وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية **المرجع:.....**

قسم:القانون الخاص

مذكرة نهاية الدراسة لنيل شهادة الماستر

دور الذكاء الاصطناعي في حماية الأمن السيبراني وتعزيز السيادة الرقمية

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق **التخصص: قانون قضائي**

من إعداد الطالبة: **تحت إشراف الأستاذ:**

_بوزيد فاطيمة **_بوسحبة جيلالي**

أعضاء لجنة المناقشة

الأستاذ	درعي العربي	رئيسا
الأستاذ	بوسحبة جيلالي	مشرفا مقررا
الأستاذ	بن عوالي علي	مناقشا

السنة الجامعية: 2026/2025

نوقشت يوم:01 /06/ 2026

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية

مصلحة التربصات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه , الطالب (ة) :

اللقب : بوزيد الإسم : فاطيمة

الحامل(ة) لبطاقة التعريف الوطنية رقم: 406786499 والصادرة بتاريخ: 2023/09/01

المسجل(ة) بكلية: حقوق والعلوم السياسية قسم: قانون خاص

والمكلف(ة) بإنجاز مذكرة ماستر بعنوان:

دور الذكاء الإصطناعي في حماية الأمن السيبراني وتعزيز السيادة الرقمية

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2026/06/04

حررت هذه الوثيقة من طرف المحامي حمداني حياة

المصادقة على شرعية الإمضاء
السيد/ة بوزيد فاطيمة
الحامل/ة ل.ت.ت 406786499
الصادرة في 2023
مستغانم (ملحقة 29) في 4 JUIN 2026

المجلس الشعبي البلدي
و بالتفويض منه
إمضاء: حنراني منصور

إمضاء المعني

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها.

Scanned with CamScanner

بسم الله الرحمن الرحيم



﴿وَآخِرُ دَعْوَاهُمْ أَنِ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ﴾

Graduation of 20

شكر وعرفان

بسم الله الرحمن الرحيم الحمد الله الذي خلق الإنسان في أحسن تقويم,و جعل له عقلاً وو هبه بالتكريم, سبحانه رافع شأن العلم بالقلم و امتنى على الإنسان, بعث لنا خير خلقه و صفة رسله رحمةً و ملاذ رسوله المصطفى و نبيه المرتضى معلم الحكمة هادي الأمة النبي

" محمد صلى لله تعالى عليه و سلم"

ما سلكنا البدايات إلاّ بتيسيره و لا بلغنا النهايات إلاّ بتوفيقه و ما حققنا الغايات إلاّ بفضله, يسعدني أن أرفع أسمى عبارات الشكر و التقدير إلى أستاذي المشرف "**بوسحبة الجيلالي**" لما أحاطني به من اهتمام علمي و توجيهات قيمة و ما بذله من وقت و جهد و صبر في سبيل انجاز هذا العمل, لقد كان لتوجيهاته السديدة و نصائحه الحكيمة و متابعته الدقيقة الأثر البالغ في تذليل الصعوبات وإنارة الطريق أمامي طوال مسيرتي فكان نعمة الأستاذ و قدوة في العلم والأخلاق و التفاني في أداء رسالته النبيلة ,كما لا يسعني إلاّ أن اعبر عن بالغ امتناني لرقي تعامله و تشجيعه الدائم الذي منحني الثقة و الدافع للاستمرار فكانت تحفيزاته سنداً لي في كل مرحلة من مراحل هذا البحث, فله مني كل الاحترام و التقدير و أدعو الله عز وجل أن يجزيه عني خير الجزاء و أن يبارك له في علمه و عمله و يديم عليه الصحة و العافية و يجعله منارة للعلم و النجاح و العطاء .

كما لاننسى تقديم خالص الشكر والعرفان **للجنة المناقشة** على قبولهم مناقشة هذه المذكرة,و أتوجه بالشكر إلى عائلة كلية الحقوق و العلوم السياسية.

كما أتوجه بخالص الامتنان و التقدير إلى" **أخي العزيز**" رغم بعد المسافات و مرارة الغربة الا انه كان سندا حقيقيا لي بدعمه و تشجيعه الدائم وحرصه المستمر على رفعي معنوياً فله مني أصدق كلمات الشكر و العرفان على وقوفه بجانبي و أسال الله أن يحفظه و يوفقه و يحقق له كل ما يتمناه .

إهداء

الذي وفقني و من علي بالصبر و العزيمة حتى إتمام هذا البحث" الله جل جلاله"

إلى من بلغ الرسالة و أدى الأمانة و نصح الأمة إلى نبي الرحمة و نور العالمين سيدنا

"محمد صلى الله عليه و سلم"

إلى التي غطت الصعب بالإصرار, و جعلت السعي عنوان المسار ,و تركت خلفها دوامة

الإعصار, لتكتب النجاح بعز و اعتبار إلى "نفسي"

اهدي تخرجي إلى النور الذي أضاء دربي, إلى العزيز الذي زين اسمي بأجمل الألقاب و من دعمني بلا حدود و أعطاني بلا مقابل, إلى سندي الدائم إلى الرجل الذي سعى طوال حياته لأكون الأفضل "حبيبي أبي الغالي".

إلى التي احتضنتني بقلبها قبل يدها, التي سهلت لي الطريق بدعائها إلى الظل الخفي و القلب الحني, إلى سر قوتي و نجاحي إلى تلك التي كانت دائما تسير معي إلى أن أصل لوجهتي و تطمئن علي ثم تحيطني بدعواتها "أمي الغالية"

أدعو الله أن يطيل في أعماركم لأصل يوماً و أرد لكم بعضاً من جميلكم جزاكما الله عني خير الجزاء

إلى من رزقني الله نعمة وجودهم ,و أمان أيامي إلى من شددت عضدي بهم, إلى خيرة أيامي "إخوتي و أخواتي"

أدامكم الله ضلعا ثابتا لي

إلى كل من وقف إلى جانبي و ترك أثراً طيبا في قلبي أو دعم خطوة من خطواتي أو قال كلمة صنعت فرقاً, و إلى أساتذتي الكرام لكم جميعا أجمل المعاني الامتنان و الدعاء, إلى كل هؤلاء أهديكم هذا الإنجاز و ثمرة نجاحي الذي لطالما تمنيته ,ها أنا اليوم أكملت و أتممت.

المقدمة

مقدمة

التكنولوجيا في تطور مستمر, وأصبحت محط أنظار العالم لأن تطورها لا يقف عند حدٍ معين, فأصبح بإمكان الإنسان إنجاز العديد من الأعمال بأقل وقت وجهد, حيث سهلت التكنولوجيا حياة الناس وجعلتها أكثر رفاهية, فأصبحت تتغلغل إلى كل تفاصيل حياتنا, حتى أصبح لا يكاد يخلو أي مكان من أثر التكنولوجيا, ونتج عن هذه التكنولوجيا مصطلح الذكاء الاصطناعي, الذي أصبح اليوم مفهوماً متداولاً, وقد دخل على جميع المجالات العلمية التقنية منها وحتى العلوم الإنسانية.

يقصد بالتكنولوجيا مختلف الأساليب والجوانب المعنوية و المادية بما فيها من معلومات. وطرق ونظم ووسائل وأجهزة آلية الكترونية وغيرها, وتعتبر التكنولوجيا بمختلف أنواعها ومصادرها وأشكالها من ثمار المعرفة الإنسانية والبحث و الفكر و الجهد الإنساني المنظم, وبالرغم من وجود آثار جانبية سلبية للتقدم التكنولوجي إلاّ أن تطور التكنولوجيا يؤثر إيجابياً على مستويات التنمية القومية الشاملة, ويحسن من قدرات الإنسان الأساسية المرتبطة بالعلاقة بين التكنولوجيا و التنمية.

وهي التطبيق العملي على نطاق تجاري و صناعي للاكتشافات العلمية و الاختراعات المختلفة التي يتمحص عنها البحث العلمي, وأنها الجهد المنظم لاستخدام نتائج البحث العلمي[1].

حيث يتميز العصر الرقمي الذي نعيشه بسمة خاصة تختلف عن سابقته, فالبشرية على أبواب "ثورة جديدة" ستغير شكل حياة البشر, ثورة عمادها الذكاء الاصطناعي.

فهذا الأخير بتقنياته, يمر بنمو هائل, فهو يعد أحد أوجه التقنيات الحديثة التي كشفت عنها الثورة الرقمية.

[1] أماني يحيى عبد المنعم النقيب, الذكاء الاصطناعي وآثاره على المجتمع, دار الفكر الجامعي,2024,ص13,14.

مقدمة

يطلق على الذكاء الاصطناعي باللغة الانجليزية Artificial Intelligence , ويسمى أحياناً ذكاء الآلات machine Intelligence, ويستخدم اختصاراً (AI) للتعبير عنه, وهو فرع من فروع علم الحاسوب, و إحدى الركائز الأساسية التي تقوم عليها صناعة التكنولوجيا في العصر الحالي, ويشير مصطلح الذكاء الاصطناعي(AI) إلى الأنظمة و الأجهزة التي تحاكي الذكاء البشري لأداء المهام والتي يمكنها أن تحسن من نفسها استناداً إلى المعلومات التي تجمعها[1].

حيث يتكون الذكاء الاصطناعي من كلمتين: الأولى اصطناعي الانجليزية Artificial, وتشير إلى شيء مصنوع, والثانية Intelligence ويعني القدرة على الفهم أو التفكير.

هذا و يرى الأستاذ جهاد أحمد عفيفي أن الذكاء الاصطناعي هو سلوك وخاصيات تتسم بها البرامج الحاسوبية بجعلها تحاكي القدرات الذهنية البشرية وأنماط عملها ومن أهم هذه الخاصيات القدرة على التعلم والاستنتاج ورد الفعل على أوضاع لم تبرمج في الآلة.

وينتمي الذكاء الاصطناعي: إلى الجيل الحديث من أجيال الحاسب الآلي ويهدف إلى أن يقوم الحاسب بمحاكاة عمليات الذكاء التي تتم داخل العقل البشري.

يمكن تعريف الذكاء الاصطناعي باعتباره " مجموعة النظريات و التقنيات المنفذة من أجل تحقيقها آلات قادرة على محاكاة الذكاء البشري.

من جانب آخر يرى حسن نيازي الصيفي أن الذكاء الاصطناعي: هو مصطلح يبين قدرة الآلات على أداء المهام التي تتطلب عادة فهماً شبيهاً بالفهم البشري مثل رؤية البيانات أو كتابتها أو نقلها أو قراءتها أو تحليلها بحيث تقدم الآلة الوظائف المعرفية نيابة عن الإنسان.

[1] بلباي إكرام, الذكاء الاصطناعي في القانون الدولي.دراسة في المفهوم و الأطر و التطبيقات,ابن النديم للنشر و التوزيع و مؤسسة الكتاب القانوني, الطبعة الأولى,2024,ص07,27

في هذا السياق يقول الدكتور يحيى إبراهيم دهشان إنه يعد التطبيق العملي و الذي يوضح مميزات استخدام الذكاء الاصطناعي في الواقع العملي هو الموجود في بعض السيارات حالياً, والذي يساعد في التقليل من حوادث الطرق[1].

وعلى الرغم من أهمية الذكاء الاصطناعي في عالم التكنولوجيا إلاّ أنه لا يوجد تعريف جامع مانع متفق عليه للذكاء الاصطناعي, إذ يعد الذكاء الاصطناعي مجالاً أكثر من كونه مفهوماً يمكن تعريفه بسهولة فقد تعددت التعريفات المعتمدة للذكاء الاصطناعي تبعاً لتخصص الذي تطورت فيه, فالذكاء الاصطناعي مستمد من مجالات أخرى غير علوم الكمبيوتر, كعلم النفس, وعلم الأعصاب, والعلوم المعرفية, والفلسفة,واللغويات,والاحتمالية, والمنطق, وعليه يمكن تقسيم الذكاء الاصطناعي كمجال معرفي إلى العديد من الحقول الفرعية المتقاطعة بشكل كبير, مثل التعلم الآلي و الروبوتات, ومن ثم الشبكات العصبية و الرؤية, وأيضاً معالجة اللغة الطبيعية ومعالجة الكلام.

يعرف الذكاء الاصطناعي في قاموس أكسفورد بأنه:" ملكة الفهم" بما يعني " صناعة آلات تؤدي أعمالاً يتطلب أداؤها توفر الذكاء لدى الإنسان", أو أن وفق تعريف آخره مؤداه " صناعة آلات يمكنها الاعتماد على ذاتيتها دون تدخل بشري, تعمل ضمن إطار بيئة عمل متشابكة و معقدة", أو –وفق تعريف باترك هنري نستو في كتابه عن الذكاء الاصطناعي الصادر عن دار نشر أديسون ويسلي عام 1984– " هي الآلات التي يمكنها أن تؤدي ما يعجز الإنسان– في الوقت الراهن– عن أدائه" , سواء في المجال العسكري أو المدني".

فأنظمة الذكاء الاصطناعي تتطور بسرعة, ويعتقد الباحثون أن الذكاء الاصطناعي يمكن أن يصبح قوياً لدرجة أنه سيكون من الصعب على البشر السيطرة عليه, ونذكر على سبيل المثال

[1] بتشيم بوجمعة,الذكاء الاصطناعي في منظومة العدالة الحديثة على ضوء أحداث أحكام التشريع والقضاء المقارن إلى غاية سنة 2022,الناشر ألفا للوثائق,الطبعة الأولى,2023,ص38,39.

التأثيرات المباشرة على النمو الاقتصادي, وهيكل السوق, والاختلافات القطاعية بوجود الذكاء الاصطناعي و النظم الخبيرة[1].

لذا أصبحت أنظمة الذكاء الاصطناعي أداة أساسية لتعزيز القدرات الرقمية, قصد الكشف المبكر عن التهديدات و التعامل الفعال 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 بدءاً 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 والتكييف مع أساليب الهجوم الجديدة, كل هذا يجعل من أنظمة الذكاء الاصطناعي أداة لا تقدر بثمن في سبيل الكشف عن التهديدات السيبرانية و الاستجابة لها بكفاءة وفعالية أكبر.

بذلك نجد أن مسألة تعزيز السيادة الرقمية في ظل تحديات الأمن السيبراني و في 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 الأخذ بعين الاعتبار بين الاستباقية و الوقاية من التهديدات في الفضاء السيبراني, وحماية البيانات و المعطيات,والسهر على ترقية ونشر ثقافة رقمية أساسها التحسيس المستمر و اليقظة 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[2].

[1] بلباي إكرام, مرجع سابق,ص13,27,28

[2] وافي حاجة, استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية و تحقيق الأمن السيبراني, منشورات دار لامية,الجزائر ,2025,ص06.

تنطلق هذه الدراسة من إشكالية محورية تتمثل في : **الى اي مدى يساهم الذكاء الاصطناعيفي حماية الامن السيبراني و تعزيز السيادة الرقمية على ضوء التحديات الرقمية ؟.**

وللإجابة عن هذه الإشكالية المطروحة وبالنظر إلى الطابع المركب للموضوع، تم الاستعانة بالمنهج الوصفي في مرحلة أولى، من خلال التعريف بمفهوم الأمن السيبراني، وذكر أبرز أبعاده، مع ذكر أهميته، وذلك لتمهيد الأرضية النظرية لفهم الإشكال القانوني محل الدراسة. تم الاعتماد على المنهج التحليلي ، من خلال تحليل النصوص القانونية الوطنية والدولية ذات الصلة، ودراسة التطبيقات الواقعية، بشأن مدى تحقيق الذكاء الاصطناعي للأمن السيبراني، والوقوف على دوره في تعزيز السيادة الرقمية.

وبناءاً على ما سبق, ارتأينا إلى تقسيم هذه الدراسة إلى فصلين اثنين, يتناول الفصل الأول الدور القانوني والتقني للذكاء الاصطناعي, أمّا الفصل الثاني كان تحت عنوان أثر الذكاء الاصطناعي في تعزيز السيادة الرقمية.

الفصل الأول

الدور القانوني والتقني

للذكاء الاصطناعي

في تحقيق الأمن السيبراني

شهد مجال الأمن السيبراني تحولا جذريا بفعل التطور المتسارع في تقنيات الذكاء الاصطناعي, لاسيما مع الانتشار الواسع لتطبيقاته في مختلف جوانب الحياة.فقد رافق هذا التأثير الايجابي عدد من المزايا,لكنه في المقابل أفرز أيضاَ بعض التحديات و السلبيات,خاصة فيما يتصل بأمن المعلومات و البيانات. ولم يعد التقدم التكنولوجي مجرد ميزة إضافية, بل أصبح سمة أساسية للقرن الحادي و العشرين, يتجلى في الاعتماد على الأتمتة الإلكترونية في النظم الإدارية و المالية و الأمنية على الصعيدين الوطني و الدولي.

وفي هذا السياق, برز الذكاء الاصطناعي كأحد الأدوات الرئيسية التي تستخدم في تعزيز الأمن السيبراني, من خلال قدراته الحاسوبية الهائلة, و التكامل المستمر بين الشبكات الذكية, إلى جانب تطور الأعمال الإلكترونية و الاعتماد الواسع على رقمنة البيانات و المعلومات. كل ذلك يؤكد على فاعلية الأنظمة الإدارية و المالية و الأمنية 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 إستراتيجية تعتمد عليها الدول و المؤسسات في الاقتصاد و الصناعة و الخدمات, وحتى في المجالات العسكرية و السياسية. ومن أهم المجالات التي يشهد فيها الذكاء الاصطناعي تأثيراً متزايداً, مجال الأمن السيبراني, الذي بات يشكل ركيزة أساسية من ركائز الأمن الوطني و الشخصي[1].

وهنا تبرز الحاجة إلى ضرورة فهم ماهية الأمن السيبراني كمتغير جديدة في العلاقات الدولية لذلك سنتطرق إلى مفهوم الأمن السيبراني ونشأته(المبحث الأول) و الأطر لحماية الأمن السيبراني في ظل أنظمة الذكاء الاصطناعي(المبحث الثاني).

1_وافي حاجة, مرجع سابق, ص10

المبحث الأول: ماهية الأمن السيبراني و نشأته.

يعتبر الأمن السيبراني من المفاهيم التي أصبحت تتداول في الدراسات الأكاديمية نظراً لأهميتها في الحد من الاختراقات السيبرانية ومواجهة الجرائم الالكترونية بالتالي كثر استخدام هذا المصطلح عبر العالم. وعليه سنوضح في هذا المبحث مفهوم الأمن السيبراني و نشأته من خلال تقسيمه لمطلبين , نتناول في (المطلب الأول) تعريف الأمن السيبراني و أبعاده, بينما في (المطلب الثاني) نبرز أهمية الأمن السيبراني و الأهداف التي يحققها.

المطلب الأول: مفهوم الأمن السيبراني و أبعاده المختلفة.

سنتناول في هذا المطلب تعريف الأمن السيبراني(الفرع الأول) و المفاهيم المرتبطة به في(الفرع الثاني) وسنتطرق للنشأة الأمن السيبراني وأبعاده في (الفرع الثالث).

الفرع الأول:تعريف الأمن السيبراني.

هناك تعريفات متنوعة و مختلفة للأمن السيبراني, وسنتطرق لها كما يلي:

أولاً:التعريف اللغوي و الاصطلاحي للأمن السيبراني.

أ_لغةً:الأمن السيبراني مكون من لفظتين :" الأمن", و"السيبراني"[1].

الأمن:هو نقيض الخوف, أي بمعنى السلامة. و الأمن مصدر الفعل أمِنَ أمناً و أمَاناً و أمَنَةَ: أي اطمئنان النفس و سكون القلب و زوال الخوف, و يقال: أمِنَ الشر , أي سَلِمَ منه. وقد عرَّفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يهدد القيم النادرة. السيبراني: مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي, وتشير المقاربة الإيتيمولوجية لكلمة "cyber" إلى أنها لفظة يونانية الأصل مشقة من كلمة "kybernetes " بمعنى الشخص الذي يدير دفة السفينة, حيث تستخدم مجازاً للمتحكم "governor". وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات

[1] أحمد حاتم جبار عطية, الأبعاد القانونية و الاجتماعية للأمن السيبراني, مجلة الشرق الأوسط للدراسات الفقهية و القانونية,المجلد05,العدد,2025,03,ص441.

الأمريكي , و ذلك للتعبير عن التحكم الآلي , فهو الأب الروحي المؤسس للسبرنيتيقية من خلال مؤلف الشهير: Cybernetiecs or control and communication in the Animal and the machine .و أشار في كتابه إلى أن السبرنتيقية هي التحكم و التواصل عند الحيوان و الآلة و الإنسان و الآلة ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب[1].

ب_ اصطلاحاً: يعرف الأمن السيبراني على أنه مجموعة من الإجراءات المتخذة للدفاع ضد الهجمات الالكترونية التي يشنها قراصنة الكمبيوتر, بالإضافة غلى التعامل مع تبعاتها و تنفيذ التدابير المضادة اللازمة. كما يعرف أيضاً بأنه مجموع الأدوات و السياسات و مفاهيم الأمن و الآليات الوقائية و التكنولوجيات التي يمكن استخدامها لحماية البيئة السيبرانية و أصول المؤسسات و المستخدمين. و تتضمن هذه الأصول أجهزة الحوسبة المتصلة بالشبكة, الموظفين,البنية التحتية, التطبيقات, الخدمات, أنظمة الاتصالات, والمعلومات المنقولة أو المخزنة في البيئة السيبرانية. ويهدف الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسة و المستخدمين و الحفاظ عليها, بما يشمل السرية , السلامة, التوفر , وعدم الرفض. كما يعرف على أنه مجموعة الإجراءات و التدابير الوقائية التي تهدف إلى حماية الأنظمة المعلوماتية والبيانات الرقمية من التهديدات السيبرانية, بما يضمن سلامة البنية التحتية الرقمية و سرية المعلومات.يشمل هذا المفهوم حماية الشبكات , الأجهزة, البرمجيات, و البيانات من الوصول غير المصرح به أو التعديل أو الإتلاف, وفقاً للتشريعات الوطنية و المعايير الدولية. من أبعاده القانونية, يرتبط الأمن السيبراني بصون الحقوق الأساسية مثل الحق في الخصوصية , و ضمان حرمة الحياة الخاصة, بالإضافة إلى دوره في حماية الأمن القومي ومنع الجرائم الإلكترونية التي تستهدف المؤسسات و الأفراد. يفرض القانون على الجهات المعنية اتخاذ

[1]_ دحان حزام ناصر القربطي, الأمن السيبراني وحماية أمن المعلومات, دار الفكر الجامعي, الاسكندرية,2024,ص11

التدابير اللازمة لمنع الهجمات السيبرانية و معالجة آثارها, تحت طائلة المسؤولية القانونية في حالة الإخلال بهذه الالتزامات[1].

وقدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني فاعتبرته:" جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية, و الالكترونية,ومن مختلف الجرائم:هجمات التخريب, التجسس و الحوادث", في حين اعتبر الإعلان الأوروبي الأمن السيبراني أنه " قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات"[2].

ثانياَ: التعريف الفقهي و القانوني.

أ_ التعريف الفقهي للأمن السيبراني.

كان للأكاديميين دور في تعريف الأمن السيبراني, بحيث عرفه ريتشارارد كمرر Richard Akemmerr على أنه عبارة عن دفاعية من شأنها كشف و إحباط المحاولات التي تقوم بها القراصنة .

في حين عرفه إدوارد مورسو Edward Amorso على أنه:" وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو اجهزة الحاسوب أو الشركات و تشمل تلك الوسائل و الأدوات المستخدمة في مواجهة القرصنة و كشف الفيروسات ووقفها و توفير اتصالات المشفرة.

كما يعرفه كذلك للكاتبات " Pe kky Matti" في كتابهما الموسوم Technology and Cyber Sucurity :Amlytics ,Automation . حيث اعتبر الأمن السيبراني عبارة عن مجموعة من

[1] صمودي كريمة,برقعي سمر,الأمن السيبراني في الجزائر, مذكرة ماستر جامعة 08 ماي 1945 قالمة , كلية الحقوق و العلوم السياسية,تخصص قانون أعمال ,السنة الدراسية 2024_2025,ص10,11.

[2] هيبة عبد المجيد, عبد الحافظ العودة,التحديات التي تواجه الأمن السيبراني,مجلة Humanities natural Seiences jounral (HNS)المجلد06,العدد07,2025,ص725.

إجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر و عواقبها, ويتضمن تنفيذ التدابير المضادة المطلوبة.

أمّا فيما يخص الدوائر الحكومية فركزنا على أهم فواعل الدولة والهيئات المختصة بالولايات المتحدة الأمريكية, تعرف وزارة الدفاع الأمريكية الأمن السيبراني على أنه مجموعة الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها (إلكترونية و المادية) من مختلف الجرائم , الهجمات ,التخريب, التجسس و الحوادث.

تُعدّ وكالة الأمن الرقمي الأوروبية من أوائل الهيئات التي بادرت إلى تشريع هذا المجال,فعرفته بأنه قدرة النظام المعلوماتي على مقاومة محاولات اختراق أو الحوادث غير المتوقعة التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي[1].

ب_التعريف القانوني للأمن السيبراني.

1_التعريف القانوني الدولي للأمن السيبراني الدولي: نذكر التعريف الذي جاء به الاتحاد الدولي للاتصالات الصادر في تقرير حول اتجاهات الإصلاح للاتصالات عام 2010_2011 والذي يعتبر بمثابة أرضية إجماع لمختلف التوجهات الفكرية و المهنية " هو مجموعة من المهمات, مثل تجميع وسائل و سياسات , وإجراءات أمنية و مبادئ توجيهية, ومقاربات إدارة المخاطر وتدريبات وتقنيات, يمكن استخدامها لحماية البيئة السيبرانية و موجودات المؤسسات و المستخدمين"[2].

2 _تعريف المشرع الجزائري للأمن السيبراني: أعطى المشرع الجزائري تعريفاً للأمن السيبراني في المادة العاشرة 10في فقرتها الثالثة 03 من القانون رقم 18_04 المتضمن للقواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية بأنه مجموع من أدوات و السياسات ومفاهيم الأمن و

[1] بوعلام فتيحة, الأمن السيبراني في الجزائر, مذكرة ماستر في القانون الخاص, تخصص قانون خاص, جامعة مستغانم, السنة الجامعية 2024_2025,ص,09

[2] أنظر التقرير الصادر عن الإتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات عام 2011_2015.

