وشاملة، تتضمن تطوير العمليات وتحسين مقدرة الأشخاص وتيسّر استخدام التقنيات المتطورة، بواسطة تطبيقات الذكاء الاصطناعي.[1]

وإشكالية البحث تتجسّد في مدى نجاعة الاساليب القانونية والتقنية، لمواجهة الحجم الهائل من التهديدات السيبرانية المتزايدة في البيئة الرقمية، خصوصاً مع اعتماد تكنولوجيا المعلومات وتكنولوجيا التشغيل الرقمية من قبل المؤسسات والإدارات المختلفة، بحيث أصبحت تدير القطاعات الحيوية العامة والخاصة في كثير من الدول، في ظل حقيقة عدم السيطرة المطلقة على الهجمات السيبرانية، وبقاء احتمالية تعرّض الأنظمة الرقمية إلى الهجمات والاختراق بصورة كبيرة، خصوصاً مع زيادة تعقيد النظام التقني والفنّي، بسبب حالة الترابط والتكامل بين الأجهزة الحاسوبية، وربطها بشبكات رقمية من خلال استخدام البرامج الذكية المتطورة، والأجهزة الخاصة بالاستشعار المتصلة بالشبكة المعلوماتية، فضلاً عن أنَّ البحث في التطبيقات القائمة على الذكاء الاصطناعي، في الأصل، متنوع بشكل كبير، ومن ثمّ ستكون المخاوف الأمنية واحتمالية التهديدات أكبر بكثير، من التدابير التي تحصّن هذه النظم ذاتها أو تحبط من فعالية الاحتياطات اللازمة لحمايتها.

ولذلك، فإنَّ الغاية من هذه الدراسة، هي إبراز الدور الإيجابي للتقنيات المستخدمة في مجال الأمن السيبراني، والتي تعتمد على تطبيقات الذكاء الاصطناعي، وبيان الآثار الإيجابية عند دمجها مع أنظمة الأمن السيبراني، فهي في الوقت الذي تعزز أمن النظم السيبرانية، ويجعلها أكثر مرونة، وفي مقابل ذلك، بيان التحديات السلبية والمخاطر التي تواجه هذا الاستخدام، حيث أنَّ نظير تلك الإيجابيات، سيكون نشوء واقعٍ يعزّز من قدرات المهاجمين على التسلّل والاختراق من قبل المتربصين.

أمّا بالنسبة لمنهجية البحث وخطته، فإنّنا سنحاول البحث في هذا الموضوع، ضمن إطار منهج علمي وصفي، نستعرض فيه المفاهيم والأطر النظرية الخاصة بموضوعات الدراسة، وكذلك نعتمد على المنهج تحليلي الذي يمكّننا من التعمّق في استعراض الأفكار المرتبطة بالموضوع، سواء على المستويين التقني والقانوني على نحو مفصّل.

---

1. International Electrotechnical Commission, op cit,

وعلى هذا فإنّنا سنبحث موضوع هذه الدراسة، وفق هيكلية انقسمت إلى مباحث ثلاث، نخصص أولها للبحث في أهميّة استخدام نظم الذكاء الاصطناعي في مجال الأمن السيبراني والمزايا المرتبطة به، وفي المبحث الثاني، نبيّن التحديات المرافقة لاستخدام نظم الذكاء الاصطناعي في مجال الأمن السيبراني، أمّا المبحث الثالث، فسنعترض المعالجة القانونية للتحديات التي تواجه مخاطر دمج الذكاء الاصطناعي في الأمن السيبراني.

وسنختتم هذه الدراسة بخاتمة، تمثّل خلاصةً لأبرز ما توصلنا إليه من نتائج ومقترحات.

المبحث الأول

أهميّة استخدام نظم الذكاء الاصطناعي في مجال الأمن السيبراني والمزايا المرتبطة به

إنَّ الوقوف على أهميّة استخدام نظم الذكاء الاصطناعي في مجال الأمن السيبراني، والتعرف على المزايا المرتبطة به، يقتضي منا تقسيم هذا المبحث إلى مطلبين مستقلّين، نخصص الأول منهما لبيان أهميّة استخدام نظم الذكاء الاصطناعي في تطوير تقنيات الأمن السيبراني، ونخصص الثاني مزايا تطبيقات الأمن السيبراني الأساسية المرتبطة بالذكاء الاصطناعي، وكما يلي:

المطلب الأول

أهميّة استخدام نظم الذكاء الاصطناعي في تطوير تقنيات الأمن السيبراني

أصبحت التكنولوجيا المتنامية التي نشهدها اليوم، تسمح بالنمو السريع لنظم الذكاء الاصطناعي في القرن الحادي والعشرين، وذلك عندما تحولت الأفكار والنظريات المفاهيمية إلى تطبيقات ملموسة،[1] حيث بدأ ذلك بوضوح في عقد التسعينيات من القرن العشرين، واستمرت هذه التطورات في تقدّم مستمر، إلى أن بتنا نواجه اليوم عالماً من التكنولوجيا التي تحيط بنا في نواح حياتنا المختلفة، تتضمن قوة حسابية متزايدة، وتتطور بشكل واعد، سوء بالنسبة لأنظمة توليد البيانات أو بالنسبة لمعالجتها، حيث بدأ مفهوم التَّعَلُّم الآلي سائداً وبارزاً في كل مجالات استخدام تلك التطبيقات الذكية.

1. Md Fazley Rafy. Artificial Intelligence in Cyber Security, arXiv:submit/5336757 (cs.AI) 8 Jan 2024, See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/377235308, p. 2.

ومع بداية القرن الحادي والعشرين، تحول التقدم في نظم التكنولوجيا المرتبطة بالذكاء الاصطناعي، بشكل ملحوظ من حالة ثابتة إلى حالة سباق متسارع، خصوصاً مع ظهور مجمّعات البيانات الضخمة، ونماذج الخوادم المتطورة، والمعالجات المعتمدة على الذكاء الاصطناعي المتطورة، حيث مكنت الخوارزميات المحسّنة، وتطور قدرات الأجهزة الحاسوبية، مثل وحدات معالجة الرسومات (GPU: Graphics Processing Unit)،[1] نظم الذكاء الاصطناعي، من معالجة طوفان ضخم من البيانات، والتَّعَلُّم منه بكفاءة غير مسبوقة.

وقد رافق هذا التطور، ازدياد تطور شبكة الإنترنت واتساعها، مع الزيادة الهائلة في القدرات الحاوسبية، والتقدم المتسارع في تكنولوجيا معالجة البيانات، وبروز الإمكانات الحقيقية لهندسة الشبكات العصبية (NN: Neural Network)، مع قدرتها على التحليل المعلوماتي المعقد، الأمر الذي دفع بعض المؤسسات الحساسة، في نهاية القرن العشرين، كالجيش الأمريكي، إلى تأكيد الحاجة إلى الذكاء الاصطناعي، لتأمين البنية الأساسية للمعلومات الوطنية ((NII: National Information Infrastructure. ولكن على الرغم من ذلك، نجد في استخدام الذكاء الاصطناعي في مجال الأمن السيبراني، فائدة في تطوير تقنيات أنظمة النظام الأمني، وتحليل كمية هائلة من البيانات، وإجراء عمليات تفتيش حاسمة لتحديد مصدر التهديدات السيبرانية، ومواجهتها والتخفيف من آثارها.[2]

إلّا أنَّ ممّا يجدر الإشارة إليه هنا، هو أنَّ استخدام هذه النظم الذكية في مجال الأمن السيبراني لم يخلُ من التحديات، والتي باتت بارزة في مواجهة الأمن السيبراني، حيث تبرز في مجموعة من التهديدات المتنوعة، من قبيل الهجمات السيبرانية الداخلية، إلى الهجمات العابرة للحدود الوطنية، في ظل الطبيعة المترابطة لأنظمة أنظمة المعلومات العسكرية والحكومية والمدنية، لذا فإنَّ التركيز لا بدَّ أن يجري بصورة دائمة على تحسين التدابير القانونية والتقنية الخاصة بالتعامل مع التكنولوجيا المتطورة باستمرار، وهو أمرٌ بالغ الأهمية، للحفاظ على فعالية البنية الأساسية التحتية للاتصالات وللمعلومات (NII).

---

1. Jeff A Stuart and John D Owens. Multi-gpu mapreduce on gpu clusters. In 2011 IEEE International Parallel & Distributed Processing Symposium, pages 1068–1079. IEEE, 2011.

2. Enn Tyugu. Artificial intelligence in cyber defense. In 2011 3rd International conference on cyber conflict, pages 1–11. IEEE, 2011.

وفي هذا الإطار، لا بدَّ أن يكشف الستار عن حقيقة مهمة مفادها، أنّه بالرغم من المخاطر والتهديدات المرتبطة بدمج تطبيقات الذكاء الاصطناعي مع نظم الأمن السيبراني، إلّا أنّه توجد ضرورة لتبنّي التطبيقات الخاصة بالذكاء الاصطناعي، كونها تساعد في الكشف عن الخروقات التي تواجه البنية الرقمية، كاقتحام الشبكة، وإدارة المخاطر الناتجة عن التأثيرات السلبية للهجوم السيبراني، وذلك لأنَّه يُمكِّن من المساعدة في:

1- تحليل كميات هائلة من البيانات المهمة الخاصة بالهجمات السيبرانية أو المهاجمين.
2- الكشف عن أنماط الهجوم السيبراني، وتوقعات الهجوم.
3- الإبلاغ عن أدوات اقتحام الشبكة، وأساليب المهاجمين.
4- تحسين قدرات صنع القرار من قبل القائمين على الإشراف والرقابة، الخاصة بتلك القطاعات أو المؤسسات المستهدفة، لمواجهة تلك التهديدات وصدِّها.
5- تحديد سبل مواجهة تلك التحديات والمخاطر، والتخفيف من آثارها الضارة.

المطلب الثاني

مزايا تطبيقات الأمن السيبراني الأساسية المرتبطة بالذكاء الاصطناعي

اعتمدت التقنيات الحديثة في الأمن السيبراني، على الممارسات القائمة على الدمج بين التقنيات المستخدمة في مجال الأمن السيبراني ونظم الذكاء الاصطناعي، ثم تطور الأمر بعد ذلك، من استخدام نظم نماذج التَّعَلُّم الآلي التقليدية، إلى استراتيجيات التَّعَلُّم بالذكاء الاصطناعي الأكثر ديناميكيةً وتكيفاً مع الظروف والأوضاع، لتوفير حلول ذكية للأمن السيبراني، بحيث أصبح بإمكان أنظمة الذكاء الاصطناعي الحديثة تحليل كميات هائلة من البيانات والعمل بها في الوقت ذاته، لتقديم تغطية أمنية أكثر شمولاً مقارنةً بالندرة في الحجم والتعقيد.

ومن أهم المزايا التي بات يضفيها استخدام نظم الذكاء الاصطناعي في تطوير وتحسين تقنيات الأمن السيبراني هي:

1- تحديد وتحليل التهديدات الحاصلة أو المحتملة، على تفسير الأنماط والانحراف في البيانات، إذ يمكن أن تعمل الإحصائيات الاحتمالية على تحسين عملية التحليل، من خلال توفير إطار لفهم احتمالية وقوع أحداث أو سلوكيات معينة، وهو أمر بالغ الأهمية للكشف عن خروقات أو هجمات أمنية محتملة، يعد التقاط وفهم الشكوك حولها لتحليل الأمن، أمراً ضرورياً للأمن السيبراني.

2- تعمل هذه التقنيات على التركيز على المعلومات الزمنية والمكانية لحركة المرور على الشبكة، تم إنشاء قواعد الذكاء الاصطناعي القائمة على الخوارزمية الجينية (GA: Genetic Algorithm) لاكتشاف عمليات التسلل إلى الشبكة باستخدام نظام اكتشاف التسلل المتكامل مع قواعد الذكاء الاصطناعي،[1] وفي عملية اكتشاف التسلل هذه، يتم استخدام عمليات مختلفة مثل ترجمة علاقات الشبكة وحركة المرور، تم إدخال أنماط ic في القواعد بمساعدة GA التي تربط مراحل تطور الكروموسوم من خلال الاختيار وإعادة التركيب والطفرة.

3- نظراً لأن ماسح الفيروسات أصبح أقل فعالية في اكتشاف البرامج الضارة المتنوعة والكبيرة، مثل الفيروسات وأحصنة طروادة والديدان، فقد تم اقتراح إطار عمل لتسهيل تحليل تهديدات سلوك البرامج الضارة من خلال تجميع البرامج الضارة المعروفة وغير المعروفة،[2] باستخدام نموذجاً لمساحة المتجه يعتمد على التَّعَلُّم الآلي للحساب الفعّال لتعيين المتجهات كأنماط سلوكية. يراقب الإطار مكالمات وإجراءات النظام ويستخدم مجموعة تعليمات البرامج الضارة لتشفير تلك المكالمات والحجج باستخدام معرفات رقمية.

4- تمكّن نماذج التَّعَلُّم الآلي التَّطبيقات الذكية من اتخاذ قرارات أو تقديم تنبؤات تستند إلى التمثيل الرياضي للبيانات المنظمة، من خلال المعالجة المسبقة للبيانات، قبل تغذيتها إلى التَّعَلُّم الآلي، وهذه هي الخطوة الأولى لتمكين الذكاء الاصطناعي في مجال الأمن السيبراني، وغالباً ما تكون الآلية قابلة للتفسير، وتولّد رؤى في البيانات، بحسب أهمية الميزة أو ترتيب الميزات الأكثر أهمية، وذلك لاتخاذ قرارات مناسبة ودقيقة، لاكتشاف السلوك المنحرف، ومن

---

[1]. Wei Li. Using genetic algorithm for network intrusion detection. Proceedings of the United States department of energy cyber security group, 1(1):8, 2004.

[2]. Konrad Rieck, Philipp Trinius, Carsten Willems, and Thorsten Holz. Automatic analysis of malware behavior using machine learning. Journal of computer security, 19(4):639–668, 2011.

ثمَّ فإنَّ فهم قرارات النموذج، أمرٌ بالغ الأهمية في هذه الأساليب، كونها تتبع هندسة الميزات، من بعد البيانات المعالجة، ومن ثم تساعد البيانات المدربة في اكتشاف الانحراف أو القيم المتطرفة في الأنماط الضارة والتنبؤ بالتهديدات.[1]

5- إمكانية أن تُستخدم نماذج التَّعَلُّم العميق المختلفة، المعتمدة على الفهم الحاسم للشبكات العصبية في الدماغ البشري، إن كيفية تفاعل الخلايا العصبية المختلفة مع بعضها البعض لاتخاذ القرارات بشكل استباقي للأحداث المعروفة وغير المعروفة، هي الوظيفة الأساسية في نمذجة الشبكات العميقة، حيث يجري بناء إحراف ماهر ونظام اكتشاف التسلّل لتحديد الأنماط المعقدة والسلوكيات المنحرفة، وهذه النماذج قادرة على التَّعَلُّم من مجموعات البيانات الكبيرة، لفهم خروقات الأمان المحتملة، وتصنيف أنواع التهديدات وتحديد الانحراف المعروف وغير المعروف، في بيئة شبكة محدّدة بالبرمجيات (SDN: Software Defined Network).

6- تهدف بعض نماذج نظم الذكاء الاصطناعي إلى معالجة اللغة الطبيعية، واستخراج وعزل تقارير التهديدات، وإدراج أكواد البرامج الضارّة من التحليل النصي، كما أنّها تساعد في تحليل واستخراج المعلومات ذات الصلة، للمساعدة في تحديد الحوادث من سجلات الأمان،[2] وتستخدم الطريقة المضمنة معالجة اللغة الطبيعية، كمرشح لعزل المحتويات الخاصة بالأمن السيبراني عن بيانات التغذية، وتقلل معالجة اللغة الطبيعية من الحاجة إلى التدخل الموجه، في خضم العمليات العادية، من خلال تحليل البيانات غير المنظمة، مثل محتوى الأمان، وسجلات التشغيل، ومعلومات التهديد، وتوفير رؤى قيمة لمتخصص الأمن السيبراني، لأداء الإجراءات الوقائية.

وفي هذا الصدد، يُعَدُّ تحديد رسائل البريد الإلكتروني الاحتيالية، مصدر قلق واسع النطاق، لتجنّب تسرّب المعلومات الشخصية، مثل تفاصيل الحساب المصرفي، وأرقام الضمان الاجتماعي، وكلمات مرور المستخدم، حيث تفتقر نماذج التَّعَلُّم الآلي المعاصرة إلى الدقة في هذا المجال، بسبب الاعتماد على الكشف اليدوي عن الميزات التمثيلية، وتواجه نماذج التَّعَلُّم

[1]. H Wang, ZeZXeZBePJ Lei, X Zhang, B Zhou, and J Peng. Machine learning basics. Deep learning, pages 98–164, 2016.

[2]. Iqbal H Sarker, Md Hasan Furhad, and Raza Nowrozy. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2:1–18, 2021.

العميق، تحديات مُماثلة، بسبب نقص الكلمات المضمنة في النموذج، لتمثيل المحتوى بشكل صحيح، في محادثة البريد الإلكتروني.

1- نظراً للحجم الهائل لمحتوى المعلوماتي في شبكة الانترنت، وكثرة البيانات وانتشار البرامج المفتوحة المصدر، يواجه غالباً محللوا الأمن السيبراني عقبات في اكتشاف المحتوى المرتبط بالتهديدات الإلكترونية عبر الإنترنت، على الأقل في غضون الوقت الأمثل، ولهذا تم ابتكار نظام آلي ذكي لمعالجة هذه البيانات وتجاوز هذه المشكلة، عن طريق استخراج المحتوى الإلكتروني المهدد من البيانات المتاحة للجمهور عبر شبكة الإنترنت، باستخدام طريقة مضمنة بشكل طبيعي، يشار إليها باسم Doc2Vec.[1]

[1]. وهذه الطريقة، نهج قائم على الشبكة العصبية يتعلم التمثيل الموزع للمستندات، فهي تقنية تعلم غير خاضعة للإشراف تقوم بربط كل مستند بمتجه بطول ثابت في مساحة عالية الأبعاد...

Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada. Identification of cybersecurity specific content using the doc2vec language model. In 2019 IEEE 43rd annual com- puter software and applications conference (COMPSAC), volume 1, pages 396–401. IEEE, 2019.

المبحث الثاني

التحديات والمخاوف المصاحبة لدمج نظم الذكاء الاصطناعي في تقنيات الأمن السيبراني

تثير عملية دمج نظم الذكاء الاصطناعي في تقنيات الأمن السيبراني، العديد من التحديات، والمخاوف، والتي ترجع أساساً إلى الخصوصية التي تتمتع بها البيئة الرقمية والفضاء السيبراني، حث تكون هذه المخاطر مصاحبة لأي نشاط داخل الشبكة بشكل عام، حيث الجميع يكون معرضاً لهذه المخاطر، ولا ينجو منها أحد عبر الشبكة.

ولذلك فإنّ الوقوف على هذه التحديات والمخاوف، يتطلّب منّا تقسيم هذا المبحث إلى مطلبين، نخصص المطلب الأول، للتحديات المرافقة لاستخدام نظم الذكاء الاصطناعي في مجال الأمن السيبراني، أمّا المطلب الثاني، فسنبيّن فيه: المخاوف المرتبطة بدمج نظم الذكاء الاصطناعي بتقنيات الأمن السيبراني، وعلى النحو الآتي:

المطلب الأول

التحديات المرافقة لاستخدام نظم الذكاء الاصطناعي في مجال الأمن السيبراني

في الوقت الذي لم تتحقق الفرص المأمولة من دمج تقنيات الأمن السيبراني مع نظم الذكاء الاصطناعي بالكامل بعد، فإنَّ هذه التقنيات المدمجة بدأت تواجه معوقات تقف أمام هذا التقدم، وتعرقل مسيرة تطوير استخدام هذه التطبيقات في مجال الأمن السيبراني، ومن هذه المعوقات، بعض التحديات والقيود التي يفرضها الذكاء الاصطناعي ذاته، في مجال الأمن السيبراني، ففي الوقت الذي تتزايد فيه فعالية وكفاءة تقنيات الذكاء الاصطناعي الأمنية، بدأت الجهات التي تعتمد على الذكاء الاصطناعي الخبيث في إيجاد الحلول للمراوغة والتهرب من الاكتشاف، وتجاوز النظم الأمنية من خلال توليد هجمات معقدة.

وأهم هذه التحديات التي تواجه استخدام نظم الذكاء الاصطناعي في تقييمات الأمن السيبراني، هي:

1- تحدي تجميع وتحليل البيانات

حيث أنَّ النماذج والاستراتيجيات المعتمدة في الأمن السيبراني، قائمة بشكل كبير على جودة البيانات، وتوافر كمّيّة هائلة من البيانات، لتعَلُّم تمثيل الأنماط المثلى، ومن دون المعرفة المناسبة بالنظام، من خلال البيانات الضخمة والجودة، يمكن أن يفتقر الذكاء الاصطناعي إلى الأداء، للدفاع ضد التهديدات السيبرانية غير المسبوقة، ففهم هذه القيود والأنماط، يعدُّ أمراً بالغ الأهمّيّة، للاستخدام والتشغيل الفعّال لتطبيقات الذكاء الاصطناعي، فهناك العديد من التقنيات الحديثة للعمل على أبعاد ومقاييس أصغر للبيانات لتعَلُّم الأنماط، على الرغم من أن تنوع البيانات مهم، للتحليلات التنبؤية الدقيقة، أو منع التهديدات أو آلية الكشف عنها، حيث يمكن للخوارزميات، مثل التَّعَلُّم بالتحويل، وتعزيز البيانات، أن تتدرب بفاعلية على أنماط بيانات محددة للمساعدة في عملية الكشف، ومع ذلك، فإنَّ افتقارها إلى التدريب على أنماط متنوعة، يمكن أن يقوّض الأداء في الوقت الفعلي.[1]

ويمكن لطرق التَّعَلُّم بالقليل من اللقطات، والتَّعَلُّم النشط، أن تعمل على البيانات في الوقت الفعلي مع مجموعات بيانات صغيرة، ولكنها تحتاج مرة أخرى إلى الكثير من التنوع في البيانات، لمعالجة أحداث الهجوم في العالم الحقيقي بشكل صحيح، مع التعديل المستمر في استراتيجيات التسلّل، وفعاليات إلحاق الضرر بالعملية العادية من قبل المهاجمين.[2]

---

1. Sk Tanzir Mehedi, Adnan Anwar, Ziaur Rahman, Kawsar Ahmed, and Rafiqul Islam. Dependable intrusion detection system for iot: A deep transfer learning based approach. IEEE Transactions on Industrial Informatics, 19(1):1006–1017, 2022.& Moataz Abdelkhalek, Gelli Ravikumar, and Manimaran Govindarasu. Ml-based anomaly detection system for der communication in smart grid. In 2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pages 1–5. IEEE, 2022.

2. Chaoqin Huang, Haoyan Guan, Aofan Jiang, Ya Zhang, Michael Spratling, and Yan-Feng Wang. Registration based few-shot anomaly detection. In European Conference on Computer Vision, pages 303– 319. Springer, 2022. & Xueying Zhan, Qingzhong Wang, Kuan-hao Huang, Haoyi Xiong, Dejing Dou, and Antoni B Chan. A comparative survey of deep active learning. arXiv preprint arXiv:2203.13450, 2022.

وجدير بالذكر هنا، أنّه في نموذج الكشف عن الانحراف، القائم على القليل من اللقطات،[1] يرتبط عدم التعلّق بالفئة، ببيانات مجمَّعة من فئات مختلفة، حيث يقارن النموذج الميزات المسجلة العادية، بالميزات الجديدة للعثور على الاختلافات في بيانات الصورة، بمساعدة مقدر التوزيع الإحصائي، في حين أنَّ النموذج يهدف إلى تعميم الفئات، مع القليل من التَّعلُّم القصير، فقد يكون من غير الممكن تطبيقه على أنماط البيانات الجديدة في العالم الحقيقي، أو فئة غير مرئية مختلفة، وهو أمرٌ معتاد في الهجمات المعقدة، وبالنظر إلى البيانات الوفيرة المطلوبة، لاتخاذ القرارات الدقيقة واستخراج النتائج التنبؤية، فإنَّ كَمِّيَّة كبيرة من تخزين البيانات، معرَّضة أيضاً لانتهاك الخصوصية ومخاطر الأمان السيبرانية.

2- تحدي التحكم في النظم الذكية وإدارتها

هناك عقبة أخرى، تقف أمام تشغيل الذكاء الاصطناعي، تتمثَّل في التحكّم في سلوك النظام، وإدارته في الوقت الفعلي، نظراً لأنَّ تدابير الأمن السيبراني، تتطلَّب عادةً الاستجابة السريعة والوقاية، فإنَّ التأخير الضئيل بين الاكتشاف والوقاية، باستخدام تقنيات الذكاء الاصطناعي، يمكن أن يسبب أضراراً جسيمة للنظام مع حث الدفاع في الوقت الفعلي على أن يكون فعالاً.[2]

3- المباغتة والمفاجأة للهجمات الخبيثة

تجعل الطبيعة المتطورة للهجمات السيبرانية، من الصعب جداً على المطوّرين، تحدّي قدرة الأساليب القائمة على الذكاء الاصطناعي، على الأداء بشكل موثوق بشكل عالٍ، ضد الأحداث غير المسبوقة أو الاستراتيجيات المعقدة.[3]

---

1. Chaoqin Huang,Article cit.

2. Mercy Ejura Dapel, Mary Asante, Chijioke Dike Uba, and Michael Opoku Agyeman. Artificial intelligence techniques in cybersecurity management. In Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022, pages 241–255. Springer, 2023.

3. Ankit Thakkar and Ritika Lohiya. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. Artificial Intelligence Review, 55(1):453–563, 2022.

فالهجمات غير المعروفة، والتي يشار إليها عادةً باسم هجمات اليوم صفر، هي الأكثر شهرة في إلحاق الضرر بالنظام المستهدف، إذا لم يتم تحديدها في الوقت المناسب، والتخفيف منها بكفاءة، حيث تتأخر أساليب الكشف عن الذكاء الاصطناعي، القائمة على التوقّع في الأداء.[1]

4- ذكاء المهاجمين وتنوع أنماط الهجمات السيبرانية

يتسم المهاجمين نجد في الوقت الحاضر، بأكبر قدر ممكن من الدهاء والذكاء، للبقاء غير نشطين في الشبكة، من خلال التنصت فقط، والتلصص الخفي، حتى لو مرَّ عدة أشهر، قبل تنفيذ الهجمات المستهدفة، ويمكن لهذه الهجمات الإلكترونية الخفية والمتطورة وطويلة الأمد، والمعروفة باسم: التهديد المتقدم المستمر (Advanced Persistent APT:Threat)، التهرب من تدابير الأمن التقليدية بسهولة تامة،[2] حيث يمكن للمهاجمين في APT السيطرة عن بعد على الأجهزة، والتسبب في تهديد شديد لبيئة الإنترنت العالمية.

5- جسامة الآثار السلبية الناتجة عن الهجمات السيبرانية

إنَّ التقدم المستمر لنظم الذكاء الاصطناعي، يؤدى إلى زيادة فرص إساءة استخدام التكنولوجيا، ممّا يشكل مخاطر على الأشخاص المرتبطين بالشبكات التنظيمية والأنظمة الحساسة المطبّقة في الدولة أو المؤسسات في كثير من الحالات، ويمكن استخدام معرفة وقدرات الذكاء الاصطناعي، كتهديدات للأمن السيبراني، بدلاً من أن تكون بمثابة فائدة يستفيد منها الأفراد أو المجتمع في نواحي الحياة المختلفة، فمن الضروري ممارسة المراقبة والتنظيم والتحكّم الفعالين، لضمان بقاء الذكاء الاصطناعي نعمة، وليس نقمة في مجال الأمن السيبراني.

---

1. Rajesh Kumar, Rohan Kela, Siddhant Singh, and Rolando Trujillo- Rasua. Apt attacks on industrial control systems: A tale of three incidents. International Journal of Critical Infrastructure Protection, .2022 ,37:100521

2. Eman J Khaleefa and Dhahair A Abdulah. Concept and difficulties of advanced persistent threats (apt): Survey. International Journal of Nonlinear Analysis and Applications, 13(1):4037–4052, 2022.

لذا يكون من الضروري هنا، تعزيز المعرفة بهذه التهديدات، واكتشاف الثغرات، وهي أمور ضرورية أيضاً للحفاظ على آلية الدفاع التكيُّفيَّة والاستباقية، لمحاربة الجزء الخبيث من تطبيقات الذكاء الاصطناعي، الذي يستخدم في التهديدات وإثارة المخاوف الأمنية.

المطلب الثاني

المخاوف المرتبطة بدمج نظم الذكاء الاصطناعي بتقنيات الأمن السيبراني

من المؤسف اليوم، هو أن نلاحظ أنَّ الاستخدام الأكثر شهرة للذكاء الاصطناعي، هو الاستخدام السلبي الخبيث للتكنولوجيا، من قبل الجهات المارقة، التي تستهدف إلحاق الضرر بالتكنولوجيا الذكية، بنفس الأساليب المصمَّمة لحماية النظام، حيث يمكن استخدام الخصائص المعيارية للذكاء الاصطناعي، لتشكيل العملية لتتحول إلى تهديد وتدمير بدلاً من السلامة والموثوقية، ويمكن أن يظهر تأثير الاستخدام الخبيث أو المنحرف للتقنيات الرقمية المرتبطة بالأمن السيبراني، المدمجة بنظم الذكاء الاصطناعي في المظاهر الآتية:

1- الثغرات الأمنية في الفضاء السيبراني

تثير الثغرات الأمنية التي لا يخلو منها أي نظم أو أساليب الذكاء الاصطناعي، المزيد من المخاوف الأمنية، وتشكل تهديداً للاستغلال، حيث يمكن للمهاجمين التلاعب بالخوارزميات، واستدعاء سلوكيات غير طبيعية في الآلية، وشن الهجمات العدائية، وغالباً ما يتم تحويل الغرض المشروع للذكاء الاصطناعي، بهذه الطريقة من قبل مجرمي الإنترنت، للحصول على منافع ومزايا شخصية، حيث تعد هجمات التصيد الاحتيالي المتقدمة، وحالات الاختراق الآلي، والاحتيال المعقد والتلاعب والتزييف العميق، أمثلة رئيسة على المخاطر الكامنة وراء التقنيات المستهدفة بالذكاء الاصطناعي، والتي يجري تخريبها واختراقها والتلاعب بها بمساعدة الذكاء الاصطناعي أيضاً.[1]

[1]. Doowon Jeong. Artificial intelligence security threat, crime, and forensics: Taxonomy and open issues. IEEE Access, 8:184560–184574, 2020.

2- تفاقم خطورة الهجمات السيبرانية بعد دمج أساليب الاختراق والهجوم السيبراني بالذماء الاصطناعي:

يمكن أن تشكل الهجمات التي يتم دمجها مع الذكاء الاصطناعي تحدياً، لأمن النظام الرقمي، إذ يمكنها التكيف ذاتياً مع تدابير الأمن السيبراني، والتهرب من تقنيات الكشف والوقاية والتخفيف من آثارها الضارة على الأقل، وهناك زاوية أخرى للنظر لهذا الموضوع، وهي أن الذكاء الاصطناعي، يمكن أن يكون متعدد الاستخدامات الجيدة والمثالية للغاية.

فالذكاء الاصطناعي متحيز للدقة والحيادية بشكل كبير، لأنَّه لا يزال مدرَّباً على كمِّيَّة معينة من البيانات، ومع توزيع محدود في الفئات، يمكن أن يؤدي التحيّز إلى زيادة النقاط الضعيفة في النظام، لجذب الخصوم للاستفادة من تلك الثغرات.

وجدير بالذكر هنا، أنّه لتصميم تقنية الذكاء الاصطناعي بشكل أفضل، بغية إعادة تشكيل أساليب الأمن السيبراني، لمعالجة الهجمات السيبرانية المعقدة والمتطورة، يجب معالجة القيود التالية بشكل صحيح، مما يستدعي المزيد من البحث للتحسين والتطوير.

3- الهجمات المعادية المضادة لنماذج الذكاء الاصطناعي:

الطريقة الأكثر انتشارا لاستخدام تقنيات الذكاء الاصطناعي، من قبل الجهات التي تقود التهديدات الخبيثة، هي دمج الهجمات المعادية، حيث تم بناء الكتلة الأساسية لهذه الهجمات، على مفهوم التَّعَلُّم المعادي أو نماذج التَّعَلُّم العميق أيضاً، بطريقة متشابهة لأنظمة الدفاع أو الحماية السيبرانية المطبّقة في الأمن السيبراني، وبشكل عام، تعمل نماذج التَّعَلُّم الآلي والتَّعَلُّم العميق، على أساس الافتراضات المقدمة من خلال البيانات والميزات، لتصنيف السلوك الطبيعي وغير الطبيعي في العملية الخبيثة، حيث تستفيد النماذج المعادية من هذا المفهوم للتلاعب بهذه الافتراضات، لتغيير دافع النموذج المستخدم، والتسبب في عواقب وخيمة من داخل النظام الأمني ذاته.[1]

[1]. Jingfeng Zhang, Xilie Xu, Bo Han, Gang Niu, Lizhen Cui, Masashi Sugiyama, and Mohan Kankanhalli. Attacks which do not kill training make adversarial learning stronger. In International conference on machine learning, pages 11278–11287. PMLR, 2020.

وصيغة ذلك، تبدأ بنموذج الهجوم باستخدام التَّعَلُّم العدائي، وذلك بتغيير السرية في نموذج التَّعَلُّم الآلي أو التَّعَلُّم العميق، الذي يتم تشغيل تدابير أو تطبيقات الأمان عليه، ومن خلال اكتساب معرفة النموذج، والتقاط ميزات التَّعَلُّم، والتنصت على متطلبات النظام، يكتسب الفاعل المهدد معرفة كبيرة للمضي قدماً في الخطوة التالية للهجوم، والمتمثلة في المساس بالسلامة الداخليَّة للنظام، ويتم تغيير الميزات أو المدخلات التي تُستخدم لتدريب النماذج، وفقاً للغرض الخبيث للمهاجم.

ومع اكتساب المهاجم للمعرفة بالنظام في هذه العملية، يتبع ذلك المساس بالسلامة الذاتية للنظام الأمني، ويتم تغيير ميزات الإدخال المتوقعة، أو عملية التَّعَلُّم المتبعة من قبل النظام، لتغيير النتيجة المرجوة من النماذج، ومن ثم تصبح تدابير الأمان غير قادرة على تحديد الانحراف، حيث يتم تعديلها لتمرير نظام اكتشاف التسلّل أو نظام منع التطفّل، أثناء متجه الهجوم بمساعدة الهجوم العدواني.

ومن ثمَّ يتمكن المهاجم بعد ذلك، من تغيير مدى توفر الخدمات، عن طريق تغيير سلامة نموذج النظام، بحيث لا يتمكّن من التعرف على السلوكيات غير الطبيعية، ولا يمكن منع الأحداث الخبيثة أو التعرف عليها، بكفاءة من خلال تطبيقات الأمان، ومن خلال هذا الهجوم المتطور، يكون الفاعل المهدد، قادراً على المساس بالنظام الأمني السيبراني المتكامل لوكالة المخابرات المركزية، مثلاً، وإلحاق الضرر بالبنية الأساسية أو إيقاف الخدمات الحساسة ذات الصلة بأنشطتها .[1]

وغالباً ما تظهر هذه المخاطر بشكل تلاعب بالغ الدقَّة والتعقيد، ممّا يشكّل تحدياً كبيراً في الكشف ومن ثم المواجهة، وعليه، فإن هذا سيعني مواجهة عواقب وخيمة على مثل هذه الإجراءات بصورة بعيدة المدى، ممّا يؤدي إليه، من تحايل على تدابير الأمن أو تشويه أنظمة صنع القرار الآلية أو الذكية.

[1]. Ishai Rosenberg, Asaf Shabtai, Yuval Elovici, and Lior Rokach. Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR), 54(5):1–36, 2021.

4- الصعوبة البالغة في مسايرة التطور التقني الذي تعتمده الجهات المسؤولية عن الاختراق أو التهديد:

يكون المهاجمون المعتمدون على دمج تقنيات الاختراق بنظم الذكاء الاصطناعي، متقدمين بخطوة على النظم التقنية للأمن السيبراني، ولمواجهة هذه التهديدات الخطيرة، يكون من الضروري أن تخضع نماذج الذكاء الاصطناعي للتقييم والتحسين المستمر من الناحيتين الفنيّة والتقنية، كما يجب أن تتضمن هذه العملية تدريباً عدائياً بشكل متطور ومختلف، حيث يتم تعريض النماذج لسيناريوهات هجوم محتملة أثناء مراحل تطويرها، ومن ثمَّ تعزيز قوتها وقدرتها على تحمل تكتيكات مختلفة وغير متماثلة للهجوم.

وعلى الرغم من أن أنظمة اكتشاف التسلل القائمة على التَّعَلُّم العميق، يمكنها التمييز وبقدرة عالية بين التغييرات الدقيقة في الأحداث الطبيعية وغير الطبيعية، إلا أن الهجوم العدائي على أنظمة اكتشاف التسلل هذه، يمكن أن يجلب تحديات آنية مختلفة لآلية التعريف، ففي بيئة إنترنت الأشياء، ثبت أن الهجوم السيبراني يكون فعالاً للغاية في تغيير كفاءة هيكل الأمان، مع استخدام الهجمات المعادية، لا بل وثبت أن التغييرات الصغيرة، في البايتات المكونة للحزم الضارة، تقلّل بشكل فعال وواضح، من أداء النموذج التنبؤي في أنظمة الكشف عن التهديدات القائمة على إنترنت الأشياء.[1]

[1]. Han Qiu, Tian Dong, Tianwei Zhang, Jialiang Lu, Gerard Memmi, and Meikang Qiu. Adversarial attacks against network intrusion detection in iot systems. IEEE Internet of Things Journal, 8(13):10327–10335, 2020.

المبحث الثالث

المعالجة القانونية للتحديات التي تواجه مخاطر دمج الذكاء الاصطناعي في الأمن السيبراني

تُعد المواجهة القانونية واحدة من أنجع أساليب المواجهة غير التقنية للاختراق الحاصل للأمن السيبراني، حيث يمكن تفعيل القواعد القانونية الجنائية أو المدنية لمواجهة التهديدات والثغرات الأمنية الحاصلة في هذا المجال، ولهذا تعد عملية توظيف القواعد القانونية القائمة في النظام القانوني الحالي، من أهم المشاكل التي يحاول القانونيون إيجاد الحلول لها، صحيح أنَّ تطبيقات الذكاء الاصطناعي تضفي مزايا كبيرة لحياتنا اليومية، منها استمرار تطوير وتشغيل الشبكات الأمنة ومراقبة النظام، ولكن التهديدات والثغرات الأمنية المتأصلة في الشبكة العنكبوتية، تقلّل من السمعة الأمنية للتكنولوجيا، خصوصاً مع الاهتمام المتزايد بالذكاء الاصطناعي.

ومن اهم أساليب الحماية القانونية التي يمكن اللجوء إليها في هذا الصدد، سنبينها في مطلبين كالآتي:

المطلب الأول

تفعيل قواعد الحماية المدنية الخاصة بالمسؤولية المدنية والتأمين

تمثل القواعد العامة الخاصة بالمسؤولية التقصيرية، الملجأ العام للمضرور في المطالبة بالتعويض عن الأضرار الناجمة عن الهجمات السيبرانية، وفي هذا الصدد لابد من التركيز على أنَّ تفعل قواعد الحماية هذه، يقتضي أن يكون المهاجم المتسبب بالضرر معلوماً، من جهة، ومن جهة اخرى إمكانية حصر الأضرار الحاصلة.

كما يعد التأمين على المخاطر السيبرانية، أسلوباً قانونياً يمكن بواسطته التخفيف من الآثار الجسيمة التي تتسبب بها المخاطر السيبرانية، وذلك بعد أن أصبحت هذه المخاطر قابلة للتأمين ضمن شروط محددة.

وفي هذا الصدد يمكن القول، بأنّ ما تثيره مخاطر انتهاك الأمن السيبراني من منازعات تتعلّق بالملكية الفكرية، تنتج عنها اشكاليات متنوعة على المستويات القانونية والاقتصادية والمالية، فهي تكلف المستهدفين مبالغ طائلة سواء من ناحية اتساع الاضرار وكبر حجمها وصعوبة تلافي آثارها أو من ناحية كيفية تعويض الخسائر وتقدير حجم الاضرار الناجمة عن مثل هكذا انتهاكات، هذا الامر الذي نلمسه جليا في حالات انتهاك حقوق الملكية الفكرية التقليدية وحق الخصوصية، فكيف والحال قد تطور الى تزايد حالات انتهاك حقوق الملكية الفكرية عبر الفضاء الرقمي، و لنا ان نتصور مدى فداحة الاضرار والخسائر الناجمة عن هكذا انتهاكات، حيث يمكن ان تصل هذه الخسائر الى اضعاف مضاعفة عما هي في الحياة التقليدية.

وللأسف، فإنَّ هذه الطبيعة الخفية والمتقدمة والمستمرة للهجمات السيبرانية، قادرة على إحداث دمار هائل للبنى التحتية الحساسة، ويصعب بشكل خاص على الأساليب التقليدية القائمة على الذكاء الاصطناعي، مواجهتها والدفاع ضدها، كما هو الحال في أحداث متعددة، مثل، Struxnet، وهجمات BlackEnergy في عام 2015، وهجوم notpetya في عام 2017،[1] وما إلى ذلك من قائمة طويلة من الهجمات تبدأ ولا تنتهي.

لهذا تواجه كثير من الشركات العاملة في مجال التأمين، العديد من الصعوبات في تحديد ماهية المخاطر التي تبتغي التأمين عليها، ومقدار التغطية التأمينية المراد توفيرها في مثل هكذا أوضاع، وذلك لأنّها تمثّل الصورة العصرية للتطبيقات القانونية وسط هذه التطورات التكنولوجية الكبيرة،[2] وفي خضم هذه الثورة المعلوماتية الهائلة، فقد سعت شركات التأمين الى تكوين فهم كامل للمخاطر الاقتصادية الناشئة في المجالات المختلفة في الفضاء السيبراني حالياً،[3] وذلك حينما ميزت بين فئتين رئيستين من فئات الاضرار، التي تنشئ المسؤولية المدنية في البيئة الرقمية، وهي:

---

1. Daniel E Capano. Throwback attack: How notpetya accidentally took down global shipping giant maersk: Do you debate risks vs. cost of cybersecurity technologies, processes and training? maersk estimated notpetya costs at $250-300 million. Control Engineering, 70(4):39–42, 2023.

2 . Daniel J. Langin, The Economics of the Internet: Insurance and Risk Management, Advertising and other Business Models, Valuation and Tax Issues, 482 PLI/PAT 447, 449 (1997).

3 . Ibid.

- الاضرار المادية.
- أضرار النشر.[1]

و تشمل الفئة الأولى كافة الاضرار التي تنصب على الاشياء المادية، والتي تتعلق بالممتلكات المتعلقة بالفضاء الرقمي[2]، و المتمثلة بـ :

1- تدمير البيانات الحاسوبية .

2- اتلاف اجهزة الكمبيوتر او الخوادم الرئيسية .

3- قرصنة البيانات و البرمجيات .

4- فضلا عن الخسارة المقابلة لهذه الانتهاكات .[3]

المطلب الثاني

تفعيل قواعد الحماية من انتهاك الحق في الخصوصية المدنية والجنائية

عند الحديث عن اختراق التقنيات المرتبطة بالأمن السيبراني المعتمدة على نظم الذكاء الاصطناعي، لا بد أن نتذكر مخاوف الخصوصية بشكل واضح، فعندما تعالج أدوات الذكاء الاصطناعي البيانات الحساسة الداخلة في الأغراض أمنية، يمكن أن يؤدي تجميع وتحليل مجموعات البيانات الكبيرة، إلى الكشف عن معلومات شخصية من غير قصد، الأمر الذي يؤدي إلى انتهاك الخصوصية الشخصية.

---

1 . Adam H. Fleischer, Internet Torts and Cyberspace Insurance: New Issues for the Economy, 88 ILL. B.J. 268, 268 (2000).

2 . Ibid. at 273.

3 . Ibid.

ويتضخم هذا القلق بشكل أكبر، بسبب التطور المتزايد لتقنيات ونظم الذكاء الاصطناعي القادرة على استخلاص استنتاجات مفصلة من البيانات المجمعة، حيث تتمتع نماذج التَّعَلُّم العميق، بتنوع تطبيقاتها، والتي تكون واسعة النطاق في مجال الأمن السيبراني، نظراً لقدرتها القابلة للمقارنة على استخراج ميزات مهمة، من دون هندسة ميزات خارجية، بل وتوافقها لإنتاج نتائج أفضل مع البيانات المرتبطة.

وتتضمن عملية التَّعَلُّم لهذه التقنية مجموعات بيانات كبيرة، وبمساعدتها يتعلَّم النموذج، التمييز بين الأنماط المختلفة، حيث يتم تنفيذ التنبؤات أو التصنيفات، بناءً على بيانات الإدخال المقدمة لهذه النماذج.

ومع ذلك، يزداد القلق لدى المختصين في نظم الذكاء الاصطناعي والأمن السيبراني والمستخدمين لهذه النظم على حد سواء، عندما يحفظ النموذج الخصائص الأساسية أو التفاصيل من عملية التدريب، حيث يمكن في معظم الحالات أن تكون هذه البيانات خاصة أو حساسة، ومن ثمَّ تصبح مخزنات هذه النماذج مصدر قلق أمني، حيث يمكن للمهاجمين استهداف أنظمة الحماية واختراق السرية الخاصة بهذه النماذج، والحصول على مثل هذه المعلومات الحساسة والشخصية للجهات المستهدفة. [1]

فعلى سبيل المثال، إذا تمَّ تدريب النموذج على البيانات الطبية أو المعلومات المالية، فإنَّ تسرّب مثل هذه البيانات الحساسة، يمكن أن يؤدي إلى سرقة الهوية أو انتهاكات الخصوصية أو الاحتيال المالي،[2] ويمكن استغلال ثغرة تسرب البيانات هذه، من خلال الهندسة العكسية، أو استعلام النموذج، للكشف عن المعلومات الحساسة، حيث يتم تخزين البيانات أثناء مرحلة التدريب، باستخدام عملية التَّعَلُّم التعاوني، بحيث يمكن لأطراف متعددة مشاركة مجموعة محددة من مُعلِّمات النموذج، لتدريب نموذج التَّعَلُّم التعاوني المتاح، ويمكن الحصول على ميزة مرنة، من عملية التَّعَلُّم الجماعي هذه.

---

1. Briland Hitaj, Giuseppe Ateniese, and Fernando Perez-Cruz. Deep models under the gan: information leakage from collaborative deep learning. In Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, pages 603–618, 2017.

2. R Sri Skandha Moorthy and N Nathiya. Article cite.

ومع ذلك، نظراً لتوافر المُعلِّمات الجزئية في النموذج، فإنّه يمكن استغلالها بواسطة هجمات شبكات الخصومة التوليدية (GAN). حيث تعد هذه الشبكات، نموذجا مزدوجاً للشبكة العصبية، فهي شبكة تعتمد على المولّد والمميّز، فيها يحاول المولّد، إنشاء بيانات أصلية، بينما يقوم المميّز، بتمييز البيانات المولدة عن البيانات الأصلية.

وعلى الرغم من أن المولِّد يظل في البداية، النموذج الأضعف، إلّا أنَّ ملاحظات التمييز، لدى المميز تستمر في جعله أقوى، وبعد فترة، يبدأ المولّد بإنشاء بيانات غير قابلة للتمييز من تلك الأصلية، ومن ثمَّ إجراء نفس الشيء مع نموذج التَّعَلُّم التعاوني للتَّعَلُّم، حيث تعيد شبكة الخصومة التوليدية، إنشاء بيانات خاصة من المُعلِّمات المشتركة أثناء الهجوم .[1]

ومن ثمَّ يمكن لهذه الهجمات، توليد بيانات مماثلة، بناءً على تقييم المميز، واستخراج المعلومات دون الوصول إلى المعلمات المشتركة بشكل مباشر، حتى مع وجود مقياس الخصوصية التفاضلي، أو المتكامل، لحماية المعلمات المشتركة، حيث يمكن لهجوم GAN استخراج المعلومات بسهولة، نظراً لأنَّ نموذج GAN قام بتكرار البيانات، بمساعدة مُعلِّمات جزئية، ولم يسرق المعلومات بالضبط، فقد تمكن نموذج الهجوم من تجاوز تدابير الأمان السيبراني المعتمدة بصورة موازية متوافقة مع منظومة الأمن وليس بصيغة هجوم مباشر عليها.

لذلك، فإن تنفيذ تدابير حماية البيانات الصارمة، مثل إخفاء هوية البيانات، والتشفير، وبروتوكولات تخزين البيانات، والوصول إليها بشكل آمن، أمر بالغ الأهمية في مجال الأمن السيبراني، علاوة على ذلك، يجب تصميم نماذج الذكاء الاصطناعي المستخدمة في الأمن السيبراني، لموازنة الحاجة إلى الأمان مع ضرورة الحفاظ على خصوصية المستخدم.

ومن جانب آخر، فإنّه لمّا يزل سوء الاستخدام المحتمل لتقنيات الذكاء الاصطناعي في تنظيم الهجمات الإلكترونية، يمثل مشهداً مزدوج التهديد، إذ يمكن استغلال تقنيات الذكاء

1. Briland Hitaj, Giuseppe Ateniese, and Fernando Perez-Cruz, Article cite

الاصطناعي، لإنشاء برامج ضارة متطوّرة تتكيف مع الدفاعات الأمنية، وأتمتة حملات التلصص واسعة النطاق، [1] وحتى إجراء هجمات مزيفة، تتلاعب بالمحتوى الصوتي أو المرئي.[2]

وما قاد إلى تفاقم ذلك الوضع، هو إمكانية الوصول المتزايدة إلى أدوات وتقنيات الذكاء الاصطناعي، فهذا يعني أن حاجز الدخول لمجرمي الإنترنت آخذ في الانخفاض، ممّا يؤدي إلى هجمات إلكترونية أكثر تقدّماً وأفظع استهدافاً، وهذا يتطلَّب اتباع نهج استباقي في مجال الأمن السيبراني، حيث تتطور الاستراتيجيات الدفاعية باستمرار لمواجهة التهديدات التي يساعد في بنائها الذكاء الاصطناعي.

1. Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil, and Kashif Kifayat. A comprehensive survey of ai-enabled phishing attacks detection techniques. Telecommunication Systems, 76:139–154, 2021.

2. Shehzeen Hussain, Paarth Neekhara, Malhar Jere, Farinaz Koushanfar, and Julian McAuley. Adversarial deepfakes: Evaluating vulnerability of deepfake detectors to adversarial examples. In Proceedings of the IEEE/CVF winter conference on applications of computer vision, pages 3348–3357, 2021.

الخاتمة

خلصنا من خلال هذه الدراسة، إلى بيان دور الذكاء الاصطناعي في تطوير وتحسين التقنيات المرتبطة بالأمن السيبراني، والتحديات التي تواجهه، ونود في هذا المقام التركيز على ما يلي:

النتائج:

1- يعد مجال الأمن السيبراني، المجال الحاسم الذي لا يمكنه التسامح مع فشل تقنيات الذكاء الاصطناعي، كأداة لتطوير وتحسين قدرات الأمن السيبراني، فهو المجال الوحيد الذي يفصل فيه، بين الجهات الفاعلة في التهديد، والمعلومات والخدمات الحساسة.

2- أبرزت هذه الدراسة، كيفية معالجة الاحتمالات غير المحدودة للتهديدات بواسطة الذكاء الاصطناعي في مجال الأمن السيبراني، وفي ذات الوقت، إدراك التهديدات المرتبطة به، إذا لم يتم النظر في القيود المقدمة أثناء التنفيذ.

3- يمكن الحفاظ على قدرة وقوة تقنيات الأمن السيبراني من خلال دمجها مع نظم الذكاء الاصطناعي، من خلال تعزيز مقدرة تلك التقنيات على مواجهة الهجمات السيبرانية المتطورة والحد منها، خصوصاً إذا كان من الممكن تشغيل تطور الذكاء الاصطناعي بنفس معدل الهجمات.

4- وبالنظر إلى إمكانية دمج التقنيات الأخرى في تطبيقات الأمن المتكاملة مع الذكاء الاصطناعي، يمكن الدفاع عن الجهات الفاعلة والحساسة ضد التهديد بشكل فعّال، أو على الأقل يمكن تقليل التأثير السلبي الناتج عنها.

5- يمكن تفعيل النظم القانونية المدنية القائمة، في القانون المدني والقانون الجنائي، لمواجهة الآثار الوخيمة التي يجابهها المضرورون من الهجمات السيبرانية، ويعانون من فداحة الأضرار الناجمة عن الاختراق والتصيد الاحتيالي والقرصنة المعلوماتية، كما يمكن اللجوء إلى التأمين كوسيلة علاجية، يمكن بواسطتها معالجة الأضرار الناتجة عن هذه الانتهاكات الأمنية.

التوصيات:

1- من الضروري للباحثين والمطورين، بيان القيود ونقاط القوة في الذكاء الاصطناعي، ليجري مواجهتها في المستقبل، والعمل على إجراء التعديلات والتغييرات المناسبة لاتخاذ القرارات المناسبة.

2- يتم تطوير وتحسين لتقنيات الذكاء الاصطناعي، من خلال توجيه الباحثين لفهم تدفق التغييرات، التي أدت إلى تكنولوجيا الذكاء الاصطناعي الحديثة، وربط التغييرات بجلب إمكانات الذكاء الاصطناعي إلى الاتجاه المستقبلي، كما فعل العديد من الباحثين في المجالات الأخرى في أوقات سابقة.

Références

Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil, and Kashif Kifayat. A comprehensive survey of ai-enabled

Adam H. Fleischer, Internet Torts and Cyberspace Insurance: New Issues for the Economy, 88 ILL. B.J. 268, 268 (2000).

Ankit Thakkar and Ritika Lohiya. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. Artificial Intelligence Review, 55(1):453–563, 2022.

Briland Hitaj, Giuseppe Ateniese, and Fernando Perez-Cruz. Deep models under the gan: information leakage from collaborative deep learning. In Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, pages 603–618, 2017.

Chaoqin Huang, Haoyan Guan, Aofan Jiang, Ya Zhang, Michael Spratling, and Yan-Feng Wang. Registration based few-shot anomaly detection. In European Conference on Computer Vision, pages 303– 319. Springer, 2022.

Daniel E Capano. Throwback attack: How notpetya accidentally took down global shipping giant maersk: Do you debate risks vs. cost of cybersecurity technologies, processes and training? maersk estimated notpetya costs at $250-300 million. Control Engineering, 70(4):39–42, 2023.

Daniel J. Langin, The Economics of the Internet: Insurance and Risk Management, Advertising and other Business Models, Valuation and Tax Issues, 482 PLI/PAT 447, 449 (1997).

Doowon Jeong. Artificial intelligence security threat, crime, and forensics: Taxonomy and open issues. IEEE Access, 8:184560–184574, 2020.

Eman J Khaleefa and Dhahair A Abdulah. Concept and difficulties of advanced persistent threats (apt): Survey. International Journal of Nonlinear Analysis and Applications, 13(1):4037–4052, 2022.

Enn Tyugu. Artificial intelligence in cyber defense. In 2011 3rd International conference on cyber conflict, pages 1–11. IEEE, 2011.

H Wang, ZeZXeZBePJ Lei, X Zhang, B Zhou, and J Peng. Machine learning basics. Deep learning, pages 98–164, 2016.

Han Qiu, Tian Dong, Tianwei Zhang, Jialiang Lu, Gerard Memmi, and Meikang Qiu. Adversarial attacks against network intrusion detection in iot systems. IEEE Internet of Things Journal, 8(13):10327–10335, 2020.

International Electrotechnical Commission. Iec — cyber security.https://drive.google.com/file/d/1j0z2tmiajq5ff8ZfDPEwbHHIFXBwJIV5/view?usp=shari [2022].

Iqbal H Sarker, Md Hasan Furhad, and Raza Nowrozy. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2:1–18, 2021.

Ishai Rosenberg, Asaf Shabtai, Yuval Elovici, and Lior Rokach. Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR), 54(5):1–36, 2021.

ISO/IEC. Cybersecurity — guidelines for internet security. https://standards.iteh.ai/catalog/standards/sist/2d12469a-69be-4365-88bb-05df3b0212d 2023.

Jeff A Stuart and John D Owens. Multi-gpu mapreduce on gpu clusters. In 2011 IEEE International Parallel & Distributed Processing Symposium, pages 1068–1079. IEEE, 2011.

Jingfeng Zhang, Xilie Xu, Bo Han, Gang Niu, Lizhen Cui, Masashi Sugiyama, and Mohan Kankanhalli. Attacks which do not kill training make adversarial learning stronger. In International conference on machine learning, pages 11278–11287. PMLR, 2020.

Konrad Rieck, Philipp Trinius, Carsten Willems, and Thorsten Holz. Automatic analysis of malware behavior using machine learning. Journal of computer security, 19(4):639–668, 2011.

Mercy Ejura Dapel, Mary Asante, Chijioke Dike Uba, and Michael Opoku Agyeman. Artificial intelligence techniques in cybersecurity management. In Cybersecurity in the Age of Smart

Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022, pages 241–255. Springer, 2023.

Md Fazley Rafy. Artificial Intelligence in Cyber Security, arXiv:submit/5336757 (cs.AI) 8 Jan 2024, See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/377235308.

Moataz Abdelkhalek, Gelli Ravikumar, and Manimaran Govindarasu. Ml-based anomaly detection system for der communication in smart grid. In 2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pages 1–5. IEEE, 2022.

Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada. Identification of cybersecurity specific content using the doc2vec language model. In 2019 IEEE 43rd annual com- puter software and applications conference (COMPSAC), volume 1, pages 396–401. IEEE, 2019.

phishing attacks detection techniques. Telecommunication Systems, 76:139–154, 2021.

R Sri Skandha Moorthy and N Nathiya. Botnet detection using artificial intelligence. Procedia Computer Science, 218:1405–1413, 2023.

Rajesh Kumar, Rohan Kela, Siddhant Singh, and Rolando Trujillo- Rasua. Apt attacks on industrial control systems: A tale of

three incidents. International Journal of Critical Infrastructure Protection, 37:100521, 2022.

Shehzeen Hussain, Paarth Neekhara, Malhar Jere, Farinaz Koushanfar, and Julian McAuley. Adversarial deepfakes: Evaluating vulnerability of deepfake detectors to adversarial examples. In Proceedings of the IEEE/CVF winter conference on applications of computer vision, pages 3348–3357, 2021.

Sk Tanzir Mehedi, Adnan Anwar, Ziaur Rahman, Kawsar Ahmed, and Rafiqul Islam. Dependable intrusion detection system for iot: A deep transfer learning based approach. IEEE Transactions on Industrial Informatics, 19(1):1006–1017, 2022.

Symmetry, 12(5):754, 2020.

Tomas Pl˙eta, Manuela Tvaronavi˘cien˙e, Silvia Della Casa, and Konstantin Agafonov. Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases. Insights into regional development. Vilnius: Entrepreneurship and Sustainability Center, 2020, vol. 2, no. 3., 2020.

Wei Li. Using genetic algorithm for network intrusion detection. Proceedings of the United States department of energy cyber security group, 1(1):8, 2004.

Xueying Zhan, Qingzhong Wang, Kuan-hao Huang, Haoyi Xiong, Dejing Dou, and Antoni B Chan. A comparative survey of deep active learning. arXiv preprint arXiv:2203.13450, 2022.

الفصل الخامس

استخدام الذكاء الاصطناعي في تنفيذ عقوبة المراقبة الإلكترونية، دراسة تحليلية مقارنة

The Use of Artificial Intelligence in Implementing Electronic Surveillance Penalties

A Comparative Analytical Study

المستشار الدكتور

محمد جبريل إبراهيم حسن

نائب رئيس هيئة قضايا الدولة المصرية

دكتوراه القانون الجنائي بكلية الحقوق -جامعة القاهرة -مصر

عضو الجمعية المصرية للاقتصاد السياسي والإحصاء والتشريع

Email: gebrelmohamed865@gmail.com

ملخص

كان لدور الذكاء الاصطناعي في تنفيذ العدالة وترسيخ الأمن السيبراني أثر بارز في تحسين أداء هذا الدور، وكان من أبرز هذه الاستخدامات تنفيذ المراقبة الإلكترونية كعقوبات بديلة عن طريق استخدام الذكاء الاصطناعي.

وهو ما شد الانتباه بقوة باعتبار أن المراقبة الالكترونية هي رد فعل اجتماعي تجاه بعض الجرائم البسيطة والتي تستوجب حماية الشخص من الحوم حول أسباب الجريمة مرة

أخري، ومنعه من ارتياد أماكن معينة أو ممارسة أنشطه معينة، وكذلك تمنحه فرصة لإثبات أنه جدير بالاندماج في المجتمع، وقادر على العيش في مجتمعه بدون ارتكاب الجرائم.

كلمات مفتاحية: الذكاء الاصطناعي، المراقبة الالكترونية، العقوبات البديلة.

Summary

The role of artificial intelligence in the implementation of justice and the strengthening of cybersecurity has had a significant impact on improving the performance of this role. One of the most prominent uses of artificial intelligence has been the implementation of electronic surveillance as an alternative to punishment.

This has drawn strong attention, considering that electronic surveillance is a social reaction to some minor crimes, which requires protecting the person from hovering around the causes of the crime again, preventing him from frequenting certain places or practicing certain activities, and also giving him the opportunity to prove that he is worthy of integration into society, and capable of living in his community without committing crimes.

Keywords: Artificial intelligence, electronic monitoring, alternative penalties.

مقدمة

من أكثر الأنظمة التشريعية التي تأثرت بالتطورات العلمية والفكرية الحديثة هي الأنظمة العقابية ، فاحتلت العقوبة جانب كبير من اهتمام المشرعين والفقهاء والقضاة ، وكان علي أثر ذلك إلغاء العقوبات البدنية التي كانت سائدة في التشريعات القديمة ، وحصر وتقليل الجرائم التي توقع عليها عقوبة الإعدام ، والجنوح نحو التحول من الفكر العقابي البحت إلي الفكر الإصلاحي التأهيلي في الوقاية من الجريمة ، وكان من نتائج ذلك بروز العقوبات البديلة في السياسة العقابية الحديثة بما يحقق تقليل ومنع الظاهرة الإجرامية ويفي بالغرض الأساسي للعقوبة.

ولقد كان لأفكار المدرسة الوضعية في تبني فكرة تفريد العقوبة والتدابير الاحترازية، وأفكار مدرسة حركة الدفاع الاجتماعي في الاهتمام بشخص المجرم والطابع الإنساني في الجزاء الجنائي دوراً مهماً في ترسيخ الدور الإصلاحي والتأهيلي للعقوبة، وإبرازه للسياسة العقابية لتحقيق إصلاح المجرم وتأهيله للاندماج في المجتمع بدون الإخلال بأغراض العقوبة الأخرى.

وكانت المراقبة الإلكترونية من العقوبات البديلة التي شدت الانتباه بقوة باعتبارها رد فعل اجتماعي تجاه بعض الجرائم البسيطة والتي تستوجب حماية الشخص من الحّوم حول أسباب الجريمة، ومنعه من ارتياد أماكن معينة أو ممارسة أنشطه معينة، وكذلك تمنحه فرصة لإثبات أنه جدير بالاندماج في المجتمع، وقادر على العيش في مجتمعه بدون التعدي أو الإيذاء للغير.

وإذا كانت العقوبة بوجه عام هي إجراء يقرره القانون فيحدث الإيلام أو الانتقاص أو الحرمان من كل أو بعض الحقوق الشخصية لمن ثبتت مسئوليته عن الجريمة بناء على حكم جنائي صادر من محكمة مختصة، فإن المراقبة الإلكترونية تُعد وفقاً لهذا المفهوم من العقوبات الجنائية المستحدثة إذا ما تقررت بموجب نص قانوني، وإذا ما توافرت لها بعض الضمانات القانونية عند القضاء بها وعند تنفيذها، فمن غير شك يمكن لها أن تحقق الغرض من العقوبة، فتصلح المجرم، وتحقيق العدالة، وتحد من ارتكاب الجريمة عن طريق الردع العام والخاص.

وفي الحقيقة فإن الميل والجنوح نحو تطبيق نظام المراقبة الإلكترونية كعقوبة بديلة لا يعني التحيز لها، ولا يعني أن تطبيقها نوع من الرفاهية أو الاختيار بين بدائل متوافرة للتخلي عن مضمون الجزاء وإلغاء رد الفعل الجماعي تجاه الجريمة، ولكن الأمر يكون في بعض الأحيان نوع من الضرورة لمواجهة بعض مشكلات العقوبات التقليدية، وخصوصاً العقوبات المتعلقة بالحبس قصير المدة عن جرائم لا تنم عن خطورة المحكوم عليه ولا تدل على طبعه الإجرامي بأي حال من الأحوال.

فلا أحد ينكر الأزمة التي مرت بها العقوبات السالبة للحرية قصيرة المدة لما تخلفه من آثار سلبية علي المحكوم عليه وعلي أسرته وعلي المجتمع ككل ، حيث تسمح بإدماج المحكوم عليه مع عتاة الإجرام فيكتسب خبرات كبيرة من طرق ارتكاب الجرائم ، وتحرم أسرته منه كعائل لها مما يمثل عقاب للأسرة ، ناهيك عن التكلفة العالية لتنفيذها من أماكن للحبس ومأكل ومشرب وملس ودواء وهو ما يمثل عبء كبير علي كاهل الدولة ، فتأتي المراقبة الإلكترونية في إطار عصرنة العدالة من خلال الاستعانة بتقنيات الذكاء الاصطناعي في تنفيذ بدائل العقوبات السالبة للحرية لتفادى مساوئ العقوبات التقليدية.

فالمراقبة الإلكترونية هي في حد ذاتها عقوبة وإن كانت تتصف بقدر كبير من الإنسانية، إلا أنها تلبي بعض نواحي العدالة بصورة كبيرة، فهي ولا شك تُعد أحدي العقوبات التي يكون أهل المحكوم عليه في حاجة ماسة إليها أكثر من غيرهم وخاصة إذا كانوا صغار، أو كان المحكوم عليه من الأمهات، كما أنها تفي بمبدأ شخصية العقوبة ولا يمتد أثرها إلى باقي أفراد الأسرة بحرمانهم من عائلهم، فيحافظ ذلك علي شمل الأسرة ويحميها من التفكك والانفلات.

ونشير أيضاً إلى بعض الجوانب الإيجابية للمراقبة الإلكترونية، فمن ناحية الدولة فإن التوسع في استخدامها يؤدي إلى انخفاض أعداد المحبوسين في السجون، الأمر الذي سيتيح للدولة القيام بإجراء عملية تأهيل حقيقي للمحكوم عليهم، كما أن تكاليف المراقبة الإلكترونية قليلة بالنسبة لعقوبة الحبس، وبالتالي ستقلص الدولة أعباء المصروفات التي تتكبدها لتوفير متطلبات أعداد المحبوسين.

هذا بالإضافة إلى أن المراقبة الإلكترونية تتيح للمحكوم عليه الاستمرار في عمله والقيام بدوره في المجتمع، وهو ما يعني أنه لن تؤثر العقوبة في الانتقاص من دولاب العمل، والاستمرار

في دفع الضرائب، وكفالة عائلته والإنفاق عليها، الأمر الذي سيوفر على الدولة الأعباء الاجتماعية والاقتصادية للمحبوس وعائلته.

ومن ناحية أخري فإن اختيار تطبيق المراقبة الإلكترونية يعني أيضًا عدم القضاء على المستقبل الوظيفي للمحكوم عليه، بإتاحة الفرصة له للمحافظة علي وضعه وترقيته لتواجده على رأس العمل، وهو الأمر الذي يعيد تأهيل المحكوم عليه بصورة أسرع إلى المجتمع، ويجعله يجتهد في إصلاح ذاته وذلك من أهم أغراض العقوبة.

وبالرغم مما تتميز به المراقبة الإلكترونية من مميزات إلا أنها لم تخلو من النقد؛ وذلك لخلوها من الإيلام والإصلاح لشأن المجرم، ونظرة المجتمع إليها على أنها مظهر من مظاهر الإفلات من العقاب والتخفيف عن المجرمين، مما حدي بالبعض إلى المناداة بضرورة ترشيد تطبيقها حتى تتلاءم مع سياسة العقاب المعاصرة، في تحقيق الردع العام والخاص، والحرص على العدالة ومعالجة ألم المجني عليه.

مشكلة الدراسة:

تبدو مشكلة الدراسة في أن نظام المراقبة الإلكترونية لم تتبلور قواعده بصورة واضحة حتى الآن مما أدي إلى الاختلاف بين قواعده في التشريعات المختلفة، وذلك لعدم وجود معايير موحدة لتطبيق هذا النظام حتى الآن.

كما تبدو مشكلة الدراسة في أنها تتناول مصلحتين متناقضتين، مصلحة المحكوم عليه في تطبيق نظام عقابي حديث يتسم بالرأفة والرحمة، ومصلحة المجتمع الذي يرغب في تخفيف حنقه وغضبة بتنفيذ عقوبة مؤلمة على المجرم الذي اعتدي على أمن وسلامة المجتمع.

كما تبدو المشكلة في التناقض بين أغراض العقوبة التي تهدف إلى الإيلام وتحقير المجرم الذي خالف نواميس السلام والأمن والحياة الهادئة، وبين ما تسعي إليه المراقبة الإلكترونية من التخفيف عن المجرم وحفظ كرامته.