الآليات الأمنية و المبادئ التوجيهية وطرق تسيير المخاطر و الأعمال و التكوين و الممارسات الجيدة و الضمانات و التكنولوجيات التي يمكن استخدامها في حماية الاتصالات الالكترونية ضد أي حدث من شأنه المساس بتوفير و سلامة و سرية البيانات المخزنة أو المعالجة أو المرسلة[1].

[1] المادة 10 من القانون 18_04,المتضمن للقواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية, المؤرخ في10_05_2018, الصادر في الجريدة الرسمية الصادرة في 13_05_2018, العدد03,ص27

الفرع الثاني:المفاهيم المرتبطة بالأمن السيبراني.

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني, نذكر أهمها:

1. **الردع السيبراني:** في ظل تعدد التهديدات السيبرانية, التي تشمل"الحرب الرقمية" Digital Warfare, و"الإرهاب الرقمي"Digital Terrorism , و"التجسس الرقمي"Digital Espionage , بجانب التزايد المضطرد في أعداد الهجمات السيبرانية في السنوات القليلة الماضية, تتزايد أهمية " الردع السيبراني" لتأمين أجهزة الحاسوب الآلي, وأنظمة المعلومات, والبنى التحتية من ناحية, والحيلولة دون تكرار تلك الهجمات من خلال تحديد الخصم على نحوٍ دقيق وتوعده بالانتقام رداً على هجومه, من ناحية ثانية, وحماية الأمن القومي للدول الذي بات رهناً بالفضاء السيبراني,من ناحية ثالثة. في هذا الإطار, تتجلى أهمية "الردع السيبراني" الذي يثير التساؤلات حول قدرته على التصدي لمختلف الهجمات السيبرانية, ومدى فعاليته في الفضاء السيبراني في ذل اختلاف الأخير وتعقده مقارنة بالمجالات العسكرية الأخرى. . فالأسلحة والتقنيات السيبرانية الهجومية غير مكلفة نسبياً, ويمكن الحصول عليها وتطويرها بسهولة.

يعرف "الردع السيبراني" بأنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء السيبراني. وعلى الرغم من التعريف الدقيق للمفهوم, إلاّ أنه يرتبط ارتباطاً جذرياً بسياسات القوى الكبرى من جانب, والأبعاد الأمنية للفضاء السيبراني من جانب آخر[1].

2. **الفضاء السيبراني:** عرفته الوكالة الفرنسية لأمن أنظمة الإعلام"ANSSI", وهي وكالة حكومية مكلفة بالدفع السيبراني الفرنسي, بأنه:" فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية", وهو وسط بيني

[1] أحمد طارق أحمد, البيانات المتوافقة في الشبكات و الهجمات الأمنية السيبرانية ، الطبعة الأولى، مؤسسة الوراق للنشر والتوزيع، الأردن،2024,ص201

تفاعلي مستجد, تشمل عناصر المعنوية والمادية, مركب من بعض المعدات الالكترونية, وأنظمة الشبكات والبرمجيات, والمستخدمين سواء مستخدمين أو مستهلكين. كما أن هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة.

3. **الصراع السيبراني:** مع انتشار الفضاء السيبراني وسهولة الدخول, اتسع نطاق النزاعات السيبرانية وازداد عدد المهاجمين. وهناك عاملان رئيسيان لتوسع النزاعات السيبرانية: أحدهما هو التغيير الأساسي في منظور الحرب, ونمط التحولات بين الناس. ثانياً, ظهور النزاعات على المستويين المحي و الدولي, وزيادة حدة النزاعات الداخلية وبؤر التوتر بعد الحرب الباردة, كما يوفر السياق الدولي للفضاء السيبراني بيئة مفتوحة للقوى المهمشة في السياسة الدولية.[1]
4. **الجريمة السيبرانية:** مجموعة الأفعال و الأعمال غير القانونية التي تتم عبر معدات, أو أجهزة إلكترونية أو شبكة الانترنت, أو تبث عبرها محتوياتها, وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي و نظم المعلومات لارتكابها أو التحقيق فيها و مقاضاة فاعليها, فهي الجريمة المتصلة باستخدام الكمبيوتر, أو أي تصرف غير قانوني يرتكب باستخدام تقنيات المعلومات و الاتصالات.
5. **القوة السيبرانية:** يعد جوزيف ناي "Joseph nay" من أبرز المهتمين بالقوة السيبرانية حيث عرفها بأنها " القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني, أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة و التأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى, و ذلك عبر أدوات سيبرانية"[2].

[1] قطاف سليمان, بوقريت عبد الحليم,الأمن السيبراني والمضامين المفاهيمية المرتبطة به, مجلة طبنة للدراسات العلمية الأكاديمية,المجلد05,العدد,02,2022,ص49

[2] فارس محمد العمارات, إبراهيم الحمامصة,الأمن السيبراني المفهوم و تحديات العصر, دار الخليج للنشر و التوزيع, الأردن,الطبعة الأولى,2022,ص21,22.

6. **الهجمات السيبرانية:** عرفها "Michael-N-Schmit" بأنها تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو وبهدف التأثير والإضرار فيها والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة.

كما عرفها عبد القادر محمد فهيمي بأنها هجمات تستخدم فيها المنظومة الشبكية والأجهزة الحاسوبية للدولة أو الفاعلين من غير الدول لتعطيل كفاءة السيطرة و القدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين من الدول ومن غير الدول أو تقليلها أو حتى تدميرها سواء كان ذلك على مستوى منظومات قوتها العسكرية وبالشكل الذي يعرض الأمن القومي للدولة إلى تهديد جسيم[1].

7. **عزل المتصفح:** "Browser Isolation " واحدة من أكثر مصطلحات الأمن السيبراني تقدماً و التي تظهر عند مناقشة الأمن السيبراني هي"Browser Isolation" أو عزل المتصفح.

فهو آلية دفاع إلكترونية يستخدمها باحثوا الأمن السيبراني للحماية من هجمات البرمجة النصية عبر المواقع و كذلك عزل المتصفح عن التطبيقات الأخرى على الكمبيوتر.

هذا يعني أنه لا يمكن تنفيذ التعليمات البرمجية من موقع ويب على موقع آخر, مما يمنع تنفيذ البرامج النصية الضارة, فهو يعمل عن طريق منع مواقع الويب من التفاعل مع بعضها البعض, مما يمنعهم من مشاركة أي بيانات.

و يعني أيضاً أنه إذا كنت تستخدم Firefox أو Chrome أي متصفح في ويب آخر , وكنت مصاباً ببرامج ضارة أو فيروسات, فسيتم عزله عن برامج مثلAdobe photoshop أوMicrosoft word (و التي ربما تم تنزيلها على الحاسوب), إذا كنت مصاباً بفيروس ما و قمت بفتح أحد هذه التطبيقات, فلن تتأثر بالفيروس.

[1] شاري خيرة,صادقي إيمان, الأمن السيبراني وأثره في تحقيق الأمن القومي,مذكرة ماستر,جامعة محمد البشير الإبراهيمي,برج بوعريرج,كلية الحقوق والعلوم السياسية,تخصص إعلام آلي وانترنت,2023_2024,ص23,24

8. **السحابة:** هي تقنية تتيح لنا الوصول إلى ملفاتنا أو خدماتنا عبر الانترنت من أي مكان في العالم. من الناحية الفنية, فهي عبارة عن مجموعة من أجهزة الكمبيوتر ذات إمكانيات التخزين الكبيرة التي تقدم الخدمات عن بُعد[1].
9. **التشفير:** هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلوماتي جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن.

وتستخدم مفاتيح تشفير Encryptionالنصوص المرسلة وفك الشفرة من قبل صاحبها و المسموح له بتسليمها, وتستند هذه المفاتيح إلى صيغ رياضية معقدة في شكل خوارزميات وتعتمد قوة وفعالية التشفير على نوعية الخوارزميات.

1. **الاختراق:** بشكل عام الاختراق هو القدرة على الوصول لهدف معين و الدخول على الأجهزة بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بها بهدف التطفل على خصوصيات الآخرين وإلحاق الضرر بهم.

ويطلق على المخترق مصطلح(Hacker) وحينما يتمكن المخترق من إحداث الأضرار كحذف ملفات أو تشغيل ملفات مؤذية أو وضع وزراعة ملفات تجسسية (أحصنة طروادة) أو فيروسات أو أي نوع من هذه الأنواع فهو مخرب(Cracker) ويتم اختراق عن طريق معرفة الثغرات

الموجودة في النظام والتي غالباً ما تكون في المنافذ(Ports) أو الخاصة بالجهاز, ويمكن وصف هذه المنافذ بأنها بوابات للكمبيوتر على الشبكة العالمية تسمح لها بالدخول[2].

[1] عفيفي حافظ محمد, الشبكات العنكبوتية السيبرانية العالمية المبرمجة, الطبعة الأولى, مؤسسة الرواق للنشر و التوزيع,الأردن
[1] والدار الجزائرية للكتاب زموري, الجزائسر,2025,ص195.
[2] أحمد سعيد فرحات السرجاني, التحول الرقمي في تحقيق الأمن السيبراني, دار العلم والإيمان,جمهورية مصر العربية,محافظة كفر الشيخ,2025,ص126,125,178.

الفرع الثالث: نشأة الأمن السيبراني و أبعاده.

أولاً:نشأة الأمن السيبراني.

ظهر الأمن السيبراني مع نهاية الحرب الباردة, وظهور مصطلح حرب الانترنت أو الحرب السيبرانية, التي جاءت مع بداية اعتماد الدول على أجهزة الكمبيوتر في مؤسساتها و تطوير وحدة المعالجة المركزية في هذه الأجهزة, التي دخلت في عمل المؤسسات و الحكومات وحتى في الحياة اليومية, واقتصر دور الأمن السيبراني في الفترة الأولى على الحماية من الفيروسات و البرمجيات الخبيثة.

ونتج أول فيروس رقمي في سبعينات القرن العشرين على شبكة "أربانت",إحدى أوائل الشبكات في العالم لنقل البيانات باستخدام تقنية تبديل الرزم, وكان على شكل رسالة نصية بسيطة لم تتسبب بأضرار تقنية لكنها دفعة إلى اتخاذ تدابير وقائية[1].

شهد هذا العقد بأكمله نمواً وتطوراً كبير في شبكة الانترنت وترافق هذا الأمر مع نمو وتطور صناعة الأمن السيبراني, فقد تطورت أشكال ومخاطر الفيروسات وبدأت بالظهور بأشكال متعددة.

في عام 1990 تم تطوير أول كود لفيروس قادر على التحول بعد عملية الإصابة مع الحفاظ على الخوارزميات الأصلية في مكانها و الذي يعرف باسم الفيروس متعدد الأشكال.

منذ ظهور أول مضاد فيروسات كان الهدف هو زيادة طرق الحماية من المخاطر و التهديدات الأمنية المحتملة ومع تطور مجموعات القرصنة واجهت الشركات الكثير من التحديات لتحسين الحماية وتقليل مخاطر عمليات انتهاك البيانات.

[1] الجزيرة نت,"الأمن السيبراني": مفهومه وتاريخه,19 سبتمبر 2024 https://www.aljazeera.net/ ,تاريخ الإطلاع 28_02_2026, 1:03.

كما بدأت عمليات الاختراق لبطاقات الائتمان في العقد الأول من القرن الحادي و العشرون ويشمل هذا الأمر خروقات البيانات التي تستهدف بطاقات الائتمان وكانت مجموعة الاختراق Albert Gonzales من أخطر المجموعات فقد تمكنت من سرقة معلومات سرية من 45,7 مليون بطاقة ائتمان وتمكنوا من الوصول الغير المصرح به لقاعدة بيانات البائعين خلق هذا الأمر حاجة أوسع للتركيز على أمن المعلومات في مختلف القطاعات بما في ذلك التجارة الالكترونية وعمليات البيع عبر شبكة الانترنت.

جعل تعدد و تطور التهديدات و الهجمات وإيجاد طرق مبتكرة وجديدة وخاصة هجمات التصيد الاحتيالي وفقدان البيانات الشخصية عبر الانترنت وهجمات برامج الفدية, من إيجاد حلول وطرق لتقليل الانتهاكات الأمنية أمر أكثر أهمية من أي وقت مضى وبدأ استخدام الذكاء الاصطناعي و التعلم الآلي في مجال الأمن السيبراني.

الجهود المبذولة لمنع الهجمات أصبحت أمر حتمي في يومنا الحالي وتحولت الحاجة إلى القيام بذلك لطرق أكثر تطور وفعالية بالاعتماد على تقنيات التكنولوجيا الجديدة [1].

ثانياً: أبعاد الأمن السيبراني.

أ)_البعد القانوني: يرتب البعد القانوني على النشاط الفردي و المؤسسي و الحكومي في الأمن السيبراني نتائج قانونية, تستدعي قواعد خاصة و هامة لحل النزاعات التي تنشأ عنها,حيث لابد من مراعاة التحولات التقنية التي رافقت ظهور مجتمع المعلومات, فقد تم إضافة حقوق جديدة غير الحقوق الأساسية, و الحريات الإنسانية المعترف بها في الدساتير, و التشريعات الوطنية و الدولية, كحق النفاذ إلى الشبكة العالمية للمعلومات.

ب)_البعد السياسي: حيث تقوم الأبعاد السياسية على أساس حماية نظام الدولة السياسي من استخدام التقنيات في بث المعلومات و البيانات لزعزعة استقرار أمن الدول و الحكومات, وتتمثل الأبعاد السياسية في الأمن السيبراني في حق الدولة في حماية أنظمتها وواجها في

[1] جميل حسين طويلة, تاريخ الأمن السيبراني, https://www.noor-book.com/, تاريخ الإطلاع 28_02_2026, 10:29.

السعي لتحقيق استقرار وأمن شعبها, وقد أصبح بإمكان المواطن أن يتحول إلى لاعب أساسي في اللعبة السياسية فأصبح بإمكانه الاطلاع على مبررات القرارات السياسية, التي تتخذها الحكومة في دولته من خلال الكم الهائل من المعلومات, التي يمكنه الوصول إليها عبر الانترنت[1].

ج)_البعد العسكري: تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط وحدات عسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الالكتروني, بما يسمح بسهولة تبادل المعلومات وتدفقها, وسرعة اتخاذ القرارات العسكرية, ومن ثمة تحقيق الأهداف عن بعد ومن دون شك فإن عدم استغلال هذه التقنية و التسلح بها, أو تأمينها بشكل جيد من أي اختراق خارجي, سيؤدي بالضرورة إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية, ومن ثم تدمير قواعد للبيانات, و ما يلحقه من مخاطر.

د)_البعد الاقتصادي: لقد أصبح الفضاء الالكتروني جاذباً لقطاعات المجتمع كافة, وباتت المعرفة محرك الإنتاج والنمو الاقتصادي, كما أيقن الجميع أن مبدأ التركيز على المعلومات و التكنولوجيا يعد عاملاً من العوامل الأساسية للنهوض بالاقتصاد, وهو ما دفع بالدول في الآونة الأخيرة تزيد من استثمارها في المعرفة, وأصبحت عصرنة الاقتصاد مرتبطة بالتحكم في الاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين و الاجتماعيين كما أن استخدام الكمبيوتر و شبكة الانترنت في تطوير الصناعات و تحريك الاقتصاد, ومعالجة كل المعاملات الاقتصادية و المالية, وزاد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية هذه المعلومات.

[1] محمد حسن المهندي, الإطار القانوني للأمن السيبراني في المحافظة على الصحة العامة في القانون القطري:"دراسة مقارنة",مجلة الدراسات الإنسانية و الاجتماعية,جامعة وهران08,المجلد14,العدد02,2025,ص211.

فعلى سبيل المثال, يشير تقرير صادر عن شركة Emarketer إلى أن حجماً لتجارة الالكترونية بلغ 1,5 تريلون دولار في عام 2014 بزيادة نسبتها20% مقارنة بعام 2013 الذي بلغت فيه1,2 تريليون دولار[1].

هـ)_البعد الاجتماعي: ولا تقف الأبعاد الاجتماعية, عند حدود توفير اطمئنان المواطن إلى حياته اليومية, و الإفادة من طاقات تقنيات المعلومات و الاتصالات, في تطوير نشاطاته المختلفة, بل تتعداها إلى صيانة القيم الجوهرية في المجتمع: كالانتماء, والمعتقدات, إضافة إلى العادات و التقاليد, عبر إنشاء المجموعات, التي تهتم بنشر الوعي حول هذه المسائل.

في هذا السياق, يأتي التشديد من قبل الهيئات و المنظمات الدولية, على نشر ثقافة الأمن في الأمن السيبراني, و ضرورة تعاون المجتمع, بكل مكوناته, على تحقيقه و ضمانه. فمما لا شك فيه, أن المخاطر السيبرانية, تطاول المجتمع ككل, سواء, بسبب ارتكاز الخدمات الحيوية, كالطاقة, و النقل, و الصحة, و الاتصالات, وغيرها, على ما تقدمه تقنيات الاتصالات و المعلومات, من إمكانات, أو عبر ما يضخ من محتوى في الأمن السيبراني. فالمحتويات غير المشروعة, وغير المرغوب بها, ذات تأثير سلبي, أكيد على أخلاقيات مجتمع معين, و على ارتفاع نسبة الممارسات الجرمية. أمّا الأمثلة التي تساق هنا فكثيرة, ونذكر منها: الإباحية, والترويج للاتجار بالممنوعات, و الدعارة, والإرهاب, والتجنيد لقضايا تمس الأمن و السلام الدوليين. وعليه, لابد من بناء مجتمع مسؤول, ومدرك لمخاطر القضاء السيبراني , قادر على التعامل بحد أدنى من قواعد السلامة, مع إدراك للعواقب القانونية, التي يمكن أن تترتب على بعض التصرفات, التي تمارس في الأمن السيبراني[2].

[1] سمير بارة, الأمن السيبراني في الجزائر السياسات و المؤسسات, المجلة الجزائرية للأمن الإنساني,المجلد02,العدد,2017,04,ص260,261,262.

[2] حنين جميل أبو حسن,الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة), رسالة مقدمة للاستكمال متطلبات للحصول على درجة الماجستر , تخصص قانون خاص, كلية الحقوق,جامعة الشرق الاوسط,الأردن,2024,ص26,27.

المطلب الثاني: أهمية و أهداف الأمن السيبراني.

للأمن السيبراني أهمية كبيرة لكل مجتمع و لكل دولة. فالأمن السيبراني مهم على مستوى الفرد في حماية البيانات الشخصية و الصور و الفيديوهات و الحسابات الشخصية و كلمات المرور و الحسابات البنكية.و على مستوى المجتمع, من حيث حماية المجتمع من الهندسة الاجتماعية واستهداف السلوك الاجتماعي و البيانات المجمعة و الخصوصيات للمجتمع.

وعلى مستوى الشركات و المؤسسات, في حماية الأصول الالكترونية و البيانات و المعلومات وبيانات الموظفين و السيرفرات و المواقع الالكترونية وعلى مستوى الدولة, في حماية أمنها الالكتروني وحماية الأنظمة المالية والاقتصادية والعسكرية والتلفزيون والراديو من الاعتداءات الالكترونية والقرصنة والتعطيل[1].

انطلاقاً من ذلك، تتجلى أهمية الأمن السيبراني في كونه آلية لحماية المصالح الفردية والمؤسساتية والوطنية (الفرع الأول)، كما يسعى إلى تحقيق جملة من الأهداف الاستراتيجية والتقنية التي تضمن سلامة الفضاء السيبراني واستقراره (الفرع الثاني)، فضلاً عن تنوع مجالاته وأنواعه بحسب طبيعة الأنظمة والمعلومات محل الحماية، وهو ما يستدعي بيان أبرز أنواع الأمن السيبراني وصوره المختلفة (الفرع الثالث).

[1] محمود علي, عبد الرحمان,أسامة فاروق مخيم, الفضاء الالكتروني وأثره على مفاهيم القوة و الأمن والصراع في العلاقات الدولية,مجلة كلية السياسة والاقتصاد,جامعة محمد البشير الإبراهيمي,برج بوعريرج,المجلد06,العدد05,الجزائر ,2022,ص37

الفرع الأول: أهمية الأمن السيبراني.

للأمن السيبراني أهمية بالغة في الفضاء السيبراني, خاصة ما تعلق بالجانب الوقائي للبيانات و المعلومات, والاتصالات المختلفة وتكمن هذه الأهمية في النقاط التالية:

- توفير نقاط الضعف و الثغرات في الأنظمة و معالجتها.
- توفير بيئة آمنة جداً خلال العمل عبر الشبكة العنكبوتية.
- الحفاظ على المعلومات و تجانسها وسلامتها وذلك بكف الأيادي من العبث بها وتحقيق وفرة البيانات و جاهزيتها عند الحاجة إليها.
- تعرض الأمن السيبراني للاختراق من شأنه أن يحدث الكثير من الأضرار التي تلحق بسمعة الشركة أو المؤسسة وبالتالي تؤثر على مستوى التعاملات التي تقوم بها في الأسواق التجارية[1].

وبالتالي, من الضروري اتخاذ إجراءات قوية لحماية البيانات وحماية سمعة الشركة من خلال الأمن السيبراني.

- يؤدي الاهتمام بالأمن السيبراني إلى الحفاظ على استقرار الأنظمة والشبكات, فعند تعرض الشبكات الرقمية للهجمات السيبرانية, فقد يتعطل النظام بشكل جزئي أو كلي, مما يعرض سير العمل إلى مخاطر ويؤدي إلى توقف الأنشطة, وعندما تكون الأنظمة آمنة ومحمية, يمكن التأكد من استمرار عمليات الشركات والمؤسسات.
- تواجه البنية التحتية للتكنولوجيا السيبرانية تحديات كبيرة من قبل القراصنة والمهاجمين السيبرانيين, فعندما يتم اختراق البنية التحتية, يمكن للهاكرز استغلال الثغرات لسرقة البيانات أو تشويه المعلومات أو تعطيل الخدمات, ومن خلال تطبيق تدابير الأمن السيبراني المناسبة, يمكن حماية البنية التحتية للتكنولوجيا و المحافظة على استمرار توفير الخدمات و المنشآت الأساسية.

[1] عيش موسى, خيمود محمد,الأمن السيبراني,مذكرة ماستر, جامعة مولود معمري,تيزي وزو, كلية الحقوق والعلوم السياسية,تخصص قانون جنائي والعلوم الجنائية,الجزائر,2023,ص18

- يمكن القول أن الأمن السيبراني عاملاً أساسياً لتعزيز التنمية الاقتصادية, فعندما تكون البيئة الرقمية آمنة ومحمية, يمكن للشركات و الأفراد أن يستخدموا التكنولوجيا السيبرانية بثقة ويركزوا على توسيع أعمالهم وابتكار منتجات وخدمات جديدة, أصبحت الحروب السيبرانية تهدد حماية الدول و الأفراد بسبب الانتهاكات الالكترونية حيث وجود ثغرات ضعف تقنية وهجمات إلكترونية لتلحق أضار ذات تكلفة هائلة[1].

ففي عالمنا المترابط بواسطة الشبكة, يستفيد الجميع من برامج الدفاع السيبراني. فمثلاً على المستوى الفردي يمكن أن يؤدي هجوم الأمن السيبراني إلى سرقة الهوية أو محاولات الابتزاز, أو فقدان البيانات المهمة مثل الصور العائلية. كما تعتمد المجتمعات على البنية التحتية الحيوية,مثل محطات الطاقة و المستشفيات, وشركات الخدمات المالية, لذا فإن تأمين هذه المنظمات وغيرها أمر ضروري للحفاظ على عمل مجتمعنا بطريقة آمنة وطبيعية[2].

[1] أسامة بوعرفة,مفاهيم الأمن السيبراني, https://www.noor-book.com . تاريخ الإطلاع01_03_2026, 14:31

[2] لعياشي حمزة , قعفر محمد الأمين,الأمن السيبراني وحماية البيانات الرقمية في الجزائر,مذكرة ماستر,جامعة محمد البشير الإبراهيمي, برج بوعيرج,كلية الحقوق والعلوم السياسية, تخصص قانون الإعلام الآلي وانترنت,2023_2024,ص19.

الفرع الثاني: أهداف الأمن السيبراني.

يهدف الأمن السيبراني بصورة عامة إلى تعزيز حماية جميع ما يتعلق بالدولة من معاملات إلكترونية أو بالأفراد من أجل الحفاظ على سلامة جميع الأنظمة التقنية و جميع مكوناتها من أجهزة و برمجيات ومعدات من أي تدخل خارجي يشكل تهديداً وخطراً على سرية و نزاهة المعلومات والبيانات وسلامتها, ومن أهداف الأمن السيبراني مالي:

- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات, وما تقدمه من خدمات وما تحتويه من بيانات.
- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام و الخاص.
- توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.
- توفير المتطلبات اللازمة للحد من المخاطر و الجرائم السيبرانية التي تستهدف المستخدمين.
- مقاومة البرمجيات الخبيثة, وما تستهدفه من أحداث أضرار بالغة للمستخدمين.
- حماية الأجهزة والشبكات ككل من الاختراقات لتكون ردع واقٍ للبيانات و المعلومات[1].
- تأمين البنى التحتية لأمن المعلومات و البيانات الخاصة بالمواطنين.
- اتخاذ جميع التدابير اللازمة لحماية المواطنين و المستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الانترنت المختلفة.
- "حماية شبكة المعلومات من أي هجوم وذلك بعرفة آخر التقنيات و التكنيكيات الموجودة في هذا المجال ومن أهمها كشف أهداف رسائل هذا العدو و التعرف على طبيعة هذا المهاجم وكذلك ماذا يريد من خلال معرفة تكنيكاته المستخدمة و الأساليب المختلفة لكي يتم العمل على إيقاف هذا الهجوم بأسلوب علمي وتقني مُحكم يمنع هذا الهجوم".

[1] شريفة كلاع. الأمن السيبراني وأشكال التهديد: تحديات عالمية,ألفا للوثائق للنشر و التوزيع,عمان الأردن,الطبعة الأولى,2023,ص80,81.

- حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة, وضمان توافر استمرارية عمل نظم المعلومات.

ترى الدراسة أنه لنجاح أي مؤسسة ينبغي عليها تحقيق الغرض الذي أقيمت من أجله, وهذا الغرض يتحقق من خلاله استقرار المؤسسات و أمانها وأمان عملياتها الأمر الذي يمكن تحقيق من خلال أن تحظى تلك المؤسسات بالأمن السيبراني حيث تأمين بنيتها التحتية فهو أولى الأهداف التي يسعى إليها الأمن السيبراني.