التساؤلات التي تثيرها الدراسة:

تثير الدراسة عدة تساؤلات تتمثل في ماهية المراقبة الإلكترونية، وهل تلعب هذه العقوبة الدور الذي تحققه العقوبة التقليدية، وما هي طبيعة المراقبة الإلكترونية هل هي عقوبة أم تدبير احترازي؟

كما تثير الدراسة التساؤل حول دواعي استحداث المراقبة الإلكترونية كنظام عقابي حديث، وما هي الحلول التي يقدمها لحل مشكلات العقاب التقليدي؟

وهل تُعد المراقبة الإلكترونية نظام عقابي مناسب في المرحلة الحالية بالنسبة للمجرمين، أم أن السعي نحو تطبيقها ما هو إلا هرولة غير عاقلة خلف النظم الغربية في استحداث عقوبات حديثة بدون داع؟

وإذا كانت هذه السياسة العقابية مدروسة ومناسبة للوضع الحالي فما هي العقبات أمام تطبيقها؟

أهمية الدراسة:

تبرز أهمية الدراسة في أنها تتعلق بموضوع غاية في الأهمية يمكن به نقل السياسة الجنائية العقابية إلى مرحلة مختلفة، تهتم بصورة أكثر بإصلاح المحكوم عليه وتأهيله ودمجه بين أفراد المجتمع أكثر من الاهتمام بإيلامه أو تحقيره أو التنكيل به.

كما تبدو أهمية الدراسة في أنها تبرز موضوع السياسة الجنائية الحديثة في معاملة المجرمين المرتكبين للجرائم التنظيمية التي لا تنم عن الإرادة الإجرامية الآثمة، وهي السياسة التي تهتم بشخصية المجرم أكثر من اهتمامها بالجريمة، وهو الشأن الذي يسود في كافة السياسات الجنائية في مختلف الأنظمة الجنائية المقارنة.

ونظراً للأهمية التي حظي بها هذا الموضوع فقد سعت معظم التشريعات بالأخذ به، فقد سن المشرع الفرنسي قانون المراقبة الإلكترونية رقم 97 – 1159 الصادر في 19 ديسمبر 1997، كما أصدرت العديد من الدول العربية تشريعات تنظم المراقبة الإلكترونية ومنها القانون

الأردني رقم 32 لسنة 2017 الخاص بأصول المحاكمات الجزائية الذي أدخل المراقبة الإلكترونية في النظام الأردني بموجب المادة 114 مكرر من هذا القانون.

والقانون البحريني رقم 18 لسنة 2017 بشأن العقوبات والتدابير البديلة للعقوبة السالبة للحرية، والقانون الاتحادي الإماراتي رقم 17 لسنة 2018، والمرسوم بقانون التونسي رقم 29 لسنة 2020 المؤرخ في 10 يونية 2020، كما أخذت المملكة المغربية بنظام السوار الإلكتروني بناء على قانون المسطرة الجنائية من خلال المواد 1-174، و2-174، و3-174، وأخذت كذلك جمهورية الجزائر بالسوار الإلكتروني بالقانون رقم 1/18 الصادر بتاريخ 2018/1/30 بتعديل قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين.

ومن ثم فتبدو أهمية الموضوع في لفت نظر المشرع المصري للمراقبة الإلكترونية كنظام عقابي مستحدث، فالمراقبة الإلكترونية لم تحز على اهتمام المشرع المصري حتى الآن بالرغم من أن النظام التشريعي المصري قد اعتمد العديد من العقوبات البديلة والمعاملة الجنائية الحديثة كالحبس الاحتياطي والوضع تحت مراقبة الشرطة ووقف التنفيذ وغيرها من العقوبات البديلة، إلا أنه لم يعتمد المراقبة الإلكترونية كنظام عقابي حتى الآن.

الهدف من الدراسة:

تهدف الدراسة إلى التأكيد على أن المراقبة الإلكترونية كعقوبة بديلة هي شأن قضائي يصدر عن سلطة قضائية بداية من تقريره وحتى تنفيذه والإشراف على تنفيذه، فإذا صدر تقرير المراقبة الإلكترونية عن سلطة إدارية فإن ذلك يصمها بعدم المشروعية.

كما تهدف الدراسة إلى إلقاء الضوء على المراقبة الإلكترونية كبديل للعقوبات التقليدية وتفرقتها عن المراقبة الإدارية التي تقتضيها أعمال التحريات وجمع المعلومات، أو التي تتم عن طريق كاميرات المراقبة الموضوعة في الأماكن العامة للتيسير في كشف الجرائم ومعرفة المجرمين.

كما تهدف الدراسة إلى ووضع إطار قانوني واضح للمراقبة الإلكترونية كعقوبة من العقوبات البديلة وإخضاعها لمبدأ المشروعية، وتحاشي مشكلاتها المتعلقة بالاختصاص الوظيفي بإصدار قرار تطبيقها، والجهة المنفذة لها، وتحديد نطاقها من حيث الأشخاص والأماكن والأوقات، ومن حيث نوعية العقوبة المستبدلة والجريمة المرتكبة.

إلى جانب تحديد التقنية العملية لتنفيذ المراقبة الإلكترونية وتحديد كيفية استخدام الوسائل الإلكترونية الحديثة في تطبيق المراقبة الإلكترونية، وتحديد الجهة المتكفلة بمصروفات وأعباء تنفيذها.

منهج الدراسة:

اتخذنا في هذه الدراسة المنهج التحليلي النقدي المقارن، وذلك في محاولة لوضع معيار موحد لتطبيق نظام المراقبة الإلكترونية، ولقد رأينا أن هذا المنهج هو الأنسب لبيان ماهية الوضع الحالي لهذا النظام العقابي المستحدث.

خطة الدراسة:

ستكون الدراسة في مبحثين على النحو الآتي:

المبحث الأول: مفهوم المراقبة الإلكترونية وطبيعتها ونطاقها

المطلب الأول: مفهوم المراقبة الإلكترونية.

المطلب الثاني: الطبيعة القانونية للمراقبة الإلكترونية.

المطلب الثالث: نطاق تطبيق المراقبة الإلكترونية.

المبحث الثاني: الدعائم الفلسفية والموضوعية لتطبيق المراقبة الإلكترونية.

المطلب الأول: الدعائم الفلسفية لتطبيق المراقبة الإلكترونية.

المطلب الثاني: الدعائم الموضوعية لتطبيق المراقبة الإلكترونية.

المبحث الأول

مفهوم المراقبة الإلكترونية وطبيعتها ونطاقها

كان للذكاء الاصطناعي صداه التشريعي الواضح على السياسة العقابية المعاصرة ومعاملة المجرمين، ومن ذلك استخدام الذكاء الاصطناعي في تنفيذ المراقبة الإلكترونية التي تعتمد اعتماد كلي على التكنولوجيا الحديثة في تنفيذها، وهذه العقوبة البديلة يرجع أساسها لأفكار مدرسة الدفاع الاجتماعي المتمثلة في إعلاء الدور الإصلاحي والتأهيلي للعقوبة [1].

ولم تكن هذه العقوبة البديلة ضرباً من الخيال أو نبتاً أبتر ليس له جذور، ولكنها سبقتها إرهاصات وأنظمة جنائية عديدة مشابهة لها كالوضع تحت مراقبة الشرطة ووقف التنفيذ والاختبار القضائي، ومن ثم فهي تعد تطوراً طبيعياً للمعاملة العقابية التي من أهم سماتها المرونة والتطور المستمر، ونعرض تفصيل ما تقدم فيما يلي:

المطلب الأول: مفهوم المراقبة الإلكترونية.

المطلب الثاني: الطبيعة القانونية للمراقبة الإلكترونية.

المطلب الثالث: نطاق تطبيق المراقبة الإلكترونية.

---

[1] لقد أتاحت تقنيات الذكاء الاصطناعي استخدام الوسائل الحديثة في تسهيل تنفيذ العقوبات المختلفة ومنها عمليات اقتضاء العقوبات المالية كالغرامات ، ويتمثل ذلك في ربط الأجهزة والمصالح الحكومية بشبكة معلومات واحدة ، بحيث تسجل عليها بيانات الأحكام الصادرة بالإدانة فلا يتمكن المحكوم عليه من إجراء أي معاملة إلا بعد سداد الغرامات المستحقة عليه .

المطلب الأول

مفهوم المراقبة الإلكترونية

أولاً: تعريف المراقبة الإلكترونية:

المراقبة الإلكترونية التي نحن بصددها هي العقوبة البديلة التي تمثل رد الفعل القضائي تجاه الشخص الذي ثبتت مسئوليته عن ارتكاب جريمة بناء على حكم جنائي صادر من محكمة مختصة، وبالتالي لا يدخل في نطاق المراقبة الإلكترونية مراقبة الأشخاص في الأماكن العامة بكاميرات مراقبة، أو مراقبة شخص معين مشتبه فيه كأجراء من إجراءات جمع المعلومات أو التحريات المقررة في المادة 95، و 95 مكرر من قانون الإجراءات الجنائية [1] .

والمراقبة الإلكترونية هي طريقة مستحدثة لتنفيذ العقوبة السالبة للحرية ولاسيما قصيرة المدة منها ، وذلك بإبقاء الشخص في محل إقامته خلال ساعات محددة مع مراقبته إلكترونياً عن طريق وضع جهاز مع المحكوم عليه ، وهذا الجهاز يختلف علي حسب الأحوال فيكون علي هيئة شريحة أو أسورة حول معصم يد المحكوم عليه أو حول ساقة في أعلي القدم ، ويتصل بكومبيوتر مركزي يوجد في مركز المؤسسة العقابية ، بحيث يقوم الجهاز الموجود في مكان المحكوم عليه بإرسال إشارة محددة إلي الكومبيوتر المركزي لدي مكتب المؤسسة العقابية في حالة تجاوز المحكوم عليه لحدود المكان المسموح به، وبموجب هذه الوسيلة تحل الوسائل التكنولوجية محل الحارس الطبيعي بحيث تكون العلاقة مباشرة بين المؤسسة العقابية وبين المحكوم عليه [2] .

---

[1] تنص المادة 95 من قانون الإجراءات الجنائية علي أنه :- " لقاضي التحقيق أن يأمر .....وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص متي كان لذلك فائدة في ظهور الحقيقة في جنائية أو جنحة معاقب عليها بالحبس لمدة تزيد علي ثلاثة أشهر ، وفي جميع الأحوال يجب أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناء علي أمر مسبب ولمدة لا تزيد علي ثلاثين يوماً قابلة للتجديد لمدة أو مدد أخري مماثلة " كما تضمنت المادة 95 مكرراً الأمر بوضع جهاز التلفون تحت المراقبة للمدة التي يحددها رئيس المحكمة .....

[2] د/ عمر محمد سالم : المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن –دار النهضة العربية - الطبعة الثانية – ص 2 .

ولقد عرّف المشرع البحريني المراقبة الإلكترونية في المادة السابعة من القانون رقم 18 لسنة 2017 الصادر بشأن العقوبات والتدابير البديلة فنص على أن الخضوع للمراقبة الإلكترونية يكون بمراقبة حركة وتنقل المحكوم عليه إلكترونياً بواحدة أو أكثر من وسائل المراقبة الإلكترونية المتاحة بوزارة الداخلية.

كما عرّف المشرع الإماراتي نظام المراقبة الإلكترونية في المادة 355 من قانون الإجراءات الجنائية رقم 17 لسنة 2018 الصادر بتعديل بعض أحكام قانون الإجراءات الجنائية الاتحادي رقم 35 لسنة 1992 فنص علي أنها حرمان المتهم أو المحكوم عليه من أن يتغيب في غير الأوقات الزمنية المحددة له عن محل إقامته أو أي مكان آخر يعينه الأمر الصادر من النيابة العامة أو المحكمة المختصة بحسب الأحوال ، ويتم تنفيذه عن طريق وسائل إلكترونية تسمح بالمراقبة عن بُعد ، وتلزم الخاضع لها بحمل جهاز إرسال إلكتروني مدمج طوال فترة الوضع تحت المراقبة .

كما عرف المشرع الجزائري المراقبة الإلكترونية في نص المادة 150 مكررا من القانون رقم 1/18 بشأن قانون السجون وإعادة الإدماج الاجتماعي للمحبوسين ونص على أن الوضع تحت المراقبة الإلكترونية إجراء يسمح بقضاء المحكوم عليه كل العقوبة أو جزء منها خارج المؤسسة العقابية عن طريق حمل الشخص المحكوم عليه طيلة المدة المذكورة في المادة 150 مكرراً لسوار إلكتروني يسمح بمعرفة تواجده في مكان تحديد الإقامة المبين في مقرر الوضع الصادر عن قاضي تطبيق العقوبة.

وعلى ذلك فإن نظام المراقبة الإلكترونية يتضمن نظاماً إلكترونياً لمراقبة المحكوم عليه عن بُعد من خلال السماح للمحكوم عليه بالبقاء في منزله ومراقبة تحركاته من خلال الاستعانة بجهاز يعرف بالسوار الإلكتروني يثبت في معصمه أو في أسفل ساقه [1] .

[1] د/ أسامة حسنين عبيد : المراقبة الجنائية الإلكترونية –دراسة مقارنة –بحث منشور في مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية –العدد الثاني والثانون – 2009 – ص 7 .

وخلاصة ما تقدم فإن عماد المراقبة الإلكترونية هو استخدام تقنيات الذكاء الاصطناعي المتمثلة في وسائط إلكترونية حديثة وربطها بالمحكوم عليه لضمان بقائه خلال فترة زمنية محددة في المكان والزمان المتفق عليهما بين المحكوم عليه وبين السلطة القضائية الآمرة بها [1] .

وهذه المراقبة تمكن إدارة المؤسسة العقابية من مراقبة المحكوم عليه عن بُعد، ومعرفة وجوده في المكان المحدد في الزمن المحدد أو غيابه، ويصدر بتنظيم هذه المراقبة وطريقة تنفيذها حكم قضائي بُعد موافقة المحكوم عليه عن تطبيقها عليه [2] .

وعلى ذلك يمكن القول بأن المراقبة الإلكترونية هي أحد البدائل الرضائية للعقوبات السالبة للحرية التي بمقتضاها يتم متابعة الشخص الخاضع لها من خلال استخدام تقنيات حديثة من قبل أجهزة إنفاذ القانون خارج السجن في أماكن وأوقات محددة سلفاً، ومن خلال إخضاعه لمجموعه من الالتزامات والشروط ويترتب علي مخالفة هذه الالتزامات معاقبته بعقوبة سالبة للحرية [3] .

كما أن المراقبة الإلكترونية تصلح لأن تكون نظاماً بديلاً للحبس الاحتياطي في مرحلة التحقيق والذي وإن كان ليس عقوبة ولكنه نوعاً من المعاملة العقابية أثناء مرحلة التحقيق ، وهو نوع يقره القانون ويعُمل به في كثير من الأنظمة التشريعية وفي العديد من الحالات .

كما أن المراقبة الإلكترونية هي شأن قضائي يصدر في الغالب الأعم من الأنظمة من المحكمة التي أصدرت الحكم الأصلي ، حتي وإن كانت المراقبة مقترحة من المحكوم عليه ذاته أو من المسئول عن المؤسسة العقابية أو عن النيابة العامة علي حسب الأحوال .

---

[1] د/ صفاء أوتاني : الوضع تحت المراقبة الإلكترونية " السوار الإلكتروني " في السياسة العقابية الفرنسية –مجلة دمشق للعلوم الاقتصادية والقانونية –المجلد الخامس والعشرين –العدد الأول 2009 – ص 129 .

[2] د /أيمن رمضان الزيني : الحبس المنزلي - مجلة كلية الدراسات العليا - أكاديمية مبارك للأمن ،القاهرة، مصر، العدد الثاني عشر -يناير 2005 - ص 282 .

[3] د/ رامي متولي القاضي : المراقبة الإلكترونية في القانون الفرنسي والمقارن –مجلة الشريعة والقانون –كلية الحقوق جامعة الإمارات العربية المتحدة –العدد الثالث والستين - يوليو 2015 –ص 286 .

كما أن نظام المراقبة الإلكترونية يتم بحثه بعد صدور حكم بعقوبة سالبة للحرية أو أثناء مرحلة التحقيق فيستبدل نظام المراقبة الإلكترونية بالحبس الاحتياطي بشرط موافقة المحكوم عليه.

ثانياً: العناصر الفنية للمراقبة الإلكترونية

تتبني التشريعات المختلفة أسلوب البث المتواصل لتنفيذ الوضع تحت المراقبة الإلكترونية عن طريق السوار الإلكتروني، وهي طريقة تتبناها أغلب دول العالم التي أخذت بنظام المراقبة الإلكترونية [1] ، ووفقاً لهذا الأسلوب يسُمح للمحكوم عليه البقاء في بيته، لكن تحركاته تبقى محدودة ومراقبة عبر جهاز إلكتروني يشبه الساعة [2]، حيث يضع المحكوم عليه جهازاً يتكون من سواراً مثبتاً في معصمه أو في أسفل قدمه ، وهو عبارة عن مرسل إلكتروني يحتوي على جهاز إرسال يبث إشارات متتالية محددة كل 15 ثانية إلى مُستقبِل مثبت في مكان إقامة الخاضع للرقابة سواء منزله أو مكان عمله أو دراسته ، وهذا المُستقبل يرسل عن طريق الخط الهاتفي رسائل أو إشارات إلى الكومبيوتر الموجود لدي الجهة العقابية التي تتولى المتابعة ، هذه الجهة الأخيرة تستقبل الإشارات المرسلة في المنطقة الجغرافية المحددة كنطاق للمراقبة [3] .

ومن خلال هذه الإشارات و المعلومات يمكن التثبت من عمل الجهاز و التحقق من وجود الشخص الخاضع للرقابة في المكان المحدد، ومن ثم التأكد من احترام الشخص للالتزامات المفروضة عليه بموجب نظام المراقبة الإلكترونية [4].

---

(1) Conte Philippe et Maistre Du Chambon ; Patrich ;droit penal ; geneal ; coll u Armand colin ; 5eme ed ; Paris;2001;P 315 et

(2) راجع المادة السابعة من القانون رقم 18 لسنة 2017 بشأن العقوبات والتدابير البديلة الصادر في مملكة البحرين، وراجع أيضاً المادة 355 من قانون الإجراءات الجنائية رقم 17 لسنة 2018 الصادر بتعديل بعض أحكام قانون الإجراءات الجنائية الاتحادي رقم 35 لسنة 1992 .

(3) د / صلاح محمد الحماد: نظام المراقبة الإلكترونية كبديل للعقوبة السالبة للحرية قصيرة المدة –مجلة الشارقة للعلوم القانونية –العدد يونيه 2021- ص 189 .

(4) د/ محمد سيف نصر عبد المنعم: بدائل العقوبات السالبة للحرية في التشريعات الجنائية الحديثة –رسالة دكتوراه –كلية الحقوق جامعة القاهرة 2004 – ص 15 .

وفي حالة خرق المحكوم عليه لهذه الالتزامات بعدم احترامه لأوقات الحضور أو تعطيل جهاز الاستقبال أو جهاز الإرسال أو محاولة نزع الجهاز، فإن هذا الجهاز يرسل إنذار لمركز المراقبة [1] .

ويتضح مما تقدم أن تنفيذ المراقبة الإلكترونية من الناحية الفنية يتم من خلال ثلاثة عناصر وهي: -

العنصر الأول: جهاز إرسال يتم وضعه في يد المحكوم عليه أو في أسفل الساق وأعلي القدم، ويتمثل هذا الجهاز في شريحة إلكترونية توضع في أسورة تعلق في معصم الخاضع للرقابة أو في قدمه [2].

العنصر الثاني: جهاز تجميع والتقاط الإشارات من جهاز الإرسال ويوضع بالقرب من جهاز الإرسال وفي المكان المحدد لإقامة المحكوم عليه الخاضع للرقابة، ويرتبط بخط تلفوني أو بشبكة إنترنت [3].

العنصر الثالث: جهاز استقبال الإشارات وهو جهاز كومبيوتر مركزي يوجد في مكان إدارة المؤسسة العقابية، ويستقبل الإشارات المجمعة من جهاز التقاط الرسائل المرسلة من الأسورة المعلقة في معصم أو قدم المحكوم عليه، فيتيح تعقبه ومعرفة تحركاته [4].

ولا يجوز للمحكوم عليه بالمراقبة الإلكترونية التحرك إلا في نطاق محدد، حيث يتم حصر وتحديد تحرك المحكوم عليه في مساحة محددة، فإذا تجاوز هذه المساحة يكون قد خالف الحكم الصادر بالمراقبة فتتخذ ضده الإجراءات القانونية اللازمة لذلك، حيث يتم مراقبة التحركات تلقائياً وفي الحال وعن بعد [5].

---

[1] د/ عماد الفقي: النظم البديلة للحبس قصير المدة –دراسة مقارنة –دار النهضة العربية 2017 – ص 35 .

[2] د / صلاح محمد الحماد : نظام المراقبة الإلكترونية كبديل للعقوبة السالبة للحرية قصيرة المدة –مرجع سابق- ص 189 .

[3] د/ محمود محمد بهجت عبد الرحمن : التكييف الفقهي والقانوني للسوار الإلكتروني كعقوبة مستحدثة – بحث منشور في مجلة كلية الشريعة والقانون بتفهنا الأشراف –الدقهلية - العدد الثالث والعشرين –سنة 2021 – ص 865 .

[4] د/ ساهر إبراهيم الوليد : مراقبة المتهم إلكترونياً كوسيلة للحد من مساوئ الحبس الاحتياطي –مجلة الجامعة للدراسات الإسلامية –جامعة غزة فلسطين –مج 21 –عدد 1 –يناير 2018 – 78 .

[5] تختلف هذه المساحة من نظام تشريعي لآخر علي حسب الأحوال .

كما لا يجوز للمحكوم عليه تعطيل الأسورة الإلكترونية أو العبث بها، أو محاولة تعطيل جهاز التقاط وتجميع الإشارات المرسلة من الأسورة الإلكترونية، حيث يتم معرفة ذلك في الحال عن طريق إرسال إشارة بذلك إلى الكومبيوتر المركزي الموجود في مكتب إدارة المؤسسة العقابية [1].

ثالثاً: -العناصر المادية للمراقبة الإلكترونية:

يتطلب تطبيق نظام المراقبة الإلكترونية توافر بعض العناصر المادية، حيث يشترط استخدام نظام السوار الإلكتروني توافر بعض العناصر المادية وفق ما أكده المشرع الفرنسي في المادة 732 مكرر8 من قانون الإجراءات الفرنسي المعدلة بموجب القانون رقم 2004-204 حيث يجب استخدام جميع الوسائل التقنية بشكل يضمن احترام كرامة الشخص وخصوصيته وحياته الخاصة، وتتمثل هذه العناصر فيما يلي:

ـــوجود مكان أو محل إقامة ثابت أو إيجار مستقر [2].

ـــوجود خط هاتفي ثابت [3].

ـــشهادة طبية تؤكد أن حالة الشخص الصحية تتوافق مع وضع السوار الإلكتروني.

ـــالحصول على موافقة مالك العقار أو مؤجره، إذا كانت إقامة الشخص في غير منزله.

ويجب التأكد من توافر هذه العناصر المادية والأجهزة والأدوات التقنية، والتحقق من الوضع الاجتماعي والعائلي للمحكوم عليه، من خلال تحقيق تقوم به إدارة المساعدة على

---

[1] اعتبر المشرع الفرنسي تعطيل أو تحييد جهاز المراقبة عن بعد جريمة هروب من المراقبة الإلكترونية ، وهو ما تضمنه نص المادة 12 من القانون رقم 97 -1159 بشأن المراقبة الإلكترونية .

[2] في هذه العقوبة خرج المشرع علي القواعد العامة في تنفيذ العقوبات السالبة للحرية و المتمثلة في قضاء العقوبة السالبة للحرية في السجون المعدة لذلك وفقاً للمادة 478 إجراءات جنائية مصري .

[3] لم تتعرض التشريعات المختلفة لكيفية توفير هذا الخط الهاتفي الثابت ، وهل يكون توفيره علي حساب الخاضع للمراقبة أم توفره المؤسسة العقابية ، مع العلم أن المعتاد في مثل هذه الحالات أن يكون توفير الأجهزة علي نفقة صاحب المصلحة ، وهو الخاضع للمراقبة الإلكترونية .

الاندماج الاجتماعي والاختبار، وذلك طبقاً للمادة 57-13من قانون الإجراءات الجنائية الفرنسي [1].

يتمثل الهدف من التحقيق الأولي الذي تجريه هذه الأخيرة-أي إدارة المساعدة على الاندماج الاجتماعي والاختبار-في ضمان توفيق قرار الوضع تحت السوار الإلكتروني، فتحدد أوقات الحضور حسب المعطيات المهنية والعائلية للمحكوم عليه، كما يهدف التحقيق الأولي إلى التأكد من أن الشخص المقترح وضعه تحت المراقبة الإلكترونية يعيش في بيئة مناسبة وملائمة لتطبيق هذا النظام بالشكل الصحيح [2].

وعلي ذلك يتم التحقق من أماكن وجود الشخص وتحركاته عن طريق وسائل الاتصالات الهاتفية ، ويقوم الجهاز بتسجيل نموذج لصوت المحكوم عليه ويعامل علي الرقابة والتوثيق المستمر لحضور أو غياب المحكوم عليه من المنزل وذلك كله عن طريق المكالمات الهاتفية من قبل الحاسب الآلي المركزي حيث يقوم الشخص الخاضع للمراقبة الإلكترونية بإجراء اتصال تلفوني من منزله أو من المكان المحدد لإقامته إلي مركز المراقبة خلال فترات زمنية متتابعة ويقوم الكومبيوتر المركزي الموجود بمركز المراقبة بمقارنة بصمة الصوت الأصلية للمحكوم عليه الذي يخضع لهذا النظام والتي تم تخزينها بالكومبيوتر المركزي قبل بداية تطبيق الوضع تحت المراقبة الإلكترونية أو عن طريق الأقمار الصناعية بحيث يتم مراقبة المتهم مراقبة كاملة .

المطلب الثاني

الطبيعة القانونية للمراقبة الإلكترونية

المراقبة الإلكترونية نظام جديد من الأنظمة العقابية بحيث تكون هذه المراقبة هي بديل للعقوبة التقليدية، ولذلك حرصت معظم التشريعات على تحديد نطاقه من حيث الأشخاص

---

[1] د/ راشد حمد البلوشي : نظام المراقبة الإلكترونية بواسطة السوار الإلكتروني كبديل للعقوبات السالبة للحرية –دراسة مقارنة بحث منشور في مجلة كلية القانون الكويتية العالمية – السنة العاشرة –العدد الرابع – سبتمبر 2022 – ص 229 .

[2] د/ كامل السعيد : العقوبات المطبقة علي الصغار –ورقة عمل قدمت إلي ملتقي الاتجاهات الحديثة في العقوبات البديلة – مؤتمر الرياض 2011 .

الخاضعين له، ومن حيث نوعية العقوبة التي حلت محلها المراقبة، وكذلك من حيث المكان والزمان الذي تنفذ فيه المراقبة [1].

فقد اختلفت النظرة إلى طبيعة المراقبة الإلكترونية، فهناك اتجاه يري أنها عقوبة جنائية، بينما ذهب اتجاه أخر إلى أنه تدبير احترازي، ورأي اتجاه ثالث أن المراقبة الإلكترونية ذات طبيعة مزدوجة فهي تدبير احترازي عندما تطبق في مرحلة ما قبل النطق بالحكم، وهي عقوبة عندما تطبيق بعد النطق بالحكم، أما الاتجاه الرابع فيذهب إلى أن المراقبة الإلكترونية لا هي عقوبة خالصة، ولا هي تدبير احترازي خالص ولكنها نظام حديث من أنظمة السياسة العقابية [2]، ونعرض تفصيل ما سبق فيما يلي: -

أولاً: المراقبة الإلكترونية عقوبة جنائية

المراقبة الإلكترونية تحمل معني العقوبة الجنائية، لأنها تصدر عن سلطة قضائية علي أثر دعوي جنائية، وتتضمن في طياتها عناصر العقوبة من تحقيق العدالة، والردع العام والخاص، والإيلام النفسي للخاضع لها عن طريق تقييد حريته، وما تحمله المراقبة الإلكترونية من الالتزامات المختلفة المترتبة عليها من معني الإكراه والقسر، وذلك هو جوهر العقوبة [3].

فمن الالتزامات التي تقع على عاتق الخاضع للمراقبة الإلكترونية ضرورة الاستجابة لطلبات الاستدعاء من السلطات المختصة بتنفيذ المراقبة الإلكترونية، والالتزام بعدم ارتياد الأماكن التي حددها قرار القاضي، فالمراقبة الإلكترونية ليست في جوهرها سوي عقوبة على المحكوم عليه ينفذها خارج محبسه [4].

---

[1] د/ عمر محمد سالم : مظاهر استخدام التكنولوجيا الحديثة في مجال القانون الجنائي – المراقبة الإلكترونية والتحقيق الجنائي عن بعد الطبعة الأولي دار النهضة العربية 2013 – ص 19 .

[2] د/ رامي متولي القاضي : إطلالة علي أنظمة التسوية الجنائية في القانون الفرنسي –دار النهضة العربية 2011 – ص 1 ، ود / محمد الجبالي عبد الفتاح : بدائل العقوبات السالبة للحرية قصيرة المدة –دراسة مقارنة –دار النهضة العربية 2023 – ص 55 .

[3] د/ عمر محمد سالم : المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن –مرجع سابق – ص 35.

[4] د/ عبد الرحمن خلفي : العقوبات البديلة –دراسة فقهية تحليلية تأصيلية مقارنة –المؤسسة الحديثة للكتاب –بيروت 2015 – ص 76 .

كما أن المراقبة الإلكترونية لا تكون إلا وفق حكم ينطق به القاضي مباشرة في صلب الحكم، وهو ما يجعلها عقوبة بدون شك [1].

ولكن مما يتناقض مع معني العقوبة في المراقبة الإلكترونية هو طابعها الرضائي، فهي لا تطبق في معظم التشريعات إلا إذا رضي بتطبيقها الشخص المحكوم عليه بعكس العقوبة التي تحمل طابع القسر والإجبار، ومن جهة أخري فإن المراقبة الإلكترونية تنحصر بصفة خاصة كعقوبة بديلة للعقوبات السالبة للحرية قصيرة المدة ولا يمتد تطبيقها على العقوبات المختلفة كالعقوبات الشديدة أو العقوبات المالية.

كما أن الغرض الذي تحمله العقوبة بصفة أساسية هو الإيلام والتحقير والردع العام والخاص [2]، وهو ما لا يتوافر بصورة واضحة في المراقبة الإلكترونية التي تتصف بالرأفة والإصلاح والتأهيل.

ثانياً: المراقبة الإلكترونية تدبير احترازي:

إذا كان الغرض من المراقبة الإلكترونية هو إبعاد الخاضع للمراقبة الإلكترونية عن ارتكاب الجريمة، وتحييد خطورته الإجرامية، وإعادة دمجه اجتماعياً بين أقرانه من أفراد المجتمع، وهو عين الغرض من الذي تهدف إليه التدابير الاحترازية [3].

ويعتبر البعض أن المراقبة الإلكترونية هي أحدي وسائل المتابعة القضائية الاجتماعية التي تفرض على المحكوم عليه في جناية أو جنحة خطيرة بعد استنفاد العقوبة السالبة للحرية أو كتدبري تكميلي للإفراج المشروط بحيث يعتبر السوار الإلكتروني وسيلة أو إجراء يهدف إلى الحد من العود إلى الجريمة، ويخضع لمبدأ الشرعية الجنائية، ولا يطبقه غير القاضي بحكم يصدر منه [4].

---

[1] د/ محمود محمد بهجت عبد الرحمن : التكييف الفقهي والقانوني للسوار الإلكتروني كعقوبة مستحدثة – مرجع سابق – ص 865.

[2] د/ رؤوف عبيد : القسم العام من التشريع العقابي –دار الفكر العربي 1979 – ص 76 .

[3] د/ فهد الكساسبة : وظيفة العقوبة ودورها في الإصلاح والتأهيل –دار الثقافة للنشر –عمان الأردن 2010 – ص 17 .

[4] د/ محمد مصباح القاضي : التدابير الاحترازية في السياسة الجنائية الوضعية والشرعية –دار النهضة العربية –ص 35 .

ولكن ما يتناقض مع طبيعة المراقبة الإلكترونية كتدبير احترازي هو أن تطبيقها يكون في الغالب بعد ارتكاب جريمة بسيطة وبعد صدور حكم فيها بالحبس قصير المدة فيختار القاضي من العقوبات ما يتناسب مع المحكوم عليه لعدم خطورته ، في حين أن التدابير الاحترازية لا توقع إلا إذا كان من يخضع لها قد ارتكب جريمة خطيرة وتظهر فيها الخطورة الإجرامية للمجرم، فيتم اللجوء إلي التدابير الاحترازية لمنع ارتكاب جريمة أخري نظراً لارتباط التدابير الاحترازية بالخطورة الإجرامية للمجرم ، فلا محل لتطبيقها إذا انتفت الخطورة الإجرامية .

كما تتناقض صفة الرضائية التي تتصف بها المراقبة الإلكترونية مع صفة القسر والإجبار التي تتصف بها التدابير الاحترازية التي لا يتوقف تطبيقها على رضاء المحكوم عليه.

كما أن التدبير الاحترازي غير محدد المدة فلا يمكن للقاضي معرفة مدة زوال الخطورة، ومن ثم فيربط تطبيقها بزوال الخطورة الإجرامية للمحكوم عليه، وفي ذلك تختلف المراقبة الإلكترونية مع التدابير الاحترازية.

ثالثاً: -الطبيعة المزدوجة للمراقبة الإلكترونية

تختلف النظرة إلى المراقبة الإلكترونية علي حسب المرحلة الإجرائية التي تطبق فيها، فإن تم تطبيقها في المرحلة السابقة على صدور الحكم في الدعوي الجنائية -على المحبوسين احتياطياً -اكتسبت المراقبة حينئذ صفة التدبير الاحترازي، حيث يكون الفرض هنا أنها تحل محل الحبس الاحتياطي في تحقيق غايته التي من بينها الحيلولة دون هرب المحبوس احتياطياً أو منعه من ارتكاب جرائم جديدة نظراً لخطورته الإجرامية [1].

أما إذا طبقت المراقبة في مرحلة التنفيذ العقابي أي بعد صدور الحكم بإدانة الجاني، فإنها تكون ذات طبيعة عقابية لأنها تنطوي على تقييد للحرية، ومع ذلك فهي ليست عقوبة بالمفهوم التقليدي ولكنها عقوبة تهذيبية بناءة تحمل طابع المكافأة عن حسن سلوك المحكوم عليه

[1] د/ محمود محمد بهجت عبد الرحمن : التكييف الفقهي والقانوني للسوار الإلكتروني كعقوبة مستحدثة – مرجع سابق – ص 865.

في أوقات سلب الحرية، وهو ما انتهي إليه الفكر العقابي الحديث في تدرج نظم المؤسسات العقابية [1].

ويتضح مما تقدم أن نظام المراقبة الإلكترونية يمكن أن يتصف بالطبيعة العقابية، كما يمكن أن يتصف بالطبيعة الاحترازية، وهذا يتوقف على طريقة تطبيقه من حيث المرحلة، فهي احترازية إذا طبقت في المرحلة السابقة على صدور الحكم في الدعوي الجنائية حيث يتم استبدال حجز المتهم على ذمة القضية بالمراقبة الإلكترونية خشية هروبه، أما إذا طبقت في المرحلة التالية لصدور الحكم، فإنها تكون بمثابة عقوبة جنائية بموجب حكم قضائي [2].

رابعاً: المراقبة الإلكترونية نظام حديث للمعاملة العقابية

يري البعض أن المراقبة الإلكترونية ما هي إلا وسيلة أو أسلوب حديث لتنفيذ العقوبات السالبة للحرية خارج المؤسسات العقابية، ويمكن من خلالها تلافي الآثار السلبية الناجمة عن تنفيذ العقوبة داخل هذه المؤسسات، وتطبق هذه الوسيلة على فئة من المحكوم عليهم ممن تثبت ظروفهم أنهم أهل لهذه المراقبة الإلكترونية كوسيلة عقاب حديثة [3].

ووفقاً لهذا الرأي فإن المراقبة الإلكترونية لا تُعد عقوبة، ولا تُعد تدبير احترازي أيضاً، فهي لا تُعد عقوبة لأنها:

من ناحية لا تنفذ في المكان المخصص لحبس الأفراد وهي السجون وأماكن الاحتجاز التي حددها القانون، ولكنها تنفذ في مكان متفق عليه بخلاف الأماكن المحددة قانوناً [4].

---

[1] د/ راشد حمد البلوشي : نظام المراقبة الإلكترونية بواسطة السوار الإلكتروني كبديل للعقوبات السالبة للحرية –مرجع سابق – ص 229 .

[2] د/ رامي متولي القاضي : المراقبة الإلكترونية في القانون الفرنسي والمقارن – مرجع سابق –ص 16.

[3] د/ صفاء أوتاني : الوضع تحت المراقبة الإلكترونية "السوار الإلكتروني " –مرجع سابق –ص 55 .

[4] د/ محمد مصباح القاضي : التدابير الاحترازية في السياسة الجنائية الوضعية والشرعية – مرجع سابق –ص 39 .

ومن ناحية أخري أن سلب الحرية يفترض استمرار منع المحكوم عليه من حرية التنقل والحركة، وهو ما لا يتوافر في المراقبة الإلكترونية التي تنفذ في منزل المحكوم عليه، ويسمح له فيها بالتحرك داخل نطاق محدد [1].

كما أن سلب الحرية لا يُعد تدبير احترازي بما ينضوي عليه من قسر وإلزام للمحكوم عليه، بعكس المراقبة الإلكترونية التي يشترط فيها الرضائية وموافقة المحكوم عليه [2].

وعلى ذلك فقد اعتبر المنظم السعودي المراقبة الإلكترونية وسيلة مستحدثة لتنفيذ العقوبات، وذلك في مشروع قانون التدابير الاحترازية والعقوبات البديلة لعقوبة الجلد أو السجن الذي لا تتجاوز مدته ثلاث سنوات والتي تخضع لسلطة القضاء التقديرية ويكون من شأنها تحقيق المصلحة المرجوة من العقاب وضمان حق المجني عليه وحقوق المجتمع [3]، ولقد نصت المادة الثامنة عشرة من المشروع صراحة على أنها تقييد للحرية خارج السجن.

خامساً: رأينا في طبيعة المراقبة الإلكترونية

نميل إلى الاتجاه الأخير الذي يري أن المراقبة الإلكترونية هي نظام مستحدث من أنظمة العقاب، فالمراقبة الإلكترونية أسلوب جديد ومستقل بذاته لتنفيذ العقوبة السالبة للحرية، وإن كان يتفق مع الأنظمة التقليدية في أغراض العقوبة وأهدافها إلا أنه يعتمد اعتماد كلي على التقنيات التكنولوجية الحديثة في تنفيذ العقوبة.

ولا شك أن تنفيذ الإجراء الصادر من قاضي التنفيذ في خارج السجن بضوابط معينة، مع إلزام الخاضع لهذا الإجراء بالتزامات محددة يمثل نظام متفرد للعقاب في السياسة الجنائية الجديدة.

فهو يحقق أغراض العقوبة من ردع خاص في شأن الخاضعين له من الأفراد الذين ليس لهم باع طويل في الإجرام، ولا تتحمل طبيعتهم العقوبات التقليدية من حبس في السجون، كما أنها من جانب أخر تحقق الإصلاح والتأهيل لهؤلاء المجرمين، وكل ذلك في صورة من

---

[1] د/ شريف كامل : الحبس قصير المدة في التشريع الجنائي الحديث –مرجع سابق – ص 33 .

[2] د/ محمود محمد بهجت عبد الرحمن : التكييف الفقهي والقانوني للسوار الإلكتروني كعقوبة مستحدثة – مرجع سابق – ص 865.

[3] راجع المادة الأولي من مشروع قانون العقوبات البديلة السعودي .

العقاب لم يكن لها شبيه في النظام العقابي التقليدي، ومن ثم فهي نظام مستحدث ومتفرد له صفات خاصة تستند إلى التقنيات التكنولوجية الحديثة في تنفيذه.

المطلب الثالث

نطاق تطبيق المراقبة الإلكترونية

نظام المراقبة الإلكترونية نظام مستحدث من أنظمة تنفيذ العقوبة الجنائية، ولذلك فقد حرصت التشريعات المختلفة على تحديد نطاق المراقبة الإلكترونية من حيث الأشخاص والأماكن والوقت ونوع العقوبة وحصرها في حدود معينة، ونعرض هذه النطاقات فيما يلي: -

أولاً: -نطاق المراقبة من حيث الأشخاص

يطبق نظام المراقبة الإلكترونية على الأشخاص بصرف النظر عن سنهم، إذ يطبق هذا النظام على الأشخاص البالغين وعلى الأحداث الذين لا تقل سنهم عن الثالثة عشر من عمرهم ولا تزيد عن ثمانية عشر عاماً، بشرط صدور حكم ضدهم، وبعد موافقة ولي أمر الحدث [1]، وكذلك يمتد نظام المراقبة الإلكترونية إلى الأشخاص المحبوسين احتياطيا، نفصل ذلك على النحو الآتي:

1- الأشخاص المحكوم عليهم: -

يجوز تطبيق نظام المراقبة الإلكترونية على ثلاث طوائف من الأشخاص المحكوم عليهم وهم:

الطائفة الأولي: الأشخاص المحكوم عليهم بعقوبة سالبة للحرية قصيرة المدة لا تزيد عن سنة ، فيشترط أن تكون العقوبة المحكوم بها علي الشخص عقوبة سالبة للحرية ، فلا يتصور تطبيق هذا النظام بدلاً من تطبيق عقوبة مالية كالغرامة أو المصادرة أو الغلق ، وكذلك لا يجوز تطبيقها كبديل للتدابير الاحترازية أو العقوبات الأخرى كالاختبار القضائي أو وقف

---

(1) يختلف الحد الأدنى لسن الخاضع للمراقبة الإلكترونية باختلاف التشريع العقابي ، ففي إنجلترا وويلز حدد المشرع سن الثامنة عشر (18سنة) كحد أدنى لسن المحكوم عليه الذي يراد تطبيق هذا النظام عليه .

التنفيذ أو العمل للمنفعة العامة ، ومرجع ذلك أن التشريعات تنظر للمراقبة الإلكترونية علي أنها وسيلة حديثة لتنفيذ العقوبة السالبة للحرية لا بوصفها عقوبة أصلية بالمعني الدقيق [1] .

ومن جهة أخري فإنه يشترط لتطبيق نظام المراقبة الإلكترونية أن تكون العقوبة قصيرة المدة، فلا تزيد العقوبة السالبة للحرية المحكوم بها على الشخص عن سنة [2].

الطائفة الثانية: المحكوم عليهم بعقوبات سالبة للحرية لمدة طويلة قد تصل إلى عشر سنوات، ولكن يكون المحكوم عليه قد قضي أكثرها ولم يتبق منها سوي عام واحد، بمعني أن تكون المدة المتبقية من العقوبة لا تزيد عن سنة [3].

الطائفة الثالثة : المحكوم عليهم الذين يجوز لهم الاستفادة من نظام الإفراج الشرطي، وفي هذه الحالة يتم تطبيق نظام المراقبة الإلكترونية بحسبانها إجراء تمهيدي يسبق هذا الأخير[4] ، وتشمل هذه الفئة المحكوم عليهم المشمولين بعفو رئاسي أو أميري، فقد طبقت وزارة الداخلية الكويتية نظام المراقبة الإلكترونية علي المسجونين الذين صدر بشأنهم عفو أميري تطبيقاً للمادة 239 من قانون الإجراءات والمحاكمات الجزائية رقم 17 لسنة 1960 وتعديلاته التي تنص علي أنه :- " للأمير بعد صدور حكم بالعقوبة ضد شخص معين وقبل تنفيذ هذا الحكم أو أثناء التنفيذ أن يصدر أمراً بالعفو عن العقوبة المحكوم بها أو تخفيفها أو إبدالها بعقوبة أخف منها " .

وكان تطبيق ذلك وفق ضوابط معينة وفي حدود القضايا التنظيمية البسيطة، حيث تستثني من ذلك القضايا الخطيرة الماسة بأمن الدولة والاعتداء على المال العام فتقوم إدارة

---

[1] د/ عبد الرحمن خلفي : العقوبات البديلة –دراسة فقهية تحليلية تأصيلية مقارنة –مرجع سابق – ص 79 .

[2] أ/ خلود محمد أسعد إمام : وضع الأحداث تحت الرقابة الإلكترونية كعقوبة بديلة للحبس : مرجع سابق – ص 76 .

[3] د/ راشد حمد البلوشي : نظام المراقبة الإلكترونية بواسطة السوار الإلكتروني كبديل للعقوبات السالبة للحرية –مرجع سابق – ص 229 .

[4] د/ محمد عبد الرحمن عبد المحسن : استخدام السوار الإلكتروني كبديل للعقوبة السالبة للحرية في القانون المصري –مرجع سابق – ص 559 .

تنفيذ الأحكام بوضع آلية لتتبع المساجين الذين يفرج عنهم في الفترة القليلة المتبقية من مدة عقوبتهم لقضائها في منازلهم أو في الأماكن التي يتفق عليها [1].

ويلاحظ في كل الحالات السابقة أن مدة المراقبة الإلكترونية لا يجوز أن تزيد عن سنة بالنسبة لأي فئة من فئات الأشخاص الخاضعين للمراقبة، ومع ذلك فإن بعض التشريعات تحظر تطبيق نظام المراقبة الإلكترونية على فئات معينة من الأشخاص المحكوم عليهم، حيث تنص المادة 34 فقرة (أ) من قانون العدالة الجنائية في إنجلترا وويلز الصادر عام 1991 على عدم ملائمة الفئات التالية من السجناء المحكوم عليهم بعقوبات سالبة للحرية قصيرة المدة والتي لا تزيد مدتها على أربع سنوات لتطبيق نظام الحبس المنزلي عليهم وهم: -

- المحكوم عليهم بعقوبة لاقترافهم جرائم العنف والجنس.
- العائدون لدرب الجريمة من المحكوم عليهم بعقوبة سالبة للحرية خلال فترة تطبيق نظام الإفراج الشرطي عليهم.
- المحكوم عليهم الخاضعون لأمر قضائي بالعلاج الطبي بمقتضى نصوص المواد 37 و45و 47 فقرة أ من قانون الصحة العقلية الصادر في عام 1983.
- المحكوم عليهم الذين تتزايد احتمالات مغادرتهم للبلاد، والمطبق عليهم نص المادة 42 من قانون العدالة الجنائية الصادر في عام 1991.
- السجناء الذي تم إيداعهم في السجن مرة أخرى، بمقتضى نص المادة 40 من قانون العدالة الجنائية الصادر في عام 1991، لارتكابهم جرائم جديدة قبل نهاية الفترة الأولى من الحكم.
- يضاف إلى ما سبق فإن المحكوم عليهم لاقترافهم جرائم جنسية والمطبق عليهم نص الفقرة الأولى من جرائم الجنسية الصادر في عام 1994، لا يجوز تطبيق نظام الحبس المنزلي عليهم.

---

[1] تصريح لرئيس لجنة العفو الأميري الكويتي بشأن عدم الممانعة القانونية في تطبيق نظام العقوبات البديلة في بعض العقوبات البسيطة علي غرار ما هو متبع في كثير من دول العالم وذلك حتي يصدر تشريع خاص يتعلق بهذا الشأن - جريدة الأنباء الكويتية بتاريخ 2021/5/7 .

هذا ونشير إلى أن نظام السوار الإلكتروني يمكن تطبيقه على الرجال والنساء، كما يمكن أن يشمل المحكوم عليهم وكذلك الأشخاص الموضوعين تحت المراقبة القضائية من المتهمين[1].

كما تشترط بعض التشريعات ضرورة أن يكون المحكوم عليه لائقاً صحياً لتطبيق المراقبة الإلكترونية، وألا يلحقه ضرر صحي من وضع الأسورة الإلكترونية أو الجهاز الخاص بالمراقبة على جسمه، وعلى ذلك نصت المادة 150 مكرر 7 من القانون الصادر برقم 1/18 بتعديل قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين بدولة الجزائر بتاريخ 2018/1/30.

2- الأشخاص المحبوسين احتياطياً:

قد تتطلب الخطورة الإجرامية لبعض المتهمين وبالنظر إلي جسامة الجريمة المتهمين فيها أن يقتضي ذلك حبسهم احتياطياً علي ذمة القضية بالرغم من احتمالية براءتهم ، وإذا كان نظام المراقبة الإلكترونية أنه نوع من تقييد الحرية أو المراقبة بسلب حريته بإيداعه أحدي المؤسسات العقابية لضمان عدم هروبه ومنعه من ممارسة إجرامه أو التحرز من التأثير علي الشهود أو العبث بأدلة الجريمة ، ومن ثم يكون هذا النظام هو الأنسب لهذه المرحلة التي لم تثبت فيها الإدانة كما لم تثبت فيها البراءة ، فيتعين علي الخاضع لها احترام الالتزامات المفروضة عليه وعدم الخروج عليها بمغادرة المكان أو بمقابلة شخص إلا بتصريح من القاضي ، وهي إجراء يتخذ لضرورة التحقيق أو كتدبير أمني ويختص قاضي التحقيق الذي تعرض عليه الأوراق بوضع المتهم تحت المراقبة القضائية ، ولعل هذه المراقبة الإلكترونية تكون أنسب للمتهم الذي لا يزال بريئًا حتي تثبت إدانته .

ثانياً: -نطاق المراقبة من حيث المكان والزمان:

يتحدد نطاق المراقبة الإلكترونية من خلال الحكم الصادر بها من حيث المكان ومن حيث الزمان، ففيما يتعلق بنطاق المكان فقد اشترطت بعض التشريعات أن يكون للمحكوم

---

[1]د/ راشد حمد البلوشي : نظام المراقبة الإلكترونية بواسطة السوار الإلكتروني كبديل للعقوبات السالبة للحرية –مرجع سابق – ص 229 .

عليه موطن مستقر، ومحل إقامة ثابت، ومرجع ذلك أن نظام المراقبة الإلكترونية في بداية تطبيقه كان يقوم على فكرة الإقامة الجبرية وعدم مغادرة المحكوم عليه للمكان المحدد لإقامته [1].

وقد يكون هذا المكان هو بيت المحكوم عليه أو محل عمله أو محل دراسته، وقد تحدد بعض التشريعات مسافة معينة لا ينبغي للمحكوم عليه أن يتخطاها، وإلا تم إرسال إشارات من جهاز الإرسال إلى الكومبيوتر الموجود لدي السلطة المختصة بتنفيذ العقاب.

أما فيما يتعلق بالنطاق الزماني للمراقبة الإلكترونية، فإن معظم التشريعات لا تجعل المراقبة الإلكترونية لكل الوقت بل تجعله لبعض الوقت لتكون في ساعات محددة يخضع فيها المراقب للرقابة، مع الإشارة إلى أن ذلك لا يعني التخلي عن الأجهزة المثبتة للمراقبة في وقت معين بل أنها تعمل طوال الوقت، ولكن يحدد للمحكوم عليه وقت معين للالتزام بالبقاء والتواجد في المكان المحدد للإقامة [2].

ولقد جاءت هذه الضوابط ملبية لمتطلبات حقوق الإنسان والحفاظ على كرامته، وهو ما حرص على تكريسه قانون العقوبات والتدابير البديلة للعقوبة السالبة للحرية الصادر برقم 18 لسنة 2017 في دولة البحرين الذي حرص على الاتفاق مع أغراض العقوبات الحديثة من إصلاح وتأهيل.

ولقد نصت المادة الثامنة عشرة من مشروع قانون العقوبات البديلة السعودي علي أنه: -» عند تطبيق عقوبة تقييد حرية المحكوم عليه خارج السجن في نطاق مكاني محدد ومناسب، يجوز للقاضي الأمر باتخاذ التدابير المناسبة مثل وضع القيد الإلكتروني في معصمه أو إلزامه بالحضور أمام الشرطة أو غيرها في ساعة محددة، ويجب أن يتضمن الأمر بإيقاع هذه العقوبة تحديد الجهة التي يحضر أمامها وساعة الحضور ويجب على تلك الجهة إشعار المحكمة بمدي التزام المحكوم عليه بالحضور من عدمه".

---

[1] د/ محمد عبد الرحمن عبد المحسن : استخدام السوار الإلكتروني كبديل للعقوبة السالبة للحرية في القانون المصري –مرجع سابق – ص 559 .

[2] د/ محمود محمد بهجت عبد الرحمن : التكييف الفقهي والقانوني للسوار الإلكتروني كعقوبة مستحدثة – مرجع سابق – ص 865 .

ثالثاً: نطاق المراقبة الإلكترونية من حيث نوعية العقوبة

يشترط لتطبيق نظام المراقبة الإلكترونية شرط أساسي يتمثل في أن تكون العقوبة سالبة للحرية قصيرة المدة، ومن ثم لا مجال لتطبيقه على العقوبات الأخرى كالسجن طويل المدة، أو العقوبات المالية كالغرامة.

أما فيما يتعلق بتطبيق نظام المراقبة الإلكترونية في نهاية مدة تنفيذ العقوبة بالنسبة للأشخاص المحكوم عليهم بعقوبة سالبة للحرية، فإنه يشترط أن تكون المدة المتبقية من العقوبة تساوي أو تقل عن سنة.

كما يمكن تطبيق نظام الوضع تحت المراقبة الإلكترونية على المحكوم عليه الخاضع للإفراج الشرطي، فتكون المراقبة الإلكترونية أحد الالتزامات المفروضة عليه ضمن إطار الإفراج المشروط، بشرط ألا تتجاوز مدة الخضوع سنة [1].

وعموماً فإن نطاق تطبيق المراقبة الإلكترونية من حيث العقوبة يختلف من نظام تشريعي لأخر، فوفقاً للمادة 380 من المرسوم بقانون اتحادي رقم 17 لسنة 2018 الصادر بدولة الإمارات بتعديل بعض أحكام قانون الإجراءات الجزائية فإن لكل محكوم عليه بعقوبة مقيدة للحرية لمدة لا تقل عن سنتين ولا تزيد على خمس سنوات أن يتقدم بطلب إلى النيابة العامة للإفراج عنه ووضعه تحت المراقبة الإلكترونية مدة تنفيذه الباقي من العقوبة عن طريق الوسائل الإلكترونية «.

أما المشرع الفلسطيني فأجاز تطبيق المراقبة الإلكترونية كعقوبة بديلة للعقوبات السالبة للحرية التي تصل مدتها إلى ثلاث سنوات وفقاً للمادة 1/4 من قانون مراقبة سلوك المجرمين الفلسطيني.

---

[1] أ / خلود محمد أسعد إمام : وضع الأحداث تحت الرقابة الإلكترونية كعقوبة بديلة للحبس : مرجع سابق – ص 76 .

في المملكة العربية السعودية فقد حدد المنظم السعودي في المادة الأولي من مشروع قانون العقوبات البديلة نطاق المراقبة الإلكترونية كعقوبة بديلة لعقوبة الجلد أو السجن الذي لا تتجاوز مدته ثلاث سنوات [1].

وفي النظام الإماراتي ظهر من نص المادة 363 من المرسوم بقانون رقم 17 لسنة 2018 أنه لا يجوز إصدار الأمر بالوضع تحت المراقبة الإلكترونية على الجرائم المعاقب عليها بالإعدام أو السجن المؤبد والجرائم الماسة بأمن الدولة الداخلي والخارجي والجرائم التي أوجب فيها القانون الحكم بتدبير الإبعاد عن الدولة.

وعلى ذلك فقد طبق القضاء الإماراتي المراقبة الإلكترونية على المحكوم عليهم في جرائم تعاطي المخدرات والمؤثرات العقلية [2].

وفي فرنسا لم يطلق المشرع الفرنسي تطبيق نظام المراقبة الإلكترونية بديلاً عن أي عقوبة سالبة للحرية بل اشترط حداً أقصي لهذه العقوبة بحيث لا تزيد على الحبس لمدة سنتين، وعلى ذلك نصت المادة 723 -7 من قانون الإجراءات الجنائية الفرنسي.

---

[1] نري أن تطبيق المراقبة الإلكترونية كبديل لعقوبة الجلد وفقاً للنظام السعودي فيه مجافاة للصواب ؛ لأن الجلد عقوبة بدنية يقصد منها الإيلام الجسدي ، وليس عقوبة سالبة للحرية ، ومن ثم فلا تناسب بين المراقبة الإلكترونية والجلد .

[2] حكم محكمة النقض الجزائي في القضية رقم 1288 لسنة 2019 - م جزائي السنة 13 – ق . أ . - أبو ظبي بجلسة 2019/12/31.

المبحث الثاني

الدعائم الفلسفية والموضوعية لتطبيق المراقبة الإلكترونية

لم يكن نظام المراقبة الإلكترونية وليد اللحظة أو أنه نشأ صدفة بدون ترتيب ولكنه نظام له جذور فلسفية عميقة مؤسسة على إعلاء وتدعيم قرينة البراءة من جهة ومن جهة أخري تبني فكرة إصلاح وتأهيل المجرم وإدماجه في المجتمع.

ولقد ساعد كذلك على رواج المعاملة العقابية البديلة ومنها المراقبة الإلكترونية دعائم موضوعية عديدة كتكاليف تنفيذ العقوبات التقليدية الباهظة، مع مساوئ تطبيقها وسوء نتائجها، ونعرض فيما يلي للدعائم الفلسفية والموضوعية لنظام المراقبة الإلكترونية على النحو الآتي:

المطلب الأول: الدعائم الفلسفية للمراقبة الإلكترونية.

المطلب الثاني: الدعائم الموضوعية للمراقبة الإلكترونية.

المطلب الأول

الدعائم الفلسفية لتطبيق المراقبة الإلكترونية

للمراقبة الإلكترونية جذور تاريخية دعت إلى تطبيقها، وكذلك أسس فلسفية تسند إلى فكرة إصلاح وتأهيل المجرم، وإعادة دمجه في المجتمع، ولا شك أن فكر الفلاسفة يؤثر تأثيراً مباشراً في السياسة التشريعية الجنائية، ولقد ظهر ذلك واضحاً حينما أثر فكر المدرسة التقليدية القديمة والحديثة المتمثل في فكرة العقد الاجتماعي والمنفعة الاجتماعية كأساس لحق الدولة في العقاب، فأدي ذلك إلى سياسة العقوبات القاسية بحسبان أن المجرم قد خالف العقد الاجتماعي وتعدي علي حق المجتمع ومن ثم يستحق العقاب القاسي [1].

[1] من أهم مؤسسي هذه المدرسة المفكر الفرنسي جان جاك روسو ، وقد اتسمت العقوبة في ظل فكر هذه المدرسة بالمغالاة والقسوة.

وتلي فكر المدرسة التقليدية بعهديها، فكر المدرسة الوضعية بأفكارها المعتدلة والتي تبنت الأخذ بأسلوب التدابير الاحترازية وتفريد الجزاء الجنائي ليناسب كل فرد بقدر جرمه وتصنيف المجرمين حسب الفروق النفسية والاجتماعية والعضوية [1].

ثم جاءت مدرسة حركة الدفاع الاجتماعي الحديثة والتي تخففت من أفكار المفكر جراماتيكا المتطرفة في عدم الاعتراف بالقانون الجنائي ومفاهيمه في معاملة المجرم والأخذ بقانون الدفاع الاجتماعي، فجاء المفكر مارك أنسل بحركة الدفاع الاجتماعي الجديدة التي أبقت على مفاهيم القانون الجنائي، وركزت على شخصية المجرم، والاهتمام بالطابع الإنساني في معاملته، وأعلت من فكرة الإصلاح والتأهيل للمجرم [2].

ولا شك أن هذه الأفكار قد مثلت إرهاصات للسياسة العقابية الحديثة التي تهدف إلى معاملة عقابية فاعلة، وتقوم على قضاء العقوبة خارج أسوار السجون بما يحفظ كرامة الإنسان ولا يمس بسمعته، ويحافظ على الروابط الأسرية، وفي نفس الوقت يؤدي دور العقوبة التقليدية في الإصلاح والتأهيل وإعادة الدمج في المجتمع بالإضافة للردع العام والخاص للمجرم [3].

وفيما يلي نرصد بعض الأسس الفلسفية لنظام المراقبة الإلكترونية على الوجه الآتي: -

أولاً: ذيوع فكرة إصلاح وتأهيل المجرم كأساس للمعاملة العقابية البديلة:

على أثر تطور الفكر العقابي تقدمت فكرة إصلاح المجرم وتأهيله على بقية أغراض العقوبة من تحقيق للعدالة وردع للمجرم، فكان الهدف الأساسي للعقوبة هو إعادة المجرم إلى المجتمع وإدماجه فيه، وبمقتضي ذلك تحولت وظيفة العقوبة من مجرد الإيلام والانتقام والتحقير، إلى وظيفة العلاج والإصلاح والتقويم عن طريق آليات عقابية مستحدثة لترشيد السياسة

---

[1] من أقطاب هذه المدرسة لومبروزو ، وانريكو فري ، وجاروفالو ، وقامت أفكار هذه المدرسة علي أساس الردع الخاص وتفريد الجزاء والمسئولية القانونية وليس الأخلاقية .

[2] C.Cardet : le placement sous surveillance sous surveillance electronique ;L'Harmatt an 2003 P13.

[3] عادل يحيي قرني : الضوابط المستحدثة للحبس الاحتياطي في ضوء القانون رقم 145 لسنة 2006 المعدل لبعض أحكام قانون الإجراءات الجنائية الصادر بالقانون رقم 150 لسنة 1950 –دار النهضة العربية –الطبعة الأولي 2007 – ص 56 .

العقابية، وكان من أهم هذه الآليات توفير بدائل غير تقليدية للعقوبات السالبة للحرية وخاصة قصيرة المدة [1].

وتقوم فكرة الإصلاح والتأهيل علي منع المجرم من الوقوع في براثن الجريمة، وإبعاده عن أسبابها بكافة السبل، وذلك بعدم وضعه مع عتاة الإجرام في مكان واحد، والبعد عن تحقيره والحط من كرامته ووصمه بالدونية طوال حياته بوصفه بأنه رد سجون، مما يغذي في نفسه اليأس من الصلاح أو من محو تاريخه السيء، فيندفع نحو الانجراف في الإجرام [2].

ولا شك أن في إصلاح المجرم وتأهيله وإعادة دمجه في المجتمع فيه مصلحة للمجرم ذاته، ولأسرته وللمجتمع بأكمله، حيث يؤدي إصلاح هذا المجرم إلي كف شر إجرامه عن غيره من أفراد المجتمع، ويكون عنصراً نافعاً لنفسه ولأسرته ولمجتمعه.

فلاقي نظام المراقبة الإلكترونية رواجاً في الفكر العقابي في التشريعات الحديثة لدول عديدة؛ وذلك لما تتصف به من إنسانية وحفظ لكرامة الإنسان، فليس معني وقوع الإنسان في شراك الجريمة أن يتم تجريده من وصف الإنسانية ومعاملته بقسوة كما كان يعامل العبيد في العصور الوسطي [3].

ولقد أكد هذا النظام ما تبناه الإعلان العالمي لحقوق الإنسان من مبادئ، فأورد في المادة الخامسة منه والتي نصت على أنه: -» لا يجوز إخضاع شخص للتعذيب أو لعقوبات قاسية أو غير إنسانية أو حاطه بالكرامة "

وتماشي المشرع المصري مع هذه الأفكار، فأكد على إنسانية العقوبة في المادة 51 دستور 2014 التي تنص على أنه " الكرامة حق لكل إنسان ولا يجوز المساس بها وتلتزم الدولة باحترامها وحمايتها «.

---

(1) د/ سامح المحمدي : فلسفة البدائل غير الإحتجازية في ترشيد السياسة العقابية " المراقبة الإلكترونية نموذجاً " بحث منشور في المجلة الجنائية القومية –المجلد الرابع والستين –العدد الأول –مارس 2021 – ص 115 .

(2) د/ محمود محمد بهجت عبد الرحمن : التكييف الفقهي والقانوني للسوار الإلكتروني كعقوبة مستحدثة – مرجع سابق – ص 866.

(3)C.Cardet : le placement sous surveillance sous surveillance electronique ;L'Harmatt an 2003 P13.

كما نصت المادة 56 من دستور 2014 على أن السجن دار إصلاح وتأهيل، وتخضع السجون وأماكن الاحتجاز للإشراف القضائي، ويحظر فيها كل ما ينافي كرامة الإنسان أو يعرض صحته للخطر.

وهذا ما ردده المشرع في المادة 40 من قانون الإجراءات الجنائية التي نصت على أنه: -» لا يجوز القبض على أي إنسان أو حبسه إلا بأمر ...كما تجب معاملته بما يحفظ عليه كرامة الإنسان ولا يجوز إيذاؤه بدنياً أو معنوياً.

كما استعان المشرع المصري في القانون رقم 145 لسنة 2006 ببعض التدابير التي يستعاض بها عن الحبس الاحتياطي بغرض إبعاد المتهم عن الجريمة ومحاولة إصلاحه وتأهيله، حيث يجوز لسلطة التحقيق أن تلجأ إلى إلزام المتهم بعدم مبارحة مسكنه أو موطنه، وإلزامه بأن يقدم نفسه لمقر الشرطة في أوقات محددة، وكذلك حظر ارتياده لأماكن محددة [1].

ثانياً: مبدأ أصل البراءة كأساس للمعاملة العقابية البديلة أثناء مرحلة التحقيق:

مبدأ الأصل في الإنسان البراءة يعني أن الإنسان برئ الذمة من وجوب أي شيء أو إلزامه بأي شيء، كما أن إلزامه بشيء يكون خلافاً للأصل [2].

ويقتضي ذلك احترام الإنسان ومراعاة حقوقه وإحسان الظن به، وعدم التنكيل به لأنه برئ من الانتساب إلى الإجرام حتى يثبت ذلك، وبالتالي يكون برئ من العقاب [3].

ويتفرع عن هذا الأصل فرعين ، أولهما : براءة الإنسان قبل إدانته بحكم جنائي لارتكابه جريمة معاقب عليها ولكن لم تثبت إدانته خلال مرحلة التحقيق ونظر الدعوي إلي ما قبل

---

[1] تنص المادة 201 من قانون الإجراءات الجنائية المستبدل بها القانون رقم 145 لسنة 2006 في فقرتها الثانية علي أنه :- " يجوز للسلطة المختصة بالحبس الاحتياطي أن تصدر أمراً بأحد التدابير الآتية :- 1- إلزام المتهم بعدم مبارحة مسكنه أو موطنه 2- إلزام المتهم بأن يقدم نفسه لمقر الشرطة في أوقات محددة 3- حظر ارتياد المتهم لأماكن محددة .

[2] د/ محمود محمد بهجت عبد الرحمن محمد : التكييف الفقهي والقانوني للسوار الإلكتروني كعقوبة مستحدثة – مجلة الشريعة والقانون بتفهنا الأشراف –دقهلية- العدد الثالث والعشرين لسنة 2021 –الجزء الأول – ص 865 .

[3] C.Cardet : le placement sous surveillance sous surveillance electronique ;L'Harmatt an 2003 P13.

صدور الحكم [1] ، وثانيهما عدم معاقبة الإنسان عن الأفعال التي يرتكبها بدون إرادة آثمة ، ولكن وضعها المشرع في قالب الجريمة بنصوص تشريعية وعاقب علي ارتكابها، ويشمل ذلك الجرائم التنظيمية الصغيرة التي لا تعبر عن شخصية خطيرة كالمخالفات المرورية ومخالفات أولوية الدخول وغيرها من الجرائم التنظيمية ، وكذلك الجرائم غير العمدية التي لا تنبأ عن أي نزعة إجرامية كالتشخيص الخطأ من قبل الطبيب، فهذه الجرائم لا يجب معاقبة الشخص عليها عقاب تقليدي بالحبس حتي ولو ثبتت إدانته عليها بحكم جنائي نهائي ، ونقول أن عدم العقاب هنا ينصرف إلي العقاب الجنائي فقط إلا أنه لا يمنع من العقاب الإداري .

ومما لا شك فيه أن معاقبة الشخص قبل صدور الحكم في مرحلة المحاكمة بعقوبات سالبة للحرية، وكذلك معاقبته جنائياً بهذه العقوبات عن جرائم تنظيمية هي في الأصل لا تمثل جرائم، فهي تبدو مشروعة قبل صدور نص بتجريمها، وكذلك يمكن إلغاء النص الصادر بتجريمها فتبدو مشروعة مثل جرائم مخالفة تحديد زراعة محصول معين في منطقة معينة والتي تختلف نطاق تحديدها من زمن لأخر أو مكان لأخر، هذه الجرائم لا تنبأ عن إرادة إجرامية آثمة تستحق العقاب، وإن كان يمكن معاملتها معاملة عقابية خاصة كالتغريم مثلاً.

ومن هنا جاءت فكرة استدعاء العقوبات البديلة التي لا تغالي في إيلام المجرم، ولا تهدر كرامته، ويمكن تدارك الخطأ في تطبيقها، والرجوع عنها إذا تبين وجود خطأ في تنفيذها ولو بعد صدور الحكم النهائي، ولا غرو أن الأخطاء القضائية من الأمور المتوقعة، فالقاضي بشر يخطئ ويصيب وليس منزه عن مجانبة الصواب، وإلا ما جعل القضاء على درجات.

وعلي ذلك فإننا نري أن تطبيق نظام المراقبة الإلكترونية في مرحلة التحقيق وقبل الحكم النهائي علي المتهم يُعد مناسباً لهذه المرحلة لما تتصف به هذه العقوبة من يسر ومرونة ومحافظة علي كرامة المتهم ، ومن جهة أخري فهي ترغم المتهم علي البقاء في مكانه وتحت بصر سلطة التحقيق وتقيده عن ارتكاب أي فعل يهدد بالعبث في أدلة الجريمة أو محاولة التأثير علي الشهود ، في حين أن الحبس الاحتياطي في هذه المرحلة يُعد من أخطر الإجراءات التي تتخذها

[1] د/ أحمد لطفي السيد مرعي : نحو تدعيم مبدأ أصل البراءة في الإجراءات الجنائية –دار الأهرام للإصدارات القانونية والنشر والتوزيع 2023 – ص 78 .

سلطة التحقيق بإيداع المتهم في السجن –قبل صدور حكم بالإدانة- وهو ما يتعارض مع مبدأ أصل البراءة .

ثالثاً: مبدأ تفريد العقوبة علي حسب كل مجرم على حدة كأساس للمعاملة العقابية البديلة:

تقوم العقوبات البديلة علي أساس تفريد العقوبة عن طريق تركيز الاهتمام على شخصية المجرم بما يحيط به من ظروف مختلفة بصرف النظر عن الضرر الناجم عن أفعاله، فمن خلال الاهتمام بتلك الشخصية والتعمق في دراستها يمكن تحديد أنسب طرق المعاملة العقابية لها، ويمكن للقاضي بناء على ذلك أن يتخير الجزاء المناسب لكل مجرم على حدة تبعاً لحالة كل منها[1].