وبالتالي هذا الأمر يساهم في استقرار المنظمات وحماية معلوماتها ومعلومات العاملين بها وبالتالي تحقيق الأمان النفسي للعاملين بجعلهم يبدعون أكثر في أداء مهامهم الوظيفية كذلك أن الأمن السيبراني في حد ذاته يسعى إلى تحقيق الكثير من الأهداف.[1]

[1] فاطمة علي إبراهيم, رحاب يوسف,وليد محمود السيد,"الأمن السيبراني والنظافة الرقمية", المجلة المصرية لعلوم المعلومات,مجلد09,العدد,02,2022,ص399.

الفرع الثالث: أنواع الأمن السيبراني.

وفق ما جاءت به الكثير من الدراسات فإن أنواع الأمن السيبراني كثيرة أهمها الآتي:

1. **أمن الشبكات:** وقد أشير بأن هذا النوع يختص بالحماية و المحافظة على البنية التحتية للشبكات و البيانات التي تسبح فيها من الهجمات السيبرانية, وذلك بواسطة عدة وسائل دفاعية كجدار الحماية والذي يستخدم من أجل منع الوصول غير المصرح به, وكذلك استخدام نظام كشف التسلل السيبراني من أجل رصد الأنشطة المشبوهة والتنبيه من خطرها, وكذلك أمن فبن(Vpn) هذا لأجل تأمين الاتصالات عبر الشبكة الدولية للمعلومات الانترنت.
2. **أمن البيانات:** يقوم هذا الأمن بالتركيز على حماية البيانات من التسريب و التلف أو الاستخدام غير المصرح به, تتم هذه الحماية بعدة وسائل مثل التشفير والذي هو عملية تحويل البيانات الالكترونية إلى رموز غير معروفة و مفهومة من الصعب قراءتها أو معرفتها دون إعادتها إلى سابق ما كانت عليه, والغرض من هذا الأمن هو حماية البيانات أثناء النقل والتخزين, وكذلك بواسطة إدارة البيانات, والتي تهدف إلى ضمان أن البيانات تستخدم وتخزن بشكل آمن, وأيضاً تتم الحماية بواسطة النسخ الاحتياطي [1].
3. **أمن النهايات:** الغرض من هذا الأمن هو حماية الأجهزة المتصلة بالشبكة كالحواسيب و الهواتف الذكية وهذا النوع يستخدم الحماية عن طريق عدة وسائل كبرنامج مكافحة الفيروسات والذي يهدف لمسح ومنع البرمجيات الخبيثة, وكذلك استخدام إدارة التحديثات من أجل التأكد من أن كافة الأجهزة تستعمل أحدث البرامج و الإصلاحات الأمنية, وكذلك بواسطة التحكم في الوصول من أجل ضمان المستخدمين المصرح لهم فقط بإمكانهم الوصول

[1] عطية السحاتي, الأمن السيبراني ودوره في حماية الفضاء السيبراني للمؤسسات التي تعمل في المجال الجوي الوطني, , تاريخ الإطلاع 28_02_2026, 23:16 _ https://www.noor-book.com.

إلى الأجهزة و البيانات, هذا وقد أشير بأن هذه الأنواع من الأمن السيبراني تؤمن الأمن السيبراني كاملاً.

4. **أمن التطبيقات:** وهذا النوع من الأمن السيبراني يستخدم مع مراحل تطوير البرامج وبعد نشرها, ويتم ذلك بواسطة اختبارات الاختراق و التي بواسطتها يتم تحديد الثغرات الأمنية في التطبيقات, وكذلك بواسطة تحديثات الأمان

لغرض إصلاح الثغرات والحفاظ على أمن التطبيقات, وكذلك بواسطة الحماية من البرمجيات الخبيثة من أجل منع تثبيت البرمجيات الضارة.

إذن هناك عدة أنواع للأمن السيبراني وهي أمن البيانات وأمن الشبكات, وأمن التطبيقات و أمن النهايات و الجنود الذين يستخدمون الوسائل الدفاعية و الهجومية هم الفئة التقنية المتخصصين في تقنية المعلومات والحاسوب والاتصالات والتكنولوجيا وسياساتها تضع من متخصصين في الأمن القومي [1].

5. **أمن المعلومات:** عملية تصميم ونشر أدوات لحماية المعلومات الهامة من التلف و التعطيل و التعديل, إذ أنه يحمي سلامة وخصوصية البيانات, سواء في التخزين أو أثناء النقل. ويشمل التشفير وإدارة نقاط الضعف.
6. **الأمن التشغيلي:** عملية إدارة المخاطر لجميع الأمن السيبراني الداخلي, ويشمل العمليات و القرارات الخاصة بمعالجة أصول البيانات وحمايتها, بالإضافة إلى الأذونات التي يمتلكها المستخدمون عند الوصول إلى شبكة, والإجراءات التي تحدد كيف وأين يمكن تخزين البيانات أو مشاركتها.
7. **أمن البنية التحتية:** هو إجراء أمني يحمي البنية التحتية الحيوية, مثل اتصالات الشبكة أو مركز البيانات أو الخادم أو مركز تكنولوجيا

[1] عطية السحاتي, الأمن السيبراني ودوه في حماية الأمن القومي, 2026_02_28 ,23:30 _.-https://www.noor-book.com

المعلومات, وذلك بهدف الحد من نقاط ضعف هذه الأنظمة من الفساد أو التخريب أو الإرهاب. وتشمل البنية التحتية أنظمة الإمداد بالطاقة ونقلها, ونظام التبريد, وإمدادات المياه, وغيرها.

8. **الأمن السحابي:** يتضمن أمان السحابة حماية أنظمة التخزين السحابية الأساسية في جميع الأوقات بسبب الكميات الهائلة من البيانات المخزنة عليها. ويمكن أن يتضمن خدمات الأعمال المخزنة في مركز البيانات[1].

[1] شرح معنى "الأمن السيبراني",https //hbrarabic.com, تاريخ الاطلاع 22:48,01_03_2026

المبحث الثاني: أطر حماية الأمن السيبراني في ظل أنظمة الذكاء الاصطناعي.

يعد كلا من الأمن السيبراني و الذكاء الاصطناعي من صور التطور التكنولوجي الهائل الذي نعيشه منذ سنوات, وقد اكتسبا هذان المجالان شهرة هائلة في التكنولوجيا الحديثة, نظراً لأدوارهما الحاسمة في تشكيل العالم الرقمي, إذ حرصت المؤسسات على الاستعانة بأدوات وأنظمة الأمن السيبراني التي تعمل بالذكاء الاصطناعي حتى تتمكن من اكتشاف التهديدات والاستجابة لها بشكل أسرع, هناك علاقة وثيقة بين الذكاء الاصطناعي والأمن الالكتروني أو السيبراني, إذ يتم تطوير أنظمة الذكاء الاصطناعي التي يمكن استخدامه لتعزيز الأمن السيبراني, إلى جانب تنفيذ تدابير أمنية لحماية أنظمة الذكاء الاصطناعي من الاختراق أو التلاعب. فيعد تزايد الجرائم الالكترونية مثل سرقة البيانات والتصيد الاحتيالي, لجأت المنظمات إلى عدة وسائل لمكافحة تلك التهديدات, فاستعانت بفرق الأمن السيبراني المؤهلة المجهزة بأحدث التقنيات ومنها تقنية الذكاء الاصطناعي, التي تساعد على الكشف السريع عن الأنشطة الضارة ومواجهتها. وتحمي الشبكات من الهجمات الالكترونية, ويعمل الذكاء الاصطناعي في مجال الأمن السيبراني على إنشاء تطبيقات آمنة بشكل افتراضي, تقضي على نقاط الضعف وتزيد من الدقة في اكتشاف المشكلات وتسريع التحقيقات, وأتمتة آليات الاستجابة[1].

وعليه سنتطرق إلى الدور للذكاء الاصطناعي في حماية الأمن السيبراني في (المطلب الأول) ثم العوائق التي تواجه الذكاء الاصطناعي ضمن (المطلب الثاني).

[1] بوالديار نوال,بوالديار فوزي,الذكاء الاصطناعي والأمن السيبراني"المدلول والتحديات", مداخلة في ملتقى وطني,بعنوان تحديات الأمن السيبراني في عصر الذكاء الاصطناعي_علاقة تأثر وتأثير,جامعة الشهيد الشيخ العربي التبسي_تبسة,كلية الحقوق والعلوم السياسية,30_11_2025,ص30

المطلب الأول: الدور للذكاء الاصطناعي في حماية الأمن السيبراني.

يعتبر الذكاء الاصطناعي أحد أهم إنجازات الثورة الصناعية الرابعة, حيث يتوقع أن يستمر في النمو و يكتسب أهمية على مستوى عالمي نظراً للخدمات والتقنيات السريعة التي يوفرها, وعلى الرغم من فوائده, إلاّ أنه يثير تحديات ومخاطر تتعلق بالأمن السيبراني .

لذلك فالحديث عن مستقبل آمن في ظل استخدام الذكاء الاصطناعي يتطلب مواكبة التقدم في هذا المجال عبر وضع قوانين سريعة وفعالة تنظم خطوات تطوير أدوات الذكاء الاصطناعي, كما يتطلب تعزيز التعاون الرقمي بين الدول لإنشاء فضاء الكتروني عالمي مشترك والاستفادة من نقل التكنولوجيا الرقمية ليتماشى مع تطورات الذكاء الاصطناعي ودمجها في بنية النظم الالكترونية [1].

الفرع الأول: الاستخدامات للذكاء الاصطناعي في الأمن السيبراني.

تزداد استخدامات الذكاء الاصطناعي في الوقت الحاضر منها استخدام عمليات تسجيل الدخول الحيوية لخلق عمليات تسجيل دخول آمنة إمّا عن طريق مسح بصمات الأصابع أو شبكية العين أو طبعات اليد, كما يمكن استخدام هذا الأمر بمفرده أو مع كلمة المرور, ويتم استخدامه بالفعل في معظم الهواتف الذكية و الحواسيب الجديدة , لكون عدد من الشركات كانت ضحية لخروقات أمنية عرضّت عناوين البريد الالكتروني والمعلومات الشخصية وكلمات المرور للخطر, وقد كرر خبراء الأمن السيبراني في مناسبات متعددة أن كلمات المرور معرضة بشكل كبير للهجمات السيبرانية, ممّا يهدد المعلومات الشخصية ومعلومات بطاقة الائتمان وأرقام الضمان الاجتماعي وهذه كلها أسباب تجعل تسجيل الهوية الحيوية مساهمة إيجابية من قبل الذكاء الاصطناعي[2].

---

[1] السبتي آسيا, بوقريط عمر, دور الذكاء الاصطناعي في تحقيق الأمن السيبراني,المجلة الدولية للبحوث القانونية والسياسية,المجلد08,العدد03,2024ص16.

[2] علاء عبد الرزاق سالمي, مدخل إلى الذكاء الاصطناعي السيبراني,المنظمة العربية للتنمية الإدارية جامعة الدول العربية,2022ص06.

يسمح استخدام أدوات الفحص للمؤسسات باكتشاف نقاط الضعف الشائعة بشكل استباقي واتخاذ إجراءات للتخفيف من المخاطر المحتملة. ومن بين الثغرات الأمنية الأكثر شيوعاً التي يمكن اكتشافها بواسطة أدوات الفحص المتمثلة في إدارة البرامج والتصحيحات القديمة واحدة من أكثر الثغرات شيوعاً التي يمكن لأدوات الفحص تحديدها هي البرامج القديمة وإدارة التصحيحات الأمنية. لا تقوم العديد من المؤسسات بتحديث برامجها بأحدث التصحيحات الأمنية, مما يجعلها عرضة للثغرات الأمنية المعروفة. يمكن لأدوات الفحص أن تكتشف إصدارات البرامج القديمة والتصحيحات البرمجية المفقودة وتوفر رؤى مهمة لمساعدة المؤسسات على تحديد أولويات إدارة التصحيحات البرمجية. على سبيل المثال, يمكن لأدوات فحص الثغرات الأمنية تحديد الصدارات القديمة من أنظمة التشغيل و خوادم الويب, ممّا يسلط الضوء على الحاجة إلى التصحيح الفوري لمعالجة الثغرات الأمنية المعروفة[1].

يعد الأمن السيبراني أحد التحديات الرئيسية في العصر الرقمي الحديث. وقد أدى ظهور التهديدات السيبرانية المتقدمة إلى ضرورة توفير حلول فعالة لحماية البيانات والأنظمة الهامة. وهنا يأتي دور الذكاء الاصطناعي لتعزيز الأمن السيبراني ومكافحة التهديدات الإلكترونية.

إن التطورات الحديثة في مجال الذكاء الاصطناعي هي المفتاح لتحقيق أمن أفضل في العالم الرقمي؛ حيث يمكن للذكاء الاصطناعي أن يوفر حلولاً ذكية للكشف عن الهجمات الإلكترونية واكتشافها، وحماية البيانات الحساسة، واكتشاف الثغرات الأمنية، وتحليل سلوك المستخدم للكشف عن الاحتيال[2].

[1] معمري حفيظة, مجيدي يحيى, ركابي صدام, آثار الذكاء الاصطناعي على الأمن السيبراني دراسة حالة الجزائري, مذكرة ماستر,تخصص سياسة عامة, جامعة الشهيد حمة لخضر_الوادي,كلية الحقوق والعلوم السياسية,2023_2024,ص40,41.

[2] حنان براهمي, مرجع سابق,ص39.

أولاً:مفهوم التهديد السيبراني.

التهديدات التي تواجهها نظم المعلومات و إمكانية اختراقها بأبعادها المختلفة, وذلك لأن أي اختراق محتمل لهذه الأنظمة يشكل تهديدات أمنية خطيرة، مثل تلك التي تؤثر على حركة الطيران والمعاملات من خلال آليات التجارة الإلكترونية والمصارف والمؤسسات والمنظمات الأخرى التي تستخدم هذه العمليات الأساليب الآلية الحديثة في المعاملات. هذا إضافة إلى إمكانية اختراق منظمات الاتصال والتحكم في إدارتها, فالتهديدات السيبرانية هي استغلال الحاسبات وتكنولوجيا المعلومات في تخريب وتدمير البنية المعلوماتية للخصم ، بل وتعطيل شبكات الدفاع الجوي واختراق أنظمة المعلومات للبريد الإلكتروني لمكاتب رؤساء الدول والتجسس عليهم وفق خطة ممنهجة، وهذا ما تقوم به الولايات المتحدة وأجهزة مخابراتها لزعزعة استقرار البلاد وتقسيمها وتدميرها من الداخل باستخدام بعض مواطنيها وجماعاتها الداخلية للتعدي على إدارة البلاد ونشر الفوضى دون تدخل عسكري يكلف أمولًا وأرواحاً.

فالتهديدات السيبرانية أو الهجمات السيبرانية هي التي تهدد أمن المجتمع وأمن الاقتصاد الوطني والجانب الأمني والعسكري للدول،كما أن للتهديدات السيبرانية أهداف مسطرة، حيث تمس كلا من الجانب المعنوي والجانب المادي وعلى جميع الأصعدة، لكن ما يتوجب على الدول المعرضة لتلك التهديدات وضع خطط إستراتيجية من أجل مكافحتها والتخلص منها[1].

ثانياً:الثغرات الأمنية الشائعة التي تم اكتشافها بواسطة أدوات الفحص.

في البيئة الرقمية اليوم، حيث تتطور التهديدات السيبرانية باستمرار وتصبح أكثر تطوراً الضروري أن تبقى المؤسسات متقدمة بخطوة على نقاط الضعف المحتملة. إحدى الطرق الفعالة لتحديد الثغرات الأمنية في الأنظمة هي من خلال فحص الثغرات الأمنية.

يسمح استخدام أدوات الفحص للمؤسسات باكتشاف نقاط الضعف الشائعة بشكل استباقي

[1] أحمد السيد النجار، محمد عبد الهادي علام, "حروب المعلومات من يواجهها؟"، مجلة الأهرام, العدد 139,يوليو2015. ،ص .26

واتخاذ إجراءات للتخفيف من المخاطر المحتملة التي يمكن اكتشافها يسلط هذا القسم الضوء على بعض الثغرات الأمنية الأكثر شيوعاً بواسطة أدوات الفحص، ويؤكد على أهمية فحص الثغرات الأمنية. (IDRB أفضل ممارسات كشف التسلل والاستجابة له) .

1. _إدارة البرامج والتصحيحات القديمة:

واحدة من أكثر الثغرات الأمنية شيوعاً التي يمكن لأدوات الفحص تحديدها هي البرامج القديمة وإدارة التصحيحات الأمنية, لا تقوم العديد من المؤسسات بتحديث برامجها بأحدث التصحيحات الأمنية، مما يجعلها عرضة للثغرات الأمنية المعروفة. يمكن لأدوات الفحص أن تكتشف إصدارات البرامج القديمة والتصحيحات البرمجية المفقودة وتوفر رؤى مهمة لمساعدة المؤسسات على تحديد أولويات إدارة التصحيحات البرمجية. على سبيل المثال، يمكن لأدوات فحص الثغرات الأمنية و تحديد الإصدارات القديمة من أنظمة التشغيل وخوادم الويب، مما يسلط الضوء على الحاجة إلى التصحيح الفوري لمعالجة الثغرات الأمنية المعروفة.

2. كلمات المرور والمصادقة الضعيفة:

لا تزال كلمات المرور الضعيفة وآليات المصادقة غير الكافية تشكل نقطة ضعف كبيرة للمؤسسات. يمكن لأدوات الفحص تقييم قوة كلمات المرور، وتحديد كلمات المرور الافتراضية أو التي يمكن تخمينها بسهولة، ووضع علامة على الحسابات التي لا تحتوي على سياسات كلمات مرور مطبقة. ومن خلال الكشف عن نقاط الضعف هذه، يمكن للمؤسسات فرض سياسات أقوى لكلمات المرور، أو تنفيذ مصادقة متعددة العوامل، أو إجراء تدريب لموظفين لرفع مستوى الوعي حول أهمية ممارسات المصادقة القوية. على سبيل المثال قد تسلط أداة فحص الثغرات الأمنية الضوء على حسابات المستخدمين التي تحتوي على كلمات مرور ضعيفة مثل "password123"، مما يدفع المؤسسة إلى فرض متطلبات كلمة مرور أقوى[1].

[1] حنان براهمي, مرجع سابق,ص41.

3. إعدادات الأمان التي تم تكوينيا بشكل خاطئ:

يمكن أن تؤدي إعدادات الأمان التي تمت تهيئتها بشكل خاطئ إلى تعريض أنظمة المؤسسة وبياناتها لتهديدات محتملة دون قصد. يمكن لأدوات فحص الثغرات الأمنية أن تكتشف التهيئة الخاطئة في جدران الحماية وأجهزة التوجيه والتحكم في الوصول وإعدادات الأمان الأخرى. يمكن لهذه الأدوات تحديد المنافذ المفتوحة والخدمات غير المرغوب فيها وبروتوكولات التشفير الضعيفة التي قد تجعل النظام عرضة للوصول غير المصرح به أو اختراق البيانات, على سبيل المثال، يمكن لأدوات فحص الثغرات الأمنية تحديد جدران الحماية التي تسمح بالاتصالات الواردة من أي عنوان ، مما يشير إلى وجود خطأ في التكوين يحتاج إلى اهتمام فوري.

4. التصحيحات الأمنية المفقودة:

يعد الحفاظ على تحديث التصحيحات الأمنية المطبقة أمراً ضرورياً لحماية الأنظمة من الثغرات الأمنية المعروفة. ومع ذلك، غالباً ما تواجه المؤسسات صعوبة في تحديد وتطبيق التصحيحات الأمنية اللازمة في الوقت المناسب. يمكن لأدوات فحص الثغرات الأمنية البحث تلقائيا عن التصحيحات الأمنية المفقودة في أنظمة التشغيل وتطبيقات البرامج والمكونات الخارجية. من خلال الحصول على رؤية شاملة للتصحيحات المفقودة، يمكن للمؤسسات تحديد أولويات إدارة التصحيحات وتقليل فرصة المهاجمين المحتملين لاستغلال الثغرات المعروفة[1].

5. إصدارات البرامج الضعيفة:

يمكن لأدوات الفحص أيضاً اكتشاف إصدارات البرامج الضعيفة المعرضة للهجمات والثغرات المعروفة. يمكن لهذه الأدوات أن تقارن إصدارات البرامج المثبتة مع قواعد بيانات

[1] أحمد السيد النجار، محمد عبد الهادي علام,مرجع سابق,ص27.

الثغرات الأمنية لتحديد البرامج التي قد تحتوي على ثغرات أمنية معروفة. على سبيل المثال، يمكن لأدوات فحص الثغرات الأمنية تحديد خوادم الويب التي تشغل إصدارات قديمة من Apache, يحتوي هذا الأباتشي على ثغرة أمنية معروفة يمكن استغلالها للوصول غير المصرح به من خلا تحديد إصدار البرنامج الضعيف، يمكن للمؤسسة اتخاذ إجراءات فورية لتحديث أو استبدال البرنامج المتأثر، مما يقلل من خطر الاستغلال.

تلعب أدوات الفحص الثغرات الأمنية دوراً رئيسيا في تحديد الثغرات الأمنية الشائعة التي يمكن أن تشكل تهديدا خطيراً للوضع الأمني للمؤسسة, ومن خلال الكشف عن البرمجيات القديمة وكلمات المرور الضعيفة والتهيئة الخاطئة والتصحيحات المفقودة وإصدارات البرامج الضعيفة، توفر هذه الأدوات رؤى قيمة تمكن المؤسسات من معالجة الثغرات الأمنية بشكل استباقي وتعزيز الأمن العام من خلال إجراء فحوصات منتظمة للثغرات الأمنية، يمكن للمؤسسات البقاء في طليعة التهديدات المحتملة وتقليل مخاطر الهجمات الناجحة وضمان الدفاع القوي ضد التهديدات الإلكترونية المتطورة[1].

[1] نفس المرجع,ص28.

الفرع الثاني: الأدوار الرئيسية الذكاء الاصطناعي في مجال الأمن السيبراني.

أصبح الذكاء الاصطناعي مؤخراً وسيلة مهمة تستخدم في مجال الأمن السيبراني, وقد بدأت معظم المنظمات باستخدام أنظمة الذكاء الاصطناعي للكشف عن الهجمات السيبرانية والوقاية منها, نتيجة لتزايد حجم وتعقيد هذه التهديدات يومياً. حيث يمكن الذكاء الاصطناعي في صدد هذه الهجمات مايلي:

أولاً: اكتشاف ومنع التهديدات.

_الكشف عن التهديدات: يمكن لأنظمة الذكاء الاصطناعي تحديد المخاطر المعروفة وغير المحددة باستخدام خوارزميات متطورة ونماذج التعلم الآلي (ML) التي تحلل كميات كبيرة من البيانات وتحدد الأنماط التي تشير إلى وجود تهديد. كما يستخدم التعلم العميق (DL) بهدف التعرف على البرامج الضارة, وعمليات التصيد الاحتيالي وغيرها من التهديدات الالكترونية وتصنيفها. بالإضافة إلى استخدام معالجة اللغة الطبيعية لتحليل مصادر البيانات غير المنظمة, مثل مواقع التواصل الاجتماعي والمنتديات الالكترونية ومحتويات الروابط, لتحديد التهديدات المحتملة. كما يمكن لهذه النماذج استخراج المعلومات من البيانات النصية واستخدامها لتحسين دقة كشف التهديدات المحتملة.كما يمكن لهذه النماذج استخراج المعلومات من البيانات النصية واستخدامها لتحسين دقة كشف التهديدات.

_منع التهديدات: يمكن لأنظمة الذكاء الاصطناعي تحديد التهديدات السيبرانية المحتملة واتخاذ تدابير استباقية لمنعها والحد من التسبب بأضرار جسيمة[1].

[1] أحمد محمد, دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني,مجلة العلوم الإنسانية والطبيعية,المجلد06,العدد10,2025,ص367.

ثانياً: الاستجابة للحوادث وتخفيف آثارها.

_الاستجابة التلقائية للحوادث: يمكن للذكاء الاصطناعي أتمتة الرد على حوادث الأمان عن طريق تنفيذ إجراءات محددة مسبقاً بناءً على التهديدات المعترف بها يسرع هذا من أوقات الاستجابة ويقلل من تأثير انتهاكات الأمان.

_ تحليل الأدلة الجنائية بدعم الذكاء الاصطناعي: يساعد الذكاء الاصطناعي في تحليل آثار حوادث الأمان, ممّا يساعد المحترفين في مجال الآمان السيبراني على فهم نطاق الهجوم, وتحديد مصدره, وتنفيذ التدابير اللازمة.

ثالثاً: التحليل التنبؤي وإدارة المخاطر.

_توقع التهديدات المحتملة: يمكن للذكاء الاصطناعي تحليل البيانات التاريخية والاتجاهات الناشئة لتوقع التهديدات المحتملة في المستقبل, يمكن هذا النهج الإستباقي للمؤسسات تنفيذ تدابير وقائية قبل حدوث هجوم.

_تقييم المخاطر وترتيب الأولويات:تقوم أدوات تقييم المخاطر التي تعتمد على الذكاء الاصطناعي بتحديد أولويات الضعف استناداً إلى الأثر المحتمل, ممّا يساعد المؤسسات على توجيه الموارد بفعالية لمعالجة المخاوف الأمنية الأكثر أمية بشكل فعال.

رابعاً: المصادق والتحكم في الوصول.

_المصادقة البيومترية: تعمل أنظمة القياسات الحيوية التي تعمل بالذكاء الاصطناعي على تعزيز مصادقة المستخدم من خلال التحقق من السمات الجسدية أو السلوكية الفريدة[1].

_التحليل السلوكي لتحديد هوية المستخدم: يقوم الذكاء الاصطناعي بتحليل أنماط سلوك المستخدم لتحديد الحالات الشاذة, والوصول غير المصرح به المحتمل, ممّا يعزز تدابير مراقبة الوصول.

[1] نفس المرجع,ص 367.

خامساً:أتمتة الأمن.

_التحديثات و التصحيحات الأمنية التلقائية: يقوم الذكاء الاصطناعي بأتمتة عملية نشر التحديثات الأمانية والتصحيحات تلقائياً, مما يقلل من نافذة الضعف للبرمجيات و الأنظمة.