فينتج عن ذلك توجيه الأنظار إلى الصفة الإصلاحية والتأهيلية للجزاء الجنائي، والتنبيه إلى أهمية تأهيل المجرم وإصلاحه، بما يسهم في اندماجه في المجتمع مرة أخري [2].

ويتضمن مبدأ تفريد العقوبة التأكيد على احترام حقوق الإنسان ووجوب إحاطة الجزاء الجنائي بكافة الضمانات والتمسك بمبادئ الشرعية الجنائية والمساواة والتناسب بين العقوبة والجرم، وعدم المغالاة، وعدم الأخذ بجريرة العقوبة من لم يرتكب الجريمة فيما يعرف بشخصية العقوبة [3].

ومن مقتضيات التفريد العقابي أن الذي يقوم بتطبيق العقوبة السلطة القضائية المخولة والمختصة بذلك، ويكون الإشراف القضائي ضرورة للإشراف على تنفيذها بحسبان أن القاضي الجنائي هو الأقدر على معرفة المتهم عن قرب ومعرفة ظروفه، فيتم إعداد سجل جنائي للمجرم وإنشاء ملف له يسمي ملف الشخصية للاستعانة به في مراحل الدعوي المختلفة فيمكن القاضي

---

[1] د/ نبيل العبيدي : أسس السياسة العقابية في السجون ومدي التزام الدولة بالمواثيق الدولية –دراسة معمقة في القانون الجنائي –المركز القومي للإصدارات القانونية –القاهرة –سنة 2015 .

[2] د/ أحمد فاروق زاهر : دور الوسائل التكنولوجية في تنفيذ الجزاءات الجنائية –المراقبة الإلكترونية الثابتة والمتحركة –مجلة الفكر القانوني والاقتصادي –جامعة بنها – مصر 2011 .

[3] د/ رمسيس بهنام : علم الوقاية والتقويم – الأسلوب الأمثل لمكافحة الإجرام –منشأة المعارف بالإسكندرية 1985 – ص 32 .

من العلم بظروف المتهم الشخصية من حيث سنه وجنسه وحالتاه الاجتماعية ومركزه المادي والأسري والاجتماعي، وهو ما ييسر عملية تحديد الجزاء المناسب لكل حالة على حده.

كما يقتضي مبدأ تفريد العقوبة قيام المشرع بتحديد أنماط السلوك التي يعتبرها جريمة تمس الهيئة الاجتماعية، وفرض العقوبات التي تتناسب مع جسامة الفعل والأضرار الناشئة عنه ليختار منها القاضي العقوبة المناسبة، وهذا الاختيار لا يتم بصورة عشوائية إنما بعد دراسة مختلف الجزاءات الجنائية المتاحة وفق تطور المجتمع ومفاهيمه السياسية والاقتصادية والاجتماعية والخلقية.

وحيث لم تُعد الجزاءات محصورة في النظم التقليدية المعتادة ، فلم يقتصر الأمر على العقوبات باعتبارها الألم الذي يتناسب مع جسامة الجريمة المرتكبة والذي يصيب المحكوم عليه في حياته أو حريته أو ذمته المالية ، وإنما اتسع الأمر ليشمل سلسلة من العقوبات البديلة التي تطبق على طائفة معينة من الجناة الذين وفق قياسات معينة ينبئ وضعهم الجنائي عن عدم صلاحية العقوبة التقليدية في إصلاحهم وتقويمهم، وهكذا اتسعت فرصة الاختيار أمام القاضي الجنائي حال القيام بدورة في مكافحة الجريمة ، وما هذا إلا نتيجة للتطور الذي شهدته أبحاث علم العقاب والسياسة العقابية، ووسائل تطبيقها في ظل التقدم التكنولوجي المذهل .

رابعاً: تطور أغراض العقوبة من القصاص إلي الكفاح ضد الجريمة:

كان لدراسات علم العقاب أثرها في تطوير أغراض الجزاء الجنائي وأساليب المعاملة العقابية ، ففي الوقت الذي كانت فيه العقوبة هي الجزاء الأساسي بدأ علماء القانون الجنائي في القرن الثامن عشر في الانتقال بالعقوبة من مرحلة اعتبارها مجرد قصاص تستوجبه قواعد الأخلاق أو مجرد اعتبارها تعويضاً عادلاً ومستحقاً للمجتمع إلى مرحلة الوظيفة الوقائية للعقوبة ،إذ يجب على العقوبة أن تلعب دوراً في حماية المجتمع بمنع تكرار الجريمة سواء من غير المحكوم عليه وهو ما يسمى بالردع العام Prévention générale ، وسواء من المحكوم عليه ذاته وهو ما يسمى بالردع الخاص Prévention spécial[1] .

[1] د/ رؤوف عبيد : القسم العام من التشريع العقابي – مرجع سابق – ص 77 .

وفي المرحلة التي كان ينظر فيها للعقوبة على أساس أن لها طابع القصاص والانتقام اصطبغت بما يسمى بالوظيفة الاستبعادية للعقوبةFonction d'élimination ، والتي ترى أن كفاح المجتمع ضد الجريمة لا يكون إلا بإقصاء المجرم عن المجتمع ككل. من هنا ازدادت أهمية عقوبة الإعدام وكذلك العقوبات السالبة للحرية -خاصة طويلة المدة أو المؤبدة-لأنها تؤدي في النهاية إلى إبعاد المحكوم عليه عن المجتمع؛ لذا فإن الدراسات العقابية في هذه المرحلة كانت تسمى " بعلم السجون "Science Pénitentiaire"[1].

وإزاء العيوب التي ظهرت للوظيفة الاستبعادية للعقوبة، لما لها من نتائج سلبية على المحكوم عليه ذاته وعلى أسرته وعدم تناسبها مع الجرائم القليلة الجسامة من وجهة النظر الاجتماعية، بدأ الاهتمام بغرض عقابي أخر للجزاء الجنائي ألا وهو غرض الردع الذي قد يتحقق بطريق التخويف La dissuasion par l'intimidation أو بطريق الإصلاح La dissuasion par l'amendement.

والطريق الأول له قسمان : الأول هو الردع العام الموجه للكافة من الناس لما يحدثه الجزاء الجنائي الواقع على عاتق المحكوم عليه من ترهيب لبقية أفراد المجتمع وإحباط الإرادة الإجرامية لديهم ، وهذا الردع يتفاوت فيه الناس بحسب نوع الجريمة المرتكبة فهي تختلف من كونها جريمة تقليدية أم أنها جريمة تنظيمية ، فالعقوبات المقررة لجرائم التهرب الضريبي والجمركي والجرائم المرورية ومخالفات البناء وقمائن الطوب ومخالفة الدورات الزراعية ، وللمخالفات عموماً لا تحدث درجة التخويف بذات القدر الذي تحدثه العقوبات في الجرائم الأخرى، كما أن الردع يتفاوت حسب نوع العقوبة ودرجة جسامتها ، فالإعدام أشد من الحبس في درجة الردع كما أن هذا الأخير له أثر رادع أشد من الغرامة.

ويتوقف أخيراً غرض الردع العام على نوعية المجرم، فالمجرم العاطفي مثلاً لا يمثل العقاب في ذهنه قبل الإقدام على فعله الآثم، كما أن هناك طوائف أخرى تقل لديها حدة الردع لما يثور لديهم من باعث الأمل من الإفلات من العقاب.

---

[1] راجع توصيات المؤتمر السادس والسابع للأمم المتحدة لمنع الجريمة ومعاملة المجرمين 1980 و 1985 .

أما القسم الثاني فهو التخويف الذي ينصرف إلى المحكوم عليه وحده، أو ما يسمى بالردع الخاص، وهذا التخويف ينصرف أثره للمستقبل بعد تنفيذ العقوبة، بمعنى أنه يستهدف الحيلولة بين المحكوم عليه وبين العودة إلى سلوك سبيل الجريمة مرة أخرى، غير أن هذا التخويف الخاص في حالات العقوبة القاسية السالبة للحرية وأحيانا المغالى فيها، من شأنه أن يجعل المحكوم عليه أكثر عدوانية وكراهية للهيئة الاجتماعية لما للسجن من أثر سلبي على صحة ونفسية وجسد وأسرة المحكوم عليه.

ولقصور وظيفة الردع بشقيقها العام والخاص عن مكافحة الجريمة كان لابد أن تنهج الدراسات العقابية نهجاً حديثاً في النظرة إلى أغراض الجزاء الجنائي وأساليب المعاملة العقابية، الأمر الذي تم على يد أنصار المدرسة الوضعية الإيطالية، التي لا تنظر للجسامة الذاتية للواقعة الإجرامية كأساس للعقاب وإنما للخطورة الإجرامية للفاعل واحتمال وقوع الجريمة منه في المستقبل.

من هنا ظهر الطريق الثاني ألا وهو الردع بطريقة الإصلاح ، أي العمل بأساليب مختلفة على دفع المحكوم عليه في المستقبل وبعد انتهاء مرحلة التنفيذ العقابي إلى التوافق في سلوكه مع القواعد الاجتماعية السائدة في المجتمع ، وبالجملة تحوله إلى رجل شريف ، وهذا الهدف -كما ترى المدارس العقابية في فرنسا خاصة مدرسة الدفاع الاجتماعي - هو من مهام الإدارة العقابية التي يجب أن تعمل على خلق وتنمية الإرادة داخل المحكوم عليه وتهذيبه وتأهيله كي يعتاد على العمل الشريف في أعقاب خروجه من المؤسسة العقابية، وهذا يلقى على هذه الإدارة عبء تثقيفي وعبء القيام بالرعاية الصحية والاجتماعية للمحكوم عليه ، سواء أكان ذلك أثناء مرحلة التنفيذ العقابي أو بعد ذلك في إطار ما يسمى بالرعاية اللاحقة للمحكوم عليه بهدف ضمان تأهيله وانخراطه عضوا نافعاً في المجتمع، وقد أصبح تحقيق هذا الهدف أهم ما يشغل الباحثين في علم العقاب [1] .

هذا التطور دفع البعض - ومع سيادة هذه المفاهيم الحديثة في المعاملة العقابية - إلى إطلاق اصطلاح "علم معاملة المجرمين Science de traitement des délinquants " على ذلك العلم الذي يعكف على دراسة القواعد التنفيذية لمختلف الجزاءات الجنائية -عقوبات

[1] د/ رمسيس بهنام : علم الوقاية والتقويم – مرجع سابق – ص 33 .

وتدابير- ودراسة وسائل المكافحة العامة للجريمة والوقاية منها ، هذا الأمر الذي تهتم به منظمة الأمم المتحدة في إطار دعوتها المتكررة للعديد من المؤتمرات الدورية والتي تنعقد كل خمس سنوات حول "الوقاية من الجريمة ومعاملة المذنبين" ومنها المؤتمر الأول الذي انعقد بمدينة جنيف بسويسرا عام 1955 وفى هذا المؤتمر تم عرض المشروع الذي أعدته سكرتارية الأمم المتحدة حول قواعد الحد الأدنى لمعاملة المذنبين وتم إقراره واعتماده من قبل المجلس الاقتصادي والاجتماعي للأمم المتحدة في 31 يوليو 1957 ليمثل جملة القواعد التي أجمع الخبراء في المجال العقابي على قبوله بوجه عام كمبادئ وأساليب صالحة في مجال معاملة المسجونين وإدارة المؤسسات العقابية ، وليعد بمثابة دليل العمل في مجال الإصلاح العقابي.

ونخلص مما تقدم إلى أن الدراسات العقابية الحديثة لم تُعد تقتصر على دراسة كيفية تنفيذ العقوبات والتدابير ال احترازية Mesures de sûreté أياً كان نوعها، بل أصبحت تتناول فوق ذلك أساليب المعاملة العقابية التي تجري داخل المؤسسة العقابية أو التي تجري خارجها كالإفراج الشرطي ووقف التنفيذ ونظام الرعاية اللاحقة والمراقبة الإلكترونية

المطلب الثاني

الدعائم الموضوعية لتطبيق المراقبة الإلكترونية

على أثر تطور الفكر العقابي فقد شاعت أفكار مؤثرة في مجال السياسة العقابية الحديثة، ومن هذه الأفكار أن العقاب بسلب الحرية في كثير من الجرائم لا يمثل بصورة مطلقة العلاج المناسب لمواجهة الجريمة، سواء في تحقيق الردع العام والخاص، أو في إعادة تأهيل وإصلاح المجرم، وذلك بسبب المساوئ التي تحيط بتطبيق أنظمة العقاب التقليدي ([1]).

ومن هذه المساوئ ما يترتب عليها من آثار سيئة على المجرم وعلى أسرته وعلى مجتمعه، فهي تصم المحكوم عليه بوصمة الإجرام، وتحرم الأسرة من عائلها، وتكلف الدولة مصاريف طائلة، وتزحم السجون بالمتهمين، وتمنع من إعادة إصلاح وتأهيل المجرم، نفصل ذلك فيما يلي:

---

[1] د/ سامح المحمدي : فلسفة البدائل غير الإحتجازية في ترشيد السياسة العقابية " المراقبة الإلكترونية نموذجاً " مرجع سابق – ص 120 .

أولاً: أزمة تكدس السجون بالمسجونين

تكدس السجون يجعل ضرر العقوبة أكثر من نفعها، حيث لا تكفي لتحقيق المعاملة المناسبة للمحكوم عليه لإعادة تأهيليه وإصلاحه، وهذا الازدحام يكون عائق أمام معاملة عقابية مناسبة تصلح من شأن المحكوم عليه وتؤهله للإدماج في المجتمع، وهو ما يؤدي إلي تضاءل الدور الإصلاحي للمؤسسات العقابية [1].

فلا شك أن تكدس وازدحام السجون يمثل عقبة في تحقيق أهداف العقوبة من ناحيتين، فمن ناحية فإن التكدس يزيد من إيلام المحكوم عليه لبقائه في السجن في ظروف غير ملائمة [2]، ومن ناحية أخري فإن التكدس والازدحام يمنع من تحقيق إصلاح المحكوم عليه أو تأهيله كهدف أساسي للعقوبة [3].

ثانياً: التكاليف الباهظة لتنفيذ العقوبات التقليدية

تنفيذ العقوبات التقليدية يمثل إرهاق شديد لخزينة الدولة الناتجة عن كثرة أعداد النزلاء من المساجين في السجون، لتوفير احتياجاتهم من مأكل وملبس ورعاية صحية واجتماعية، هذا بالإضافة إلى الحاجة إلى إنشاء سجون جديدة لاستيعاب تزايد المحكوم عليهم من المساجين [4].

ومن جهة أخري فإن العقوبات التقليدية السالبة للحرية فيها تعطيل للقوة العاملة عن الإنتاج بسبب وضع أشخاص منتجين داخل السجون وهم قادرون على العمل والإنتاج [5].

---

(1) د/ حسين الرفاعي : تكدس السجون وبدائل المؤسسات العقابية –مجلة الفكر الشرطي –شرطة الشارقة بدولة الإمارات العربية المتحدة –العدد الثالث ديسمبر سنة 1993 – ص 155 وما بعدها .

(2) د/ سامر إبراهيم الوليد : مراقبة المتهم إلكترونياً كوسيلة للحد من مساوئ الحبس الاحتياطي –دراسة تحليلية –مجلة الجامعة الإسلامية للدراسات الإسلامية –القاهرة 2013 .

(3) د/ عطية مهنا : مشكلة ازدحام السجون – دراسة مقارنة – بحث المجلة الجنائية القومية – المجلد 46 – العدد الثالث – نوفمبر 2003 .

(4) د/ شريف سيد كامل : الحبس قصير المدة في التشريع الجنائي الحديث –مرجع سابق – ص 9 .

(5) د/ عماد الفقي : النظم البديلة للحبس قصير المدة – مرجع سابق – ص 17 .

ثالثاً: تضاءل فاعلية العقوبات التقليدية في منع الجريمة.

تلاحظ أنه بالرغم من قسوة العقوبات التقليدية السالبة للحرية إلا أنها لم تحد من الجريمة، ولم تؤد الغرض منها، بل على العكس من ذلك تؤدي إلى احتراف المحكوم عليه للجريمة بعد أن يكون قد اختلط بالعتاة من المجرمين الذين يعلمونه طرق وأساليب ارتكاب الجرائم، ويزيلون من قلبه رهبة ارتكابها، فيخرج من السجن أكثر جرأة على ارتكاب الجرائم [1].

ومن ثم فإن العقوبة التقليدية لم تمثل رادع للمجرم ولا لغيره بعد أن استسهلها الناس واعتادوا على قضائها بدون أن تمثل لهم أي رهبة أو خشية، فلم تصبح لها فاعلية في منع الجريمة [2].

رابعاً: التخفيف من أعباء مرحلة ما بعد قضاء العقوبة:

لا شك أن العقوبة السالبة للحرية لما تتصف به من إمعان في الإيلام تولد لدي المحكوم عليه شعوراً بالمهانة والاحتقار يظل يؤلمه خلال فترة قضائه للعقوبة، ويلازمه بعد خروجه منها، وهو ما يتسبب في ظهور العديد من الأمراض النفسية لدي المحكوم عليهم مثل الاكتئاب والقلق والاغتراب النفسي [3] .

ويظهر كذلك أثر الإمعان في تحقير المحكوم عليه في نظرة المجتمع إليه؛ لأن ارتكاب الجريمة يمثل وصمة عار في جبينه وجبين كل أفراد عائلته ويسجل في صحيفة حالته الجنائية[4]، وهو ما يجعله يعيش بعد قضاء عقوبته وخروجه من السجن معاناة مع المجتمع الذي يزدريه ويحتقره، فيصبح غير قادر علي التعايش مع المجتمع [5].

---

[1] د/ عبد الرؤوف مهدي : السجن كجزاء جناوي في ضوء السياسة الجنائية الحديثة –مجلة القانون والاقتصاد سنة 1978 .

[2] د/ رمسيس بهنام : علم الوقاية والتقويم –الأسلوب الأمثل لمكافحة الإجرام –منشأة المعارف بالإسكندرية 1985 – ص 28 .

[3] د/ راشد حمد البلوشي : نظام المراقبة الإلكترونية بواسطة السوار الإلكتروني كبديل للعقوبات السالبة للحرية –دراسة مقارنة – مجلة كلية القانون الكويتية العالمية –السنة العاشرة –العدد الرابع سبتمبر 2022 – ص 229 .

[4] د/ محمد جبريل إبراهيم : الإطار القانوني للتسجيل الجنائي أو كارت المعلومات –مرجع سابق – ص 76 .

[5] د/ سامح المحمدي : فلسفة البدائل غير الإحتجازية في ترشيد السياسة العقابية " المراقبة الإلكترونية نموذجاً " مرجع سابق– ص 115 .

خامساً: عصرنة إجراءات العدالة:

في ظل التحول الرقمي فقد بدا واضحاً الأخذ ببعض منجزات التكنولوجيا في تنفيذ وتطبيق العدالة بداية من كتابة المحاضر وإجراء التحقيقات والاستعانة بالفيديو كونفيرانس والحضور الافتراضي في الجلسات تجديد الحبس الاحتياطي [1] .

ولقد امتد نطاق الاستعانة بالتكنولوجيا إلى تنفيذ بعض العقوبات البديلة ومن أهمها المراقبة الإلكترونية التي تتيح للسلطة المختصة بتنفيذ العقاب فرصة المراقبة للمحكوم عليه أثناء تنفيذ حبسه المنزلي من خلال وسائل إلكترونية متصلة بمكان تواجد المحكوم عليه في منزله [2].

ولم تقف تقنيات الذكاء الاصطناعي عند حد المراقبة الإلكترونية بل امتدت هذه التقنيات إلى استحداث طرق جديدة تستهدف تسهيل عمليات اقتضاء العقوبات المالية كالغرامة والمصادرة، ويتمثل ذلك في دفع الغرامات عن طريق ربط الأجهزة والمصالح الحكومية التي يتعامل معها الفرد والتي تسجل عليها الأحكام الصادرة بالإدانة [3]

---

[1] د/ عمر محمد سالم : مظاهر استخدام التكنولوجيا الحديثة في مجال القانون الجنائي –المراقبة الإلكترونية والتحقيق الجنائي عن بعد –الطبعة الأولي دار النهضة العربية 2013 – ص 22 ، ود/ عادل يحيي قرني : التحقيق والمحاكمة الجنائية عن بعد –دراسة تحليلية تأصيلية لتقنية الفيديو كونفيرنس في المجال الجنائي –دار النهضة العربية 2006 – ص 28 .

[2] د/ عماد الفقي : النظم البديلة للحبس قصير المدة – مرجع سابق – ص 56 .

[3] د/ عمر محمد سالم : نحو تيسير الإجراءات الجنائية –دراسة مقارنة –دار النهضة العربية 1997 – 35 .

خاتمة الدراسة

تناولت الدراسة مفهوم المراقبة الإلكترونية كنظام عقابي حديث، وخصائصه وطبيعته من حيث كونه عقوبة أم تدبير احترازي، ونطاق تطبيقه من حيث الأشخاص والأوقات والأزمان والجرائم، ووضح من خلال ذلك أهمية استخدام الذكاء الاصطناعي في تنفيذ العقوبات البديلة.

نتائج الدراسة:

1. المراقبة الإلكترونية نظام حديث ومتميز وله ذاتيته من بين أنظمة العقاب، ويجمع بين مزايا العقوبة ومزايا التدبير الاحترازي، ولقد سارعت العديد من الدول إلى تطبيقه.
2. المراقبة الإلكترونية تختلف عن غيرها من الأنظمة المشابهة، مثل الوضع تحت مراقبة الشرطة، الإفراج الشرطي، فهي نظام عقابي حديث له ذاتيته واستقلاليته.
3. نظام المراقبة الإلكترونية هو الأكثر ملائمة للأحداث وللنساء العائلات لما يحققه من إصلاح وإعادة تأهيل للعودة للمجتمع، وكذلك يجمع شمل الأسرة ببقاء المحكوم عليه في بيته بين أسرته.
4. المراقبة الإلكترونية حققت نجاحاً في مجال العقوبات الأحكام الاحتياطي، حيث تحافظ على قرينة البراءة، ولا تقيد حرية المحكوم عليه بالسجن قبل ثبوت التهمة عليه.
5. المراقبة الإلكترونية تتحاشى مساوئ العقوبات التقليدية، فتمنع اختلاط المحكوم عليهم بعتاة المجرمين، وتقلل نفقات المساجين وتمنع اكتظاظ السجون، وتحقق الإصلاح والتأهيل.
6. المراقبة الإلكترونية تتميز بالمرونة حيث يمكن تعديل شروطها وتغيير ضوابطها، ويمكن سحب القرار الصادر بتطبيقها، وكذلك ألزام المحكوم عليه بتنفيذها وإلا عوقب على مخالفتها.

توصيات الدراسة:

1- توصي الدراسة بوضع إطار تشريعي للمراقبة الإلكترونية عن طريق نص تشريعي خاص أو تعديل في النصوص القائمة وذلك لوسم هذه العقوبة بالصفة الشرعية، ويحدد هذا الإطار مفهومها ونطاق تطبيقها وشروطها وآثارها على المحكوم عليه وعلى المجتمع.

2- توصي الدراسة بعدم التوسع في تطبيق نظام المراقبة الإلكترونية، وإحاطته بضوابط صارمة عند التطبيق حتى يؤتي بثماره كنظام عقابي حديث.

3- توصي الدراسة بالتوسع في الأخذ بنظام المراقبة الإلكترونية كنظام عقابي بديل في العقوبات اليسيرة السالبة للحرية قصيرة المدة، وعقوبات الحبس الاحتياطية، وبالنسبة للأحدث والنساء العائلات.

4- توصي الدراسة بالاستفادة من التجارب السابقة في التشريعات المقارنة التي تناولت نظام المراقبة الإلكترونية، والأخذ بما يتناسب منها مع المجتمع المصري.

5- توصي الدراسة بإسناد الاختصاص بتقرير تطبيق المراقبة الإلكترونية للقاضي المختص، والنأي بها عن السلطة التنفيذية لتفادي الإخلال بمبدأ شرعية الجرائم والعقوبات، ومبدأ الفصل بين السلطات.

6- توصي الدراسة بإعداد الكوادر البشرية والفنية لتطبيق المراقبة الإلكترونية، وتأهيل أعضاء النيابة العامة والقضاة ومأموري الضبط القضائي والمختصين بالتنفيذ للقيام بأعباء المراقبة الإلكترونية علي أكمل وجه.

7- كما توصي الدراسة بضرورة اهتمام المراكز البحثية بالبحث في موضوع نظام المراقبة الإلكترونية، وعرض عيوبه ومزايا وإعداد نظرية عامة للعقوبات البديلة.

8- توصي الدراسة بجعل المراقبة الإلكترونية وسيلة فعالة لمواجهة مغالاة المشرع في التجريم التنظيمي لكل صغيرة وكبيرة من الأفعال التي لا تنم عن الإرادة الإجرامية الآثمة.

قائمة المراجع

1- د/ أحمد فتحي سرور: العقوبة الرضائية في الشريعة الإسلامية والأنظمة الجنائية المعاصرة –دار النهضة العربية 2010

2- د/ أسامة حسنين عبيد: المراقبة الجنائية الإلكترونية –دراسة مقارنة –بحث منشور في مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية –العدد الثاني والثمانون – 2009.

3- د /أيمن رمضان الزيني: الحبس المنزلي -مجلة كلية الدراسات العليا -أكاديمية مبارك للأمن، القاهرة، مصر، العدد الثاني عشر -يناير 2005.

4- د/ راشد حمد البلوشي: نظام المراقبة الإلكترونية بواسطة السوار الإلكتروني كبديل للعقوبات السالبة للحرية –دراسة مقارنة بحث منشور في مجلة كلية القانون الكويتية العالمية – السنة العاشرة –العدد الرابع – سبتمبر 2022.

5- د/ رامي متولي القاضي: المراقبة الإلكترونية في القانون الفرنسي والمقارن –مجلة الشريعة والقانون –كلية الحقوق جامعة الإمارات العربية المتحدة –العدد الثالث والستين -يوليو 2015.

6- د/ ساهر إبراهيم الوليد: مراقبة المتهم إلكترونياً كوسيلة للحد من مساوئ الحبس الاحتياطي –مجلة الجامعة للدراسات الإسلامية –جامعة غزة فلسطين –مج 21 –عدد 1 –يناير 2018.

7- د/ صفاء أوتاني: الوضع تحت المراقبة الإلكترونية " السوار الإلكتروني " في السياسة العقابية الفرنسية –مجلة دمشق للعلوم الاقتصادية والقانونية –المجلد الخامس والعشرين –العدد الأول 2009.

8- د / صلاح محمد الحماد: نظام المراقبة الإلكترونية كبديل للعقوبة السالبة للحرية قصيرة المدة –مجلة الشارقة للعلوم القانونية –العدد يونية 2021.

9- د/ عبد الرحمن خلفي: العقوبات البديلة –دراسة فقهية تحليلية تأصيلية مقارنة – المؤسسة الحديثة للكتاب –بيروت 2015

10- د/ عماد الفقي: النظم البديلة للحبس قصير المدة –دراسة مقارنة –دار النهضة العربية 2017.

11- د/ عمر محمد سالم: المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن –دار النهضة العربية -الطبعة الثانية.
12- د/ فهد الكساسبة: وظيفة العقوبة ودورها في الإصلاح والتأهيل –دار الثقافة للنشر –عمان الأردن 2010.
13- د/ كامل السعيد: العقوبات المطبقة على الصغار –ورقة عمل قدمت إلى ملتقي الاتجاهات الحديثة في العقوبات البديلة – مؤتمر الرياض 2011.
14- د/ محمد المنجى: الاختبار القضائي أحد تدابير الدفاع الاجتماعي – منشأة المعا رف بالإسكندرية -الطبعة الأولي 1982.
15- د/ محمد جبريل إبراهيم: الإطار القانوني للتسجيل المعلوماتي أو كارت المعلومات – دراسة تحليلية –دار النهضة العربية 2020.
16- د/ محمد سيف نصر عبد المنعم: بدائل العقوبات السالبة للحرية في التشريعات الجنائية الحديثة –رسالة دكتوراه –كلية الحقوق جامعة القاهرة 2004.
17- د/ محمد عبد الرحمن عبد المحسن: استخدام السوار الإلكتروني كبديل للعقوبة السالبة للحرية في القانون المصري –دراسة مقارنة –بحث منشور في مجلة كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية –العدد الثامن والثلاثين – العدد الثاني.
18- د/ محمود محمد بهجت عبد الرحمن: التكييف الفقهي والقانوني للسوار الإلكتروني كعقوبة مستحدثة – بحث منشور في مجلة كلية الشريعة والقانون بتفهنا الأشراف –دقهلية العدد الثالث والعشرين –سنة 2021.

المراجع الفرنسية:

Desportes Frederic et Electragol Penal 1999 P.131 Leguneec – franic : Droit Penal general : coll Corpus- Droit. Priv ; Economical 8 emme ed. Prairs.2001 ; n 1056.

Conte Philippe et Maistre Du Chambon ; Patrich ; droit penal ; geneal ; coll u Armand colin ; 5eme ed ; Paris ; 2001 ; P 315 et.

Chapter 06

International experiences in the field of using artificial intelligence to protect the cybersecurity of countries

-reading the American, British and Singaporean experience–

Dr. Manel Boukourou, (Algeria) ,

*University of Constantine1

Mentouri Brothers

manel.boukourou@umc.edu.dz

Abstract:

This study addresses the topic of using artificial intelligence techniques to protect countries' cybersecurity, with a focus on the experiences of leading countries in this field by highlighting the importance of artificial intelligence in improving the ability of these countries to confront increasing cyber threats. In this context, we reached several results, including: The most important of which is that the selected international models have achieved significant progress in the use of artificial intelligence in the field of improving cybersecurity, early detection of attacks and analysis of big data. However, these successes are not without legal challenges, such as violations of privacy and data censorship, as well as legal liability that

may arise in the event of hacks or technical errors. As for the proposals, the most important of them is the need to strengthen legal frameworks to keep pace with the progress taking place in the field of smart technology and to enhance international cooperation through the exchange and transfer of expertise and experiences

Keywords : Artificial intelligence - cybersecurity - international experiences - positives - obstacles.

الملخص:

تتناول هذه الدراسة موضوع استخدام تقنيات الذكاء الاصطناعي لحماية الأمن السيبراني للدول، مع التركيز على تجارب رائدة في هذا المجال من خلال تسليط الضوء على أهمية الذكاء الاصطناعي في تحسين قدرة هذه الدول على مواجهة التهديدات السيبرانية المتزايدة، وفي هذا السياق توصلنا الى عدة نتائج ومن أهمها أن النماذج الدولية المختارة حققت تقدمًا كبيرًا في استخدام الذكاء الاصطناعي في مجال تحسين الأمن السيبراني، والكشف المبكر عن الهجمات وتحليل البيانات الضخمة. إلا أن هذه النجاحات لا تخلو من التحديات القانونية، كانتهاك الخصوصية والرقابة على البيانات، فضلاً عن المسؤولية القانونية التي قد تنشأ في حال حدوث اختراقات أو أخطاء تقنية. أما فيما يخص الاقتراحات المتوصل اليها فتتمثل أهمها في ضرورة تعزيز الأطر القانونية لتتماشى مع التطول الحاصل في مجال التكنلوجيا الذكية وتعزيز التعاون الدولي من خلال تبادل ونقل الخبرات والتجارب.

الكلمات المفتاحية: الذكاء الاصطناعي-الأمن السيبراني -التجارب الدولية-الإيجابيات – العوائق.

Introduction

With the increasing reliance on digital technology in various fields, the need to enhance cybersecurity has become an urgent necessity to confront the increasing cyber threats in our current era. This is what has made most countries rely in this field on artificial intelligence, which aims to develop systems and software that mimic the mental capabilities of humans. For its superior ability to learn, adapt, make decisions, and solve problems in various fields such as healthcare, manufacturing, machine translation, civil and military robotics, and cybersecurity protection through a set of measures and procedures aimed at protecting electronic information and data from unauthorized access. or use, modification, or destruction by protecting networks and information systems from electronic attacks and potential threats that may affect the confidentiality, privacy, and integrity of information in the digital space, by relying on privacy protection laws and protecting personal information through smart applications that provide innovative capabilities. To analyze data, detect threats and respond to them more efficiently

Therefore, this research paper aims to study the role of artificial intelligence applications in improving cybersecurity by detecting threats, protecting against malware, and confronting cyberattacks, and this will not happen until we identify the areas in which artificial intelligence technology is used. And revealing the most prominent applications of artificial intelligence used to improve cybersecurity. Relying on pioneering experiences in this field, namely the United States of America, the United Kingdom, and Singapore. In addition

to identifying the obstacles and challenges that may face the application of these technologies, while proposing solutions and suggestions on how to improve the role of artificial intelligence in improving cyber protection systems by exploiting artificial intelligence techniques to monitor systems, detect threats faster and more accurately, keep up with modern threats, and innovate new solutions. In addition to reducing costs and human errors, as well as achieving an effective and rapid response to crises and attacks by applying artificial intelligence to analyze data in a real-time manner... etc. The problem of the study emerges as follows:

How can artificial intelligence technologies enhance the cybersecurity protection of countries, and have leading countries such as the United States of America, the United Kingdom, and Singapore been able to achieve actual success in this field?

To address this problem, we decided to use the descriptive approach and the analytical approach to analyze the various tools and techniques in the field of artificial intelligence and their use in protecting cybersecurity, in addition to the critical approach to identify gaps and obstacles and suggest alternatives and solutions. To study this topic, we divided the study into two axes as follows:

-**The first axis**: The conceptual framework. Cybersecurity and artificial intelligence and its role in confronting cyber threats.

-**The second axis**: Selected models of successful countries in the field of using artificial intelligence techniques to protect cybersecurity.

The first axis: The conceptuel Framework of cyber Security and artificiel intelligence and its rôle in confronting cyber threats.

With the rapid development of technology, cyber threats have become more complex and widespread, which requires the adoption of advanced technologies to detect them. Therefore, artificial intelligence is one of the most important tools that have proven effective in improving cyber threat detection mechanisms. Below we will highlight the role of artificial intelligence in analyzing data, detecting malware, and being proactive in confronting cyber attacks.