_المراقبة المستمرة و الأمان التكيفي: يقوم الذكاء الاصطناعي بمراقبة حركة الشبكة وسجلات النظام وأنشطة المستخدمين بشكل مستمر في الوقت الفعلي,متكيفاً مع تدابير الأمان بناءً على التغيرات و التهديدات الناشئة.

سادساً: اكتشاف الاحتيال.

يمكن تدريب أنظمة الذكاء الاصطناعي على التعرف عل احتيالات المعاملات المالية, بما في ذلك احتيال بطاقات الائتمان وغسيل الأموال يمكن للذكاء الاصطناعي اكتشاف الأنشطة المشكوك فيها وإعلام السلطات من خلال دراسة اتجاهات البيانات[1].

سابعاً: التحليل التنبؤي.

تحليل البيانات بطريقة تنبؤية, يتيح للذكاء الاصطناعي اكتشاف التهديدات السيبرانية المحتملة مسبقاً. وتمكين فرق الأمان من اتخاذ إجراءات وقائية باستخدام خوارزميات التعلم الآلي للبحث عن الاتجاهات في البيانات.

ثامناً:دعم التحقيقات.

يمكن للذكاء الاصطناعي المساعدة في التحقيقات في الجرائم السيبرانية من خلال تحليل كميات هائة من البيانات, وإيجاد الأنماط التي قد تشير إلى أصل الهجوم. وهذا يمكن أن يساعد في تحديد هوية المشتبه بهم, وتطوير القضية ضدهم.

[1] بوكر رشيدة, الجرائم السيبرانية وتكنولوجيا الذكاء الاصطناعي,دار إيلياء للنشر والتوزيع,2024,ص,112, 110,111.

وفقاً لتقرير Capgemini حول تطورات الأمن السيبراني, فإن أهم ميزة رئيسية للذكاء الاصطناعي هي الأمن السيبراني, فأهم الوظائف التي تخص الذكاء الاصطناعي في الأمن السيبراني هي:

_يمكن 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 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 تلقائياً وتحليل نشاط الخادم بدقة وتحديد المخاطر المحتملة في حركة المرور المعلومات.

_التوفير و التوفير في التكاليف: تتأثر العديد من المؤسسات مالياً بانتهاك البيانات كل عام, ولا يمكننا تجاهلها ولا إيقاف المجرمين,حيث وجدت الدراسة فرقاً بنسبة 80% من 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 ChatGPT , وعلى الرغم من المخاوف بشأن مخاطر الذكاء الاصطناعي, هناك مزايا مهمة تجعل من ChatGPT أداة مفيدة لصناعة الأمن, واستخدامه له فوائد عديدة في زيادة الإنتاجية, ومساعدة المهندسين, وتدريب الموظفين, إنفاذ 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.[1]

[1] محمد دحماني, الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني,مجلة الفكر القانوني والسياسي,المجلد07,العدد02,2023,ص604,205,206.

الفرع الثالث: تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني.

الأنظمة الخبيرة تُعد من أهم تطبيقات الذكاء الاصطناعي، وتحظى باهتمام خاص نظرًا لدورها المهم في معالجة وحل مختلف قضايا الأمن.

_استخدام أنظمة الأمن السيبراني الخبيرة:

يُعرَّف النظام الخبير بأنه "نظام معلومات حاسوبي يتكون من أدوات تفاعل مع المستخدمين، وأدوات استخدام، وخبرة مهنية. الغرض من النظام الخبير هو تقديم المشورة والحلول للمشاكل في مجال محدد. المشورة المقدمة مشابهة لما يقدمه خبير في ذلك المجال. يمكن للنظام أيضًا حل المشاكل أو توضيح كيفية الوصول إلى حل، وتوفير أدوات لحل مشاكل مماثلة."

يعتمد نجاح الأنظمة الخبيرة على عدة مكونات رئيسية بما في ذلك:

– الخبرة: تشمل هذه المعرفة بالمشكلة، والنظريات، والقواعد، واستراتيجيات حل مختلف المشاكل، وتساعد الخبراء على اتخاذ قرارات أفضل.

– الخبراء: يتمتع الخبراء بالقدرة على تحديد المشكلات وحلها بسرعة وبشكل مناسب، وتفسير الحلول، والتعلم من الخبرة، وإعادة تنظيم المعرفة.

– الاستدلال والتفسير: تمت برمجة النظام للمساعدة في الاستدلال و استخلاص النتائج.

– القواعد واللوائح: تستند أنظمة الخبراء إلى القواعد، وتخزين المعرفة، وإجراءات حل المشكلات.

– القدرة على التفسير: من خلال نظام فرعي يُسمى نظام التفسير، تحاكي أنظمة الخبراء التفكير البشري وتقدم أشكالًا مختلفة من المساعدة المشابهة لما يقدمه الخبير في هذا المجال[1].

1 DJABALLAH Hakima , AHADDAD Mourad, Applications of Artificial Intelligence in Enhancing Cybersecurity A Study of Opportunities and Challenges, Herodotus' Journal of the Human and Social Sciences, Volume: 9 / N°: 5 (2025),p13

وأيضاً هناك مجموعة من الأدوات مفتوحة المصدر متاحة لاكتشاف التزييف العميق للأخبار والتي من بينها نجد مايلي:

_Deep Lab Face: هو برنامج شائع لإنشاء واكتشاف التزييف العميق للأخبار فهو يوفر أدوات لتدريب نماذج التعلم العميق لإنشاء مقاطع الفيديو التي تتم 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.

_Facetorch:يركز على اكتشاف التلاعب بالوجه بالفيديو من خلال مجموعة من الشبكات العصبية لمكافحة مختلف أشكال الغش والتزييف[1].

بالإضافة إلى تطبيقات أخرى تعمل على إثبات الجرائم السيبرانية باستخدام الشبكات العصبية, وهي آلية الكترونية 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 مايلي:

_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.

[1] هاشم عبد الله الحاتم علي,وآخرون,توظيف تقنيات الذكاء الاصطناعي في التحقيق من المحتوى الإخباري بالتطبيق على عينة من الأخبار بموقع جمينة الإخباري,مجلة بحوث ودراسات في الميديا الجديدة,المجلد05,العدد03,2024,ص42.

_شبكة IDS-NNM: عبارة عن نظام لإثبات جرائم الاختراق الالكتروني باستخدام الشبكة العصبية المعتمدة على النمذجة , وقد أثبتت التجارب العلمية فعاليتها في إثبات جميع محاولات الاقتحام في اتصالات الشبكة دون إعطاء أي تنبيهات خاطئة, كما تم استحداث 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 نظراً لقابليتها على الانتقال والتكيف في البيئات التي تم نشرها[1].

[1] حمد عبد الله علي النيادي, الدليل السيبراني المستمد من الذكاء الاصطناعي, المجلة القانونية, المجلد14,العدد2022,04,ص1249

الفرع الرابع: فوائد استخدام الذكاء الاصطناعي في الأمن السيبراني.

تتمثل فوائد استخدام أدوات وأنظمة الأمن السيبراني التي تعمل بالذكاء الاصطناعي فيما يلي:

1- التعامل مع الكثير من البيانات:

يجد موظفو الأمن السيبراني صعوبة كبيرة في مراجعة جميع الأنشطة يدويًا بحثًا عن التهديدات المحتملة، وهنا تتجلى فائدة الذكاء الاصطناعي الذي يقوم تلقائيًا بمسح وتحديد التهديدات ويسهل من عملية الكشف عنها ويعزز من الحماية ضدها.

2- تقليل العمليات المزدوجة:

من أهم فوائد استخدام الذكاء الاصطناعي في المجال الأمني، قدرته على الكشف عن التهديدات الأمنية الأساسية بانتظام ومنعها، إضافة إلى دوره في التحليل الشامل لتحديد الثغرات الأمنية المحتملة، وهو ما يمكّن الشركات من تنفيذ أفضل ممارسات أمن الشبكة دون التعرض لخطر الخطأ البشري أو الملل الذي يصيب موظفي فرق الأمن السيبراني.

3- تسريع أوقات الكشف والاستجابة:

عند قيام الشركات بدمج الذكاء الاصطناعي مع الأمن السيبراني؛ فهي تضمن الكشف السريع عن التهديدات الأمنية والاستجابة لها، لأن الذكاء الاصطناعي يقوم بمسح النظام بالكامل ويحدد التهديدات مبكرًا، ويسهل من المهام الأمنية[1].

[1] الذكاء الاصطناعي والأمن السيبراني: العلاقة والفرق بينهما وتحدياتهما, https://bakkah.com/ar/knowledge-center / تاريخ الاطلاع 14/ 05/ 2026, على الساعة 16:58.

4- محاربة الروبوتات الضارة:

هناك الكثير من الروبوتات التي تُستخدم في الأنشطة الضارة مثل نشر البرامج الضارة وسرقة البيانات، ويمتلك الذكاء الاصطناعي القدرة على تحديد أنماط تلك الروبوتات والتعرف عليها وحظرها.

5- تأمين المصادقة:

يوفر الذكاء الاصطناعي العديد من الأدوات مثل ماسحات بصمات الأصابع والتعرف على الوجه، وهي الأدوات المطلوبة لتأمين المصادقة أثناء محاولات تسجيل الدخول على المواقع التي تحتوي على معلومات حساسة وتتطلب طبقة أمان إضافية للحماية.

وتساعد تلك الأدوات على اكتشاف محاولات تسجيل الدخول الاحتيالية والهجمات الإلكترونية التي تهدف إلى سرقة البيانات.

6- تحسين الدقة والكفاءة:

توفر أنظمة الأمن السيبراني القائمة على الذكاء الاصطناعي دقة وكفاءة أفضل مقارنة بالحلول الأمنية التقليدية، كما تمتلك خوارزميات الذكاء الاصطناعي القدرة على التعرف على الأنماط التي لا تستطيع العين البشرية اكتشافها، وهو ما يزيد من دقة اكتشاف الأنشطة الضارة[1].

[1] الذكاء الاصطناعي والأمن السيبراني: العلاقة والفرق بينهما وتحدياتهما, https://bakkah.com/ar/knowledge-center / تاريخ الاطلاع 14/ 05/ 2026, على الساعة16:58.

الفرع الخامس: أدوات الأمن السيبراني المدعومة بالذكاء الاصطناعي.

الذكاء الاصطناعي يتطلب أمن المؤسسات الحديثة أدوات قادرة على العمل بسرعة فائقة، ومعالجة كميات هائلة من بيانات التهديدات، وتقديم معلومات إستخبراتية قابلة للتنفيذ دون إرهاق فرق الأمن. تلبي حلول الأمن السيبراني المدعومة بالذكاء الاصطناعي هذا المطلب من خلال تحسين دقة اكتشاف التهديدات، وأتمتة إجراءات الاستجابة للحوادث، وتقليل معدلات الإنذارات الكاذبة، وتعزيز الوضع الأمني العام للمؤسسة بشكل منهجي عبر جميع طبقات بيئته

1. حلول أمن نقاط النهاية المدعومة بالذكاء الاصطناعي:

توفر هذه الحلول حماية للأجهزة الطرفية مثل أجهزة الكمبيوتر المحمولة والمكتبية والأجهزة المحمولة من البرامج الضارة وبرامج الفدية. ويقوم الذكاء الاصطناعي بتحليل سلوك الجهاز في الوقت الفعلي، ويستخدم التعلم العميق لاكتشاف التهديدات غير المعروفة قبل تنفيذها .

2. جدار الحماية من الجيل التالي القائم على الذكاء الاصطناعي:

توفر جدران الحماية من الجيل التالي المدعومة بالذكاء الاصطناعي حماية متقدمة ضد التهديدات، ومنع الاختراقات، والتحكم في التطبيقات. فهي تقوم بفحص الحزم بعمق وتحظر التهديدات المعروفة وغير المعروفة قبل وصولها إلى الأنظمة الحيوية.

3. إدارة معلومات وأحداث الأمان (SIEM) :

تقوم حلول SIEM المدعومة بالذكاء الاصطناعي بجمع وتحليل بيانات الأمان عبر البيئة. وهي تعمل على أتمتة فرز التنبيهات، واستبعاد الإنذارات الكاذبة، ومساعدة فرق مركز عمليات الأمن على الاستجابة للتهديدات الحقيقية بشكل أسرع[1] .

[1] الذكاء الاصطناعي في الأمن السيبراني: الفوائد الرئيسية , واستراتيجيات الدفاع والاتجاهات المستقبلية, https://www.fortinet.com/resource , تاريخ الاطلاع 14/ 05/ 2026, على الساعة 23:49.

4. حلول أمن الحوسبة السحابية المدعومة بالذكاء الاصطناعي:

تراقب هذه الحلول بيئات الحوسبة السحابية بحثًا عن بيانات مشبوهة. كما توفر بيانات مشبوهة. كما توفر حماية متسقة وفرضًا للامتثال عبر عمليات النشر متعددة السحابات.

5. حلول NDR المدعومة بالذكاء الاصطناعي للكشف عن التهديدات السيبرانية:

تستخدم حلول الكشف والاستجابة للشبكات (NDR) الذكاء الاصطناعي لمراقبة حركة مرور الشبكة والكشف عن التهديدات التي تتجاوز الأدوات التقليدية. فهي تحدد الحركة الجانبية والنشاط المشبوه، مما يؤدي إلى إطلاق استجابات آلية قبل حدوث الضرر[1].

[1] الذكاء الاصطناعي في الأمن السيبراني: الفوائد الرئيسية , واستراتيجيات الدفاع والاتجاهات **المستقبلية**, https://www.fortinet.com/resource , تاريخ الاطلاع 14/ 05/ 2026, على الساعة 23:49.

المطلب الثاني: العوائق التي تواجه الذكاء الاصطناعي في ضمان الأمن السيبراني.

تتمثل أساساً في عوائق بشرية وأخرى مادية قد تجعل من دور الذكاء الاصطناعي في الأمن السيبراني مهدد ممّا يستدعي مواجهتها والتصدي لها من خلال دراسة هذه التحديات ومحاولة إيجاد حلول لها[1].

الفرع الأول:تحديات الأمن السيبراني في عصر الذكاء الاصطناعي.

على الرغم من أن الذكاء الاصطناعي يوفر فرصاً مهمة لتعزيز فعالية الأمن السيبراني, إلاّ أن التوسع في استخدامه يفرز تحديات متزايدة ومعقدة, إذ بات يشكل أداة ذات استخدام مزدوج, توظف في الحماية والهجوم على حدٍ سواء, الأمر يصعب من عملية التنبؤ بالتهديدات ويزيد من سرعة تطورها وتتمثل أبرز هذه التحديات فيما يلي:

_التحيز في صنع القرار: تثار أسئلة حول المسائلة والمسؤولية في توظيف الذكاء الاصطناعي في مجال الأمن السيبراني, على اعتبار أن أنظمة الذكاء الاصطناعي أصبحت أكثر استقلالية وقدرة على اتخاذ القرارات المستقلة, فمن المسؤول عندما يتخذ نظام الأمن السيبراني المدفوع بالذكاء الاصطناعي قراراً تنتج عنه عواقب غير مقصودة, وبالتالي إن تحقيق التوازن الصحيح بين الاستقلالية والإشراف البشري أمر بالغ الأهمية لتجنب النتائج السلبية غير المقصودة, حيث يمكن أن يؤدي ضعف التفاعل البشري الآلي إلى عدم فعالية التواصل بين أنظمة الذكاء الاصطناعي والقادة البشريين, ممّا قد يؤدي إلى سوء الفهم واتخاذ قرارات غير فعالة وتطبيق قرارات آلية دون تدخل بشري, وتثير هذه المخاوف تساؤلات حول فقدان السيطرة البشرية على الآلات وإمكانية السلوكيات الضارة في المجتمعات.

_أضرار عرضية: قد يؤدي الاعتماد على تقنيات الذكاء الاصطناعي إلى أخطاء فنية وأضرار عرضية, وهذا مثير للقلق بشكل خاص عندما يتعلق الأمر باستخدام البيانات التي تحتوي على

[1] محمد مختار, الأمن السيبراني مفاهيم المستقبل, مجلة اتجاهات الأحداث, العدد02,2025,ص06.

معلومات أو خوارزميات متحيزة في مجال الأمن السيبراني, فقد يؤدي ذلك إلى قرارات تمييزية ضد جماعات أو أفراد معينين وأن تكون لها عواقب وخيمة على المنظمة.

_الأضرار الأخلاقية: يعد البعد الأخلاقي من أبرز التحديات التي تفرض نفسها عند توظيف الذكاء الاصطناعي في مجالات أمن المعلومات, فمع تزايد الاعتماد على الخوارزميات الذكية في اتخاذ قرارات أمنية حساسة, تبرز تساؤلات جوهرية تتعلق بالمسائلة, الخصوصية, التحيز فيمكن أن يؤدي تحيز الذكاء الاصطناعي وانعدام الشفافية إلى استهداف غير عادل كما يمكن أن يؤدي هذا إلى تعريف خاطئ على أنه تهديد داخلي,ممّا يتسبب في ضرر لا يمكن إصلاحه, على سبيل المثال, قد تصنف أنشطة بعض المستخدمين بشكل خاطئ على أنها تهديدات بناءً على أنماط غير موضوعية موجودة في البيانات[1].

_الافتقار إلى 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, إلاّ أن الجهات الضارة تستطيع استخدامها في الوصول إلى المعلومات الحساسة أو مواجهة البنية التحتية.

كما يمكن للمهاجمين السيبرانيين أيضاً الاستفادة من الذكاء الاصطناعي في شن هجمات أكثر تعقيداً من خلال التعلم من البيانات لفهم الأهداف ونقاط الضعف المحتملة بشكل أفضل[2].

_إساءة استخدام الذكاء الاصطناعي: أحد المخاوف المهمة أيضاً هو استخدام الذكاء الاصطناعي في تطوير البرمجيات الخبيثة والهجمات السيبرانية المتطورة,لاستعانة منفذي

[1] سارة بخوش, الذكاء الاصطناعي والأمن السيبراني:الوظائف والتحديات,المجلة الجزائرية للعلوم الإنسانية و الاجتماعية,المجلد09,العدد01,2025,ص145,146.

[2] بن أحمد فاطمة الزهراء, صحراوي بن شيحة, الذكاء الاصطناعي وتحسين الأمن السيبراني للمنظمات: دراسة حالة شركة مايكرسوفت,المجلد11,العدد01,2025,ص284.

الهجمات الالكترونية بأنظمة ذكاء اصطناعي في تهديد البنية التحتية للمؤسسات, وفي هذا تشكل تقنية Deepfake تهديداً كبيراً للأفراد والمنظمات وحتى الأمن القومي,حيث يمكن من خلالها إنشاء محتوى واقعي للغاية.

إضافة إلى أن البيانات التي تتناولها وخوارزميات الذكاء الاصطناعي قد تكون متحيزة ضد أفراد أو مجموعات وفقاً لعوامل ديموغرافية أو ثقافية,ممّا يؤدي إلى تحليلات خاطئة من قبل هذه الخوارزميات.

_تكلفة التنفيذ: إن دمج تكنولوجيا الذكاء الاصطناعي في الأمن السيبراني يمكن أن يكون مكلفاً ويتطلب الكثير من الموارد أجهزة متخصصة, وبنية تحتية داعمة, وقدرة معالجة كبيرة وقوة لتشغيل العمليات الحسابية المعقدة, إضافة إلى مهارات متقدمة في مجالات الأمن والتحليلات والبرمجة والذكاء الاصطناعي, ممّا قد يشكل تحدياً في توفير الموارد البشرية المناسبة[1].

_نقص البيانات الكافية: يحتاج الذكاء الاصطناعي إلى كميات ضخمة من البيانات لتدريب الأنظمة بشكل دقيق. إذا كانت البيانات غير كافية أو تحتو ي على معلومات مغلوطة، فإن قدرة النظام على الكشف عن التهديدات تتأثر بشكل كبير.

_الهجمات المتطورة: الهجمات السيبرانية اليوم أصبحت أكثر تطوراً, وتستخدم تقنيات مثل الهندسة الاجتماعية أو البرمجيات الخبيثة المتقدمة التي قد لا تتمكن أنظمة الذكاء الاصطناعي التقليدية من اكتشافها بسرعة.

_قيود الخوارزميات: قد تحتو ي الخوارزميات المستخدمة في الذكاء الاصطناعي على ثغرات يمكن للمهاجمين استغلالها. علاوة على ذلك، قد تكون الخوارزميات بطيئة في التكيف مع أنواع جديدة من الهجمات.

[1] سارة بخوش مرجع سابق,ص147,148.

_ قضايا الخصوصية والأخلاقيات:استخدام الذكاء الاصطناعي لمراقبة سلوك المستخدمين قد يثير قضايا تتعلق بالخصوصية خصوصاً ا إذا كانت الأنظمة تقوم بتخزين وتحليل بيانات شخصية حساسة[1].

لقد أصبح الفضاء الإلكتروني ساحة المعركة الدولية الخامسة بعد البر والبحر والجو والفضاء يمكن للهجمات التي تستهدف البنية التحتية السيبرانية أن تكون مدمرة لاقتصاد بلدٍ ما، أو مدمرة بشدة لجميع القطاعات القابلة للاختراق إلكترونياً, العسكرية والمدنية على حدٍ سواء.

أولا: أنماط وعوامل تنامي التهديدات السيبرانية.

أ_أنماط التهديدات السيبرانية.

وعلى الرغم من تنوع طبيعتها ومصادرها وأهدافها، مثل التجسس وسرقة المعلومات والحرب، فإن التهديدات السيبرانية تتخذ أشكالاً عديدة وتعتمد العديد من الجهات الدولية الفاعلة على الآليات السيبرانية.

يمكن أن تتخذ الهجمات السيبرانية أشكالاً متعددة، ولكنها تصنف بشكل أساسي في:

_خطر الكوارث الطبيعية أو (العرضية للكابلات البحرية): تلعب الكابلات البحرية دوراً هاماً في توفير خدمات الاتصالات بين الدول في مجالات مثل الانترنت وشبكات الحاسوب منذ عام 2005 ،ولكن على نطاق الانتشار, فقد حدث تحول نحو التقنيات الأخف و الأصغر حجماً وهذه الكابلات عير موجودة في المياه العميقة وبالتالي فهي معرضة لعدد من المشاكل التي تؤثر على البنية التحتية. فقد شهدت دول الشرق الأوسط انقطاعاً مفاجئاً للانترنت بنسبة 80% , وفي يونيو 2005, حدثت 50% من حالات انقطاع الكابلات في المحيط الأطلسي,

[1] هيثم رزق فضل الله,دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني "دراسة تحليلية للتحديات والحلول المستقبلية", المجلة المصرية للدراسات المتخصصة, المجلد13,العدد46,الجزء 05,ابريل 2025,ص1353,1354.

وفي 27 ديسمبر 2006 ،تسبب زلزال في جنوب شرق آسيا في فقدان الاتصال بشبكة الانترنت[1].

ب_عوامل تنامي التهديدات السيبرانية .

لا يزال المهاجمون السيبرانيون يتمتعون بأفضلية على المدافعين بسبب التأثيرات المفاجئة التي لا يمكن أن تقلل من تأثيرها أي أساليب أمنية أو دفاعية سلبية أو إيجابية، كما أن هؤلاء المهاجمين لديهم القدرة على تغطية آثارهم وفي الواقع لقد ساعدت عدة عوامل على تنامي التهديدات السيبرانية لمصالح الدول ، ومن ثم إمكانية بروز حروب سيبرانية، من هذه العوامل ما يلي:

_تزايد ارتباط العالم بالفضاء الإلكتروني (السيبراني)، الأمر الذي اتسع معه خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية في الفضاء السيبراني.

_ تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الإستراتيجية مع تصاعد أدوار الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء السيبراني.

_تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية، الأمر الذي جعل من الممكن الإضرار بمصالحها من خلال الهجمات الإلكترونية في حالات العداء.

_الحرب السيبرانية أقل تكلفة من الحرب التقليدية، حيث يمكن شن الهجمات في أي وقت والوقت اللازم لتنفيذها محدود.

[1] عبد الباسط عيساوي, سفيان زيتوني,آثار الذكاء الاصطناعي على الأمن السيبراني,مذكرة ماستر, جامعة الشهيد حمة لخضر – الوادي,كلية الحقوق والعلوم السياسية, السنة الجامعية2024/2023,ص32.

_لقد أصبحت الحرب الإلكترونية إحدى الأدوات المستخدمة للتأثير على المعلومات المستخدمة في مختلف مستويات ومراحل الحرب الإلكترونية والصراع، سواء على المستوى الإستراتيجي أو التكتيكي العملاتي، بهد التأثير السلبي على هذه المعلومات وأنظمتها العملاتية.

_توظيف الفضاء السيبراني في تعظيم قوة الدول ، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى بالإستراتيجية السيبرانية للدول.

_إن مخاطر الأنشطة العدائية التي تقوم بها الجهات الفاعلة الحكومية وغير الحكومية في الحرب السيبرانية واسعة النطاق. فقد تشن هذه الجهات هجمات سيبرانية من خلا هياكلها الدفاعية والأمنية الخاصة بها، أو قد تجند قراصنة وموالين لشن هجمات ضد الدول المعادية دون روابط رسمية.

ثانيا: الجرائم الإلكترونية و الجوسسة في الفضاء السيبراني.

تتعرض دول مختلفة حول العالم للقرصنة الإلكترونية والتجسس في الفضاء الإلكتروني، والحصول على معلومات استخبراتية عسكرية ومدنية، بل وتنفيذ عمليات تدمير البيانات وتدمير المنشآت. وقد خلقت الاختلافات الوطنية في مجال الحماية وأنظمة الدفاع الإلكتروني، وقدرات الدول الرئيسية في مجال السيطرة على الفضاء الإلكتروني وإدارته وتعرضها لتحديات أمنية متنوعة منها[1].

_استهداف البنية التحتية للدول: أصبحت البنى التحتية الوطنية، المدنية والعسكرية على حدٍ سواء , هدفاً للهجمات السيبرانية ، مثل هذه الهجمات تشل أنظمة الدول، وتفسد أنظمة التشغيل، وتؤثر على تدفق المعلومات وتعطل عمل البنية التحتية الحيوية.