First - The conceptual framework of artificial intelligence and cyber Security

Before addressing the role of artificial intelligence techniques in analyzing cyber data, we must systematically review the definition of these smart technologies[1], which are considered a branch of computer science That aims to develop systems and programs capable of carrying out tasks that mimic human intelligence, as it is used in... This field is intelligent technologies that rely on the high computational capabilities of computers and information technology, to create models that interact, learn, and make decisions in a manner similar to humans. Accordingly, artificial intelligence is an essential part of modern technologies, which are widely used such as civil and

[1] Dambe, S., Gochhait, S., & Ray, S.The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) IEEE 2023.pp. 88-93

military robots. Self-driving cars, drones, and robots that manage nuclear reactors and power plants, in addition to big data analysis (Al-Masry, 2024), in addition to e-commerce, medicine, in-person or distance education through educational platforms and programmed digital applications...etc., while in the field of manufacturing, artificial intelligence plays an important rôle in improving production processes and increasing efficiency. With high accuracy and speed. [1]

As for cybersecurity, it is defined as: protection of communications networks, information systems and data, including devices connected to the Internet[2], where its role is represented in the preventive measures and standards that must be followed and complied with to confront cyber threats, and limit violations or unauthorized access to them[3], as it is the activity that ensures the protection of resources. Human and financial resources related to information and communications technologies, and ensures the ability to recover from losses and damages resulting from potential risks and threats, allowing the normal situation to be restored as quickly as possible[4]. On the other hand, cybersecurity aims to achieve several dimensions, namely: the military dimension, in which

[1] - Irshaad Jada, Thembekile O. Mayayise, intelligence on organisational cyber security: An outcome of a systematic literature review, journal Data and Information Management,2024pp1-2

[2] sia-Ching Chang -Suliman Hawamdeh. Cybersecurity for Information Professionals: Concepts and Applications,Auerbach.2020,p120

[3] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access, 8-2020*, p45.

[4] - Ajay Singh.ntroduction to Cybersecurity: Concepts, Principles, Technologies and Practices. Orient Blackswan. 2023.p175

cybersecurity aims to maintain the protection of digital security for the military sector within the country, which allows for smooth communication across military networks, which facilitates the exchange of information and orders, which allows for complete control of the weapons system, such as Drones, guided missiles and satellites. And radars...etc., in addition to the economic dimension, which aims to provide stability to the financial sector, financing operations, and financial transactions from any intrusion into their environment and digital data, in addition to the social dimension, as cybersecurity aims to achieve the social dimension, especially with the expansion of the circle of Internet users, which requires providing an environment A secure digital platform that allows them to access the risk of hacking their information and personal data and prevents illegal uses from third parties.[1]

In addition to That, the political dimension, as cyber Security seeks to protect the confidential documents of politicians, which often leads to diplomatic crises between countries, such as Russia's cyber interference in the American elections, without forgetting the legal dimension, as the development of smart technology requires

[1] - Kaspersky knows cybersecurity Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term "cybersecurity" applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Available ait the link

https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

the enactment of legislation by improving the legal frameworks for dealing with it. With legal and non-online activities,

Second - applications of artificial intelligence used to improve cyber Security and machine learning

to analyze and protect data in the digital environment, as these technologies allow identifying unusual patterns in data movement to detect cyberattacks such as malware and distributed attacks. (DDoS). Through machine learning, huge amounts of data can be analyzed quickly and accurately, which helps predict future threats based on historical data[1]. Techniques such as deep learning are also used to analyze unstructured data such as text or images to identify suspicious patterns. Artificial neural networks contribute to improving Detecting abnormal behavior across networks Network behavior analysis also allows monitoring data traffic to detect attacks that may go unnoticed.

In addition to the above mentioned, smart technology helps detect attacks via email or encrypted conversations. In addition to the above, predictive algorithms contribute to making proactive decisions to improve protection strategies. Accordingly, these technologies work to improve the speed and efficiency of cybersecurity systems, through rapid detection and immediate response. On threats. Hence, the artificial intelligence techniques used to enhance cybersecurity include a wide range of innovative

[1] - Damien Van Puyvelde -Aaron F. Brantly. Cyber Security: Politics, Governance and Conflict in Cyberspace.John Wiley & Sons.2024.p118

tools and methods, the most important of which we will discuss: the most important of which are intrusion detection systems (IDS), which rely on artificial intelligence to analyze data movement and detect suspicious activities. Which may indicate hacking attempts. An example is Darktrace, which uses machine learning to analyze network behavior and detect attacks in real time. In addition to predictive analysis systems, it is used to anticipate future threats based on previous data, such as deep learning techniques that help derive patterns that indicate the possibility of threats occurring. An example of this is the Microsoft Azure Sentinel platform, which relies on predictive analysis to anticipate threats before they occur.[1]

Cybersecurity automation systems (SOAR)[2] also play an important role, as they allow automatic response to security incidents to reduce the time it takes for human intervention. The most prominent of these systems is the Cortex XSOAR system from Palo Alto Networks, which allows for complete automation of security operations. In addition to what was mentioned, it is noted that in the field of malware detection, artificial intelligence helps in identifying malicious software even if it is new or unknown. Cylance tool is an applied example that uses artificial intelligence to detect

[1] - Damien Van Puyvelde ,Aaron F. Brantly .op.cit. p119

[2] SOAR signifie orchestration, automation and response to the security. SOAR will indicate the pressure on the information equipment in integration with automated responses to various events. The SOAR system can be used as a program to adapt to this organization. Please allow the devices to write a comment SOAR can use these objects in the near future, such as at different times, to select the number of personnel information or the actual personnel editor in order to engage in creative projectss Available at the link://www.fortinet.com/fr/resources/cyberglossary/what-is-soar

malicious software before it is implemented. In addition to behavioral analysis techniques, it focuses on studying the behavior of users and devices to detect unusual activities. An example of these technologies is the Exabeam platform, which relies on analyzing user behavior to detect suspicious activities.

Artificial intelligence systems are also used in the field of denial-of-service (DDoS) attacks to analyze data traffic and detect attacks in real time. Cloudflare is an example of this, using artificial intelligence to protect networks from DDoS attacks. Artificial intelligence also relies on intelligent encryption to improve encryption protocols based on potential threats and changing data. This is implemented in AI-powered encryption systems to secure sensitive data. In this regard, many companies use artificial intelligence applications in cybersecurity, such as IBM, which offers the QRadar platform to analyze security data and detect threats in real time, Amazon Web Services (AWS), which provides tools such as GuardDuty to detect and analyze malicious activities, and Google Cloud, which relies on... Artificial intelligence systems to protect networks from DDoS attacks and secure data.

We conclude from all of the above that artificial intelligence represents a qualitative shift in the field of cybersecurity, as it allows for faster and more accurate detection of threats and enhances proactive strategies to deal with them. As cyber-attacks become more sophisticated, it has become necessary to adopt these technologies to protect systems and networks, and organizations must invest in these

innovative solutions to ensure a safe and protected digital environment

Third - The role of artificial intelligence in detecting malware using machine learning.

In light of the increasing and diversifying threats of malware, artificial intelligence has become a vital tool in the field of cybersecurity, especially in detecting malware by relying on modern security systems based on machine learning techniques (Machine Learning)[1] to detect malware more accurately and effectively compared to traditional methods, as these technologies provide the ability to recognize complex patterns in data that may indicate the presence of threats, even if that malware is not previously known through machine learning, which includes training models on data. Contains huge examples of malware and sound methods to make it easier for the system to learn to distinguish between the distinct patterns and characteristics of each type of software,

This allows it to identify suspicious activities that may indicate the presence of malware. In this regard, there are two main types of machine learning used in detecting malware: supervised learning and unsupervised learning. In supervised learning, the system is trained using a data set containing proven examples of valid and fake software, where the model learns the characteristics of this software, such as: Behaviors, code, and patterns that may be evidence of

[1] - Abdelrhman Samy, Ahmed A. El-Sawy, and Fatma Sakr. Recent Studies and A Review about Malware detection and classification by using Artificial Intelligence Techniques. Benha Journal of Applied Science. ol. (8) Issue (5) .2023.p89

threats. Such as using support vector (SVM) algorithms or neural networks to classify programs based on these characteristics. For example, Cylance uses machine learning to detect malware before it is executed via code analysis without the need for a huge database of known virus signatures.[1]

In unsupervised learning, data is analyzed to detect unusual patterns that may indicate a threat. Here the system is able to identify malware that has not yet been detected, based on its abnormal behavior. A real-world example of this is Darktrace, which uses machine learning to analyze network traffic in real-time and detect attacks even if the malware is new or unknown. With its ability to adapt to evolving malware, it can be targeted to bypass traditional detection methods. Behavioral analysis using artificial intelligence, for example, relies on monitoring the activities carried out by malware within a system or network, which allows threats to be detected even if that malware uses stealth techniques such as encryption or anonymization techniques. On the other hand, networks contribute Deep neural technology improves malware detection capabilities by analyzing complex data and differentiating between normal and abnormal behaviors more accurately. Which helps in predicting future threats based on the detected patterns.[2]

---

[1] - hang, Nguyen Manh, "Improving efficiency ofweb application firewall to detect code injection attacks with random forest method and analysisattributes HTTP request" Programming and Computer Software,Springer, 2020.p125

[2] - ande, Yogita and Muddana, Akkalakshmi, "Intrusion detection system us- ing deep learning for software defined networks (SDN)" 2019International Conference on Smart Systems andInventive Technology (ICSSIT),IEEE, 2019.p176

We conclude from the above that artificial intelligence contributes significantly to enhancing the ability to detect malware, not only by checking known software but also by discovering behavioral patterns that indicate the presence of threats that have not yet been discovered by expanding the use of machine learning techniques, so that organizations become more able to Confronting modern and advanced cyber attacks, which enhances the security of networks and digital systems.

Fourth - Monitoring attacks in real time and proactively repairing security vulnerabilities.

Deep learning techniques enable the analysis of data flows on networks in real time, which helps in monitoring threats immediately. These technologies rely on artificial neural networks that analyze network traffic patterns and detect suspicious activities. Deep learning systems can adapt to new attack patterns without the need for constant updating. Artificial intelligence also allows analyzing the context surrounding electronic activities to detect targeted attacks, as these technologies rely on integrating data from multiple sources, such as system logs and email, to form a comprehensive picture of the threat. In addition to the above, artificial intelligence can discover security vulnerabilities in systems and fix them before they are exploited. In Singapore, the cybersecurity agency uses systems such as AI-driven Patch

Management, which updates software and closes vulnerabilities automatically, reducing the likelihood of successful attacks.[1].

AI can also analyze historical data and past patterns to predict future attacks. For example, the United Kingdom's National Cyber Security Center (NCSC) relies on technologies such as Darktrace to analyze abnormal activities on networks and anticipate attacks before they occur. On the other hand, artificial intelligence can contribute to building defense strategies based on continuous analysis of threats. In this context, Microsoft uses Azure Sentinel, which enables organizations to identify potential vulnerabilities and develop defensive plans that reduce the impact of attacks. At the conclusion of this topic, it can be said that artificial intelligence has become an indispensable tool in improving response to cyber-attacks, through automating operations and predicting threats. Successful experiences in countries such as the United States, the United Kingdom, and Singapore highlight the importance of adopting these technologies globally to confront increasing cyber challenges. Organizations must invest in AI to ensure a secure and resilient cyber environment.

[1] -Ömer Aslan 1, Semih Serkant Aktu ˘g 2, Merve Ozkan-Okay 3,* , Abdullah Asim Yilmaz 4 and Erdal Akin. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 2023.p 42

The second axis: Selected models of successful countries in the field of using artificial intelligence techniques to protect cybersecurity.

With the escalation of cyber threats and the spread of advanced attacks, the use of artificial intelligence (AI) techniques in the field of cybersecurity protection has become extremely important. These technologies provide the ability to detect threats early, analyze big data, and take necessary actions faster and more accurately than traditional methods. From this standpoint, many countries around the world have begun to adopt these technologies in their security strategies to protect information systems and networks, which reflects the importance of artificial intelligence in facing the increasing security challenges, which we will discuss below:

First - The leading countries in using artificial intelligence in the field of cybersecurity protection

1- The United States of America:

The United States of America is one of the leading countries in applying artificial intelligence techniques in the field of cybersecurity protection. In this regard, the US government has launched several initiatives to enhance the use of artificial intelligence in protecting government systems and critical infrastructure. An example of this:

1- The US National Security Agency: The US National Security Agency (NSA) is considered one of the most prominent entities that

use artificial intelligence techniques to combat cyber-attacks, as it initially relied on traditional methods to detect threats, but it quickly adopted machine learning techniques. Learning) to enhance its capabilities in detecting the most sophisticated cyber-attacks, which began using it in the middle of the first decade of the new millennium (around 2005-2010), as this period witnessed an increase in the complexity of cyber-attacks, especially targeted attacks on sensitive infrastructure, and by 2015, the NSA had doubled down on its use of machine learning to analyze huge amounts of data collected from around the world[1]

Artificial intelligence-based systems have also been developed for predictive detection of attacks by analyzing patterns and past data, which helps provide proactive strategies to reduce risks. In addition, artificial intelligence has been used in the field of big data analysis to monitor suspicious activities and identify strange patterns in data that may indicate a cyber-attack.[2]

2- The IBM Watson for Cyber Security platform: is one of the most prominent applications that rely on artificial intelligence in the field of cybersecurity, which was launched in 2016 using deep learning and natural language processing techniques, where the

[1] - To protect and promote U.S. security, prosperity, and democratic Artificiel Intelligence technologies are at the center of an unfolding global technology revolution that could affect the well-being and security of people everywhere Available at the link
ways. https://www.state.gov/about/

[2]- Bhardwaj, A., Alshehri, M. D., Kaushik, K., Alyamani, H. J., & Kumar, M. (Retracted) Secure framework against cyber attacks on cyber-physical robotic systems. *Journal of Electronic Imaging, 31*(6), 2022.p76

primary goal of the Watson platform was to analyze security events. Faster and more accurate, as the platform can collect and analyze data from a variety of sources, including technical documents[1], online conversations, and cyber incident reports. By 2017, the platform was able to handle hundreds of thousands of data simultaneously and detect patterns that may indicate to New cyber threats

This platform has also been widely used in government institutions and major companies to analyze advanced threats and discover security vulnerabilities in networks. The role of artificial intelligence has also expanded in predictive detection of threats before they occur and rapid response to security events. Interest in this aspect began in the early second decade of the new millennium, with the increasing use of machine learning in analyzing network logs and historical data with the aim of inferring future patterns of threats. For example, the NSA was one of the first to begin using artificial intelligence to detect future attacks by using predictive algorithms to analyze historical cyber data, allowing it to prepare early for any attack that might occur. In the same context, IBM Watson has used AI technologies for predictive analysis that goes beyond just identifying known threats, but can even detect unfamiliar threats that may arise in the future based on unusual behaviors in the data.[2]

[1]- International Technical Support Organization. Using the IBM Security Framework and IBM Security

Blueprint to Realize Business-Driven Security. April 2013.p9

[2] - opcit.p10

In addition to the future expansion of the use of artificial intelligence in cybersecurity with the increasing complexity of cyberattacks, artificial intelligence techniques have become an indispensable necessity in building strong and flexible security systems. In 2020, the NSA began incorporating deep learning and reinforcement learning techniques into its security strategies, which helped it analyze network behavior more accurately and effectively. The agency has also begun applying new predictive artificial intelligence techniques to address future cyber threats that use advanced stealth techniques such as network manipulation. In 2022, the use of artificial intelligence in all security fields within the United States of America was accelerated by integrating artificial intelligence with cloud security tools and artificial intelligence-based applications, such as the Watson platform, which helped improve the speed of detection and response to advanced threats in private and government institutions. Both. It also appears that the future trend will be towards more automation in cybersecurity systems, where artificial intelligence techniques are used to conduct real-time analysis and detect intrusions or suspicious activities without the need for human intervention.

2 -United Kingdom

The United Kingdom seeks to enhance the use of artificial intelligence within the framework of national cybersecurity strategies. Under the supervision of the British National Security Service (NCSC), to increase efficiency in detecting malware and analyzing suspicious network behaviors. One of the most prominent

initiatives is the "Cyber Aware" program, which integrates artificial intelligence to analyze large-scale cyber data to detect and respond to attacks in real time. AI is also used to monitor cybersecurity in the financial sector, through techniques such as analyzing network behavior and identifying unusual patterns that may indicate potential threats. [1]

3 -Singapore

Singapore is one of the leading countries in adopting artificial intelligence in cybersecurity. In this regard, in 2018, the National Security Technology Authority (CSA) launched the National Cybersecurity Strategy, which places great emphasis on using artificial intelligence to provide advanced solutions in cybersecurity protection. By collaborating with technology companies such as Darktrace, Singapore has used machine learning techniques to detect real-time threats and analyze data traffic on government networks. Artificial intelligence has also helped improve the effectiveness of security systems in the financial and health sectors, as it is used to identify suspicious patterns and provide proactive solutions to combat attacks.[2]

[1] National Cyber Strategy 2022 Pioneering a cyber future with the whole of the UK.p08 Available at the link https://assets.publishing.service.gov.uk/media/620131fdd3bf7f78e469ce00/national-cyber-strategy-amend.pdf

[2]-Singapore.syber. landescape2023 GLOBAL TRENDS IN 2023.p9 https://www.csa.gov.sg/docs/default- Avalable at the Link source/publications/2024/singapore-cyber-landscape- 2023 .pdf

Second - Evaluating the American, British and Singaporean experience in the field of using artificial intelligence to protect cybersecurity.

Artificial intelligence (AI) has become an essential tool in cybersecurity strategies in many leading countries. The United States, the United Kingdom, and Singapore have all adopted artificial intelligence technologies to improve their security systems, confront increasing cyber threats, and enhance the ability to respond to incidents. However, these countries' experiences vary in how they apply and use artificial intelligence, which allows for an analysis of the pros and cons associated with each experience separately

First: The positives of the American experience:

1. The Usa relies on significant investment in research and development in the field of cyber defense and smart technology, as it is considered one of the countries that has invested heavily in artificial intelligence technologies to support cyber security through many agencies such as the National Security Agency (NSA). The Department of Homeland Security (DHS) uses artificial intelligence to analyze big cyber data, enhancing the ability to detect attacks early. An example of this is the use of deep learning techniques to identify unusual threats and analyze advanced patterns.[1]

[1] - 2024 report on thecybersecurityposture of the United States. 2024 report on thecybersecurityposture of the united statesmay 2024office of the national cyber directorexecutive office of the president.p29

2. Proactive prediction: Such as the use of predictive analysis techniques used by the IBM Watson for Cyber Security platform provides the United States with an important advantage in detecting attacks before they occur. Artificial intelligence helps analyze huge amounts of data to identify patterns that may indicate potential threats.

3. Public-private cooperation: The United States cooperates extensively between the government sector and technology companies such as Google, Microsoft, and IBM to develop advanced cybersecurity solutions, which enhances its ability to respond quickly.

Disadvantages:

1. Reliance on big data: Although the use of artificial intelligence depends on analyzing big data, this may lead to a violation of privacy, as large-scale data collection may expose personal and private information to violation.

.2 Challenges in consistent implementation across agencies: Although there are huge investments, coordination between government agencies in the use of AI technologies is not always effective. This can cause duplication of efforts or inefficient investment of resources.

Second: Positives of the British experience:

1. Focus on innovation and continuous modernization: The United Kingdom is adopting innovative strategies to enhance

cybersecurity, such as using the Exabeam platform to analyze user behavior and detect suspicious activities using artificial intelligence. This focus on innovation enhances the UK's capabilities to combat sophisticated attacks.

2. Effective government support: With the establishment of the National Cybersecurity Commission (NCSC), the British government provides strong support for the development and application of artificial intelligence in the cybersecurity sector, through initiatives and resources directed to the private sector and government institutions.

3. Focus on education and training: The United Kingdom encourages the development of skills in artificial intelligence in the field of cybersecurity, which contributes to building a qualified workforce to meet future challenges.[1]

Disadvantages:

1. Challenges associated with implementation within government institutions: Despite the great development in the use of artificial intelligence, the actual application in some British government institutions may face challenges related to compatibility between old systems and modern solutions based on artificial intelligence.

.2 High cost: The UK's investment in artificial intelligence in cybersecurity requires high costs, which may constitute a burden on

[1] Government Cyber Security Strategy. Government Cyber Security Strategy 2022–2030.p74

some small and medium-sized enterprises that do not have sufficient resources to take advantage of these technologies

Third: The positives of the Singaporean experience

1. Rapid and effective implementation: Singapore was one of the first countries to adopt artificial intelligence extensively to enhance cybersecurity. In particular, the National Cybersecurity Authority (CSA) is focusing on developing solutions that use machine learning to detect threats in real time, which has allowed it to achieve a quick and effective response against attacks.

2. Integrated infrastructure: Singapore provides an integrated and unified environment, where AI is integrated into government and private sector cybersecurity across the country. This integrated infrastructure makes it possible to confront cyber threats comprehensively.

3. International cooperation: Singapore seeks to participate and cooperate with other countries and technology companies to enhance cybersecurity at the regional and international levels, which contributes to the exchange of experiences and modern technology.

Disadvantages:

1. Reliance on external solutions: Despite the great development in Singapore, it relies heavily on international companies such as Darktrace to provide smart solutions, which may

cause some challenges in terms of dependence on foreign technologies.

2. Privacy violation: Using artificial intelligence to detect threats may lead to the collection and analysis of large amounts of data, raising privacy concerns among individuals and companies. In a data-intensive country like Singapore, this issue can become even more complex..

Conclusion

At the conclusion of this study, we conclude that artificial intelligence technologies play a vital role in enhancing cybersecurity protection at the country level, as they contribute to early detection of cyber threats, predicting them, and analyzing complex patterns that may be invisible using traditional methods. Which prompted more countries to use artificial intelligence in this field, such as the United States of America, the United Kingdom, and Singapore, as these countries were able to exploit these technologies to enhance their response to attacks and reduce the risks associated with them. And developing more intelligent and efficient systems in the field of threat detection. However, on the other hand, it faces many challenges and various restrictions, as the United States faces a set of challenges such as privacy and government coordination, while the British system faces issues of consistent implementation and high costs. In Singapore, challenges may include reliance on external solutions and privacy concerns. However, the success of these countries is not without, as we said, difficulties, as there remains a discrepancy in the level of application and integration between artificial intelligence technologies and national cybersecurity systems. In addition to data security, legal liability remains weak points that may affect the effectiveness of these solutions. Reliance on modern technologies also raises questions about the ability to adapt to rapidly evolving threats.

Despite these challenges, these countries remain leading models in applying artificial intelligence in the field of cybersecurity

protection, which provides valuable models for other countries in how to use these technologies and smart technologies to confront increasing cyber threats and to ensure the sustainability of these successes, which requires these countries to continue to invest in technology. And developing security laws and procedures that govern the use of artificial intelligence in this field.

Suggestions:

Strengthen the legal, regulatory, institutional, and judicial framework at the international, regional, bilateral, and national levels by developing comprehensive legal, institutional, administrative, and judicial frameworks by strengthening the cyber infrastructure and investing in improving this infrastructure, while ensuring the protection of individuals' rights, privacy, and imposing effective data control.

2. Enhancing international cooperation in the field of exchanging and transferring expertise and technologies related to cybersecurity using artificial intelligence, between the leading countries in this field and the rest of the world, which helps unify global efforts to combat common cyber threats.

3. Encouraging investment in scientific research in the field of smart technology and training human cadres specialized in artificial intelligence and cybersecurity, to ensure the sustainability of the effective use of these technologies in the future.

4. Conduct periodic assessments of artificial intelligence technologies used in cybersecurity, to keep pace with the development of threats and enhance the effectiveness of responding to them.

References

-Abdelrhman Samy, Ahmed A. El-Sawy, and Fatma Sakr. Recent Studies and A Review about Malware detection and classification by using Artificial Intelligence Techniques. Benha Journal of Applied Science. vol. (8) Issue (5) .2023

-Dambe, S., Gochhait, S., & Ray, S. The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In *2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)* 2023

- Irshaad Jada, Thembekile O. Mayayise, intelligence on organisational cyber security: An outcome of a systematic literature review, journal Data and Information Management,2024

sia-Ching Chang -Suliman Hawamdeh. Cybersecurity for Information Professionals: Concepts and Applications,Auerbach.2020

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access*.2020

- Ajay Singh.ntroduction to Cybersecurity: Concepts, Principles, Technologies and Practices.Orient Blackswan.2023

- Damien Van Puyvelde -Aaron F. Brantly. Cybersecurity: Politics, Governance and Conflict in Cyberspace.John Wiley & Sons.2024

- hang, Nguyen Manh, “Improving efficiency ofweb application firewall to detect code injection attacks with random forest method and analysisattributes HTTP request” Programming and Computer Software,Springer, 2020

- ande, Yogita and Muddana, Akkalakshmi,“Intrusion detection system us- ing deep learning for software defined networks (SDN)” 2019International Conference on Smart Systems andInventive Technology (ICSSIT),IEEE, 2019

-Ömer Aslan 1, Semih Serkant Aktu ˘g 2, Merve Ozkan-Okay 3,* , Abdullah Asim Yilmaz 4 and Erdal Akin. A Comprehensive Review of Cyber Security Vulnerabilities,Threats, Attacks, and Solutions. Electronics 2023.p 42

- To protect and promote U.S. security, prosperity, and democratic MArtificial Intelligence technologies are at

- Bhardwaj, A., Alshehri, M. D., Kaushik, K., Alyamani, H. J., & Kumar, M. (Retracted) Secure framework against cyber attacks on cyber-physical robotic systems. *Journal of Electronic Imaging, 31*(6), 2022.

- International Technical Support Organization. Using the IBM Security Framework and IBM Security

Blueprint to Realize Business-Driven Security. April 2013.

- Singapore.syber.landescape2023 GLOBAL TRENDS IN2023.p9https://www.csa.gov.sg/docs/default- Available at the linksource/publications/2024/singapore-cyber-landscape-2023.pdf

- 2024 REPORT ON THECYBERSECURITYPOSTURE OF THE UNITED STATES. 2024 REPORT ON THECYBERSECURITYPOSTURE OFTHE UNITED STATESMAY 2024OFFICE OF THE NATIONAL CYBER DIRECTOREXECUTIVE OFFICE OF THE PRESIDEN Government Cyber Security Strategy. Government Cyber Security Strategy 2022–2030

Chapter 07: Conflict between Artificial Intelligence and the Right to be Forgotten

الدكتورة بلمرداسي رفيقة

أستاذة محاضرة أ

كلية الحقوق والعلوم السياسية عنابة-الجزائر

rafikabelmerdaci@gmail.com

Abstract:

The conflict between adopting the right to be forgotten to protect individual privacy and the use of artificial intelligence (AI), which inherently cannot forget, is a complex issue. This conflict emerges from the difficulty of balancing the right to be forgotten with defining its scope in light of the unique characteristics of AI technology. It raises important questions about the impact of AI on this right, particularly given that regulatory frameworks for both areas are still developing. Therefore, there is an urgent need to bridge the substantial gap between legal regulations and technological advancements, especially concerning the protection of personal privacy.

Keywords: Right to be Forgotten; Artificial Intelligence ; Freedom of Expression ; GDPR.

Introduction:

On May 13, 2014, in the well-known case known as Google Spain, the European Court of Justice ruled in favor of the plaintiff, Mario Costeja Gonzalez, recognizing his right to delete information and data related to him, thus explicitly establishing the right to be forgotten. However, AI's handling of information and its deletion processes are different, which could manifest in future stark conflicts between the right to be forgotten and the characteristics of AI.

Establishing the right to be forgotten legally is linked to the evolution of privacy protection. However, the significant technological advancement and the integration of AI with its various features into numerous platforms and websites, especially given AI's reliance on vast databases and its inherent inability to forget due to its specialized memory handling, have increasingly posed challenges to implementing the right to be forgotten in the digital environment.

Based on the above, we can pose the following issue:

How can the legal conflict between the right to be forgotten and AI technologies be reconciled?

To address this issue, it is necessary to primarily use descriptive and analytical methodologies, with the possibility of employing historical and comparative methods as needed for research purposes.

Consequently, the research will be divided into two main sections: the first section will discuss the definition of the right to be forgotten. In contrast, the second section will be dedicated to the impact of AI on the right to be forgotten.

First Requirement: The definition of the Right to be Forgotten

The novelty and complexity of the right to be forgotten, along with its connection to technological advancements on one hand and various other rights on the other, have led to significant doctrinal debate. This debate has resulted in two main doctrinal approaches: one that provides a restrictive definition and another that offers an expansive definition.

The determination of the nature of the right to be forgotten can only be achieved through understanding both the restrictive definition of the right to be forgotten (First section) and the expansive definition of the right to be forgotten (Second section).

First section: The Restrictive Definition of the Right to be Forgotten

The concept of the right to be forgotten first appeared in legal doctrine in a memorandum related to the "Landru" case in 1956. Professor Gérard Lyon-Caen proposed the idea of "La prescription du Silence" (the prescription of silence). [1]

[1] The right to be forgotten is closely related to the right to privacy. The question arises as to whether the right to privacy encompasses an individual's right to be forgotten, or if the right to

as a legal basis for a claim filed by one of Landru's former lovers, who sought compensation for the harm caused by the release of a film by Claude Chabrol about the case. However, the court rejected the claim because the claimant herself had published her memoirs.[1]

The debate over defining the right to be forgotten precisely began with this issue. In the context of the digital space, the right to be forgotten refers to an individual's right to ensure that those responsible for processing their data do not retain it for a period beyond the original purpose for which it was collected. This

be forgotten is considered a distinct and separate right from privacy. Some legal scholars argue that a person has the right to have certain aspects of their life fade into oblivion, and once such information has been hidden under the veil of forgetfulness, it should not be revealed without their consent. According to this view, such information becomes obsolete after a certain period of silence, and once this period has elapsed, it is not permissible to disclose it, as this would effectively attempt to disrupt the completed statute of limitations. Such disclosure is seen as an infringement on the individual's rights.However, the prevailing view in legal scholarship is that it is unreasonable to suggest that the right to privacy does not include the right to be forgotten. The concept of privacy should cover the individual's entire personal life, including both present and past aspects. Information privacy, in this context, means protecting personal data of individuals who use the internet. Therefore, privacy revolves around the protection of personal information and aspects of an individual's life that should remain private unless the individual chooses otherwise.See :Ben Barghouth, Laila. "Information Privacy on Social Media in the Age of Virtual Overload: The Inevitable Shift Toward the Virtual Maze." Journal of Media and Society, Vol. 5, No. 2, December 2021, p. 160. Available at website : asjp.cerist.dz,browsed at : 26/08/2024, at 21:39.

[1] Maha Ramadan Mohamed Batyekh, "The Legal Framework of the Right to be Forgotten on the Internet," Journal of Legal Studies, No. 61, June 2023, p. 216. Available at: maal.journals.ekb.eg. Accessed on August 7, 2024, at 20:59.

definition is derived from Article 6 of the French Data Protection Act of January 6, 1978.[1]

The digital right to be forgotten protects individuals from the abuse of retaining and disseminating their digital data and is closely related to the right to privacy. Despite the significant role that the digital right to be forgotten is expected to play in protecting personal data that has been previously processed electronically, and thus in supporting and safeguarding individuals' right to privacy, Law No. 18-07, dated June 10, 2018, which relates to the protection of individuals in the field of personal data processing[2] does not explicitly address this issue, raising questions about its legal status.[3]

The decision issued by the European Court of Justice on May 13, 2014, in the case of Google Spain SL and Google Inc. vs. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, is considered one of the landmark rulings that established the parameters for exercising this right. The ruling recognized that internet users have the right to request search engines to remove or limit search results or web links that direct to web pages containing

[1] Boukhlaout El Zine, "The Digital Right to be Forgotten," Al-Mufakkir Journal, Vol. 12, No. 1, 2017, p. 550.

[2]Law No. 18-07, dated June 10, 2018 related to the protection of individuals in the field of personal data processing The Official journal No. 34, issued in 2018.

[3] Sidrati Waseela, "The Digital Right to be Forgotten in French and Algerian Law: Extent of Recognition and Implementation," Al-Nibras Journal of Legal Studies, Vol. 7, No. 1, 2023, p. 41.

personal data[1] when searching using their names. This obligation remains with the search engine even if the content is legally published.[2]

In the **Google Spain** case, Mr. González requested the removal or alteration of search results related to a real estate auction that had been published in a daily newspaper by *La Vanguardia* company. He argued that the information was outdated and no longer relevant to the public or to him personally. He asked *La Vanguardia* to delete or modify the publication and Google to remove or hide the data.[3]

The restrictive doctrinal perspective defines the digital right[4] to be forgotten as the right that provides individuals with legal means

[1] **Dawen, Zhang.** "Right to Be Forgotten in the Era of Large Language Models." Page 2. Available on website efi.edn.bnnebpc.agpcg.ncel.e. Accessed on September 2, 2024, at 18:48.
As a result of the EU data protection reform, several rights were included under Chapter 3, "The Rights of the Data Subject," in the General Data Protection Regulation (GDPR) of the European Union.

[2] arrêt de la Cour grandes chambres c 136/17 , 24 septembre 2019 , Sidrati Waseela, *op. cit.*, p. 43.

[3] Chang Chi Chang, "When AI Remembers Too Much," Washington Journal of Law, Technology & Arts, Volume 19, Issue 3, 2024, p. 24. Available on website papers.ssrn.com. Accessed on 02/09/2024 at 20:23.

[4] A good collection of sub-rights was incorporated from Articles 12 to 23 into the law, notably:

- The Right to Be Informed (Article 13)
- The Right of Access (Article 15)
- The Right to Rectification (Article 16)
- The Right to Erasure (Article 17)

to secure their right to be forgotten on the internet. This is achieved by limiting the retention of personal digital data and enabling its deletion.[1]

Another perspective defines the right to be forgotten as the obligation of those responsible for processing individuals' personal data to manage it and ensure that individuals have the right to request its deletion once the purpose for which it was collected has ended, in order to protect users from the implications of their past. This definition aligns with what was stipulated by the French National Commission on Information Technology and Freedoms (CNIL) in Article 4, Paragraph 4 of Law 78-17[2], updated on June 17, 2019, stated that, if necessary, all measures should be taken to ensure the removal or correction of inaccurate personal data as soon as possible.[3]

The right to be forgotten is widely considered a significant evolution in privacy rights in the digital age, addressing the unique challenges posed by the internet and digital technologies. The right to be forgotten is a critical aspect of the fundamental human right to privacy. It has established itself as a legal principle through the case law of the Court of Justice of the European Union. Moreover, the right to be forgotten is not an absolute right; it is subject to explicitly defined grounds for the erasure of personal data.

See : Dawen, Zhang,opcit,p4

[1]Bouzidi Ahmed Tijani, "The Right to Enter the Digital Oblivion: A Mechanism to Protect the Right to Privacy," Journal of Legal Voice, Vol. 6, No. 2, 2019, p. 1246.

[2]Law No. 78-17 dated January 6, 1978, concerning the electronic processing of data, information, and cards, and freedoms, published in the French Official Journal No. 1 dated January 7, 1978.

[3]Zidi Ahmed Tijani, op. cit., p. 1246.

Several criticisms have been directed at this restrictive definition of the right to be forgotten. These include its failure to specify the content of the right to digital oblivion via the internet, the lack of a defined time frame after which the right to oblivion can be requested, and its inadequacy in the infinite environment of the internet where this right operates. These issues have led to the emergence of an alternative perspective that broadens the scope of this right.[1]

Second section: The Expansive Definition of the Right to be Forgotten

Although proponents of this approach agree on the necessity of expanding the definition of the digital right to be forgotten, they differ on the extent of this expansion. Professor A. Aramazani defines it as the right of an individual to control and manage any personal information about them. On the other hand, legal scholar Jean-Christophe argues that the digital right to be forgotten grants natural or legal persons the power to delete information about them or request its cessation of publication after a certain period.[2]

[1]Boukhlaout El Zine, op. cit., p. 551.

[2]Ben Sheikh Mohamed Hussein, Ben Diddeh Najah, "The Right to be Forgotten: A Mechanism for Protecting Personal Data," Algerian and Comparative Public Law Journal, Volume 8, Issue 1, 2022, p 569.