_السيطرة على الأنظمة العسكرية وتعطيلها وإتلافها:ويرجع ذلك إلى إطلاق هجمات إلكترونية من قبل قراصنة محترفين وعسكريين إلكترونيين وعملاء إلكترونيين يهدفون إلى السيطرة على

[1] إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، مجلة اتجاهات الأحداث، ع 22,أوت 2017 ص56

أنظمة القيادة والتحكم عن بعد، مما يؤدي إلى إبعاد بعض أنظمة الأسلحة عن سلسلة القيادة المركزية وإعادة توجيهها ضد أطراف داخلية ودول صديقة. كما يمكنهم أيضا السيطرة على المركبات الجوية غير المأهولة والغواصات النووية في أعماق البحار والأقمار الصناعية العسكرية في الفضاء الخارجي، مما يخرج هذه الأسلحة والمعدات عن سيطرة الدولة التي تنتمي إليها. وتزداد خطورة مثل هذه الهجمات مع تطور التكنولوجيا واستحداث أنظمة لوجستية وأنظمة قيادة وسيطرة .كما تعمل الهجمات السيبرانية على تعطيل الأنظمة الإلكترونية في المنشآت العسكرية الحيوية؛ وتعطيل أو إتلاف شبكات الدفاع عن بعد العسكرية؛ واختراق الشبكات المدنية ذات الصلة بالجيش أو تعطيلها أو تدميرها؛ والتدخل في سلامة البيانات العسكرية الداخلية للدول الأخرى ومحاولة تعطيل أنظمتها أو التدخل فيها.

_سرقة المعلومات والبيانات العسكرية أو التلاعب بها: وفي هذه الحالة، فإن الهجوم الإلكتروني هو محاولة اختراق شبكة مؤسسة عسكرية وسرقة أو تزوير أو تدمير خرائط أنظمة الأسلحة أو مخططات المعدات العسكرية إلكترونيا[1].

جمع معلومات اقتصادية استخباراتية : ويتحقق ذلك من خلال اختراق قواعد البيانات المالية والمصرفية والشركات لجمع المعلومات التي يمكن أن تؤثر على الأمن القومي للدول، أو من خلال التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى .

أدى الهجوم إلى مزيد من النقاش حول طبيعة التهديدات السيبرانية والحاجة إلى تحسين الأمن السيبراني يرتبط هذا النوع من التجسس بصناعات التكنولوجيا مثل البرمجيات والتكنولوجيا الحيوية وتكنولوجيا الفضاء والاتصالات والموارد والطاقة[2].

بالإضافة إلى:

[1] نفس المرجع,ص 57.

[2] حنان براهمي, مرجع سابق,ص38.

– 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 ذلك إلى قرارات تمييزية ضد جماعات أو أفراد معينين وأن تكون لها عواقب وخيمة على المنظمة.

وعلى سبيل المثال، إذا اتخذ الذكاء الاصطناعي قرارًا قائم على المدخلات المتحيزة؛ فقد ينتج عن ذلك منع المستخدمين الشرعيين من الوصول إلى أنظمة الشركة.

– الافتقار إلى 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 ويُفقد 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 إلى المعلومات الحساسة أو مهاجمة البنية التحتية.

كما يمكن للمهاجمين السيبرانيين أيضًا الاستفادة من الذكاء الاصطناعي في شن هجمات أكثر تعقيدًا من خلال التعلم من البيانات لفهم الأهداف ونقاط الضعف المحتملة بشكل أفضل.

– انتهاك خصوصية البيانات:هناك العديد من المخاوف المُثارة 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[1].

[1] الذكاء الاصطناعي والأمن السيبراني: العلاقة والفرق بينهما وتحدياتهما, https://bakkah.com/ar/knowledge-center / تاريخ الاطلاع 14/ 05/ 2026, على الساعة16:58.

الفرع الثاني: سلبيات الذكاء الاصطناعي على الأمن السيبراني.

لا شك أن الذكاء الاصطناعي يعد أداة قوية لتعزيز وتحسين فعالية برامج الأمن السيبراني. ومع ذلك, فإن الإفراط في الاعتماد عليه قد يتحول سريعاً 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 القارات 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, إلاّ أنه لا يخلو من عيوب ومخاطر[1], منها:

- **_ارتفاع التكاليف:** من أبرز مشاكل الذكاء الاصطناعي, ارتفاع التكاليف المطلوبة لإنشاء الأجهزة التي تعمل بهذا النظام , لأن هذه العملية تتضمن صياغة خوارزميات معقدة, إضافة إلى استخدام البرامج والأجهزة الحديثة, وهو ما يزيد من التكاليف سريعاً.

وتعد هذه المشكلة تحدياً هائلاً تواجهه الشركات الصغيرة ذات الموارد المحدودة, وتواجهه أيضاً الشركات الكبيرة, لأن تكلفة تطوير مشروع الذكاء الصناعي قد ترتفع بسبب الميزات أو الوظائف أو النطاق الذي تم تصميمه به, فضلاً عن وجوب تحديث الأجهزة والبرمجيات وإجراء الصيانة للرموز والخوارزميات والبرامج المستخدمة في بناء الأجهزة التي تعمل بهذا النظام.

- **_زيادة البطالة:** من مخاطر الذكاء الاصطناعي أنه قد يتسبب في زيادة معدلات البطالة، نظرًا لزيادة اعتماد المؤسسات على الأجهزة ذات القدرات التشغيلية المستمرة في القيام بالمهام والعمليات المعقدة بدلًا من الموظفين.

[1] وافي حاجة, مرجع سابق,ص104.

- **_ضعف الإبداع** :على الرغم من القدرات التحليلية والتنبؤية التي عُرف بها الذكاء الاصطناعي؛ إلا أن عمل الأجهزة ضمن معايير محددة، أدى إلى افتقارها إلى الحس الإبداعي الذي يمتلكه البشر، إذ تستطيع تلك الأجهزة معالجة وتحليل كميات هائلة من البيانات، ولكنها لا تستطيع محاكاة المهارات البشرية الدقيقة.
- **_عدم وجود تكرار بشري**:على الرغم من قدرة الأجهزة التي تعمل بالذكاء الاصطناعي على القيام بمهام متكررة غير ضرورية؛ إلا أنها لا يمكنها التفكير مثل الإنسان، ولا تستطيع إصدار الأحكام لأنها ليست على دراية بالأخلاقيات، وبالتالي فإذا وجدت حالة لم تتم برمجتها بها؛ فقد تتعطل أو تعطي نتائج لا يمكن التنبؤ بها[1].
- **_الاستخدامات الخاطئة**: الكثير من الاختراعات التي اخترعها العلماء لأغراض هامة, ولكن عندما وقعت في الأيادي الخطأ استغلت للحروب, واستغلال الذكاء الاصطناعي لأهداف غير علمية ولا تخدم المجتمع يشكل تهديداً حقيقياً.
- **_انتهاك الحياة الخاصة وخصوصيات الإنسان**: تعتبر من أهم السلبيات التي ستنتج عن تنامي الذكاء الاصطناعي بدون تقنية ووضع ضوابط وحدود قانونية له, فجميع الخدمات التكنولوجية حالياً والتي يتسع انتشارها بكثرة تفرض على المستخدمين الموافقة على السماح لبرمجيات الذكاء الاصطناعي بسحب بيانات معينة سواء من هاتف المستخدم أو من الوسيلة التي يستخدمها في الوصول لتلك التكنولوجيا,وتقوم بتحليل تلك البيانات والوصول على اهتماماته لاستغلالها في أهداف كثيرة وأهم الأهداف التجارية[2].

[1] ايجابيات وسلبيات الذكاء الاصطناعي, https://bakkah.com/ar/knowledge-center/, 17:47_28/03/2026

[2] عبد العالم حسين الفقيه,وآخرون, الذكاء الاصطناعي_السلبيات والايجابيات وفق رؤية شرعية وقانونية وسبل المواجهة(دراسة تحيلية),مجلة جامعة البيضاء, المجلد07,العدد02,أفريل 2025,ص05

الفصل الثاني

أثر الذكاء الاصطناعي

في تعزيز السيادة الرقمية.

يشهد العالم اليوم ثورة رقمية ضخمة، بفضل التطور التكنولوجي الهائل في مجال الإعلام الآلي والاتصالات وضعت الإنسان في قلب تحولات كبرى وعميقة، شملت وعيه وسلوكه ونظرته للعالم، ومكانته فيه، هذه الثورة جعلت الإنسان يتحول إلى "إنسان رقمي"، بدأت هذه الثورة بانطلاق الحوسبة الرقمية والانترنت وتقنيات الاتصالات في خمسينيات القرن الماضي، ووصلت إلى ذروتها من خلال التطبيقات المتقدمة مثل الذكاء الاصطناعي[1], الذي برز كأحد أهم الركائز التي أعادت تشكيل مفهوم السيادة الرقمية، حيث لم يعد هذا الأخير يقتصر على مجرد التحكم في البنية التحتية المعلوماتية، بل أصبح يشمل القدرة على إنتاج البيانات ومعالجتها وتوظيفها بشكل مستقل وآمن. وفي هذا الإطار، يساهم الذكاء الاصطناعي بدور محوري في تعزيز سيادة الدول على فضائها الرقمي، من خلال تطوير القدرات التكنولوجية الوطنية، وتحسين آليات اتخاذ القرار، فضلاً عن دعم أنظمة الأمن السيبراني.

غير أن هذا التعزيز لا يخلو من تحديات، إذ يطرح الاعتماد المتزايد على تقنيات الذكاء الاصطناعي إشكاليات تتعلق بمدى فعالية الأطر القانونية والتنظيمية في حماية هذه السيادة، خاصة في ظل هيمنة بعض الفواعل التكنولوجية الكبرى واتساع الفجوة الرقمية بين الدول. الأمر الذي يستدعي البحث في الأسس المفاهيمية للسيادة الرقمية، وكذا استعراض مختلف الآليات القانونية المعتمدة لحمايتها في بيئة رقمية متطورة.

وعليه، سيتم في هذا الفصل التطرق أولاً إلى الإطار المفاهيمي للسيادة الرقمية (المبحث الأول)، ثم تحليل أطر حمايتها في ظل تنامي استخدام الذكاء الاصطناعي، مع إبراز أهم التحديات التي قد تحد من فعاليتها(المبحث الثاني).

[1] إيجر أمينة, السيادة الرقمية في العالم المعولة: التحديات و الرهانات, جامعة الجزائر 3,مجلة الدراسات القانونية والسياسية,المجلد 10,العدد 02,جوان 2024,ص 72.

المبحث الأول: الإطار المفاهيمي للسيادة الرقمية.

منذ العقد الأول من القرن الحادي والعشرين, تنافست قوى المؤسسات التكنولوجية العملاقة مع قوى الدول حتى أصبحت تسيطر على الفضاء الرقمي, وتقرر حذف وتعديل المحتوى, وبيع البيانات الشخصية, بل وتمكنت من التأثير حتى على حرية تقدير المصير للأفراد, ممّا أدى إلى ظهور فكرة السيادة الرقمية[1].

وعليه سنتناول في هذا المبحث ماهية السيادة الرقمية في المطلب الأول, أمّا بالنسبة للمطلب الثاني نرى أهميتها بالإضافة إلى أهم معالمها.

المطلب الأول:ماهية السيادة الرقمية.

يعد مصطلح السيادة الرقمية مصطلحاً حديثاً كثر تداوله مع التطور التكنولوجي الهائل لوسائل الاتصال والدور الفعال الذي أضحت تلعبه لا في تقريب الشعوب ببعضها ما جعل العالم قرية صغيرة بل في توجيه الرأي العام والتأثير على سياسات الدول, وعليه لكي نبحث في مفهوم السيادة الرقمية ينبغي البحث في تعريفها مع التعرف على بعض المصطلحات المتقاربة معها.

الفرع الأول: تعريف السيادة الرقمية وأبعادها.

مصطلح السيادة الرقمية يجمع بين لفظين قد يتبادر للوهلة الأولى أنهما ينتميان إلى عالمين أو مجالين مختلفين ومنفصلين تماماً, حيث أن السيادة كمصطلح يمكن إدراجه ضمن اهتمامات العلوم السياسية أو القانونية بينما تعد الرقمنة إحدى اهتمامات العلوم التكنولوجيا الحديثة لذا

[1] سنوسي علي,السيادة الرقمية والاستقلال التكنولوجي بين تحديات الظروف الوطنية والدولية,المجلة الجزائرية للحقوق والعلوم السياسية,المجلد09,العدد02,السنة2024,ص21.

سوف نتطرق إلى تعريف لكلا من المصطلحين على حدى السيادة و الرقمنة (لغة), على أن نفصل في مدلول السيادة الرقمية[1]من الناحية الاصطلاحية والقانونية.

أولاً: التعريف اللغوي.

فتنقسم من حيث اللغة إلى مصطلحين:

أ_السيادة: من سود, يقال: فلان سَيِّد قومه إذا أُريد به الحال, وسائِدُ إذا أريد به الاستقبال, والجمع سَادةٌ, ويقال: سادهم سُوداً سُودُداً سِيادةٌ سَيْدُودة استادهم كسادهم وسوَّدهم هو المسُودُ الذي ساده غيره فالمُسَوَّدُ السَّيِّدُ.

والسَّيِّدُ يطلق على الرب المالك و الشريف والفاضل والكريم والحليم ومُحْتَمِل أذى قومه والزوج والرئيس والمقدّم, وأصله من سادَ يَسُودُ فهو سَيْوِد, والزَّعامة السِّيادة و الرياسة.

وخلاصة المعنى اللغوي للسيادة أنها تدل على المقدم على غيره جاها أو مكانة أو منزلة أو غلبة وقوة ورأيًا وأمراً[2].

ب_الرقمنة: هي نسبة إلى كلمة "رقم" وهي طريقة لتحويل المعطيات والمعلومات إلى أرقام, عادة صفر للسلبي و واحد للإيجابي, وتخزينها داخل ذاكرة الحاسب الآلي, ما يسهل تنقلها عن طريق الشبكة العنكبوتية[3].

ثانياً: التعريف الاصطلاحي للسيادة الرقمية.

تعددت تعريفات السيادة باختلاف المنطلقات الفكرية والظروف المحيطة بنشأة مفهوم السيادة , فكلمة "Sovereignty"الانجليزية مشتقة من الكلمة اللاتنية"Superanus", التي

---

[1] بلحاج خالدية, فرعون محمد, السيادة الرقمية, مجلة البحوث في الحقوق والعلوم السياسية, المجلد11,العدد01,السنة 2025,ص463.

[2] صدام حسين قيراد, الإرهاب السيبراني وتداعياته الرقمية ,Edrrtion Best Book, الجزائر ,2025,ص25,26.

[3] https://WWW.arabicaacademiy,goo,eg,19:34,2026/04/17.

تعني"السمو" أو "الأعلى". وكان أول من استخدم هذا المصطلح هو "جون بودان" في كتابه " الكتب الستة للجمهورية", حيث قدم أول نظرية متكاملة حول السيادة.

كما" وضع جون أوستين" أحد رواد النظرية الكلاسيكية, نظرية السيادة على أساس أن الدولة هي نظام قانوني تتجسد فيه سلطة عليا تعمل كمصدر نهائي للقوة. يعد مبدأ السيادة من الركائز الأساسية التي تعتمد عليها نظرية الدولة, ولا يمكن أن توجد دولة بدون سيادة.

ففي النظام الدولي, شهد مفهوم "السيادة" تحولاً كبيراً من كونه مطلقاً إلى نسبي, وذلك نظراً 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 بعداً جديداً للتفاعلات الدولية, ممّا يتطلب إعادة تقييم آليات السيادة في هذا المجال[1].

أمّا " توماس هوبز" فقد ربط السيادة بالعقد الاجتماعي في كتابه " الليفياثان", إذ رأى أن الأفراد, للخروج من حالة الفوضى الطبيعية سلموا سلطاتهم إلى كيان أعلى هو الدولة, التي تمثل السلطة المطلقة, وهنا تصبح السيادة عند هوبز ضمانة للأمن والنظام وتستمد مشروعيتها من رضا الأفراد عبر العقد الاجتماعي.

كما يذهب" هارولد لاسكي" إلى أن السيادة تعني" القدرة القانونية والسياسية التي لا تعلوها سلطة أخرى داخل الإقليم الوطني". وهي تعاريف تركز أكثر على الجوانب القانونية لممارسة الدولة لحقوق احتكار العنف والقرار على المستوى المحلي[2].

[1] بن قطاط خديجة, تداعيات الحروب السيبرانية على السيادة الرقمية, مجلة القانون العام الجزائري والمقارن, المجلد10,العدد02,ديسمبر 2024,ص287.

[2] سعداوي عمر , السيادة الرقمية في ظل العولمة التكنولوجية والرهانات الجيوسياسية, المجلة الجزائرية للحقوق والعلوم السياسية, المجلد10,العدد02,السنة2025,ص03.

ينظر "بوهل وثيل" إلى استقلال الدولة, والاكتفاء الذاتي الاقتصادي, والحقوق الفردية على أنها جوانب رئيسية للسيادة الرقمية.

وعلى المنوال نفسه , يربط"موربل وتيمرز" أيضاً السيادة الرقمية بمفهوم الاستقلال الاستراتيجي , حيث يعرفها بأنها " القدرة على اتخاذ القرارات والتصرف بشكل مستقل بشأن الجوانب الرقمية الأساسية لمستقبلنا على المدى الطويل في الاقتصاد و المجتمع و الديمقراطية"[1].

ظهر مفهوم "السيادة الرقمية" في أوائل العقد الأول من القرن الحادي والعشرين, وفي عام 2011, قدم "بيير بيلانجر" "Pierre Bellanger", رئيس "", المحاولة الأولى لتعريف مفهوم:" السيادة الرقمية هي في التحكم في حاضرنا ومصيرنا لأنها تعبر عن نفسها ويتم توجيهها من خلال استخدام التكنولوجيات وشبكات الإعلام الآلي".

وتعرف السيادة الرقمية على أنها قيام الدولة ببسط سيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل في الانترنت, حيث أنه لا وجود للسيادة الرقمية لولا وجود الانترنت وتخطيه لحدود السيادة التقليدية المتمثلة في الفضاء المادي للدولة ضمن حدودها الإقليمية.

إن الدولة وفرض ولايتها القضائية على الانترنت من خلال تنظيم فضائها الالكتروني سعيها منها للحفاظ عليه, يكون بعزمها على ضرورة مكافحة الأفعال التي تعرض ثقة وسلامة وأمن المجتمع الافتراضي للخطر.

ويعنى بمفهوم السيادة الرقمية قدرة الدولة على التحكم في البنية التحتية الرقمية الخاصة بها وبيانات مواطنيها.[2]

[1] Gideon Mekonnen ,Iris Reychav,Digital Sovereignty in the Global South : Autonomy in a connected World,Procedia Computer Science 278(2026),p599.

[2] بوخنفر زوليخة, الشبكات المعلوماتية العملاقة على الويب GAFAMوالدولة تحديات السيادة الرقمية, مجلة الدراسات الإعلامية و الاتصالية,المجلد 03,العدد01,مارس 2023,ص99.

ثالثاً: السيادة الرقمية مفهوم ثنائي الأبعاد.

مفهوم السيادة هو مفهوم ذو بعدين السيادة في الرقمية و الرقمية في السيادة.

***أ*_الرقمية في السيادة:** يمكن أن تكون الرقمنة أداة لممارسة السيادة كونها شكلاً من أشكال الديمقراطية أو حتى وسيلة لممارستها.

في الواقع كان الأمر يتعلق بعديد الثورات والتي تم وصفها بأنها ثورات ناقلة لسيادة بل إنها السيادة في أنقى صورها, ويمكن أن تتدخل السيادة في ممارسة الديمقراطية عن طريق التصويت الالكتروني لتدخل التشريعي نتيجة التحكم الرقمي في السلطة بفضل الانترنت. فالانترنت تسمح للمواطنين بالمساواة من خلال التماسات المواطنين ثم جمعها على نحو وثيق وبشكل أعم.

تشكل مواقع المؤسسات السياسية منصة لتواصل وبالتالي يمكن مشاهدة جلسة عامة للجمعية على الصعيد الوطني وكذلك جلسات مجلس الشيوخ وبذلك يكون للمواطنين علماً بجميع القرارات والقوانين.

ب_السيادة في الرقمية: قد تعني السيادة الرقمية المزيد من السيطرة على العالم الرقمي وفوقه أي التحكم في الشفافية في المجال الرقمي أن هذا المفهوم سيؤكد مرة أخرى قدم النماذج التقليدية وتعني السيادة الرقمية أيضاً اتحلاف الحدود الرقمية من خلال إدخال بروتوكولات[1].

[1] سلاوي بشرى وآخرون, مستقبل السيادة الرقمية في ظل التكنولوجيات الحديثة , دراسة تحليلية استشرافية, مذكرة تخرج لنيل شهادة الماستر, جامعة 08 ماي1945, كلية العلوم الإنسانية والاجتماعية,السنة الجامعية 2019_2020,ص60

رابعاً: المفهوم القانوني للسيادة الرقمية.

السيادة الرقمية هي دليل سيادة الدول ، وفي حين أن أدوات سيادتها أصبحت لا يمكن فصلها عن التكنولوجيا الرقمية، فإن الدول تطالب بتوسيع سلطتها التنظيمية على الشبكات في مواجهة هيمنة الكثير من الدول كالولايات المتحدة، ومؤخرا الصين، خاصة وأن الكثير من الدول تحتفظ بمفهوم استبدادي، مما يعني الحق في بسط السيطرة على الفضاءات الرقمية، وتطبيق ما تراه من قوانين لتعزيز مصالحها. ويتبنى آخرون، في أوروبا على سبيل المثال (ألمانيا وفرنسا وغيرها)، نهجا أكثر ليبرالية، لمفهوم السيادة من حق الدولة في حماية مواطنيها وحرياتهم ضد الكيانات الخبيثة أو الكيانات المدفوعة بمصالح تجارية بحتة[1].

يقول د. محمد طه بدوي: " إن السيادة مفهوم قانوني يتمثل به فقهاء القانون منذ أن ابتدعه جون بودان الفرنسي...واقعاً سياسياً معيناً هو القدرة على الإنفراد بإصدار القرار السياسي في داخل الدولة وعلى وجه النهائية في خارجها, ومن ثم القدرة الفعلية على الاحتكار الشرعي لأدوات القمع في الداخل, وعلى رفض الامتثال لأية سلطة تأتيها من الخارج".

وهو نفس ما ذهب إليه شيبانوف "" حين قال بأن السيادة هي قدرة الدولة على اتخاذ القرارات في شؤونها الداخلية و الخارجية باستقلالية عن أي سلطة أخرى في داخل و خارج حدوده[2].

[1] سنوسي علي, مرجع سابق,ص21.

[2] محمد سعادي, القانون الإنسان الدولي, المصرية للنشر و التوزيع,25 فبراير2020,ص10.

السيادة الرقمية ليست مجرد قدرة تقنية، بل هي منظومة متكاملة تشمل السيطرة على البيانات، تطوير البنية التحتية، وتعزيز الأمن السيبراني. يمكن تلخيص أبعاد هذه السيادة في المحاور التالية:

1. **إدارة البيانات والتحكم في تدفق المعلومات** :يتطلب تحقيق السيادة الرقمية وضع سياسات وطنية صارمة تضمن بقاء البيانات داخل الحدود الجزائرية، وفقًا لقوانين تحمي خصوصية الأفراد والمؤسسات. ويشمل ذلك تبني معايير أمنية متقدمة للتحكم في تدفقات البيانات عبر الإنترنت، ومنع الاعتماد على خوادم خارجية قد تشكل تهديدًا للأمن القومي.

2. **استقلالية البنية التحتية الرقمية** :بناء شبكات اتصالات وطنية مؤمنة، وإقامة مراكز بيانات محلية تقلل الاعتماد على الخدمات السحابية الأجنبية، إضافةً إلى تطوير أنظمة تشغيل وبرمجيات محلية تتوافق مع احتياجات السوق الوطنية.

3. **التحفيز الصناعي والتكنولوجي** :دعم الشركات الناشئة في مجال التكنولوجيا، وتعزيز القدرة على تصنيع البرمجيات والمعدات الرقمية محليًا، مع التركيز على تطوير الكفاءات الوطنية في مجالات الذكاء الاصطناعي، الحوسبة السحابية، وأمن المعلومات[1].

4. **توطين التكنولوجيا** :من خلال نقل المعرفة التقنية إلى الجزائر، ودعم إنشاء مراكز بحثية متخصصة في التقنيات الحديثة لضمان تقليل الاعتماد على الشركات الأجنبية.

[1] يعقوب حرتم,السيادة الرقمية في الجزائر: بين التحديات الراهنة وآفاق الاستقلال التكنولوجي, https://tkawen.online/ تاريخ الاطلاع 22/ 04/ 2026, على الساعة 12:31.

5. **تطوير استراتيجية أمن سيبراني متكاملة** :تتضمن حماية الأصول الرقمية الوطنية من الاختراقات والهجمات السيبرانية، من خلال تأهيل كوادر محلية متخصصة، واعتماد تقنيات التشفير القوية لتعزيز أمن البيانات[1].

فالأمن السيبراني وضع آليات دفاعية وهجومية لمواجهة محاولات الاختراق، القرصنة، أو التلاعب بالمعلومات.

على سبيل المثال، عندما تقوم شركة أجنبية بتخزين بيانات ملايين المواطنين في خوادم خارجية، فإن ذلك يعرّض هذه البيانات لمخاطر سياسية وأمنية. ومن هنا، تعمل العديد من الدول على فرض قوانين تلزم الشركات باستخدام خوادم محلية، أو على الأقل ضمان تشفير البيانات ومنع الوصول غير المصرّح به[2].

الفرع الثاني: بعض المصطلحات المشابهة لمصطلح السيادة الرقمية.

برزت عدة مصطلحات متقاربة مع مفهوم السيادة الرقمية تعكس أبعاد التحكم في الفضاء الإلكتروني وإدارته. وتساعد هذه المصطلحات على توضيح مختلف الجوانب التقنية والقانونية المرتبطة بحماية البيانات، واستقلالية الدول في المجال الرقمي.

1. **_السياسة الرقمية:** يعتبر الكثيرون السياسة الرقمية على أنها مجموعة من المبادئ التوجيهية القانونية و الإجرائية التي تستند إلى التطبيق التجاري المجدي للتكنولوجيات

[1] يعقوب حرتم,السيادة الرقمية في الجزائر : بين التحديات الراهنة وآفاق الاستقلال التكنولوجي, https://tkawen.online/ تاريخ الاطلاع 22/ 04/ 2026, على الساعة12:31.

[2] قاسم دنش,السيادة الرقمية: معركة الدول لحماية بياناتها في عصر الذكاء الاصطناعي, https://www.almayadeen.net/reports, تاريخ الاطلاع 22/ 04/ 2026, على الساعة21:30.

الرقمية, ووفقاً للباحثّين والمؤلفّين يشمل موضوع السياسة الرقمية للتكنولوجيات الرقمية ظواهر الاقتصاد الرقمي ، وتحديد آثار الرقمنة، طبيعة وخصائص الفجوة الرقمية، الجوانب المختلفة والمترابطة للحياة الرقمية، والإشارة إلى التناقضات في الطرق التي تؤثر بها موارد المعلومات على العمليات الاجتماعية، والنمو الاقتصادي، والبنية الاقتصادية، والتطوير المنهجي للجودة في مجتمع المعلومات, بالإضافة ,إلى ذلك, تم توضيح مكونات حاسمة لإنشاء السياسة الرقمية، أبرزها أن تتضمن السياسة الرقمية نوع تكنولوجيا المعلومات المستخدمة (التقنيات الخلوية على سبيل المثال)، الاعتماد على نموذج المجتمع الرقمي المختار ،حيث توجد ثالثة نماذج يمكن استخدامها لتشكيل اقتصاد المعلومات :مجتمع المعلومات، الرقمنة على نطاق واسع، الرقمنة على نطاق صغير، ربط التغييرات الحالية بطبيعتها الهيكلية و الابتكارية .

2. _**التحول الرقمي:** هو الانتقال من استخدام الأساليب التقليدية إلى الاعتماد على التكنولوجيا داخل المؤسسات والقطاعات المختلفة، وذلك بهدف تعزيز الكفاءة التشغيلية وتحسّين وتوسيع الخدمات المقدمة للأفراد ويشمل هذا التحول مواءمة التقنيات الرقمية مع استراتيجيات الأعمال، لتعزيز وتحسين كفاءة العمليات[1].

كما يقصد به السعي إلى تحقيق إستراتيجية المنظمات وتطوير نماذج الأعمال و التشغيل المبتكرة و المرنة من خلال الاستثمار في التقنيات و تطوير المواهب و إعادة تنظيم العمليات و إدارة التغيير لخلق قيمة و خبرات جديدة للعملاء و الموظفين و أصحاب العلاقة , يبدأ أساساً من وجود إستراتيجية تعمل على تحقيق الهدف الأساسي من التحول الرقمي وهو خدمة الإنسانية و في ذات الوقت مساعدة المنظمات على البقاء و الاستمرار في ضوء العمل الأخلاقي, ومن الخطأ أن نعتقد أن رقمنة البيانات بمعنى تحويل النظم القديمة سواء كانت نظم يدوية أو نظم معلومات تقليدية إلى بيئة الأعمال

[1] بن بية عادل ، بلقرشي إيمان , السياسة الرقمية في الجزائر بين التحول المنشود وتحديات السيادة الرقمية, مجلة الناقد للدراسات السياسية, المجلد09 / العدد: 01(2025),ص57,58.

الالكترونية تعمل في ظل تكنولوجيا المعلومات إنه تحول رقمي. حقيقة الأمر فإن تقنية المعلومات تعتبر أمر ضروري وحيوي لنجاح التحول الرقمي[1].

3. _**الردع الالكتروني:** الردع تعني كبح أو وقف اندفاعه, كف وزجر ومنع و يقال عملية رادعة أي عملية تجربها القوات الأمنية لصد هجوم مرتقب, وهو كل إجراء أو تصرف يؤدي إلى إقناع طرف إلى الكف عن إتيان سلوك ما, وقد يكون تهديداً أو تشريعاً أو قراراً أو غيرها.

أمّا في الشؤون السياسية الدولية فيعرفه الجنرال "أندريه بوفر", بأنه: " منع دولة معادية من اتخاذ قرار باستخدام أسلحتها أو بصورة أتم منعها من العمل أو الرد إزاء موقف معين باتخاذ مجموعة من التدابير والإجراءات التي تشكل تهديداً كافياً حيالها, والنتيجة التي يراد الحصول عليها بواسطة التهديد هي نتيجة سيكولوجية نفسية".

وتعد نظرية الردع "Deterrence theory" إستراتيجية عسكرية ظهرت من خلال الحرب الباردة ويستخدم هذا المصطلح للإشارة إلى الإستراتيجية المحتملة لإلحاق ضرر للمتعدي مع التأكيد له بإمكانية تجنب هذا الضرر أو دفعه"[2].

4. _**الاختراق:** الاختراق بشكل عام هو القدرة على الوصول لهدف معين والدخول على الأجهزة بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بها بهدف التطفل على خصوصيات الآخرين و إلحاق الضرر بهم, ويطلق على المخترق مصطلح (Hacker) وحينما يتمكن المخترق من إحداث الأضرار كحذف ملفات أو تشغيل ملفات مؤذية أو وضع وزراعة ملفات تجسسية (أحصنة طروادة) أو فيروسات أو أي نوع من هذه الأنواع فهو مخرب(Cracker) ويتم الاختراق عن طريق معرفة الثغرات الموجودة في

[1] حسين مصيلحي, التحول الرقمي الإطار المستقبلي لنظم وتكنولوجيا المعلومات,دار الكتب و الوثائق,الطبعة الأولى,2024,ص12.

[2] بلحاج خالدية, فرعون محمد,مرجع سابق, ص466.

النظام والتي غالباً ما تكون في المنافذ أو (Ports) الخاصة بالجهاز, ويمكن وصف هذه المنافذ بأنها بوابات للكمبيوتر على الشبكة العالمية تسمح لها بالدخول[1].

فيتم اختراق الشبكات والتجسس عبر اختراق الأنظمة والحصول على بيانات حساسة في مجالات متعددة, تستغل لاحقا في تحقيق أهداف اقتصادية وأمنية, وفي حالات أخرى يتم تدمير أو تعديل البيانات المخزنة, من خلال تغييرها بما يخدم الجهة المهاجمة أو محو محتواها بالكامل[2] .

5. **السيادة في البيانات:** تشير السيادة في البيانات إلى قدرة الدول أو المؤسسات على التحكم الكامل في بياناتها، من حيث التخزين، المعالجة، والتحليل، مع ضمان الالتزام بالقوانين المحلية وحماية الخصوصية.

هذا المفهوم يرتبط بشكل وثيق بتقنيات حديثة مثل مراكز البيانات المحلية (Local Data Centers)، النماذج اللغوية الضخمة (Large Language Models – LLMs) ، و حوكمة الذكاء الاصطناعي.(AI Governance) وتشمل عنصرين:

_إقامة البيانات (Data Residency) وذلك لتحديد مكان تخزينها وضمان خضوعها للقوانين المحلية,

_خصوصية البيانات (Data Privacy) وذلك بحماية حقوق الأفراد ومنع إساءة استخدامها وفقًا للتشريعات.

وتكمن أهميتها في:

_تعزيز الأمان الرقمي:(Digital Security) تخزين البيانات محليًا في مراكز بيانات

[1] أحمد سعيد فرحات السرجاني,التحول الرقمي في تحقيق الأمن السيبراني,دار العلم والإيمان,2025,ص178.

[2] الشيماء مخالفية, كريمة لعيساوي, السيادة الرقمية: تكيف العقيدة الدفاعية الجزائرية مع التهديدات الأمنية الجديدة , المجلة الجزائرية للعلوم الاجتماعية و الإنسانية, المجلد13, العدد02(2025),ص394.

آمنة يقلل من المخاطر الأمنية الناتجة عن الاعتماد على مزودي خدمات خارجيين.

_حماية الخصوصية:(Privacy Protection) يضمن التحكم المحلي الالتزام بالقوانين الوطنية المتعلقة بحماية البيانات مثل لوائح (GDPR) أو القوانين المحلية.

_تعزيز الاستقلال التقني:(Technological Independence) الاعتماد على مراكز بيانات وتقنيات ذكاء اصطناعي محلية يقلل من التبعية للجهات الخارجية ويعزز الابتكار الداخلي.

_تطوير النماذج اللغوية الضخمة:(Large Language Models - LLMs)

السيادة في البيانات تلعب دورًا أساسيًا في تدريب النماذج اللغوية باستخدام بيانات محلية تعكس الثقافة واللغة الخاصة بكل مجتمع، مما يضمن تطوير تقنيات تخدم الاحتياجات المحلية.

_تمكين الابتكار:(Innovation Enablement) مع التحكم الكامل في البيانات، يمكن للمؤسسات الاستفادة منها في تطوير تطبيقات ذكاء اصطناعي مخصصة لحل تحديات محلية.

السيادة في البيانات لم تعد مجرد مفهوم أو فكرة، بل أصبحت ضرورة ملحة لضمان الأمان الرقمي، حماية الخصوصية، وتعزيز الابتكار في عصر الذكاء الاصطناعي. فالدول اليوم تسعى إلى بناء أنظمتها الذكية الخاصة بها عبر تعظيم الاستفادة من مواردها الرقمية والتحكم الكامل في بياناته[1].

[1] مجدل القحطاني, ماهي السيادة في البيانات؟,https://www.linkedin.com/posts/dr-mejdal , تاريخ الاطلاع 24 04 2026,على الساعة 16:34.

الفرع الثالث:العلاقة بين السيادة والرقمنة.

تطور مفهوم السيادة، أي سلطة الكيان الحاكم على حكم نفسه دون تدخل خارجي، من التقليدي على قدرة الحاكم على اتخاذ القرارات النهائية إلى رؤية تؤكد وتركز على السيادة الشعبية, حيث أصبحت السيادة اليوم تشير في المقام الأول إلى استقلال الدولة, أي السيادة الشعبية وتمتع المواطنين في حق تقرير المصير من خلال ممارسة حقوقهم غير القابلة للتصرف .

بالنسبة للخطاب الأول, المسمى بالاستثناء السيبراني, أن المجال الرقمي يختلف اختلافاً جوهرياً عن المجال التناظري, مما يستلزم النظر إلى البيئات الرقمية بشكل مختلف عن جميع التطورات التكنولوجية السابقة, وقد اكتسب هذا الإطار المفاهيمي أهمية ملحوظة خلال انتشار الانترنت التجاري في التسعينات, إلاّ أنه لا يزال يتجلى في المناقشات العامة و الأكاديمية وتستند أيديولوجية الاستثنائية السيبرانية إلى الاعتقاد بأن الأهمية المتزايدة لاتصالات الشبكات عبر الحاسوب تعني تآكل سيادة الدولة.

تعد حوكمة الانترنت متعددة الأطراف تهديداً ثانياً أقل مباشرة للسيادة بالمعنى التقليدي, وينصب التركيز هنا على المسؤوليات العديدة غير السيادية التي يجب على الحكومات الاضطلاع بها ضمن إطار تنظيمي حيث يرى حوكمة مسؤولية المتأثرين بها بشكل مباشر, بدلاً من التركيز على قصور الدول في إدارة الشؤون الرقمية, وقد تطورت منذ بدايات المجتمع التقني العديد من العمليات اللامركزية, التي اتسمت بالكفاءة واتخاذ القرارات القائمة على الجدارة[1].

[1] بن بية عادل ، بلقرشي إيمان , مرجع سابق,ص59

الفرع الرابع: نشأة السيادة الرقمية.

يمر مفهوم السيادة الرقمية باضطرابات تأثر عليه وتغير من جوهره, وذلك بسبب ثورة المعلومات والاتصالات والتقنيات الرقمية هذه الظاهرة التي يعود تاريخها إلى نهاية التسعينات والتي لا تزال تتطور إلى اليوم.

يعود منشأ المصطلح إلى فرنسا حتى انتشر مفهوم السيادة الذي ارتبط بالرقمنة والتكنولوجيا تدريجياً في أوائل العقد الأول من القرن الحادي والعشرين, ودعا العديد من الخبراء والمراقبين إلى إعادة النظر في مفهوم السيادة التي ستصبح أدواته الأساسية قريباً لا تنفصل عن التكنولوجيا وهذا يعني إعادة تنظيم المشروع الديمقراطي بما في ذلك مسألة إدارة الانترنت والشبكات والكمبيوتر وتطوير دستور الانترنت على أساس المبادئ المشتركة وصيغت في اتفاق دولي 2009 خلال ندوة نظمت طرح وزير الداخلية إشكالية عن هذا المفهوم مشيراً إلى أن سيادة الدولة تمارس على الإقليم بينما تتجاهل الانترنت حدود الدولة الجغرافية كما تساءل أيضاً عما إذا كانت سيادة الدولة تتوقف حيث يبدأ الفضاء الرقمي كما أكّد على ضرورة توسيع مجال سيادة القانون إلى الفضاء الرقمي.

وهنا عرفها الفرنسي بيير بيلانجر على أنها " السيطرة على حاضرنا ومصيرنا كما يتجلى ويسترشد باستخدام التكنولوجيا وشبكات الكمبيوتر"[1].

وبعد قضية سنودن الشهيرة تم تأسيس العديد من الجمعيات والمجالس والمعاهد تحت اسم السيادة الرقمية والغرض من ذلك التفكير من أجل تنظيم الحياة المدنية في عصر الرقمنة والتعريف بتحديات السيادة الرقمية لعامة الجمهور و المسؤولين, وكذلك اقتراح تدابير قادرة على

[1] نفس المرجع,ص59.

تعزيز السيادة سواء الجماعية أو الفردية وعلى الهياكل الملموسة وتعريف قيمة البيانات الرقمية للمواطنين.

وتم تعميم المشكلة على مستوى دول الاتحاد الأوروبي أين قامت بعدة تقارير صدر من مجلس الشيوخ الأوروبي والتي قام بنشرها معنوناً ذلك بعبارة الاتحاد الأوروبي مستعمرة رقمية أخرى دور جديد و إستراتيجية جديدة للاتحاد الأوروبي في حكم عالم الانترنت, وإن المؤسسات الأوروبية مدعو إلى النظر في السيادة في بعدها الرقمي والوقوف أمام التحديات التي تواجهها[1].

المطلب الثاني: أهمية السيادة الرقمية و معالمها.

أمام الثورة الرقمية الحديثة التي أفرزت وجود فضاء سيبراني يقوم على أساس بنية عالمية لتكنولوجيا المعلومات والاتصال، شهد العالم سباقًا متسارعًا للتحكم في هذا الفضاء[2].
حيث أصبحت الدول تعتمد بشكل متزايد على الأنظمة الرقمية في إدارة شؤونها الاقتصادية والإدارية والأمنية. كما أدى هذا التطور إلى بروز تحديات جديدة تتعلق بحماية البيانات وضمان استقلال القرار الرقمي. وفي هذا السياق، تبرز السيادة الرقمية كضرورة حتمية لضمان تحكم الدول في بياناتها وبناها التحتية الرقمية، وحماية أمنها القومي من مختلف التهديدات السيبرانية.

الفرع الأول: أهمية السيادة الرقمية.

وتتجلى أهمية السيادة الرقمية في نواحي عدة نذكر منها.

[1] سلاوي بشرى وآخرون, مرجع سابق,ص54,55.

[2] نريمان فتيئية, خولة هاني,الحرب السيبرانية من منظور القانون الدولي التنظيم الدولي وسبل الواجهة,المكتبة الوطنية الجائرية2023,تاريخ النشر جوان 2023,ص14.

_القضايا الاقتصادية: لا يوجد مجتمع آمن من التجسس العلمي و الاقتصادي و التجاري, وعليه فحماية الشركات وسرية البيانات ضرورية, والسيادة الرقمية هي الوسيلة الأمثل لمكافحة استرداد, واستخدام البيانات لأغراض تجارية وتسويقية.

_التحديات السياسية: السيادة الرقمية وسيلة للإدارة وحماية المؤسسات قصد استعادة الثقة للمواطنين, والمشاركة في حماية خصوصياتهم وبياناتهم الشخصية, وحماية البنى التحتية الحرجة للدول.

_قضايا الأمن القومي: واجهت الدول و الشركات والمواطنين تهديدات كبرى وما فضيحة Cambridge Analytica إلا خير دليل على ذلك بفعل استخدام البيانات لتأثير على نوايا التصويت.

ناهيك عن الجرائم القرصنة و التلاعب والتخريب و الإرهاب, وما إلى ذلك من سرقة هوية احتيال بالبطاقة المصرفية...مما جعل من أمن الكمبيوتر قضية وطنية وهنا تكمن أهمية السيادة الرقمية في تحقيق هذا الأمن للفضاء الالكتروني, سواء بالنسبة للمواطنين أو الشركات أو الدول.

_الرهانات الإستراتيجية: من خال تجنب تسرب البيانات إلى الخارج وخاصة الولايات المتحدة الأمريكية, ومن المهم الحفاظ على قدرة مستقلة في اتخاذ القرار و العمل, ومن الضروري الحفاظ على السيادة الوطنية في مواجهة التهديدات الجديدة الناتجة عن الرقمنة المتزايدة للمجتمع[1].

وتكمن أهميتها أيضاً في.

_حماية البيانات الوطنية والمؤسسية:

[1] سلاوي بشرى وآخرون,مرجع سابق,ص57.

غالبًا ما تستغل تهديدات الأمن السيبراني غموض الاختصاص القضائي. عندما توجد معلومات حساسة على البنية التحتية التي تحكمها القوانين الأجنبية، فهناك خطر كبير من الوصول غير المصرح به أو الإفصاح عن البيانات القسرية أو الاعتراض. تهدف السيادة الرقمية إلى سد هذه الفجوات من خلال توطين البيانات وتأمين الأنظمة البيئية الرقمية من التأثير القانوني أو التكنولوجي الخارجي.

_تمكين الامتثال القانوني والتنظيمي:

مع استحقاق أطر العمل مثل لائحة حماية البيانات العامة (GDPR) ومشروع قانون حماية البيانات الشخصية في الهند، يتعين على المؤسسات الاحتفاظ بالبيانات داخل مناطق جغرافية محددة وبموجب ضمانات قانونية محددة. تدعم الأطر الرقمية السيادية الامتثال لهذه التفويضات، مما يضمن احترام ممارسات معالجة البيانات لقوانين الخصوصية والأمن المحلية.

_الاستقلالية الإستراتيجية والمرونة الاقتصادية:

تمكّن السيادة الرقمية الدول والمؤسسات من السعي نحو الاعتماد على الذات التكنولوجية. من خلال تعزيز الابتكار الأصلي في الخدمات السحابية وأدوات الأمن السيبراني والبنية التحتية القطِع الملموسة للحاسوب، يمكن لأصحاب المصلحة تخفيف الاعتماد على مقدمي الخدمات الأجانب الذين قد يكونون عرضة للعقوبات أو تجسس أو القيود التجارية.

كما تعزز هذه الاستقلالية الاستقرار الاقتصادي من خلال دعم الصناعات المحلية ورعاية النظم البيئية التقنية المحلية وبناء قوى عاملة سيبرانية ماهرة قادرة على استدامة البنية التحتية السيادية دون الاعتماد على الدعم الأجنبي[1].

[1] جو لي ,ما المقصود بالسيادة الرقمية؟, https://www.trendmicro.com/ar_sa/what-is/data-sovereignty/digital-sovereignty.html , تاريخ الاطلاع 22/04/2026,على الساعة 22:00

الفرع الثاني:معالم السيادة الرقمية.

يقصد بالمعالم هي المظاهر التي تتجلى من خلالها السيادة الرقمية, أي كيف تتحقق السيطرة و التحكم في المجال الرقمي سواء من طرف الدولة أو الأفراد أو الشركات.

تتحدد المعاني التي توضح معالم السيادة الرقمية في نقاط رئيسية تكمن في:

أولاً: السيادة الرقمية هي سيادة الدول.

والتي تطالب بها الدول, فهي المؤتمر العالمي للاتصالات الدولية عام 2012 أعلنت الصين وروسيا والمملكة السعودية على سبيل المثال أنها تريد استعادة حقوقهم السيادية على الشبكة العالمية, ويمكن أن تكون السيادة الرقمية أيضاً مطالبة جماعية, بالسيادة الجماعية, من قبل مجموعات من المستخدمين الرقميين الذين يزعمون أنهم مرتبطون بتحديد القواعد المعمول بها والمشاركة في تنظيم حماية بياناتهم على الشبكات, والاعتراف بحق مجتمعات المستخدمين في التنظيم الذاتي أو التأثير على قيادات اتخاذ القرار.

لقد تغيرت الطريقة الكلاسيكية في تشكيل المجتمعات في العالم الرقمي فلقد تم الانتقال إلى المجتمعات الرقمية المدنية السياسية في الفضاء العمومي الرقمي, ممّا يؤدي إلى التفكير في السيادة الشعبية على مستوى مجتمعات المستخدمين الذين يتخلون عن حرية الانترنت مقابل القواعد المتفق عليها[1].

ثانياً: السيادة الرقمية هي سيادة فردية.

من حيث قدرة الفرد على تقرير مصيره ليأمر بنفسه لتحكم في بياناته, ويتجسد ذلك في حرية اختياره لمحركات البحث و كذلك من حيث قبول أو رفض شروط الاستخدام العامة, هل هو قادر على الحفاظ على سرية اتصالاته, والتحكم في بياناته أو أنشطته على محركات البحث

[1] سلاوي بشرى وآخرون, مرجع سابق,ص58.

التي يتم الكشف عنها من قبل الشركات التقنية الأجنبية بشكل عام, هل يستطيع أن يختار ما يريد قراءته والدروس التي يرغب في تعاملها, والفنادق التي يرعب في الإقامة فيها, إذن يجب على الفرد أن يفكر في طريقة يواجه بها استبداد الخوارزميات.

تنعكس هذه السيادة في المطالبة بحقوق معينة منها حرية الوصول إلى الانترنت والحق في حماية البيانات الشخصية, والحق في تقرير المصير الإعلامي.

وتظهر معالم هذه الفكرة أيضاً من خلال تأملات فكرة الحكم الذاتي الرقمي, الذي يجعل السيادة الرقمية ممكنة, واستعادة السلطة للأفراد من خلال التكنولوجيا الرقمية, ويتجلى ذلك بشكل خاص في تمكين الأفراد من التحكم التام في جميع التكنولوجيات ومواكبة التطور.

ثالثاً: السيادة الرقمية في سيادة الشركات.

وهي التي تستحوذ حرفياً على العالم الرقمي, ولديهم في الواقع القدرة على التحكم في المستخدمين, وفرض قواعد عليهم لإثبات وجودهم.

يشير البروفيسور بلاندين إلى أن الدول تتنافس في قدرتها على القيادة و الامتثال من قبل الشركات التقنية التي تتمتع بالسيادة بفضل مركزهم المهيمن في العالم, وقد مست التطورات التكنولوجية حالياً جميع مجالات الحياة منها التجارة و رقمنة التراث, ومكافحة الجريمة و الأمن, وإنتاج العملة الرقمية ومعلومات السكان, وتنظيم الاتصالات والسياسات الصحية و النقل, وتمارس سلطة هذه الشركات بشكل جيد على الإقليم غير المادي, وعلى السكان ومستخدمي الانترنت[1].

[1] نفس المرجع,ص59.58.

المبحث الثاني: أطر حماية السيادة الرقمية في ظل الذكاء الاصطناعي.

السيادة الرقمية أصبحت تواجه تحديات متزايدة في ظل التطورات السريعة لاستخدامات الذكاء الاصطناعي, حيث يفتح هذا التطبيق مخاطر في مجال الأمن القومي, عليه وجب البحث أكثر في الآليات الكفيلة بالكشف عن مختلف المخاطر الناجمة عن الاستعمال السيئ المحتمل لتقنيات الذكاء الاصطناعي و الأطر القانونية لتعزيز السيادة الرقمية للدولة على الصعيد الوطني و الدولي.و التي توجه كيفية التحكم الدولي , حيث أن لا يمكن تحقيق السيادة الرقمية بشكل كامل دون أساس قانوني متين. توجه الأطر القانونية الوطنية و الدولية كيفية تحكم الدولة في بيئتها الرقمية, لا سيما في مجالات مثل إدارة البيانات, والجرائم الالكترونية, و الاتصالات عبر الانترنت[1].

المطلب الأول: الهجمات السيبرانية .

إن القيام ببعض الأفعال المرتبطة باستعمال الأدوات الاتصالية لاسيما الانترنت, هو اعتداء على السيادة الرقمية للدولة, إذ أصبحت هذه الأفعال اليوم تعتبر جرائم جديدة تتوفر على جميع أركان الجريمة وتسمى "الجريمة المعلوماتية".

الفرع الأول: الجرائم الماسة بسرية وسلامة نظم المعلومات.

هذا النوع من الجرائم يشمل الدخول الغير مشروع, الاعتراض الغير مشروع, المساس بسلامة البيانات, المساس بسلامة النظام المعلوماتي, إساءة استخدام الأجهزة.

أ: الدخول الغير مشروع.

نصت اتفاقية "بودابست" (الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية, بتاريخ 08/11/2001)على هذه الجريمة في المادة الثانية تحت عنوان " الدخول غير القانوني"،

[1] Salah Ghechir , Digital Sovereignty and Cyber Security:Legal and Strategic Implication For Algeria,university of Algiers1,journal of the Human and Sociall Sciences,volume 09,N:05(2025),p03

وأشارت المذكرة التفسيرية الاتفاقية بودابست بأن الدخول غير المشروع يعد الجريمة الرئيسية التي تنطوي على التهديد والتعدي على الأمن المعلوماتي، بمعنى السرية والسالمة وإتاحة النظم والبيانات المعلوماتية، إذ أن هذا الدخول يمكن أن يترتب عليه الوصول إلى بيانات سرية مثل كلمة المرور, فتعرضت الكثير من أنظمة الحاسبات الآلية، وبصفة خاصة تلك التي تعمل من خلال شبكات المعلومات، إلى اختراق بواسطة أشخاص تقنية أنظمة المعلوماتية وما في حكمها لعام 2004 في المادة الثالثة:" كل من دخل عمدا وبغير وجه حق موقعا أو نظاما معلوماتياً يعاقب بالحبس.. والغرامة.... أو بإحدى هاتين العقوبتين"وجرمت هذه الجريمة أيضا في المادة 06من الاتفاقية العربية(المتعلقة لمكافحة جرائم تقنية المعلومات, المؤرخة في ديسمبر 2010).

ب: الاعتراض غير المشروع.