The expansive definitions of the digital right to be forgotten align with the structural and technical nature of the internet[1]. Once personal information is published online, internet users lose control over it as it spreads from one site to another and from one person to another. Furthermore, outdated information, which may originally have been incorrect, can remain published by others..[2]

The terms "right to be forgotten" and "right to electronic erasure" are among the most commonly used in various legal texts. This right aims to empower individuals to make decisions regarding the processing or retention of their information on electronic networks, which could otherwise lead to personal harm.[3]

---

[1]In 1914, the United States first brought legal attention to the issue of being forgotten from the public eye, particularly concerning the publication of personal information without consent. This early focus laid the groundwork for developing privacy laws aimed at protecting individuals' rights to control their personal data and maintain their anonymity. See: Meem Arafat Manab, "Eternal Sunshine of the Mechanical Mind," ARi XV, 2024, page 3. Available on the website arxiv.org, accessed on 02/09/2024.

[2] The same reference, same page.

[3]Personal data is defined as any information, regardless of its medium, related to an identified or identifiable person, referred to below as the data subject, either directly or indirectly, particularly by reference to an identification number or to one or several specific elements of their physical, physiological, mental, economic, cultural, or social identity. The term 'right to be forgotten' has raised some issues due to the use of similar terms in comparative jurisprudence and law. To resolve issues with terminology, legal scholars often oppose using the term 'right to be forgotten' and prefer the term 'right to oblivion.' Similarly, the term 'historical erasure' has been replaced with 'right to electronic data erasure.'

The French National Commission on Information Technology and Freedoms (CNIL) has adopted an expansive definition of the right to be forgotten. The European Commission, in its communication to the European Parliament, defines the right to be forgotten as the right of data subjects to prevent their data from being processed and to have it fully erased when it no longer serves its legitimate purposes. The European Commission also acknowledges that every individual has the right to correct or erase their personal data when it is no longer necessary for the legitimate purposes for which it was collected, when individuals withdraw their consent for its retention, or when they object to its retention..[1]

Based on the above, we can define the right to be forgotten as the right of data subjects to control what they deem appropriate, whether by modifying or permanently erasing their data from digital memory.

The topic of the right to be forgotten is closely linked to the relationship between memory and personal identity. The Google ruling marked a turning point in protecting this right, not only because it enforced the right itself but also because it imposed specific obligations on internet operators within the European Union and, by extension, influenced practices in other regions, including the

[1]Mahmoud Zaki Zaki Zidan, op. cit , p 392.

United States. Since May 2018, Law No. 679/16 (General Data Protection Regulation, GDPR) has been applied in such cases and is considered the main reference for this right..[1]

The European Court of Justice's decision on May 13, 2014, in Case C-131/12, which involved Google against the Spanish Data Protection Agency, affirmed that individuals can request the removal of links to outdated and irrelevant information that appears when searching their names. The effective and actual recognition of the right to be forgotten began at the judicial level with this ruling, which was in favor of the plaintiff, a Spanish citizen named Mario Costeja González, granting him the right to remove information and data related to him. This included a global auction announcement resulting from the seizure of his assets due to accumulated social security debts.[2]

In 2012, the concept of the right to be forgotten was formally established in the European legal framework as a legal norm, initially applying only to minors[3] under Article 17 of the GDPR. However,

[1] Andres Guadamuz,developing a right to be forgotten, EU internet law, November 2017, available on website researchgate.net,browsed on:07/08/2024 at 19:14.

[2] infoCuria.europa.eu, browsed on:07/08/2024 at 19:30.

[3] Article 17 of GDPR.

after the official adoption of the GDPR in 2018, the right to be forgotten became applicable to all natural persons, not just minors.[1]

Regarding the definition issued by the European Commission, it is limited to personal data, which implies that it applies solely to natural persons. Similarly, the European Court of Justice, in its ruling on May 13, 2014, defined the right to be forgotten as an obligation for search engines to remove from search results or links that include information about an individual published by third parties.[2]

The right to be forgotten generally manifests in two forms: the first is the right to de-indexing (droit de déréférencement), which involves removing indexed data from search engine results, and the second is the right to erasure (droit à l'effacement), which involves the complete removal of personal data.[3]

---

[1]Anna Popwicz-Pazdej, Why Generated AI Models Do Not Like the Right to Be Forgotten," *Adam University Law Review*, Volume 15, 2023, p. 218. Available on website ppuam.amu.com. Accessed on 26/08/2024 at 21:24.

[2] The right to be forgotten was first recognized in India through a ruling by the Supreme Court in the case of Sri Vasunathan in 2017.

[3] According to Article 17 of the EU General Data Protection Regulation (GDPR), the term "personal data" refers to any information related to an individual, This may raise issues related to collective information, such as data concerning an entire family rather than an individual alone.

The right to be forgotten has not been officially recognized in Australia. While it has been adopted by European Union countries following the judicial recognition in the Google Spain case, as well as in Argentina and the United States, several reservations about its implementation continue to pose obstacles.[1]

Second Requirement: The Impact of Artificial Intelligence on the Right to be Forgotten

Artificial intelligence has a significant impact on the right to be forgotten in terms of its concept and scope, which necessitates a thorough study a technical Overview of AI's Handling of Data Erasure(First section),and also adapting Legal Texts to the Development of Artificial Intelligence(Second Section).

First section: A Technical Overview of AI's Handling of Data Erasure

Artificial intelligence (AI) has evolved rapidly, necessitating that legislators keep pace with this advancing technology. Unfortunately, current laws do not adequately address the complexities and challenges posed by AI. One of the areas where legislation remains insufficient is privacy protection. AI has

[1] Alexander Lalor. "In Support of Incorporating the Right to Be Forgotten in Australia." Available at Human Rights.unsw.edu.au. Accessed on 27/08/2024 at 12:12.

fundamentally altered our understanding of privacy, which has traditionally focused on how individuals process information, specifically how they remember and forget. This gap in understanding has become particularly apparent with the adoption of the right to be forgotten, highlighting privacy rights as reflected in laws such as the European Union's Regulation 679/2016 concerning data protection from search engines and the internet.

At first glance, this issue might seem straightforward, but it presents several practical and technical challenges in today's digital environment. The concept of data deletion, as embodied in the right to be forgotten and AI, is complex. This section will explore the issues related to AI memory to understand why current privacy laws fail to address the realities of AI technology. Additionally, it will address the central question of how privacy laws should be drafted in the age of AI.

The most complicated issue with guaranteeing the right to be forgotten is related to the ability to delete or erase personal data from AI models. Generative AI models learn from data, including personal

data uploaded as input, which makes it challenging and difficult to remove such data.[1]

Some scholars argue that the primary issue concerning the right to be forgotten relates to freedom of expression. If this right is not clearly defined, the gap between privacy and freedom of expression, especially between Europe and the United States, may widen, potentially leading to internet jurisdiction issues. Consequently, the European Commission has asserted that, in theory, the right to be forgotten aims to protect individuals' privacy rather than erase past events or restrict press freedom.

The expansion of the reasons for infringement opens the door to potential abuses arising from the use of AI in privacy-related matters, particularly in tracking individuals' movements and health conditions through the collection and processing of personal data, which is a crucial aspect of privacy. In this context, General Comment No. 16 of the International Human Rights Committee emphasizes the role of personal data in privacy, granting individuals the right to verify information about them, the purposes for its retention, and the entities that hold it.

[1] Anna Popwicz-Pazdej,opcit, p 219.

The right to be forgotten is fundamental to digital privacy, allowing individuals to erase personal information available on the internet. However, AI poses significant challenges to the effective erasure of individual data.

Unlike the traditional internet, where manual erasure was feasible, artificial intelligence (AI) technology has made such erasure nearly impossible. This difficulty is highlighted by transparency issues in AI models such as OpenAI's GPT-3. In an era of widespread interlinking, personal information is easily tracked and disseminated. Technologies like advanced software create persistent profiles that outlast individual account deletions. Given these considerations, the right to be forgotten needs to be reassessed through a deeper understanding of AI memory, developing advanced databases supported by modern technologies, and creating a legal framework that keeps pace with technological advancements. This right is crucial not only for protecting individuals' privacy but also for ensuring the reliability of AI's predictive capabilities and enhancing trust in our digital systems.

Furthermore, transparency is a significant issue. Most individuals cannot access or understand algorithms, making it difficult to control them without infringing on the privacy of those who lack sufficient knowledge. Additionally, many algorithms are dynamic and constantly evolving, requiring up-to-date knowledge

that is challenging for individuals to maintain. These complexities introduced by AI impose restrictions on privacy rights through algorithms. The right to be forgotten cannot be simply transferred to the realm of AI, as it does not forget in the same way humans do; it is more complex and presents several issues. For example, knowledge-based systems, such as those using Database Management Systems (DBMS), raise fundamental questions about the impact of data erasure on the quality of results and whether data is truly erased. This is particularly concerning with algorithms that use knowledge bases as references, prompting further questions about the methodology of data erasure to ensure that data is effectively removed.

Second Section: Adapting Legal Texts to the Development of Artificial Intelligence

To fully understand all aspects of the subject, it is necessary to study the Scope of the Right to be Forgotten and AI (Subsection One), Balancing the Right to be Forgotten with Other Rights (Subsection Tow), Bridging the gap between legal texts and technological development in Algeria (Subsection Three).

Subsection One: the Scope of the Right to be Forgotten and AI

This involves specifying the conditions under which individuals can request the deletion or removal of their personal data from the Internet or electronic databases. This includes identifying the types of data that can be erased, the circumstances under which individuals can exercise this right and the exceptions that apply, such as cases where information is of public importance or needs to be retained for legal or historical reasons.

1. Personal Data: The right to be forgotten typically covers data that directly or indirectly identifies an individual, such as names, addresses, phone numbers, or any other information related to a person's private life.

Legal scholars have not yet reached a comprehensive and universally accepted definition of the right to privacy due to its difficulty encompassing all its varied aspects. However, efforts have been made to define it. For instance, Dr. Ahmed Fathi Surour establishes the right to privacy as encompassing personal secrets, emotional life, aspects distinguishing personal life such as marital and family life, home privacy, personal data, photos, private correspondence, professional life, health, political opinions, religious beliefs, and more.

Information privacy refers to the right of individuals, groups, or organizations to control when, how, and to what extent their

personal information is shared with others. It also involves the right to regulate the collection, automated processing, storage, distribution, and use of personal information.[1]

2.Data No Longer Necessary: The right to be forgotten typically encompasses data that is no longer relevant to the purpose for which it was collected. For example, if data was collected for a specific transaction and that transaction has ended, an individual may request the deletion of that data.

3.Outdated Data: If data is outdated or no longer reflects the truth, individuals may have the right to request its removal.

Subsection Tow: Balancing the Right to be Forgotten with Other Rights

This involves balancing individuals' rights to erase or remove their data from the internet and databases with other important rights, such as the public's right to access information and freedom of expression. This balance has several aspects:

1. Freedom of Expression and the Right to Access Information: The application of the right to be forgotten may restrict the ability to publish or make information available to the public, which could

[1] Nassreddine Mabrouk. "The Right to Privacy." , Al-Sirat Journal, Vol. 5, No. 1, 2023, p. 595. Available at :ASJP.CERIST.DZ , Accessed on 26/08/2024 at 21:24.

negatively impact press freedom and freedom of expression. The right to be forgotten may conflict with freedom of expression, especially when the information to be removed relates to a public figure or significant historical events. In such cases, it is essential to consider the implications for public knowledge and historical record. Laws must balance the individual's right to privacy with the public's right to access information.

2. Scope of Digital Erasure: The scope of exercising the right to digital erasure is related to digital memories, which include all information pertaining to a person's activities while using any information system or electronic means, regardless of its type, that contributes to defining their digital identity. Examples include blogs, social media platforms, e-commerce sites, and search engines.

Legal opinions vary on the extent of the right to be forgotten. Some argue that this right to request the removal of online content related to an individual is limited to cases where the content is inaccurate, incomplete, excessive, or irrelevant. Others believe that it is an absolute right, to allow individuals to request the deletion of any information related to them on the internet without distinction. However, some caution that this right could allow governments to request the removal of electronic content related to corruption cases,

such as news and documents concerning those cases[1]. In this context, Article 17 of the General Data Protection Regulation (GDPR) stipulates that the right to be forgotten cannot be exercised if it concerns the exercise of freedom of expression, compliance with a legal obligation, public interest, scientific or historical research, statistical purposes, or the exercise of a legal defense right.[2]

Since the "Google Spain" ruling, Google has received over 1.1 million removal requests, with 82% of these from the private sector. Requestors seek to protect themselves from unwanted public exposure based on information related to personal and professional matters.[3]

3.public interest:

In some instances, it may be necessary to retain certain information for public interest reasons, such as information related to crimes or corruption. Clear exceptions to the right to be forgotten

[1] Ameen Al-Khantouri. "Features of Regulating the Right to Digital Erasure." Sada Journal of Legal and Political Studies, No. 5, 2020, p. 36. Available at :ASJP.CERIST.DZ , Accessed on 27/08/2024 at 17:21.

[2] Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, 1950 (ECHR).
USA: Consumer Privacy Bill of Rights Act, Do Not Track Online Act, 2013.

[3] UTA Kohl. "The Right to Be Forgotten: A Protection Law and True Western Cultures of Privacy." Cambridge University Press, UK, 2023, p. 743. Available at cambridge.com. Accessed on 26/08/2024 at 18:55.

should be established to ensure transparency and accountability. However, the exposure of an individual's name and image in public can lead to potential humiliation[1] and should be managed carefully by the individual. Just because personal information has entered the public domain for a specific purpose does not mean it can be used by others indefinitely. The General Data Protection Regulation (GDPR) aims to balance the right to privacy with public interests, including areas such as public health, national security, and law enforcement.[2]

Subsection Three: Bridging the gap between legal texts and technological development in Algeria

In terms of the Algerian legislator, who was slow to catch up with legislation concerning personal data, they had to wait until 2018 to enact a specific law on this subject. This delay was somewhat mitigated by the new constitutional principles introduced by the amendment to the 1996 Constitution through Law 16-01 issued on March 6, 2016. The first paragraph of Article 46 emphasized the importance of protecting private life and the confidentiality of correspondence. At the same time, it gave special importance to

[1] Gallia, Manuel. "The Right to Be Forgotten: A Balance Between Privacy and Public Rights." LLD, Texas University of Martha, 2015, p. 20. Available at: researchgate.com. Accessed on August 31, 2024.

[2] Same reference, p 749.

personal data by recognizing the protection of natural persons in data processing as a fundamental right that the law must uphold and penalize any violations.

To reinforce this principle, the Algerian legislator issued Law 18-07 on June 10, 2018, concerning the protection of natural persons in data processing. Although this law does not explicitly mention the right to "digital forgetting," it includes other rights that support this principle, as will be discussed later.

The Algerian legislator was not isolated from developments in other legislations and thus did not overlook defining both the data controller and the data processor. According to Article 3 of Law 18-07, the data controller is defined as "any natural or legal person, whether public or private, or any other entity that, alone or in conjunction with others, determines the purposes and means of processing."

Considering the overall legal texts regulating privacy protection in Algerian legislation, it is evident that the Algerian legislator has not explicitly addressed the right to be forgotten. Although an analysis of the legal texts suggests a tendency similar to that of the European Union in regulating this issue, the Algerian framework remains significantly behind global advancements. This

highlights a considerable legal gap between the right to be forgotten and developments in artificial intelligence.

Thus, it can be concluded that substantial efforts are needed to both legally enshrine the right to be forgotten in a clear manner and to draft legal provisions that comprehensively regulate this right. Additionally, there is a need to ensure a balance between this right and the challenges posed by artificial intelligence, which has become indispensable in every country worldwide.

The design of legal amendments for personal data regulation should involve creating clear rules on how data is collected and used by artificial intelligence (AI). These rules must ensure transparency and align with effective data removal techniques from AI systems. This necessitates integrating data protection principles into AI design through encryption and secure storage techniques. Achieving this requires collaboration among developers, legal and regulatory bodies, and effective monitoring mechanisms. It also involves updating legal texts based on technological advancements. Integrating privacy principles into AI technology needs multidisciplinary efforts from academics, engineers, cyber security organizations, and tech executives. In Algeria, several key institutions support this, including the National Agency for the Promotion of Information and Communication Technologies in Education, the National Center for Research and Development of Information and Communication

Technologies (CNRST)[1], the National Authority for Personal Data Protection (CNIL)[2], and the National Institute for Research in Information Technology(NIRIT) .Here is the revised text with corrections and improvements

These institutions must focus on bridging the gap between legal texts and technological development through national conferences and interdisciplinary meetings. The Algerian legal system, supported by a set of legal texts, can serve as a foundational basis for establishing the right to be forgotten within the Algerian legal framework, similar to other countries. This is crucial for protecting individuals' rights and privacy, while allowing the benefits

[1] Law No. 09-04 dated August 5, 2009. (2009). Law on the Protection of Personal Information in Information Technology. Official Journal, Issue No. 55, August 5, 2009. Algeria. Ordinance No. 15-02 dated January 23, 2015"Concerning the protection of personal data and including individuals' Official Journal, No. 6, dated January 23, 2015.

[2]Ordinance No. 06-03 dated July 15, 2006

"Concerning the establishment of the National Agency for the Promotion of Information and Communication Technologies in Education" Official journal No. 46, published on July 15, 2006. Ordinance No. 01-01 dated May 15, 2001"Concerning the establishment of the National Center for Research and Development of Information and Communication Technologies "Official journal of Algeria, No. 30, published on May 15, 2001.

Ordinance No. 15-02 dated January 23, 2015"Concerning the protection of personal data", Official journal of Algeria, No. 6, published on January 23, 2015.

Ordinance No. 93-08 dated January 25, 1993, "Concerning the establishment of the National Agency for S Ordinance No. 02-05 dated February 4, 2002,"Concerning the establishment of the National Institute for Information Technology Research" Official Gazette of Algeria, No. 8, published on February 4, 2002. Scientific Research and Technology" Official journal of Algeria, No. 6, published on January 25, 1993.

of artificial intelligence to be utilized without infringing on personal privacy. Given the significant advantages and potential improvements AI brings to various fields, completely abandoning AI technologies is not a feasible option. Therefore, the only viable solution is to strive for a balance between legally enshrining the right to be forgotten and the indispensable benefits of artificial intelligence.

Conclusion:

The increasing use of artificial intelligence (AI) technologies poses a real challenge to the legal implementation of the right to be forgotten. Protecting data privacy has become more complex and requires a coordinated effort between technological and legal fields to address the gap between current laws governing the right to be forgotten and advancements in AI technology.

Based on the above, the key findings are:

1. **Technological and Legal Challenges:** With the growing use of AI technology, there are technological and legal challenges as information may be present in various systems, making it difficult to track.
2. **Need for Modern Legislation:** There is an urgent need for updated legislation to keep pace with technological developments to close the gap between the law and reality.
3. **Balancing Act:** The main challenge is finding a balance between maintaining the effectiveness of AI and protecting the right to be forgotten, which requires both advanced technologies and updated laws.

Recommendations:

1. **Develop Advanced Deletion Techniques:** AI technologies should be developed to enable the automatic removal or concealment of personal data after a certain period.
2. **Establish Data Retention Policies:** Policies should define a specific period during which personal data is retained, after which it should be automatically deleted or concealed.
3. **Integrate Privacy Principles:** Developers should incorporate privacy principles into AI systems, ensuring that the protection of personal data is a fundamental aspect of these systems.

Bibliography List:

1-References:

- Maha Ramadan Mohamed Batyekh, "The Legal Framework of the Right to be Forgotten on the Internet," Journal of Legal Studies, No. 61, June 2023. Available at: maal.journals.ekb.eg. Accessed on August 7, 2024.

- Boukhlaout El Zine, "The Digital Right to be Forgotten," Al-Mufakkir Journal, Vol. 12, No. 1, 2017.

-Sidrati Waseela, "The Digital Right to be Forgotten in French and Algerian Law: Extent of Recognition and Implementation," Al-Nibras Journal of Legal Studies, Vol. 7, No. 1, 2023.

- "Arrêt de la Cour Grandes Chambres C-136/17," September 24, 2019

-Bouzidi Ahmed Tijani, "The Right to Enter the Digital Oblivion: A Mechanism to Protect the Right to Privacy," Journal of Legal Voice, Vol. 6, No. 2, 2019.

- Ben Sheikh Mohamed Hussein, Ben Diddeh Najah, "The Right to be Forgotten: A Mechanism for Protecting Personal Data," Algerian and Comparative Public Law Journal, Volume 8, Issue 1, 2022.

- Andres Guadamuz, "Developing a Right to be Forgotten: EU Internet Law," November 2017, available at researchgate.net, accessed on August 7, 2024.

- infoCuria.europa.eu, accessed on August 7, 2024.

- Ben Barghouth, Laila. "Information Privacy on Social Media in the Age of Virtual Overload: The Inevitable Shift Toward the Virtual Maze." Journal of Media and Society, Vol. 5, No. 2, December 2021, p. 160. Available at asjp.cerist.dz, accessed on August 26, 2024.

- Chang Chi Chang, "When AI Remembers Too Much," Washington Journal of Law, Technology & Arts, Volume 19, Issue 3, 2024 , Available on website papers.ssrn.com. Accessed on 02/09/2024 at 20:23.

- Nassreddine Mabrouk, "The Right to Privacy," Al-Sirat Journal, Vol. 5, No. 1, 2023, p. 595. Available at asjp.cerist.dz, accessed on August 26, 2024.

- Ameen Al-Khantouri, "Features of Regulating the Right to Digital Erasure," Sada Journal of Legal and Political Studies, No. 5, 2020, p. 36. Available at asjp.cerist.dz, accessed on August 27, 2024.

- UTA Kohl, "The Right to Be Forgotten: A Protection Law and True Western Cultures of Privacy," Cambridge University Press, UK, 2023, p. 743. Available at cambridge.com, accessed on August 26, 2024.

- Gallia, Manuel. "The Right to Be Forgotten: A Balance Between Privacy and Public Rights." LLD, Texas University of Martha, 2015. Available at: researchgate.com. Accessed on August 31, 2024.

- Dawen, Zhang. "Right to Be Forgotten in the Era of Large Language Models." Page 2. Available on website: efi.edn.bnnebpc.agpcg.ncel.e. Accessed on September 2, 2024, at 18:48.

- Anna Popwicz-Pazdej, Why Generated AI Models Do Not Like the Right to Be Forgotten," Adam University Law Review, Volume 15, 2023, p. 218. Available on website ppuam.amu.com. Accessed on 26/08/2024 at 21:24.

- Meem Arafat Manab, "Eternal Sunshine of the Mechanical Mind," ARiXV, 2024, page 3. Available on the website: arxiv.org, accessed on 02/09/2024.

2- Laws:

G. Law No. 78-17 dated January 6, 1978, concerning the electronic processing of data, information, and cards, and

freedoms, published in the French Official Journal No. 1 dated January 7, 1978.

H. Ordinance No. 93-08 dated January 25, 1993, concerning the establishment of the National Agency for Scientific Research and Technology, Official Journal of Algeria, No. 6, January 25, 1993.

I. Ordinance No. 01-01 dated May 15, 2001, concerning the establishment of the National Center for Research and Development of Information and Communication Technologies, Official Journal of Algeria, No. 30, May 15, 2001.

J. Ordinance No. 02-05 dated February 4, 2002, concerning the establishment of the National Institute for Information Technology Research, Official Journal of Algeria, No. 8, February 4, 2002.

K. Ordinance No. 06-03 dated July 15, 2006, concerning the establishment of the National Agency for the Promotion of Information and Communication Technologies in Education, Official Journal No. 46, July 15, 2006.

L. Law No. 09-04 dated August 5, 2009, Law on the Protection of Personal Information in Information Technology, Official Journal, Issue No. 55, August 5, 2009.

M. Ordinance No. 15-02 dated January 23, 2015, concerning the protection of personal data, Official Journal, No. 6, January 23, 2015.

N. Law No. 18-07, dated June 10, 2018, related to the protection of individuals in the field of personal data processing, The Official Journal No. 34, issued in 2018.

الفصل الثامن

الذكاء الاصطناعي ودوره في مكافحة التطرف والإرهاب، الاستاذ

Artificial intelligence and its role in combating extremism and terrorism

الاستاذ المساعد الدكتور

نبيل العبيدي

الخبير الأكاديمي في مكافحة الإرهاب الدولي

عضو الهيأة الاستشارية للمجلة العلمية لجهاز مكافحة الإرهاب العراقي

جامعة بيان-إقليم كردستان/العراق

EMAIL : nabeel.alobaidi@bnu.edu.iq

المقدمة

إن التطور التكنلوجي الحديث قد تم استخدامه من قبل التنظيمات الإرهابية واستثماره في أعمالهم الإرهابية والإجرامية، وقد استغلت تلك التنظيمات الآن التكنلوجيا الحديثة ومنها الذكاء الاصطناعي في التدريب عبر الأنترنت وتحولت من الطرق الكلاسيكية التدريبية

التقليدية قبل تنفيذ أي عملية إرهابية إلى طرق حديثة وعن بعد من خلال التدريب الإلكتروني على استخدام الأسلحة والمتفجرات وكافة طرق تنفيذ أعمالها الإرهابية.

ومن سمات الذكاء الاصطناعي انه يمتلك قدرات هائلة في التطور وله القدرة في التأثير بشكل معمق في جوانب الحياة المختلفة، ومن هذه الجوانب ما يمكن ان يستغله الارهابيون في تحقيق غياتهم واهدافهم الجرمية واستغلال ذلك في التدريب الالكتروني الذي يتلقه افراد التنظيم الارهابي واستغلالهم لتكنلوجيا وتسخيرها في جرائمهم الارهابية.

وجريمة التدريب الإلكتروني لتنظيمات الإرهابية تعد من الجرائم الخطرة والمبتكرة الحديثة، اذ لجات اليها التنظيمات الإرهابية ومنها تنظيم القاعدة وتنظيم داعش الإرهابي بعد ان بدأت مواردهم المالية بالاضمحلال والتناقص والرقابة الشديدة على الدعم التي تحصل عليه ولهذا لجأت هذه التنظيمات إلى التدريب الإلكتروني واستخدام التكنلوجيا لا غرض إجرامية وإرهابية في تدريب عناصرهم الإرهابية.

والذكاء الاصطناعي يلعب دور في اتجاهيين أحدهما ايجابي والاخر سلبي، والجانب الايجابي فيه انه يساعد على معرفة وتحديد نوعية الاشخاص اللذين هم عرضة لتأثر بالأفكار التي تتصف بالتطرف والتشجيع على الارهاب والمساهمة في ارتكابه والسعي باي طريقة من اجل تطوير الاعمال الارهابية والتدريب بأقل تكلفة على تنفيذ الاعمال الارهابية.

وتعتبر مواجهة التدريب الإلكتروني الجنائية ضرورة من ضرورات مكافحة الجرائم الإرهابية بكافة أنواعها وإيقاع اشد العقوبات الجنائية ضد مرتكبها، واستخدام طرق جنائية في مكافحة الجريمة تتماشى مع تطورات العصر الحديثة.

أولاً: أهمية البحث: تكمن أهمية البحث من خلال المتابعة عبر كافة وسائل الإعلام التي نتابعها في نقل الأعمال الإرهابية التي ترتكبها التنظيمات الإرهابية والذي أصبح لنا تصور كامل عن قساوة التدريبات التي تقوم بها وأصبحت لديها قدرة قتالية شديدة الوقعة، وقد تطورت وانتقلت هذه التدريبات من كلاسيكية تقليدية إلى تدريب الكتروني يحقق غايته وهذا ما يجب الحذر منه وذلك من خلال المواجهة الجنائية. وبما ان الارهابيون يسخرون جل

قدرات في تسخير الذكاء الاصطناعي فانه يمثل مخاطر لها جانب التهديد وزعزعة الأمن والسلم داخل المجتمع وهذا ما وجدناه في الوقت الحاضر باستخدام الذكاء الاصطناعي بشكل واسع من قبل بعض التنظيمات الارهابية.

ثانياً: إشكالية البحث: تتمحور اشكالية البحث في أسئلة مهمة جدا وهي:

السؤال الأول: ما هو الذكاء الاصطناعي؟ وما هو التدريب بشكل عام؟ والتدريب الذي ينتهجه هذه التنظيمات الإرهابية؟

السؤال الثاني: كيف نمت فكرة تطوير القدرات القتالية لمسلحي التنظيمات الإرهابية؟

السؤال الثالث: كيف يمكن مواجهة هذه الأعمال من خلال مواجهتا جنائيا؟

السؤال الرابع: كيف يمكن سيطرة الجهد الاستخباري على التدريب الإرهابي الإلكتروني واستغلال الذكاء الاصطناعي؟

السؤال الخامس: كيف يمكن مواجهة الذكاء الاصطناعي الجرمي الذي يستخدمه الإرهابيون؟

ثالثاً: منهجية البحث: سوف نتناول في بحثنا هذا المنهج الاستقرائي والاعتماد على مجريات وتسلسل الأحداث.

رابعا: خطة البحث: نتيجة لحداثة البحث فإننا نرى ان نقسم البحث إلى مبحثين رئيسين هما:

المبحث الأول: ماهية الذكاء الاصطناعي والتدريب

المبحث الثاني: الذكاء الاصطناعي واستخداماته الجرمية من قبل التنظيمات الإرهابية

الكلمات المفتاحية: الذكاء، الاصطناعي، التدريب، التنظيم، الإرهابي

المبحث الأول

تعريف الذكاء الاصطناعي والتدريب

Artificial intelligence & Training

نرى ان الذكاء الاصطناعي قد فرض نفسه وهو مصطلحٌ شاملٌ للتطبيقات التي تؤدي مهام مُعقدة كانت تتطلب في الماضي إدخالات بشرية مثل التواصل مع العملاء عبر الإنترنت أو ممارسة لعبة الشطرنج. يُستخدم غالبًا هذا المصطلح بالتبادل مع مجالاته الفرعية، والتي تشمل التعلم الآلي (ML) والتعلم العميق.

وان عملية التدريب ايضا أصبحت لها هدفها الأساس وهو ان يكتسب الفرد المدرب خبرة ومعرفة وبما يحتاج اليها الفرد في سبيل حصوله على معلومات وكذلك يكون هدف التدريب على مستوى منظمات ومجتمع، ألا ان هذا لا يمكن تحقيقه إلا ان يكون هناك عمل مخطط له وهادف يكون البدء بتوعيه من يكون هو الفرد المدرب الذي هو بحاجة ماسة إلى هذا التدريب والتفكر بشكل جدي ومستمر وبعد ذلك يتم التحديد على أساس الحاجة وكذلك الأولية من خلال استخدام الأساليب العملية المتطورة والتخطيط ذات الطبيعة الاستراتيجية ([1]).

وبناءً على ما تقدم سوف نقسم البحث إلى:

المطلب الأول: مفهوم الذكاء الاصطناعي

المطلب الثاني: تعريف التدريب

المطلب الأول

مفهوم الذكاء الاصطناعي

Artificial intelligence

[1]- حيدر، عصام: التدريب والتطوير ، الجامعة الافتراضية السورية ، دمشق، 2020، ص 3.

وهو قدرة الكمبيوتر الرقمي أو الروبوت الذي يتحكم فيه الكمبيوتر على أداء المهام المرتبطة عادة بالكائنات الذكية. يتم تطبيق هذا المصطلح بشكل متكرر على مشروع تطوير الأنظمة التي تتمتع بالعمليات الفكرية المميزة للبشر، مثل القدرة على التفكير، واكتشاف المعنى، والتعميم، أو التعلم من التجارب السابقة. منذ تطوير الكمبيوتر الرقمي في أربعينيات القرن العشرين، ثبت أنه يمكن برمجة أجهزة الكمبيوتر لتنفيذ مهام معقدة للغاية -مثل اكتشاف البراهين النظرية الرياضية أو لعب الشطرنج -بكفاءة كبيرة. ومع ذلك، وعلى الرغم من التقدم المستمر في سرعة معالجة الكمبيوتر وسعة الذاكرة، لا توجد حتى الآن برامج يمكنها أن تضاهي المرونة البشرية الكاملة في مجالات أوسع أو في المهام التي تتطلب الكثير من المعرفة اليومية. ومن ناحية أخرى، وصلت بعض البرامج إلى مستويات أداء الخبراء والمهنيين من البشر في أداء مهام محددة معينة، بحيث يوجد الذكاء الاصطناعي بهذا المعنى المحدود في تطبيقات متنوعة مثل التشخيص الطبي، ومحركات البحث الحاسوبية، والتعرف على الصوت أو الكتابة اليدوية، وروبوتات الدردشة [1].

والذكاء الاصطناعي عبارة عن مجموعة من العلوم والنظريات والتقنيات (بما في ذلك المنطق الرياضي والإحصاء والاحتمالات وعلم الأحياء العصبي الحسابي وعلوم الكمبيوتر) التي تهدف إلى تقليد القدرات المعرفية للإنسان. بدأت هذه التقنية في ظل الحرب العالمية الثانية، وترتبط تطوراتها ارتباطًا وثيقًا بتطورات الحوسبة، وقد أدت إلى قيام أجهزة الكمبيوتر بأداء مهام متزايدة التعقيد، والتي لم يكن من الممكن في السابق تفويضها إلا إلى الإنسان [2].

والذكاء الاصطناعي قد يضيف ميزة إلى العمل الذي تقوم به وذلك من **خلال:**

1- قيامه بتوفر إدراك وفهم أكثر بكثير من الحالات الاعتيادية لهذا الكم الهائل من البيانات.

---

[1] -B.J. Copeland, artificial intelligence SEP 2023
https://www.britannica.com/technology/artificial-intelligence VISIT 6-9-2023

[2]- Darrell M. West, What is artificial intelligence? ,4 oct 2018 , https://www.brookings.edu/articles/what-is-artificial-intelligence/ visit 6-9-2024 .

2- اعتماد الذكاء الاصطناعي على تنبؤ مهام معقدة ومهمة.

والشيء بالشيء يذكر ان لكل عمل دافعه من اجل اعتماده فالعوامل التي دفعت إلى اعتماد الذكاء الاصطناعي هي [1]:

أولاً: هناك بيانات كبيرة جدا وهي متاحة للاستعمال والتعلم لغرض ان تكون هناك تنبؤات صحيحة.

ثانياً: ان الذكاء الاصطناعي وفر تقنية تطبيق تنافس كبير بين شركات بحيث مكنها من توفر اتخاذ قرارات أفضل.

ونتيجة لما تقدم فان ظهور الحلول والأدوات التي تعتمد على الذكاء الاصطناعي يعني أن بإمكان المزيد من الشركات الاستفادة من الذكاء الاصطناعي بتكلفة أقل وفي وقت أقل. يشير مصطلح الذكاء الاصطناعي الجاهز للاستخدام إلى الحلول والأدوات والبرامج التي تحتوي إما على قدرات ذكاء اصطناعي مضمنة أو تعمل على إتمام عملية صنع القرار الخوارزمي.

يتضمن الذكاء الاصطناعي الجاهز للاستخدام قواعد بيانات ذاتية الإصلاح ونماذج مسبقة الإنشاء للتعرف على الصور وتحليل.

المطلب الثاني

تعريف التدريب

[1] -Kolb, David A. (1984). "Experiential Learning: experience as the source of learning and development". Englewood Cliffs,NJ: Prentice-Hall, inc.

Definition Of Training

يهدف التدريب إلى بناء خبرة أساسية يتم اكتسابها نتيجة النقص الموجود لدى الفرد وهذا التدريب لا يمكن ان يكون فقط للفرد الذي يلتحق جديد لهذه الوظيفة أو الانتماء إلى مؤسسة أو اكتسابه مهارة جديدة وإنما يكون ايضا إلى تنمية تلك المهارات وتجدد الأفكار التي يتدرب من اجلها سواء كانت تدريبات وأنشطة عسكرية أو مدنية[1].

نحن أمام حقيقة ان التدريب يشكل أهمية ليست قليلة للفرد بغض النظر ان كان في بداية التحاقه بهذه الوظيفة او تلك لأنه يساعد على تنمية الأفكار والابداع في العمل وتحقيق الاهداف التي يروها من هذا العمل[2].

ولهذا فان التدريب له تعاريف عديدة ومطروحة على مستويات مختلفة سواء كان تدريب اداري او تدريب أمنى او تدريب على مستوى عسكري من قبل قوات حكومية او تدريب من قبل مجاميع مسلحة او تنظيمات ارهابية فكل لديه هدف يسعى الى تحقيقه.

وهنا نوضح اهم تعريفات التدريب وهي متعددة لكن يمكن اختيار البعض منها لكي يتم لكل المهتمين المقارنة بين مضمون كل منه لأجل تحديد المؤثر بها.

التعريف الأول: يعرف التدريب على انه ذلك النشاط العملي الهدف منه تطوير قدرة الفرد ومهارته من اجل القيام بعمل محدد ويحقق الهدف المرجو من هذا التدريب.

التعريف الثاني: يقصد به ذلك الجهد المخطط والهادف يقوم به أفراد ومنظمات من اجل توفير فرص مناسبة لكي تنمي راس المال سواء بشري او فكري ومساعدته في مشاركته

---

[1]-Gary Dessler: Fundamentals of Human Resource Management (What's New in Management) Paperback – Illustrated, 4 Jan. 2018, p 62.

[2]- العزاوي، نجم: التدريب الإداري، دار اليازوري العلمية، عمان الاردن، 2006، ص 33.

وتنميته على تحقيق أهادفه التي حددها في اطار استراتيجي وتنمية تتصف بالشمول والاستدامة[1].

التعريف الثالث: يعد التدريب الأمني وهو جزء من التدريب العسكري الذي يكون هدفه كسب المعرفة وتنامي مهاراتهم التي تجعل من رجال الأمن لديهم المقدرة على تنفيذ مهام ووظائف تحقيق امن البلد واستقراره والقضاء على جميع أشكال الجرائم ومنها الجرائم الإرهابية[2].

ولما ذكر من تعاريف أعلاه فإنها تدل على شيء مهم وهو ان التدريب عنصر مهم جدا في تنمية قدرات أفراد المجتمع وأحداث تغيير نحو الأفضل وتنمية أفكار المتدرب وأعداءه قوة على التحمل خصوصا بما يتعلق بالتدريب الجسدي ومن هذا التدريب هو التدريب الميداني للقوات الأمنية والعسكرية كافة وكذلك ما تستخدمه المجاميع المسلحة والإرهابية من تدريب عنيف في معسكراتهم التدريبية.

ومن أجل ان يكون هناك تدريب الكتروني ناجح يتطل ما يلي:

أولاً: التخطيط الكامل: يجب ان يكون هناك تخطيط كامل لنظام التدريب الذي سوف يتم تلقي المتدرب عليه. وهذا يقع ضمن مسؤولية متعددة الجهات وهذا كله يمكن ان يقع ضمن التدريب الإلكتروني.

ثانياً: التنفيذ الإلكتروني للمتدرب: ومن خلال ذلك يتم تطبيق ما تم التخطيط الاستراتيجي له وذلك من خلال القيام بالتدريب الإلكتروني الافتراضي في مرحلة تتسم بالمرونة.

---

[1]- الكبيسي، عامر خضير: التدريب الإداري والأمني- رؤية معاصرة للقرن الحادي والعشرين-، جامعة نايف العربية للعلوم الأمنية، الرياض ، السعودية، 2010، ص 13.

[2]- صوفان، عاكف يوسف: مع,وقات العمل التدريبي في المجال الشرطي ودور التقييم والقياس في دعم مسيرته، مجلة الفكر الشرطي العدد 38، الإمارات العربية المتحدة، 2001،ص 31،

ثالثاً: التقييم للتدريب الإلكتروني: وهذا يتم من خلال أسس ومعايير لغرض تعديل التطوير ورسم استراتيجية للتدريب الإلكتروني([1]).

والتدريب له أنواع مختلفة حسب المعيار الذي يصنف فقد يكون تدريب فردي وقد يكون تدريب جماعي او تدريب في موقع العمل او خارج مكان عمل المتدرب([2]). وهذه الأنواع من التدريبات قد تكون تدريبات في مؤسسات مدنية وقد تكون في مؤسسات أمنية أو تكون تدريبات بشكل منتظم وقانوني او تكون تدريبات في ارتكاب جرائم جنائية أو إرهابية كما تكون تدريبات المجاميع المسلحة او التنظيمات الإرهابية وهي اشد انواع التدريب الذي نذكره لكون هذه الأخيرة تحدث نوع من التخويف والهلع وزعزعة الأمن والنظام .

وهذا التدريب الذي تمارسه المنظمات الارهابية عادة ما يكون في معسكرات سرية للغاية ويستخدم فيها اشد انواع التدريب العنيف. كما مارسته التنظيمات الإرهابية في أفغانستان ومنها تنظيم القاعدة الذي استقطب الأف من المتطوعين الإرهابيين في معسكرات تدريب في أفغانستان وضمن معسكرات تدار من قبل تنظيم القاعدة من اجل القيام بأعمال في دول ومناطق عديدة في العالم [(3)]. وتستخدم المعسكرات القاعدة لتدريب الإرهابيين وتطوير الأساليب الجديدة لشن الهجمات، وهي تشكل تهديدًا كبيرًا للأمن العالمي والاستقرار.

وكما أسلفنا سابقاً ان التدريب الإلكتروني يتميز بميزة مهمة وهي توفير الوقت والجهد والتكاليف التي لها قيمة في مرحلة التخطيط للتدريب الإلكتروني. ويؤثر بشكل مباشر محتوى التدريب الإلكتروني وجودته وكذلك توافر الدعم.

---

[1]- الحربي معالي: مفهوم التدريب الإلكتروني، مقال منشور على موقع المعهد العالي للخدمات الإدارية، الهيئة العامة للتعليم التطبيقي والتدريب، https://e.paaet.edu.kw/institutes تاريخ الزيارة 10-4-2024

[2]- Emilio Bartezzaghi · Luca Solari , Training evaluation Marco Guerci.45 in Italian corporate universities: a stakeholder-based analysis , International Journal of Training and Development , November 2010; Volume 14 (4), pp. 291 - 308

[3]- تنظيم القاعدة.. التأسيس والتاريخ والقيادات، مقال منشور على موقع الجزيرة نت ، https://www.aljazeera.net/encyclopedia/2015/3/16 تاريخ الزيارة 8-4-2023 .

المبحث الثاني

الذكاء الاصطناعي واستخداماته الجرمية من قبل التنظيمات الإرهابية

بما ان التدريب يعتبر عنصر مهم جدا في تنمية مهارات الفرد وعلى جميع المستويات فان أهميته في تغيير وتحسين وتطوير وكذلك كثير من يرى ان التدرب هو عملية ذات طبيعة مستمرة تقدم إلى الفرد من اجل تغيير سلوك فني وذهني. ولمواجهة احتياجات قد تحدد قبل بدء التدريب من قبل أطراف التدريب وهما كل من الفرد والعمل. وهذه التدريبات الإلكترونية يستخدم في الذكاء الاصطناعي بشكل واسع نتيجة لإتاحة المعلومات ووفرتها بشكل بسيط وسهل جدت.

ومن هنا نرى تقسيم هذا المبحث إلى:

المطلب الأول: التدريب الجرمي الإلكتروني لتنظيمات الإرهابية باستخدام الذكاء الاصطناعي

المطلب الثاني: استخدام الذكاء الاصطناعي في الجهد الاستخباري في مكافحة التدريب الإلكتروني الارهابي

المطلب الثالث: اليات الذكاء الاصطناعي ودورها في مكافحة التطرف والارهاب.

المطلب الأول

التدريب الجرمي الإلكتروني لتنظيمات الإرهابية باستخدام الذكاء الاصطناعي

التدريب له مكانة كبيرة في إعداد الأفراد بشكل جيد، وطرق التدريب مختلفة حسب المكان الذي يقام به التدريب ومن هذه الطرق قد يكون التدريب الكتروني وهو ما أصبح مشاعاً كثيرا خصوصا في فترة عدم القدرة على الانتقال إلى مكان إقامة الدورات التدريبية أو بسبب تحجيم الحركة وعدم المقدرة بسبب أوضاع استثنائية. يتم اللجوء إلى التدريب الإلكتروني.

ويعتبر التدريب الإلكتروني نوع من أنواع التدريب الذي يتم تقديمه من خلال استخدام تقنيات التكنولوجيا الحديثة وهو ما ساهم في زيادة رقعة التدريب في تقليل تكاليف الحصول على تدريب معين لموضوع متخصص.

ان انتشار التكنولوجيا في دول العالم وبشكل سريع ودون رقيب أدى إلى سوء استخداماتها المتعدد من قبل أفراد المجتمع واستخدام شبكة الانترنت على وجه الخصوص لأغراض جرمية وتسخيرها في خدمة جرائمهم اصبح واضح لدى المجتمع الدولي([1]).

وبالإضافة إلى ان الإرهابيين يستخدموا الانترنت لأغراضهم الإرهابية المختلفة والإجرامية في إعداد الخطط والتواصل بينهم وتسخير الأعلام في قضاياهم الإرهابية وتجنيد أعضاء جدد في شبكاتهم والتحري عن الأهداف ونشر دعايتهم وتسويقهم لها عبر الانترنت. ولهذا فان استثمارهم واستخدامهم للشبكة بشكل واسع. وهذا مما سهل للإرهابيين ان يستخدم الانترنت لغرض التدريب عن بعد قبل سفر هؤلاء المجرمين الى ساحات القتال والمناطق التي تتواجد فيها صراعات ونزاعات كما هو الحال في العراق وسوريا وبعض الدول الافريقية بالإضافة

1- Maura Conway ,Terrorism and Internet governance: Disarmament Forum , core issues. 2007 (3. vol,) p 27 ",

الى استخدام الانترنت في تدريب الكثير منهم على صنع المتفجرات بشكل علمي وتقني ودقة متناهية في العمل والوصول الى اماكن تنفيذ العمليات الارهابية.

ولدى مراجعة الصكوك التي أصدرتها الأمم المتحدة وعلى المستوى العالمي والتي تتعلق في مكافحة الإرهاب لم نجد أي صك ملزم للدول بن يكون هناك أي تشريع يتطرق لاستخدام الانترنت من قبل الإرهابين وهم في حقيقة الأمر ان هناك استخدام مخصوص للأنترنيت في الأعمال الجرمية الإرهابية[1].

واستخدامات الانترنت من قبل التنظيمات الإرهابية متعددة ولكن التركيز في المرحلة الحالية هو عن طريق استخدام التدريب الجرمي الإلكتروني وهو تدريب من يرغب في التطوع في صفوف تلك التنظيمات إلى القيام بالتدريب عن بعد ولو بشكل مبدئي لحين وصوبه إلى المناطق التي يمكن ان ينفذ في العمليات الإرهابية وهذا مما لوحظ أثناء سيطرة تنظيم الدولة الإسلامية داعش على مناطق في العراق وسوريا فكان هناك تجنيد لهؤلاء الإرهابيين والقيام بالتدريب وتزويدهم بالمعلومات الكاملة والدقيقة عن المناطق التي يصلون اليها.

وقد جرمت القوانين ومنها قانون المملكة المتحدة في المحتوى السادس من قانون مكافحة الإرهاب في بريطانيا للعام 2000 على جرائم متعددة ومنها تلك التي يتم فيها استخدام الانترنت وهذا طبيعي ان يقع التدريب الجرمي الإلكتروني من ضمن هذه الاستخدامات الإلكترونية، وجرمت المادة 54 من قانون الإرهاب الأفعال التي ترتكب من خلال الانترنت وهي (تجنيد الأفراد أو استقبالهم أو من خلال الدعوة التي توجه لهم لغرض تدريبهم، او ما يتصل بكافة الأعمال الإرهابية)[2].

وفي أوروبا ألزمت المادة 3 والصادر من مجلس الاتحاد الأوربي الإطاري (-2008 919-JHA) والمؤرخ في نوفمبر 2008 بتعديل القرار الإطاري (JHA-475-2002) بخصوص

[1]- سايمن شير كليف: استخدام الانترنت في أغراض إرهابية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، نيويورك ، 2012، ص 31.

[2] - www.gov.uk/government/publications Visit 10-4-2023

مكافحة الإرهاب، وكذلك أشارت المادة الخامسة من اتفاقية مجلس أوروبا على ان يلتزم أعضاء الاتحاد الأوروبي بتجريم كافة الأفعال الإرهابية ومنها التدريب بكل أنواعه والتجنيد([1]).

ونتيجة لتطورات التكنلوجية التي يمر بها العالم في العصر الحالي فقد ظهرت وسائل متعددة ومتطورة أساء الإرهابيون فيها إلى استخدام التكنولوجيا في أغراضهم الغير مشروعة. ولهذا يتوجب ان تكون هناك طرق حديثة في متابعة المحتويات المستعملة على شبكة الانترنت والتحقق من الاستعمال الأمن لها، وتجنب الأدوات التحقيقية التقليدية، والتعرف على جميع الوسائل المتوفرة لكل من يحاول ارتكاب أي نشاط غير مشروع وذلك عن طريق استخدامه للشبكة العنكبوتية الانترنت واستحداث برامج تحتوي على إمكانية التعرف على هوية من يحاول استعمال الأنترنت في الأعمال الإرهابية.

ولهذا فان استخدام شبكة الانترنت في التدريب الجرمي الإلكتروني من قبل التنظيمات الإرهابية يحتاج إلى متابعة متقدمة وخصوصا نحن أمام استعمال للشبكة بشكل لا قيود ولا حدود في عالم افتراضي يتيح استعمال واسع ومتنوع ومتعدد المعلومات ويمكن ان يحصل على التدريب الإلكتروني جميع أفراد المجتمع الارهابي وفي أي دولة لان الشبكة ماحة للجميع.

[1]- مكتب الأمم المتحدة المعني بالمخدرات والجريمة، خلاصة قضايا الارهاب 2010https://www.unodc.org/documents تاريخ الزيارة 6-9-2023.

المطلب الثاني

استخدام الذكاء الاصطناعي في الجهد الاستخباري في مكافحة التدريب الإلكتروني الارهابي

ان المتتبع للأعمال الإرهابية المرتكبة يرى ان هناك استخدام لشبكة الأنترنت واستغلالها بشكل واسع من قبل التنظيمات المتطرفة وخاصة تلك الجماعات التي ترتبط بحركة الجهاد العالمي. اذ ان شبكة الانترنت تدعم الجماعات الإرهابية في كافة أعمالها العدوانية منذ بداية التخطيط والتجنيد والدعم والتدريب.

ولهذا فان لشبكة الانترنت دور فعال وكبير في نشر وتسويق الأفكار الإرهابية ووصول شبكاتهم الإرهابية إلى اقصى بقاع العالم وعولمتها بشكل واضح لكون تواجد الأفكار الإرهابية وانتشارها على الشبكة يمثل العقل ذات الصبغة المادية لهذه التنظيمات وهي متاحة بدون أي متابعة استخبارية أو رقابية فنية([1]).

وتغلب صفة الاشتهار على عمل المجاميع الإرهابية والتنظيمات بانها تستخدم طابع التجنيد والتدريب أكثر من بقية أعمالها من خلال شبكة الانترنت، اذ تعمل تلك التنظيمات على توفر المعلومات التي تساعد المجندين للأعمال الإرهابية بتوفرها بشكل واسع على الشبكة([2]).

ومن هنا ونتيجة لاستخدام الكثيف للشبكة العنكبوتية الانترنت من قبل التنظيم الارهابي فانه ينبغي البحث في طرق معالجة استخدام الانترنت وخاصة في عملية التجنيد والتدريب وبالأخص التدريب لان استغلال الشبكة لهذا الغرض يمكن ان يوفر الجهود الكبيرة لهذه التنظيمات في إتمام أعمالهم الإجرامية والإرهابية في تدريب مجنديهم وهنا تعتبر حلقة متواصلة

1- Maura Conway, "Terrorism and the Internet: New Media - New Threat?", Parliamentary Affairs, Vol.59, Issue.2, 2006, p 284.

2- Francesca Bosco, "Terrorist Use of the Internet", in : Uğur Gürbüz (Edit), Capacity Building in the Fight Against Terrorism, IOS Press, Amsterdam, 2013, p 42.

بين التجنيد والتدريب وتسهيل المهمة وهي مكملة بعضها لبعض وخاصة أنها أي – التجنيد والتدريب- عملية ذات ارتباط تشعبي ولا يمكن الكشف عنها بسهولة إلا من خلال عمل استخباري كبير ومجهود استثنائي[1].

وعلى سبيل المثال فقد لجأ تنظيم القاعدة إلى استخدام شبكة الانترنت كان مرتبطاً في تدمير المعسكرات الإرهابية لتنظيم القاعدة بعد أحداث 11 أيلول، وهذا كان الدافع وراء لجوء التنظيم إلى التواصل عبر شبكة الانترنت من اجل المحافظة على التواصل بين أعضاءه المنتشرين في إرجاء العالم. ولكون التنظيمات والمجاميع الإرهابية كان اعتمادها منذ تزايد انتشارها على الانترنت فكان لابد من متابعتها بشكل مستمر ودقيق من قبل الأجهزة الاستخبارية لغرض المتابعة الدقيقة والتحليل للمعلومات والمراقبة التامة للمواقع وكذلك للمنتديات التي تدار من قبل التنظيمات الإرهابية ولكي تفهم الأجهزة الاستخبارية الأيدلوجية الإرهابية والأفكار التي تدار بها تلك المواقع وخاصة تلك التي تنشر طرق التجنيد والتدريب[2].

ولهذا فان اعتماد التنظيمات على الشبكات العنكبوتية قد أتاح للأجهزة الاستخبارية من فهم أيدولوجيات تلك التنظيمات وطرق تصريف أعمالها وتحركاتهم وتدريب أعضائها وخصوصا التدريب الإلكتروني الذي لجأت اليه في الفترة الأخيرة[3].

وهذا مما جعل تتبع تلك التنظيمات أسهل والعمل على اتخاذ أسلوب فعال من اجل السيطرة على الأفعال الإرهابية ووضع حد لها.

---

1 -Charles Darwin, On the Origin of Species, The Pennsylvania State University, Pennsylvania, 2001.

2- Wayne A. Downing And Michael J. Meese, Harmony and Disharmony: Exploiting al-Qa'ida's Organizational Vulnerabilities, CTC Report, Combating Terrorism Center (CTC), New York, February 14, 2006, p 5.

3 - Brynjar Lia and Thomas Hegghammer, "Jihadi Strategic Studies: The Alleged Al Qaida Policy Study Preceding the Madrid Bombings", Studies in Conflict & Terrorism, Taylor & Francis Inc, Vol.27, No.5, 2004, p 361.

ونستخلص من هذا المطلب ان جمع وتحليل أي معلومة استخبارية للأنشطة الإرهابية من قبل أجهزة الاستخبارات يعد عامل مهم جدا في تعطيل جميع مخططات التنظيمات الإرهابية ومنها التدريب الإلكتروني الذي يعد عامل رئيسي في تنفيذ الهجمات الإرهابية، اذ يتم التعرف عليها من خلال غرف الدردشة والمواقع الإلكترونية والإرهابية المنتشرة على مواقع التواصل الاجتماعي والقنوات التي تستخدم شبكات الانترنت([1]).

ولهذا لابد لنا من تهيئة الموظفين المتخصصين في استخدام التكنلوجيا بشكل جيد وتكون لهم خبرن في جمع المعلومات من خلال شبكات التواصل الاجتماعي ورصد المواقع التي تديرها التنظيمات الإرهابية وتحليل ما منشور على تلك المواقع لغرض السيطرة عليها وبشكل فعلي وواقعي.

وان استخدام الذكاء الاصطناعي في مكافحة الإرهاب من خلال التنبؤ بالعمليات الإرهابية، وتحديد العلامات الحمراء للتطرف، والكشف عن المعلومات الخاطئة والمحتوى المضلل الذي ينشره الإرهابيون، وإزالته، وتوفير متطلبات تحليل البيانات الثقيلة.

المطلب الثالث

اليات الذكاء الاصطناعي ودورها في مكافحة التطرف والارهاب

اتاحت التطورات التي مرت في هذا العصر ان يتم استخدام الذكاء الاصطناعي على مستوى كبير في مختلف جوانب الحياة، اذ اوجد نموذج افتراضي من اجل التفاعل من خلال وسائل الاتصالات الحديثة والمتنوعة وكان له دور كبير في عملية التداخل مع اجهزة الاتصال وكذلك مع وسائل التواصل الاجتماعي الاخرى التي يمكن اعتراضها ومعرفة التهديدات الارهابية وهذا يعد موضوع في غاية الاهمية وهنا ظهرت الاهمية الكبيرة له وخاصة في الجانب الأمني. اذ أسهم التطور التكنولوجي في اعطاء دافع كبير الى تطور الذكاء الاصطناعي وتسخيره في مكافحة التطرف والارهاب والعمل الاستباقي الذي تستخدمه الاجهزة الأمنية عند حالة

[1] - United Nations, The Use Of The Internet For Terrorist Purposes, United Nations, New York , 2012, p 70.

التأهب في ورود معلومات امنية عن هجوم ارهابي يعد له، وكذلك يعمل الذكاء الاصطناعي على حل الاشكالات التي تواجه الفرد في حياته اليومية وخاصة بما يتعلق بالتعليم والصحة والحياة الاقتصادية، وهنا يظهر لنا ان لذكاء الاصطناعي ادوار امنية ووظيفية في حياتنا نحن الافراد [1].

إن تقنيات التكنولوجيا بمختلف انواعها لها الدور الكبير في محاربة الارهاب بمختلف مجاميعه الارهابية وتنظيماته القاتلة ولا يوجد اي نظام سواء عسكري او أمني له القدرة المنيعة بشكل تام قادر على صد جميع هجمات التكنولوجيا الحديثة والمتمثل بالفضاء السبيراني.

اذ يعد الذكاء الاصطناعي عاملاً مهم في مضاعفة القوة الالية في مكافحة لتطرف كونه يلعب دور ايجابي واساسي من خلال آلياته المتمثلة في:

القيام بإجراءات البحث في ادق المعلومات وتتبعها. وهذه آلية تعد من الاليات المعقدة جدا اذ لا يمكن ان نتخيل حجم وكم المعلومات التي يمكن اللجوء الى معالجتها من اجل الوصول الى المعلومة التي نبحث عنها. بالإضافة الى التشابه في تلك المعلومات التي تعطيها. وخير مثال على ذلك هي الاجهزة التي تعلق بالتصوير والمراقبة، كما ظهرت هناك تقنية جديدة وهي التعرف على الوجه وهي من وسائل الذكاء الاصطناعي التي لا يمكن تجاهلها وهي اداة من خلالها يمكن التعرف على مرتكب العمليات الارهابية بسهولة وايضا على من يقوم بالترويج للأفكار التطرف والعنف([2]).

الالية الثانية التي يقوم بها الذكاء الاصطناعي هي تقليل الوقوع في الخطأ في مرحلة مهمة عند تنفيذ اعمال ارهابية او التخطيط لها وهي مرحلة البحث لغرض التوصل الى المتورطين في هذه الاعمال الارهابية، وايضا في مرحلة الملاحقة لغرض القبض وتطبيق القانون عليهم، وهذا يعد عامل في غاية الاهمية في دقة المعلومة الأمنية في تتبع الارهاب ومواجهته،

---

[1]- إيهاب خليفة، الذكاء الاصطناعي وحل أزمات التنمية في الدول الفقيرة، آراء المستقبل، مركز المستقبل للأبحاث والدراسات المتقدمة، أبوظبي، الإمارات العربية المتحدة، 2023.

[2]- David Ekanem, Artificial intelligence as a mechanism for crime control in Nigeria, Lambert Academic publishing, 2020, p 108.

وبث الثقة بين افراد المجتمع بالاعتماد على الاجهزة الأمنية في مكافحة التطرف والارهاب وهذا مناخ تسعى اجهزة الأمن الى تحقيقه([1]).

لذكاء الاصطناعي دور مهم في مكافحة التطرف والارهاب وذلك من خلال التعرف على الافراد الذين يتأثروا بالأفكار المتطرفة، وهذا يؤدي الى تحديد وحصر هؤلاء المتطرفين والذين يمكن تجنيدهم وتصنيفهم على انهم متطرفون او ارهابيين. ثم تلو هذه المعرفة مرحلة اخرى وهي مرحلة التحصين وفي هذا يستخدم الذكاء الاصطناعي برامج يتم توجيه فيها الاشخاص المستهدفين المتوقع انحرافهم الفكري المتطرف والعمل على استخدام الارشاد في سبيل ابعاد هؤلاء الذين يحتمل ان يتأثروا بالأفكار المتطرفة وانتقالهم الى المجاميع الارهابية.

يساهم الذكاء الاصطناعي في تحديد شخصية الجماعة الارهابية او الشخص الذي غرر به في العمل الارهابي في اي مرحلة من مراحل العمل سواء تقديم الدعم او التنفيذ او التخطيط، وهذا كله يجري من خلال عملية التحليل للمعطيات التي هي محل للتحري، مثال ذلك ما هو نوع السلاح المستخدم، نوع العملية ومكان تنفيذها؟([2]).

من الاليات التي تستخدم في مكافحة الدعاية الارهابية التي تنشر على وسائل التواصل الاجتماعي وخاصة على موقع (فيس بوك) وهو سيد وسائل التواصل الاجتماعي وعمودها اذ يقوم الذكاء الاصطناعي بمطابقة الصور ومن ثم تحديد الصور ومقاطع الفيديو التي يقوم الارهابيون بنشرها، ومن بعد ذلك قيام الذكاء الاصطناعي منع نشر تلك الصور.

---

[1]-سامح راشد، الذكاء الاصطناعي في مواجهة الإرهاب فرص وتحديات، دورية "آفاق استراتيجية"، العدد 4، مركز معلومات مجلس الوزراء، أكتوبر 2021، القاهرة، ص 63.

[2]- Mohamed Alfatih, Chun Lin li, and Naila Elhag Saadalla, prediction of groups responsible for terrorism attack using tree-based models, proceedings of the 2019 international Conference on Artificial Intelligence and Computer Science, Association for Computing Machinery, July 2019, p p 320-324.

استخدام الفيس بوك للذكاء الاصطناعي وذلك لغرض انشاء قاعدة بيانات تحدد البصمات الرقمية للمنظمات الارهابية([1]).

ولهذا فان الذكاء الاصطناعي يلعب دور مهم وحيوي في مكافحة التطرف والارهاب اذ تسعى الدول في الغالب الى امتلاك التقنيات الحديثة بشكل كبير ومنها الذكاء الاصطناعي من اجل مضاعفة قوتها في بسط الأمن على اراضيها ومكافحة الارهاب والتطرف بجميع اشكاله ومن ناحية أخرى، يسعى الفاعلون من غير الدول إلى امتلاك تقنيات الذكاء الاصطناعي أيضًا لكي تكافئ قوتهم قوة الدول. في هذا الشأن، يصرّح ستيوارت راسل، عالم الكمبيوتر في جامعة كاليفورنيا، بأنه يشعر بالقلق من أن أكبر الفائزين من تقدم تقنيات الذكاء الاصطناعي هم الفاعلين من غير الدول مثل التنظيمات الإرهابية. وعلى الرغم من أن هذه التنظيمات ليست في طليعة تطوير تقنية الذكاء الاصطناعي، فإنه يمكنها الوصول إلى تقنيات الذكاء الاصطناعي هذه من خلال السوق السوداء، والحصول عليها من خلال الأبواب المغلقة([2]).

وبين مكافحة التنظيمات الإرهابية من جانب الدول باستخدام تقنيات الذكاء الاصطناعي، ورد فعل هذه التنظيمات باستخدام التقنيات نفسها، يحدث ما يسمى عسكرة الذكاء الاصطناعي وحصره في الاستخدامات العسكرية فحسب، بدلًا من الاستفادة من هذه التقنيات في المجالات الاقتصادية والاجتماعية. بجانب استخدام تقنيات الذكاء الاصطناعي عسكريًا، ينبغي عدم تجاهل استخدامه في المجالات الأخرى.

ان التوقع في مكافحة الارهاب يحتاج الى استخدام الذكاء الاصطناعي والذي يسمح في جمع معلومات عن طريق البيانات الرقمية ذات لكم الهائل والمتنوع اذ إن الخوارزميات التي تدعم النماذج التنبؤية مبرمَجة ذاتيًا على أساس التعامل مع البيانات. وفي العديد من المجالات،

[1]- Bernard Marr, Weaponizing Artifical intelligence: the scary prospect of Al-Enabled terrorism, Forbes, April 23. 2018. https://bernardmarr.com/weaponizing-artificial-intelligence-the-scary-prospect-of-ai-enabled-terrorism/

[2] -Joseph Pozzi, Weaponization of artificial intelligence, Published Master Thesis, Proquest, 2018.

يكون من المستحيل تحليل البيانات من دون مثل هذا النهج، كما سيكون من المستحيل بناء النماذج من دون بيانات([1]).

[1]- Kathleen McKendrick, Artificial intelligence prediction and counter terrorism, Chattem House, Britain, August 2019.

الخاتمة

عند دراستنا في هذا البحث عن موضوع استخدام الذكاء الاصطناعي في التدريب الإلكتروني لتنظيم الإرهابي فان هذه الدراسة قد تطرقت فيها إلى موضوع مهم وهو استخدام الذكاء الاصطناعي في التدريب الإرهابي من قبل التنظيمات الإرهابية المتطرفة وأن التدريب الذي لجات اليه التنظيمات الإرهابية بسبب إجراءات الحكومات في دول العالم بالضغط والمتابعة والتضييق عليها في التنقل والحركة.

وقد برزت لدينا نتائج وهي:

ان التدريب بشكل عام يعد وسيلة مهمة في تطوير قدرات الفرد والانتقال به من حالة إلى حالة أحسن.

لتدريب أسس مهمة جدا وهي التخطيط والتنفيذ والمتابعة وهي عوامل أساسية من اجل الحصول على نتائج غنية ومحققة جدا.

ان استخدام الذكاء الاصطناعي في التدريب الإلكتروني اثبت فاعليته بشكل كبير وخاصة في الفترة الماضية وخلال انتشار جائحة كورونا وقد أدى دور كبير من خلال إدارة الورش التدريبية.

ان التدريب الإلكتروني الذي نعنيه هنا هو التدريب الجرمي الإلكتروني لأعضاء التنظيمات الإرهابية والذي تروم من خلاله تنفيذ أعمال جرمية وإرهابية ضد أفراد المجتمع الأمن.

أما اهم التوصيات:

أولاً: نحن نرى انه ينبغي على الأجهزة الأمنية عامة وأجهزة الاستخبارات خاصة التدريب بشكل دقيق على استخدام الحاسوب بشكل واسع وخاصة برامج التواصل الاجتماعي.

ثانياً: العمل على متابعة كافة أعضاء التنظيمات الإرهابية في مناطق تواجدهم ومن خلال متابعة مقاهي الانترنت بشكل مستمر.

ثالثاً: المتابعة الحثيثة للمواقع الإرهابية على شبكة الانترنت ومن خلال براج استكشافية ذات تقنية عالية وتتبع حركات الإرهاب.

رابعاً: تقديم الدعم الكامل لأجهزة الاستخبارات وتطوير قدراتهم في استخدام الذكاء الاصطناعي في عملياتهم الاستخبارية.

خامساً: تطوير قدرات الأجهزة الأمنية على العمل التكنلوجي والمتابعة الإلكترونية.

المراجع

- حيدر، عصام: التدريب والتطوير، الجامعة الافتراضية السورية، دمشق، 2020.

- العزاوي، نجم: التدريب الإداري، دار اليازوري العلمية، عمان الأردن، 2006.

- الكبيسي، عامر خضير: التدريب الإداري والأمني-رؤية معاصرة للقرن الحادي والعشرين-، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2010.

- صوفان، عاكف يوسف: معوقات العمل التدريبي في المجال الشرطي ودور التقييم والقياس في دعم مسيرته، مجلة الفكر الشرطي العدد 38، الإمارات العربية المتحدة، 2001.

- سايمن شير كليف: استخدام الانترنت في اغراض ارهابية، مكتب الامم المتحدة المعني بالمخدرات والجريمة، نيويورك، 2012،

المواقع الإلكترونية

www.gov.uk/government/publications

- مكتب الامم المتحدة المعني بالمخدرات والجريمة، خلاصة قضايا الارهاب 2010 https://www.unodc.org/documents

- تنظيم القاعدة. التأسيس والتاريخ والقيادات، مقال منشور على موقع الجزيرة نت، https://www.aljazeera.net/encyclopedia/2015/3/16

- الحربي معالي: مفهوم التدريب الالكتروني، مقال منشور على موقع المعهد العالي للخدمات الادارية، الهيئة العامة للتعليم التطبيقي والتدريب، https://e.paaet.edu.kw/institutes

المصادر الانكليزية

-Brynjar Lia and Thomas Hegghammer, "Jihadi Strategic Studies : The Alleged Al Qaida Policy Study Preceding the Madrid Bombings", Studies in Conflict & Terrorism, Taylor & Francis Inc, Vol.27, No.5, 2004.

-Charles Darwin، On the Origin of Species، The Pennsylvania State University، Pennsylvania, 2001.

- · Emilio Bartezzaghi · Luca Solari، Training evaluation Marco Guerci.45 in Italian corporate universities: a stakeholder-based analysis، International Journal of Training and Development، November 2010; Volume 14 (4).

-Francesca Bosco، "Terrorist Use of the Internet»، in: Uğur Gürbüz (Edit)، Capacity Building in the Fight Against Terrorism، IOS Press، Amsterdam, 2013.

-Gary Dessler: Fundamentals of Human Resource Management (What's New in Management) Paperback – Illustrated, 4 Jan. 2018.

- Maura Conway، "Terrorism and the Internet: New Media - New Threat?»، Parliamentary Affairs، Vol.59، Issue.2, 2006.

- Maura Conway, Terrorism and Internet governance: Disarmament Forum, core issues. 2007 (3. Vol,).

Kathleen McKendrick, Artificial intelligence prediction and counter terrorism, Chattem House, Britain, August 2019.

- United Nations، The Use Of The Internet For Terrorist Purposes، United Nations، New York، 2012،

- Wayne A. Downing And Michael J. Meese، Harmony and Disharmony: Exploiting al-Qaida's Organizational Vulnerabilities، CTC Report، Combating Terrorism Center (CTC)، New York، February 14, 2006.

الفهرس