يمكن أن يطلق عليها تسمية جريمة التجسس المعلوماتي والاعتراض غير القانوني للبيانات وهي التسمية التي اعتمدتها اتفاقية بودابست، فالتجسس من العمليات القديمة حيث كان الإنسان يتجسس على أعدائه لمعرفة أخبارهم والخطط التي يعدونها لمهاجمته، ولهذا كان للتجسس أهميته الكبيرة على كافة مستويات النزاعات الإنسانية التي مر بها البشر منذ بدأ الخليقة. لقد كان نتيجة الثورة المعلوماتية وانتشار شبكات الاتصالات وتزاوجها مع شبكات المعلوماتية وظهور شبكة الانترنت هدفا للمحتالين ومحترفي الأعمال التجسسية ، فكان نتيجة استخدام الشبكات المعلوماتية ومنه ازدهرت وتحولت وسائل التجسس والتصنت من الطرق التقليدية إلى الطرق الإلكترونية , فقد أدى الاستخدام المتزايد للحاسبات الآية تضرر في المجال العسكري والاقتصادي والسياسي والصناعي والإداري و حتى الشخصي، فبظهور الحسابات بدأت مسألة الحصول على المعلومات تأخذ أبعادا جديدة، حيث تطورت أساليب جمع هذه المعلومات حيث" باتت هذه الأساليب تعتمد اعتمادا كبيرا على التكنولوجيا الرقمية" [1].

[1] شحيرط أحمد ,قريبيز مراد, مخبر الحقوق والعلوم السياسية,جامعة الاغواط الجزائر,تحديات الانترنت لسيادة الدول(السيادة الرقمية),مجلة البحوث القانونية والاقتصادية,المجلد05, العدد01, السنة2022,ص305.

ج:المساس بسلامة البيانات.

إن ما يسمى "الخصوصية الرقمية" هي و صف لحماية البيانات الشخصية للفرد، والتي يتم نشرها وتداولها من خلال وسائط رقمية، وتتمثل البيانات الشخصية في كل البيانات التي نستخدمها في تفاعلنا على الانترنت أثناء استخدامنا للحاسب الآلي أو أي من وسائل الاتصال الرقمي بالشبكة العنكبوتية، فسياسة التجسس الرقمي، التجسس، أو "المراقبة" – كما تطلق عليه الحكومات– هي متابعة ورصد ألداء وأنشطة الأفراد في تفاعلهم مع حياتهم اليومية، وقد توسع استخدام الحكومات للتجسس على مواطنيها أو حتى مواطنين دول أخرى معا التطور التقني ، حيث انه في منتصف العقد الأخير من القرن العشرين تبنت الحكومات تقنيات أكثر تطورا لمجاراة انتشار استخدام الهاتف المحمول و الإنترنت[1].

د :المساس بسلامة النظام.

قد تستهدف الجرائم الواقعة على النظام المعلوماتي التي إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي، وهذه المكونات هي تلك المعدات التي تستخدم في تشغيله كالأسطوانات و الشرائط و الكابلات...إلخ .كأن تكون محلاً للسرقة أو الإتلاف العمدي كإحراقها أو إفساد أسطوانات التشغيل المغناطيسي بتعريضها إلى أي مجال مغناطيس متلف إما جرائم الاعتداء على المكونات المنطقية، فهي تقع إما على البرامج التطبيقية و إما على برامج التشغيل،أما جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي فتتم من خلال التلاعب بالمعلومة فيها أو عن طريق إتلافها

[1] نفس المرجع,ص307.

هـ :إساءة استخدام الأجهزة.

جرائم إساءة استعمال الأجهزة أو البرامج المعلوماتية وجرائم كل من قدم أو أنتج أو وزع أو حاز بغرض الاستخدام جهازا أو معلوماتياً أو أية بيانات معلوماتية معدة أو كلمات سر أو كودات دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقا.

وتتمثل في تقديم أو إنتاج برامج أو توزيع أجهزة معلوماتية لأغراض سيئة وتدخل ضمنها أيضاً بيع كلمات الأسرار و البيانات للأشخاص دون وجه حق ما يسهل اختراق المواقع و الحاسبات الخاصة وبالتالي انتهاك خصوصية الأشخاص و بياناتهم الرقمية سواء أجريت المعالجة الالكترونية بواسطة شخص خاص أو عام, فهو ما قد يؤدي إلى تلف البيانات و ضياعها[1].

الفرع الثاني: الهجومات على نظم المعلومات.

شهد العالم المعاصر تطورًا متسارعًا في مجال تكنولوجيا المعلومات، مما جعل نظم المعلومات ركيزة أساسية في تسيير مختلف القطاعات الحيوية، سواء الإدارية أو الاقتصادية أو الأمنية. غير أن هذا الاعتماد المتزايد عليها جعلها عرضة لمخاطر متعددة، أبرزها الهجومات السيبرانية التي تستهدف سلامة البيانات وسرية المعلومات واستمرارية الأنظمة. وتتنوع هذه الهجومات من حيث طبيعتها وأساليبها، حيث قد تأخذ شكل اختراقات غير مشروعة، أو فيروسات معلوماتية، أو هجمات تعطيل الخدمة وغيرها . حيث أنه تعتبر الهجومات مناورة هجومية تستهدف أنظمة معلومات الكمبيوتر أو البنية التحتية أو شبكات الكمبيوتر , فالمهاجم هو شخص أو عملية تحاول الوصول إلى البيانات أو الوظائف أو المناطق المحظورة الأخرى في النظام دون الحصول على إذن، ويحتمل أن يكون ذلك بقصد ضار , يمكن استخدام الهجوم

[1] بلحاج خالدية, فرعون محمد,ص470,471.

الإلكتروني من قِبل دول ذات سيادة أو أفراد أو مجموعات أو مجتمع أو منظمات أو حتى عصابات، وقد تنشأ هذه الهجمات الإلكترونية (السيبرانية) من مصدر مجهول[1].

أولاً:الهجوم الإلكتروني.

يعني استخدام الطاقة الكهرومغناطيسية أو الأسلحة المضادة للإشعاع لمهاجمة الأفراد و المرافق بهدف إضعاف القدرة القتالية للعدو وتقليل استخدامه الفعال للطيف المغناطيسي. تشمل هذه الهجمات التشويش و التضليل الكهرومغناطيسي. وعادةً ما تؤدي الخسائر الناتجة عن الهجوم الالكتروني إلى خسائر مادية كبيرة, على عكس الحروب التقليدية التي تتضمن خسائر بشرية. ومن أمثلة الهجوم الالكتروني تعطيل أنظمة الدعم اللوجستي لتقليل دعم للقوات المعادية وخفض فاعليتها, والتحكم في أنظمة توليد الكهرباء[2].

ثانياً: التجسس الالكتروني انتهاك للسيادة الرقمية.

يعتبر التجسس الإلكتروني أحد أهم المراحل التمهيدية للعمليات الحربية السيبرانية، ويعرف على أنه وسيلة لاعتراض غير مصرح به لأنظمة الاتصالات والشبكات والبيانات بهدف الحصول على معلومات والتلاعب بها, ويعد التجسس الالكتروني من أولى أشكال التهديد التي تمس الأمن القومي الوطني، وتشكل خطراً على مصالح الدول والأفراد[3] .

كما يشير التجسس السيبراني إلى المحاولات المتعمدة لاختراق أجهزة الكمبيوتر والمواقع الإلكترونية الخاصة بالدولة المنافسة أو الخصم، بهدف سرقة معلومات سرية. يسعى هذا النوع من التجسس للحصول على قاعدة بيانات ضخمة تتعلق بالأنظمة والأسرار العسكرية والسياسية

[1] هجوم سيبراني,https://ar.wikipedia.org/wiki تاريخ الاطلاع 01/05/2026, على الساعة 18:55.

[2] بن قطاط خديجة, مرجع سابق,ص 290.

[3] كريم رقولي , لخضر نويوة،الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية .مجلة طبنة للدراسات العلمية الأكاديمية. المجلد 2 ،العدد 02, 2019 ص،74.

والأمنية والاقتصادية والصناعية[1] . أمّا التجسس على الشبكات ويقصد به الدخول غير المصرح والتجسس على شبكات الخصم، دون تدمير أو تغيير في البيانات. والهدف منه الحصول على المعلومات قد تكون خطط عسكرية أسرار حربية، اقتصادية، مالية، أو سياسية، مما يؤثر سلباً وأيضاً الدخول على مهام الخصم، إلى الأنظمة الخاصة للدول لإضعافها وضرب المصالح القومية لها، من قبل الدول التي تريد للقوى العظمى زوال مكانتها[2].

في العصر الحالي، أصبح التجسس يتجاوز النطاق العسكري والحربي ليشمل مجالات متعددة مثل الاقتصاد، التكنولوجيا، السياسة، والصناعة. ورغم أن التجسس العسكري لا يزال يحتل مكانة هامة و يعتبر من أخطر أنواع التجسس، إلا أن طبيعة المعلومات المطلوبة اليوم قد تغيرت بشكل كبير. في الماضي، كانت المعلومات السرية تتمحور حول حجم الجيوش وتجهيزاتها، وكانت هذه المعلومات تعتبر بالغة الأهمية. أما الآن، فقد أصبحت هذه البيانات متاحة بشكل أوسع، حيث تنشر في الصحف ووسائل الإعلام، وتظهر الخرائط التي تمثل توزيع القوات في مناطق النزاع و تناقش بشكل علني. التجسس الحديث يركز أكثر على المعلومات الدقيقة والمتقدمة، مثل التكنولوجيا العسكرية الحديثة، البيانات الإستراتيجية الاقتصادية، والمعرفة المتعلقة بالتطورات العلمية والصناعية. هذا التغيير يعكس التحولات الكبيرة في مفهوم الأمن القومي وأهمية المعلومات في العصر الرقمي[3] .

[1] شريفة كلاع، الأمن السيبارني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد 15 ،العدد 1 ،2022 ،ص 295.

[2] هناء رشيد محيسن كزار, التهديدات السيبرانية وأثرها على العلاقات الأمريكية الصينية, الجامعة العراقية مجلة كلية القانون والعلوم السياسية, العدد 28 السنة 2025,ص398.

[3] سامية بوشوشة، حياة سلماني، التجسس الالكتروني وطرق مكافحته، مجلة العلوم الاجتماعية والإنسانية، جامعة تبسة، المجلد 16 ،العدد 1 ، 2023, ص54.

ثالثاً: الاختراق الالكتروني.

هو عملية دخول غير مصرح بها إلى الأنظمة الإلكترونية المختلفة وأجهزة الكمبيوتر، وذلك من خلال تحديد بعض الثغرات في الشبكات حيث يتم استغلالها في عملية القرصنة واختراق المعلومات والبيانات الحساسة .

علمًا بأن على الرغم من كون هذا المصطلح يشير إلى العديد من الأشياء السلبية إلا أنه يكون مفيد في بعض الحالات المعينة لكنه يرتبط بشكل كبير بالدلالات السلبية والجرائم الإلكترونية .

علاوة على أن هناك العديد من أنواع الاختراقات الالكترونية التي يتم الاستعانة بها لسرقة البيانات وتحقيق أهداف معينة [1].

يتضمن اختراق الأنظمة للحصول على معلومات استخباراتية عن دولة أو منظمة، فهو نظام أو برنامج مصمم لاستغلال بيانات الخصم وإلحاق الضرر بها، بالإضافة إلى تعطيل نظامه الحاسوبي، بهدف التفوق عليه في المجالات الأمنية، العسكرية، والسياسية. تتم هذه العملية على مستويات متعددة، سواء كانت فردية، مؤسسية، أو على مستوى الدول. يأخذ الاختراق الإلكتروني أشكالًا متنوعة، لكنه يسعى في النهاية إلى الوصول إلى المعلومات الحيوية للخصم والاستيلاء عليها، من خلال استخدام أنظمة حاسوبية تستهدف البنية التحتية المعلوماتية للجهة المقصودة [2].

---

[1] أنواع الاختراقات الالكترونية أبرز الهجمات السيبرانية,https://routesa.ap , تاريخ الاطلاع 01/05/2026, على الساعة 19:55.

[2] بن قطاط خديجة, مرجع سابق,ص291.

تتعدد أنواع الاختراقات الالكترونية التي يتم اللجوء إليها لهدف معين لتشمل كل من ديدان الكمبيوتر التي تعتبر من أبرز أنواع الاختراقات الالكترونية التي تهدف إلى سرقة البيانات والمعلومات وتعطيل الشبكات، ويكون ذلك عن طريق استغلال جميع ثغرات الأمان الموجودة في الأجهزة والأنظمة، وهي من البرامج الذكية التي تنتشر عبر الأجهزة وتتكاثر بشكل تلقائي دون حاجة إلى مستخدم .

بالإضافة إلى الفيروسات التي تعتبر كأحد أنواع الاختراقات الالكترونية التي تهدف إلى تعطيل الأنظمة وتدمير البيانات، وهي برامج خبيثة تنتقل إلى الأجهزة بشكل تلقائي عند فتح ملف مصاب بأحد الفيروسات، ويمكنها نسخ نفسها من أجل الانتشار عبر أجهزة أخرى .

كما تعد حجب الخدمة كذلك من بين أهم أنواع الهجمات الإلكترونية التي تؤدي إلى إيقاف الخدمات من الوصول إلى العملاء المستحقين وحجبها عن المستخدمين، وذلك عن طريق زيادة الضغط على الخوادم وزيادة حجم الطلب مما يؤدي إلى تعطيل الخدمة .

تعتبر برامج التجسس من أخطر أنواع الاختراقات الالكترونية التي تهدف إلى التجسس على الأنشطة الشخصية، وكذلك سرقة المعلومات في حالات التجارة غير القانونية، ويتم استخدام برامج خبيثة من أجل جمع البيانات والمعلومات التجارية الخاصة بالشركات الكبرى وكذلك البيانات الشخصية .

كما تعمل هجمات التصيد على الإيقاع بأحد الأفراد أو المؤسسات المحددة، ويكون عن طريق إرسال رسائل احتيالية تبدو أكثر مصداقية أو مجموعة من الروابط التي تخترق معلومات حساسة على الأجهزة الإلكترونية عند النقر عليها [1].

[1] أنواع الاختراقات الالكترونية أبرز الهجمات السيبرانية,https://routesa.ap , تاريخ الاطلاع 01/05/2026, على الساعة 19:55.

رابعاً: الهجمات على البنية التحتية الحيوية.

قد تبدو هجمات الحرمان من الخدمة ذات ضرر نسبي ضئيل في الفضاء السيبراني للدول، لكنها قد تسبب تكاليف وخسائر مادية كبيرة إذا استمر انقطاع الخدمة لأسبوع كامل. وإذا استهدفت الهجمات البنية التحتية، فإن الخسائر على أرض الواقع تكون هائلة، خاصة عند استهداف العمليات الصناعية والأنظمة الإدارية المرتبطة بها. على سبيل المثال، يمكن لمجموعة من الهاكرز التلاعب بالأنظمة الخاصة بالطاقة، مثل أنابيب نقل النفط والغاز، ومصانع إنتاج الوقود، ومحطات توليد الكهرباء[1].

بغض النظر عن العدد الدقيق للأنشطة والعمليات الإلكترونية التي تستهدف البنية التحتية الحيوية، فقد وقعت العديد من الحوادث الفعلية التي تبرر القلق المتزايد بشأن تأمين هذه البنية التحتية التي أصبحت مترابطة بشكل متزايد. على سبيل المثال، في أوائل عام 2020 ،أجبرت هجمات الجرائم الإلكترونية التي استهدفت مستشفى جامعة برنو في التشيك المستشفى على تعليق العمليات الجراحية المجدولة وتحويل المرضى إلى مرافق أخرى قريبة. وفي حادثة أخرى قبل أربع سنوات، أبلغت شركة توزيع الكهرباء الأوكرانية عن انقطاع في الشبكة دام عدة ساعات نتيجة هجوم إلكتروني استهدف أجهزة الكمبيوتر وأنظمة التحكم الإشرافي وجمع البيانات (SCADA5)، مما تسبب في انقطاع التيار الكهربائي عن حوالي 225,000 عميل[2].

خامساً: القرصنة الالكترونية.

نشأت القرصنة الالكترونية من عالم الجرائم الالكترونية التي تدور في الفضاء الرقمي,في حين لم تنشأ ظاهرة قرصنة أسماء النطاقات مع تأسيس منظمات مثل ICANN, بل ظهرت مع

[1] نور الدين حامد علي إبراهيم، الفضاء السيبراني: المفاهيم والأبعاد، المجلة العلمية للبحوث والدراسات التجارية، جامعة حلوان، المجلد 38 ،العدد 02, 2024,ص 738 ، 737.

[2] Lee, Robert M., Michael J. Assante & Tim Conway. 2016. 'Analysis of the Cyber Attack on the Ukrainian Power Grid.' SANS & E-ISAC, 18 March. As of 21 October 2020: https://ics.sans.org/media/EISAC_SANS_Ukraine_DUC_5.pdf, Accessed on: September 01, 2024

نمو الانترنت و ظهور التجارة الالكترونية . في البداية, عندما لم تكن الشركات التجارية تدرك تماماً أهمية التواجد في الفضاء الالكتروني و الفرص التجارية التي يمكن جلبها من خلال امتلاك أسماء النطاقات, واجهت مشكلة بالغة الخطورة, وهي القرصنة الإلكترونية لأسماء النطاقات.

يقصد بقرصنة أسماء النطاقات قيام فرد أو كيان قانوني بتسجيل علامة تجارية أو اسم تجاري مملوك لشخص آخر كاسم نطاق, ثم تأجيره أو عرضه للبيع أو حتى بيعه لمنافس وتشير الدراسات إلى أن أول حالة قرصنة الكترونية لأسماء النطاقات حدثت عام 1978 من قبل إحدى شركات الهاتف الأمريكية المحلية, لذا تعتبر الفترة بين عامي 1980 و 1989 العصر الذهبي للقرصنة الالكترونية[1].

تهدف القرصنة الالكترونية إلى المساس بالسرية وخصوصية الأفراد، أو التأثير على سلامة المحتوى من خلال تغييره أو إتلاف .لا تقتصر القرصنة على المعلومات الشخصية للمواطنين فحسب، بل تتجاوز ذلك من خلا الكشف عن أسرار أمن الدول واختراق مواقع المؤسسات الحكومية والبريد الإلكتروني لبعض قادة الدول حول العالم، خاصة قادة تلك الدول التي عانت حروبا أهلية. فقد شهدت السنوات العشر الأخيرة تسريبات غير مسبوقة تتسم بالطابع السري وبأدق التفاصيل حول شخصيات دولية مستهدفة بهدف للإطاحة بها أو خلق مشاكل واضطرابات داخل الدول التي ينتمون إليها .

سادساً: الهجمات على الأنظمة العسكرية.

تستهدف أنظمة التحكم بالأسلحة، الأقمار الصناعية، أو أنظمة الاتصالات العسكرية لتعطيل العمليات الحربية، فالهجمات على العمليات العسكرية والحكومية تشمل استهداف الأنظمة بشكل يومي، وغالبا ما تكون جزءا أساسياً منها للتجسس. هذه الهجمات تهدف إما

[1]Hajar KERMECHE , Rawia YAHIA, Technical Protection of Digital Intellectual Works ,Banta 01 University Algeria, Revue des Sciences Humaines, Vol –36 N°4, December 2025– p 104,105.

للحصول على تصاميم الأسلحة، أو الحصول على معلومات سرية، أو لفهم طريقة تفكير العدو أثناء نشوب حرب، أو لمعرفة الخطط العسكرية وتمركز القوات. لذلك، أي شبكة متصلة بالانترنت تكون عرضة للهجوم، وحتى تلك التي لا تكون متصلة قد لا تكون بمنأى عن الخطر. تعتمد الحكومات والجيوش على هذه الشبكات في أوقات السلم، ولكن هذا لا يعني أن الاعتماد عليها في حالة الحرب آمن. في الواقع، قد تنقلب ميزة التكنولوجيا العسكرية المتقدمة للجيوش الحديثة إلى كارثة في حال تعرضها لهجمات سيبرانية تؤدي إلى تعطيلها .

هذه بعض الصور التي تعكس الأشكال المختلفة للحرب السيبرانية التي تعتمد على التقنيات الرقمية للتأثير على الدول والمنظمات، حيث هذه الصور تعتبر تحدياً حقيقياً للسيادة الرقمية، وتتطلب استجابة فعالة من الحكومات لتعزيز الأمن السيبراني وحماية البيانات والمعلومات الحساسة[1].

المطلب الثاني:الآليات الإقليمية والدولية للحفاظ على السيادة الرقمية.

تحتاج الدول إلى تطبيق سياسات واستراتيجيات شاملة متعددة الأبعاد ومختلفة المستويات لتحقيق سيادتها الرقمية، تحمل خططاً مستدامة تهدف إلى تعزيز القدرة السيطرة على التكنولوجيا الرقمية وحماية البيانات و المعلومات الوطنية، و تكون بمثابة خط الدفاع الأول ضد أي تهديدات، وهي أيضاً المنطلق الرئيسي لنشر الوعي وتحقيق الكفاءة الرقمية والمحافظة على سيادة الدولة في فضائها السيبراني، ويمكن تصنيفها إلى سياسات مجابهة محلية ودولية[2].

الفرع الأول:الأطر القانونية لتعزيز السيادة الرقمية.

اعترافاً ضمنياً بحساسية موضوع السيادة الرقمية وأهميته البالغة, سعت دول العالم إلى تكريس الحامية لسيادتها الرقمية وذلك بانتهاج أساليب و آليات مختلفة سواء في الشق القانوني

[1] بن قطاط خديجة, مرجع سابق,ص292,293.

[2] ايجر أمينة, مرجع سابق,ص80.

أو التشريعي أو في شقها التنظيمي من خلال إنشاء هيئات وأجهزة توكل لها مهام الحماية والحفاظ على السيادة الرقمية للدول من أي انتهاك[1].

أولاً:المنظومة التشريعية لأمن أنظمة المعالجة الآلية للمعطيات.

حاول المشرع الجنائي الجزائري مواجهة المساس بالأمن القومي في شقه المتعلق بالمساس بأمن الأنظمة المعلوماتية من خلال حماية المعطيات والبيانات عند معالجتها بالطرق الالكترونية عند إقدامه على تعديل قانون العقوبات رقم 15_04 المتعلق بالتوقيع والتصديق الالكتروني المعدل بموجب القانون 24_06 تناوله في المادة 394 مكرر, و المادة 394 مكرر 01, المادة 394 مكرر 02, والمادة 394 مكرر 03 [2].

نجد أن المشرع الجزائري جرم هذا الفعل الاعتداء على المعطيات ليس ليحمي نظام البيانات من الناحية المادية أي البرامج والتطبيقات ، بل ليوفر الحماية للمعلومات الموجودة داخل النظام ذاته ضد أي نشاط إجرامي ، حيث نص المشرع الجزائري على هذه الجريمة من خلال نص المادة 394 مكرر 1 من قانون العقوبات[3].

نص القانون رقم 25_14 المتعلق بالإجراءات الجزائية الجزائري على إمكانية تمديد الاختصاص المحلي لوكيل الجمهورية إذا تعلق الأمر بالجرائم المتصلة بتكنولوجيا الإعلام و الاتصال طبقاً للمادة 50 من قانون الإجراءات الجزائية[4].

---

[1] بلحاج خالدية, فرعون محمد, مرجع سابق,ص 468

[2] المواد من 394 مكرر إلى المادة 394 مكرر03, من القانون رقم24_06, المؤرخ في 28 أبريل 2024, يعدل ويتمم الأمر رقم 66_156 والمتضمن قانون العقوبات,الج.الر.30,2024,ص20

[3] بوحفص راوية, الجريمة الالكترونية في التشريع الجزائري, مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق تخصص: قانون جنائي, جامعة محمد خيضر – بسكرة – كلية الحقوق والعلوم السياسية قسم الحقوق, السنة الجامعية 2018/2017,ص 31.

[4] المادة 50 من القانون رقم 25_14 , المؤرخ في 03 أوت 2025.المتعلق بالإجراءات الجزائية الجزائري,الج.الر.54,2025,ص14.

وبموجب المادة 114 من القانون رقم 25_14 إذا تعلق الأمر بهذه الجرائم, بينما اقتضت ضروريات التحقيق الابتدائي في هذه الجرائم يجوز لوكيل الجمهورية المختص اعتراض المراسلات ووضع الترتيبات التقنية دون موافقة المعنيين, من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور شخص أو عدة أشخاص يتواجدون في مكان خاص[1].

ثانياً: تحديث المنظومة التشريعية بآليات حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي.

لقد تطرق المشرع الجزائري لمفهوم المعطيات ذات الطابع الشخصي بموجب التعريف الوارد في نص المادة 03 من القانون رقم 18_07 المعدل و المتمم بالقانون رقم 25_11 , المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي, ذلك بأنها :" كل معلومة بغض النظر عن دعامتها, متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه، "الشخص المعني" بصفة مباشرة و غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"[2].

أكد رئيس السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي سمير بورحيل, اليوم الثلاثاء, ببشار أن الجزائر تدرك جيدا أهمية السيادة الرقمية وتسعى دون هوادة من خلال

[1] المادة 114 من القانون رقم 25_14 ,ص23

[2] المادة03, من القانون رقم 18_07, المؤرخ في 10يونيو 2018, المعدل والمتمم بالقانون رقم 25_11, المؤرخ في 24 يوليو 2025, المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي,الج.الر.2018,34.ص12

مؤسساتها الدستورية على تعزيزها وتوطيدها في إطار الإستراتيجية الوطنية للتحول الرقمي التي سطرها رئيس الجمهورية السيد عبد المجيد تبون.

وأبرز السيد بورحيل في كلمته خلال افتتاح الملتقى الدولي حول "السيادة الرقمية للدولة" أن "هذه الإستراتيجية تهدف إلى "بناء اقتصاد رقمي شامل وتحسين الخدمات العمومية وتعزيز الاندماج الرقمي في إطار حماية المعطيات ذات الطابع الشخصي ."

كما أشار في هذا الصدد إلى القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي قد وضع "الإطار المنظم لمعالجة المعطيات في بلادنا, مواجها الآثار المترتبة على التطور السريع لتكنولوجيات الإعلام والاتصال على الحياة الخاصة.

كما أوجب على كل من يعالج معطيات شخصية أن يتقيد بالسرية وأن يتخذ جملة من التدابير التقنية والتنظيمية حتى تعزز الحماية من أي شكل من أشكال سرقة البيانات أو الولوج غير المرخص أو تعطيل البنى التحتية الرقمية, مما يعمل على تحصين السيادة الرقمية وإدامتها[1]."

وقد نتج عن تطور تكنولوجيات الإعلام والاتصال – حسب نفس المسؤول– فضاء رقمي يسمح بالتواصل والنقاش عبر المنصات الرقمية, لافتا إلى أن هذا الفضاء "أصبح يشكل هاجسا لمعظم الدول حتى المتقدمة منها لأنه يحاول الانفلات من قبضة الضوابط التواصلية والقانونية التي تسنها وهي تتصدى جاهدة لهذه المحاولات ببسط سيادتها على هذا الفضاء الجديد الذي يدخل ضمن سيادة إقليمها الافتراضي", مما يعطي مصطلح جديد يعرف ب " السيادة الرقمية."

[1] الجزائر تسعى إلى تعزيز سيادتها الرقمية ,يوم الثلاثاء 11 نوفمبر 2025 , https://www.aps.dz/algerie/actualite-nationale/mhutp24i- , تاريخ الاطلاع القلاثاء, 11مايو 2026 19:35

وأشار السيد بورحيل إلى أن من أبرز مظاهر التحكم في هذا الفضاء الافتراضي الجديد, أمن قواعد البيانات والأنظمة المعلوماتية وحماية المعطيات ذات الطابع الشخصي .

وذكر أنه "بتخطي الانترنت حدود الدولة المادية, واستخدام التطبيقات المتقدمة على رأسها الذكاء الاصطناعي, أصبحت سيادة الدول تواجه تحديات متزايدة, وتخيم على هذه الأخيرة (أي الدول) مخاطر عدة في مجال الأمن القومي لاسيما في مجال التجسس وزرع البلبلة والدعاية والأكاذيب, ناهيك عن الهجمات السيبرانية لتعطيل البنية التحتية لدول بأكملها قصد الإضرار بمصالحها الإستراتيجية أو النيل من سيادتها الرقمية."

وأكد رئيس السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أن المشرع الجزائري يدرك تمام الإدراك أن تحكم الدولة في فضائها الرقمي هو تأكيد لسيادتها وتعزيز لضمان خصوصية مواطنيها .

وفي الختام , ثمن السيد بورحيل الأهداف التي يصبو هذا الملتقى إلى تحقيقها, مع التذكير أنه في ظل التقدم التكنولوجي السريع تظل الخصوصية وحماية المعطيات الشخصية من القضايا الحيوية التي لابد أن يعمل الجميع على تعزيزها من خلال الوعي ونشر ثقافتها والالتزام بالأخلاق والممارسات الفضلى, على حد تعبيره[1].

[1] الجزائر تسعى إلى تعزيز سيادتها الرقمية ,يوم الثلاثاء 11 نوفمبر 2025 , https://www.aps.dz/algerie/actualite-nationale/mhutp24i- , تاريخ الاطلاع القلاثاء, 11مايو 2026 19:35.

أكد أيضاً رئيس السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أن المشرع الجزائري يدرك تمام الإدراك أن تحكم الدولة في فضائها الرقمي هو تأكيد لسيادتها وتعزيز لضمان خصوصية مواطنيها. وفي الختام، ثمن السيد بورحيل الأهداف التي يصبو هذا الملتقى إلى تحقيقها، مع التذكير أنه في ظل التقدم التكنولوجي السريع تظل الخصوصية وحماية المعطيات الشخصية من القضايا الحيوية التي لابد أن يعمل الجميع على تعزيزها من خلال الوعي ونشر ثقافتها والالتزام بالأخلاق والممارسات الفضلى، على حد تعبيره. وينظم هذا الملتقى الذي أشرف على افتتاحه والي بشار أحمد بن يوسف بمبادرة من معهد الحقوق والعلوم السياسية لجامعة "طاهري محمد". وقد تضمنت أشغال اليوم تقديم عروض حول تجارب تتعلق بحماية البيانات الرقمية[1].

ثالثاً: تعزيز المنظومة التشريعية بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال.

سعت الجزائر إلى استدراك الفراغ القانوني من خلا تعزيز منظومتها التشريعية خاصةً منذ 2009 ،حيث تم صدور القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا العالم والاتصال ومكافحتها بتاريخ 05 أوت 2009(.قانون رقم 09-04 ،2009) كما احتوى هذا القانون على 19مادة موزعة على 06 فصول مستمدة من الاتفاقيات الدولية (اتفاقية بودابيست، 2001) ,وجاء هذا القانون مطابقا للتشريعات الوطنية لا سيما تلك

[1] الجزائر تسعى إلى تعزيز سيادتها الرقمية,https://www.entv.dz/ar/news , تاريخ الاطلاع السبت, 2 مايو 2026 15:36.

المتعلقة بمحاربة الفساد وتبييض الأموال وتمويل الإرهاب، حيث نص هذا القانون على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا العالم والاتصال ومكافحته [1].

نص القانون 09-04 على طائفة من الأحكام العامة لمكافحة الاعتداءات الواقعة على البيانات الشخصية مهما كانت الوسائط المتداخلة في تداولها سواء شبكات عامة أو خاصة، وبموجب المادة 13 من القانون 09-04 أعلاه أنشئت هيئة وطنية للوقاية من هذه الجرائم ومكافحتها، تحدد تشكيلتها وتنظيمها وكيفيات تسييرها عن طريق التنظيم، حيث تأخر تطبيق أحكام هذه المادة إلى غاية 2019 بصدور المرسوم الرئاسي 19_172 المحدد لتشكيلتها وتنظيمها و كيفيات تسييرها[2].

كما أن الجزائري قد أعتبر أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه، وذلك من خلال نصه في الفقرة من المادة الثانية القانون 09-04 على أن برامج سير نظام المعالجة الآلية للمعطيات تدخل ضمن المعطيات المعلوماتية[3].

رابعاً: منظومة حوكمة البيانات.

يشمل المرسوم الرئاسي رقم 25_320 المتضمن وضع المنظومة الوطنية لحوكمة البيانات ,عشرين (20) مادة موزعة على أربع (04) فصول تتضمن عناصر المنظومة الوطنية لحوكمة البيانات ، التي تهدف لا سيما إلى:

-تكريس سيادة الدولة على البيانات ذات المصلحة الوطنية؛

-ضمان إدارة منظمة ومؤمنة وشفافة وفعالة للبيانات العمومية؛

[1] شحيرط أحمد ,قريبيز مراد,مرجع سابق,ص30.

[2] تقية توفيق, جامعة خميس مليانة ،,رشيد بوبكر , جامعة تيبازة,الأطر القانونية لتعزيز السيادة الرقمية للدولة في مواجهة التحديات المتعلقة بالاستخدامات السلبية المحتملة للذكاء الاصطناعي, مجلة صوت القانون , المجلد11, العدد01, السنة2024,ص137.

[3] بوحفص راوية,مرجع سابق ,ص29.

–تحسين جودة البيانات وتعزيز قابلية التشغيل البيني وتكريس النفاذ المؤطر إلى البيانات بما يحفز الابتكار ويساعد على بروز منظومة رقمية تنافسية؛

–تعزيز الأداء وترسيخ ثقة المواطنين والمتعاملين الاقتصاديين في إدارة البيانات واستعمالها.

_التنظيم التقني للمنظومة، عبر النظام الوطني للتشغيل البيني والمراجع الخاصة بالتصنيف والفهرسة ومطابقة البيانات، وكذا الشبكة المعلوماتية المؤمنة IRIES؛

–التنظيم المؤسسي، من خلال ضبط دور المجلس الوطني لأمن الأنظمة المعلوماتية ووكالة أمن الأنظمة المعلوماتية والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وكذا المحافظة السامية للرقمنة بصفتها المسؤولة عن إدارة وتسيير الإطار التقني؛

–تنظيم أدوار مسؤوليات مختلف المتدخلين، لا سيما مصدر البيانات باعتباره المسؤول عن تصنيفها وفهرستها وموثوقيتها وجودتها وصحة مصدرها، ومستعمل البيانات المكلف باستغلالها في إطار آمن ومنظم[1].

إن تجسيد هذه المنظومة من شأنه أن يتيح الانتقال إلى نمط حديث وموحد لتبادل وتثمين البيانات، يتسم بالمصداقية والانسيابية والتأمين في المعاملات بين الإدارات العمومية والهيئات المكلفة بالمرفق العام، كما سيساهم في مواءمة السياسة الوطنية مع المعايير الدولية في مجال حوكمة البيانات وحماية الخصوصية و ترسيخ الدور الاستراتيجي للبيانات.

لا سيما تزويد بلادنا بأداة قانونية هيكلية تكفل السيادة الرقمية للدولة ، وتضمن الشفافية في التسيير العمومي ، والتنمية الاجتماعية والاقتصادية المستدامة.

وفي الختام يمكن القول أننا نتجه نحو دولة ذكية بمرجعية سيادية فإن المرسوم الرئاسي رقم 25-320 لا يمثّل مجرد إصلاح تقني، بل تحوّلًا بنيويًا في عقل الدولة. فهو يضع الأسس

[1] حوكمة البيانات في الجزائر: وضع الحجر الأساس للسيادة الرقمية وإدارة متطورة, https://www.entv.dz/ar/news , تاريخ الاطلاع السبت, 2 مايو 2026 ,17:15.

القانونية والمؤسساتية للانتقال من إدارة تعتمد على الوثيقة إلى إدارة تعتمد على البيانات الموثوقة، ومن قرار ظرفي إلى قرار مبني على التحليل والمعطيات.

الجزائر، عبر هذا النص، لا تلتحق فقط بركب التحول الرقمي، بل تسعى إلى صياغة نموذجها الخاص للسيادة الرقمية، يقوم على التحكم في البيانات، تنظيم تدفقها، وحمايتها، باعتبارها رافعة أساسية للاقتصاد الرقمي، التخطيط الاستراتيجي، وجودة السياسات العمومية[1].

فعلى الصعيد الوطني، شكّلت المنظومة الوطنية لحوكمة البيانات ركيزة أساسية ودورا محوريا في ترسيخ السيادة الرقمية للدولة، والتحكم الرشيد في البيانات باعتبارها مورداً استراتيجياً، وذلك من خلال تدعيم منظومات أمن المعلومات، وتعزيز حماية المعطيات، وضمان موثوقيتها واستدامتها. وقد أسهم ذلك في الارتقاء بجودة القرار العمومي وتوفير الأسس المعرفية اللازمة لإنجاح إصلاحات هيكلية عميقة وشاملة، تقوم على استثمار أمثل لبيانات دقيقة وموثوقة، في إطار يكرّس مبادئ الشفافية والأمن والثقة.

وإلى جانب ذلك، تضطلع هذه المنظومة بدور استراتيجي في تعزيز جاذبية الاستثمار وتنمية الاقتصاد الرقمي، من خلال إرساء إطار مؤسساتي وقانوني واضح وموثوق لحوكمة البيانات، يضمن وضوح القواعد، واستقرار التشريعات، وحماية المعطيات، بما يعزز ثقة الفاعلين الاقتصاديين والمستثمرين الوطنيين والدوليين بتحسين الولوج إلى بيانات موثوقة وقابلة

[1] حوكمة البيانات في الجزائر: وضع الحجر الأساس للسيادة الرقمية وإدارة متطورة, https://www.entv.dz/ar/news , تاريخ الاطلاع السبت, 2 مايو 2026 ,17:15.

للاستغلال، وتشجيع الابتكار وتطوير نماذج أعمال رقمية جديدة، ودعم قابلية التشغيل البيني بين الأنظمة.

كما تعد من بين المرتكزات الإستراتيجية الأساسية لتطوير واعتماد حلول وتطبيقات الذكاء الاصطناعي، التي توفّرها المنظومة الوطنية لحوكمة البيانات كونها الإطار المرجعي الكفيل بضمان إتاحة بيانات ذات جودة، مهيكلة وموثوقة، وقابلة للتشغيل البيني، بما يتيح استثمارها الأمثل في تصميم وتدريب نماذج ذكية دقيقة وذات نجاعة عالية. ويتم ذلك في كنف الالتزام الصارم بمتطلبات الأمن السيبراني، واحترام المبادئ الأخلاقية لاستخدام الذكاء الاصطناعي، وضمان حماية المعطيات، ولاسيما ذات الطابع الشخصي[1].

وأشار أيضاً إلى أن الإطار القانوني لحماية المعطيات يُعد دعامة أساسية، لكونه مكرساً دستورياً بما يضمن صون الحقوق وتعزيز الثقة في البيئة الرقمية، مبرزاً أن نجاح الدول في مسار التحول الرقمي يُقاس بمدى قدرتها على حماية البيانات الشخصية[2].

في إطار تحصين وحماية مؤسسات الدولة والهيئات الوطنية من كافة أشكال التهديدات التي قد تواجهها في فضائها السيبراني، نشرت وكالة أمن الأنظمة المعلوماتية لوزارة الدفاع الوطني، اليوم الثلاثاء 03 مارس 2026، الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة 2025-2029، في نسختها الأولى، والمصادق عليها من طرف السيد رئيس الجمهورية، القائد الأعلى للقوات المسلحة وزير الدفاع الوطني.

[1] كلمة الوزير الأول خلال إشرافه على وضع المنظومة الوطنية لحوكمة البيانات حيز الخدمة, https://www.premier-ministre.gov.dz/ar/post/ , تاريخ الاطلاع السبت, 2 مايو 2026, 17:28.

[2] بورحيل, حوكمة البيانات ركيزة أساسية لنجاح التحول الرقمي, https://www.aps.dz/algerie/actualite-nationale/mo8qjidz , تاريخ الاطلاع السبت, 2 مايو 2026, 17:35.

تمثل هذه الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، الإطار الشامل الذي يهدف إلى ضمان المرونة السيبرانية الوطنية وحماية البنية التحتية الرقمية للدولة وبياناتها، وكذا حماية المواطنين من التهديدات التي قد تواجههم في الفضاء السيبراني، خاصة في ظل توجه السلطات العليا للبلاد الرامي إلى التسريع من وتيرة التحول الرقمي على مستوى كافة مؤسسات الدولة، كما تعد ورقة طريق من شأنها المحافظة على السيادة الرقمية الوطنية وضمان الخدمات العمومية الأساسية وتعزيز ثقة المواطن في بيئته الرقمية[1].

خامساً: محافظة السامية للرقمنة.

تم إنشاء المحافظة السامية للرقمنة بوصفها هيئة سامية موضوعة تحت وصاية رئاسة الجمهورية, بمقتضى المرسوم الرئاسي رقم 23-314 المؤرخ في 06 سبتمبر سنة 2023، والمتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيرها، المعدل بمقتضى المرسوم الرئاسي رقم 25-320 المؤرخ في 30 ديسمبر سنة 2025، والمتضمن وضع منظومة وطنية لحوكمة البيانات؛ وبمقتضى المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي سنة 2020، والمتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، المعدل والمتمم[2].

[1] بيان لوزارة الدفاع الوطني, وكالة أمن الأنظمة المعلوماتية لوزارة الدفاع الوطني تنشر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029, https://www.mdn.dz/site_principal , تاريخ الاطلاع الأحد, 10 مايو 2026 ,10:47.

[2] نشر المرجعين,المحافظة السامية للرقمنة, **https://www.hcn.dz/projets/juridique/PublicationR** , تاريخ الاطلاع الإثنين, 11 مايو 2026 ,22:26.

يهدف هذا المرسوم إلى إنشاء محافظة سامية للرقمنة وتحديد مهامها و تنظيمها وسيرها,بناءً على ما جاء في المادة الأولى[1] من المرسوم الرئاسي رقم 23_314.

كما عرفت المادة 02 منه المحافظة السامية للرقمنة على أنها: " مؤسسة عمومية ذات طابع خاص, تتمتع بالشخصية المعنوية و الاستقلال المالي, توضع تحت وصاية رئاسة الجمهورية, وتدعى في صلب النص" المحافظة السامية"[2], يقع مقر هذه الأخيرة بمدينة "الجزائر العاصمة" وفقاً للمادة 03 من نفس المرسوم[3].

و تكمن صلاحيات المحافظة في تصميم الإستراتيجية الوطنية للرقمنة, بالتشاور مع القطاعات المعنية و المؤسسات والقطاع الاقتصادي والمجتمع المدني. وتكلف أيضاً بضمان متابعة الإستراتيجية الوطنية للرقمنة وتنفيذها, المادة 04 منه[4].

يعد إعداد الإستراتيجية الوطنية للتحول الرقمي، برؤية "جزائر رقمية 2030" من بين المشاريع الإستراتيجية التي التزمت بها المحافظة السامية للرقمنة منذ إنشائها، حيث تعد هذه الإستراتيجية أول مرجعية وطنية تنظم و تؤطر وتقود مسار تجسيد التحول الرقمي في بلادنا، وفق مقاربة تشاركية و تشاورية شاملة مع جميع القطاعات الوزارية والخبراء والفاعلين والمتعاملين الاقتصاديين في مجال الرقمنة، ويرتكز مضمون الإستراتيجية الوطنية للتحول الرقمي على تحسين رفاهية المواطن والمؤسسة، من خلال تسهيل وتسريع المعاملات وتحقيق

[1] المادة 01, من المرسوم الرئاسي رقم 23_314 المعدل بمقتضى المرسوم الرئاسي رقم 25-320 المؤرخ في 30 ديسمبر سنة 2025، والمتضمن وضع منظومة وطنية لحوكمة البيانات, الصادر في الجريدة الرسمية الجزائرية, الصادرة في 10 سبتمبر 2023,العدد59,ص09.

[2] المادة 02 من المرسوم الرئاسي رقم 23_ 314 , ص09.

[3] المادة 03 من المرسوم الرئاسي رقم 23_ 314 , ص09.

[4] المادة 04 من المرسوم الرئاسي رقم 23_ 314 , ص09.

اتصال عالي الجودة للجميع وتوفير خدمات عمومية مرقمنة وسهلة الولوج 100 %، إضافة إلى تطوير اقتصاد رقمي وطني خالق للثروة[1].

إن تحقيق هذه المكتسبات يتوافق ويتماشى مع قيم بلادنا، خاصة تلك المتعلقة بالمبادئ الأساسية للعدالة الاجتماعية، التي كرسها الدستور الجزائري، ومنسجمة مع التوجيهات الإستراتيجية والطموحات السامية للسيد رئيس الجمهورية، بغية تحقيق رقمنة شاملة تمس كل القطاعات، نضمن من خلالها تسريع المعاملات وإرساء مبادئ الشفافية والمساواة في الولوج والحصول على المعلومة وزيادة المردودية وتحقيق الفعالية الحكومية، ومساهمة الرقمنة في تطوير الناتج الداخلي الوطني الخام .إن الإستراتيجية الوطنية للتحول الرقمي تقوم على خمسة (05) محاور إستراتيجية، محوران منها يعدان القاعدة الأساسية لإنجاح التحول الرقمي في بلادنا، متعلقان "بالبنية التحتية الأساسية" و المتمثلة أساسا في شبكات الاتصال عالي الجودة ومراكز البيانات، وكذا "الموارد البشرية والتكوين والبحث والتطوير"، أما المحاور الثلاثة الأخرى فتستهدف مكونات الدولة والمتمثلة في السلطات العمومية التي تحكم وتسير من خلال محور "الحوكمة الرقمية"، والاقتصاد الذي يخلق الثروة من خلال محور "الاقتصاد الرقمي"، والمجتمع المدني لبلوغ الشمول الرقمي من خلال محور "المجتمع الرقمي"، ويشمل كل محور مجموعة من الأهداف الإستراتيجية، بمجموع خمسة وعشرين (25) هدفا استراتيجيا،لكل هدف منها غاية نعمل على بلوغها في الفترة الممتدة من 2025 إلى 2030 .إن الأهداف المنشودة من تنفيذ هذه الإستراتيجية الوطنية، تصبو إلى تحقيق جملة من القيم تتمثل في الشفافية والفعالية في التسيير، العدالة والمساواة لتحفيز الاقتصاد الوطني وضمان تنمية اجتماعية واقتصادية مستدامة . تقوم الإستراتيجية الوطنية للتحول الرقمي على ركيزتين اثنتين؛ إحداهما: تتمثل في

[1] الإستراتيجية الوطنية للتحول الرقمي 2025- 2030 https://www.hcn.dz/projets/juridique/SNTN , تاريخ الاطلاع الاثنين, 11 مايو 2026, 23:13.

الجانب القانوني والتنظيمي الشامل الذي ينظم و يؤطر ويضبط مجال الرقمنة في بلادنا، وهو ما تعمل عليه حاليا المحافظة السامية للرقمنة من خلال إعداد قانون الرقمنة بإشراك كل المعنيين بمجال الرقمنة في بلادنا .أما الركيزة الأخرى لهذه الإستراتيجية فتتمثل في الأمن الرقمي الذي يعد دعامة أساسية وبالغة الأهمية يرتكز عليها أمن هذه المحاور لحماية البيانات والأنظمة من التهديدات السيبرانية [1].

سادساً: إنشاء النظام الوطني للتشغيل البيني.

يُعدّ النظام الوطني للتشغيل البيني العصب الحيوي في المنظومة الوطنية للتشغيل البيني[2]، حيث عرفته المادة 09 من المرسوم الرئاسي رقم 25_320 المؤرخ في 30 ديسمبر 2025 المتضمن وضع المنظومة الوطنية لحوكمة البيانات بأنه: "النظام الذي يُمَكِن من تبادل البيانات الرقمية بطريقة آمنة، ومنظمة، وفعالة بين مختلف المؤسسات والإدارات العمومية والهيئات والمؤسسات المكلفة بخدمة عمومية، طبقا لمرجع تصنيف البيانات ومرجع فهرسة مصادر البيانات من خلال بيئة موثوقة"[3]. ويراعى عند تبادل البيانات ضمن النظام الوطني للتشغيل البيني التصنيف المحدد لهذه البيانات من طرف مصدرها .كما يُعد الإطار الحصري لتبادل البيانات الرقمية بين المؤسسات والإدارات العمومية عبر البنية التحتية للشبكة الوطنية المؤمنة المخصصة لذلك. ويمكن عند الحاجة إدراج الهيئات والمؤسسات المكلفة بخدمة عمومية في النظام الوطني للتشغيل البيني إذا كانت بياناتها مطلوبة للمعالجة ضمن هذا النظام، بالتنسيق

---

[1] مريم بن مولود, كلمة السيدة ,الاستراتيجية الوطنية للتحول الرقمي 2025-2030, https://www.hcn.dz/projets/juridique/SNTN , تاريخ الاطلاع الأحد, 10 مايو 2026 ,18:24

[2] النظام الوطني للتشغيل البيني,https://www.hcn.dz/projets/FondementTechnologique/Datashiring تاريخ الاطلاع الأحد, 10 مايو 2026 ,12:34.

[3] المادة 09 المرسوم الرئاسي رقم 25_320 **المؤرخ في 30 ديسمبر 2025** المتضمن وضع المنظومة الوطنية لحوكمة البيانات, الصدر في ج , ر,87, 2025, ص03

بين المحافظة السامية للرقمنة والقطاعات المعنية، وهذا طبقا للمادة 10 [1]من المرسوم رقم 320_25 .كما يتعين على مستخدم البيانات الحصول على موافقة مصدر البيانات عبر النظام الوطني للتشغيل البيني قصد استغلال البيانات الرقمية للغرض الذي طلبت من أجله وفقاً للتشريع و التنظيم المعمول به.طبقاً للمادة 13 [2]من نفس المرسوم, وفي هذا الصدد, نصت المادة 17 منه على أن المحافظة السامية للرقمنة تتولى وضع النظام الوطني للتشغيل البيني حيز الخدمة وإدارته، وتضمن تأمين البيانات خلال مرحلة نقلها في ظل احترام متطلبات أمن الأنظمة المعلوماتية[3].

سابعاً: الشبكة السيادية الوطنية المؤمنة المسماة ب IRIES.

بموجب المرسوم الرئاسي رقم 25-320 المؤرخ في 30 ديسمبر 2025، المتضمن وضع منظومة وطنية لحوكمة البيانات، لاسيما المادة 11 منه التي تنص على " تضع المحافظة السامية للرقمنة البنية التحتية للشبكة الوطنية المؤقتة و القائمة على ربط المؤسسات المكلفة بخدمة عمومية,بشكل منفصل عن شبكة الانترنت"[4] ، تم تكريس هذه الشبكة كبنية تحتية حصرية لتبادل البيانات بشكل منفصل عن شبكة الإنترنت، في بيئة آمنة وموثوقة، بين المؤسسات والإدارات العمومية في إطار منظم وآمن يعزز الانسجام والتكامل فيما بينها، مع اعتماد نمط تسيير موحد ضمن إطار تقني متكامل، ما يعكس وعياً كبيراً بأهمية حماية السيادة الرقمية .لقد تم من خلال هذه الشبكة ربط كل القطاعات الوزارية وكذا الهيئات العمومية فيما

[1] المادة 10 المرسوم رقم 320_25, ص03

[2] المادة 13 المرسوم قم 320_25 , ص03

[3] المادة 17 المرسوم رقم 320_25, ص03

[4] المادة 11 المرسوم رقم 320_25, ص03

بينها ومع مراكز البيانات الوطنية، إذ تتميز هذه الشبكة بقابلية التوسع بما يضمن تغطية شاملة وفعالة، مما يتيح مواكبة المتطلبات المستقبلية ودعم مسار التحول الرقمي المتسارع للدولة[1].

ثامناً: البوابة الوطنية للخدمات الرقمية.

تُعد البوابة الوطنية للخدمات الرقمية، (بنسختيها الويب والموبايل)، نقطة ولوج مركزية يحتضنها المركز الوطني الجزائري للخدمات الرقمية، وتهدف إلى تمكين المواطنين من الولوج إلى الخدمات العمومية الرقمية بطريقة موحّدة، سهلة، سريعة وآمنة، من خلال واجهة تفاعلية متقدمة تتيح إنجاز مختلف المعاملات الإدارية عبر الإنترنت، بما في ذلك الحصول على الوثائق الرسمية، متابعة طلبات الخدمات، والاستفادة من مسار رقمي مبسط. كما تعتمد البوابة الوطنية للخدمات الرقمية منهجًا مطابقًا للمعايير الدولية المعتمدة في مؤشر تطور الحكومة الإلكترونية(EGDI) ، من حيث جودة المحتوى الرقمي، نضج الخدمات، وسهولة الوصول إليها، بما يعزز الثقة الرقمية ويرفع من فعالية الخدمة العمومية. كما تجسد هذه البوابة التزام الجزائر بتطوير إدارة عمومية عصرية، أكثر نجاعة وشفافية وفي متناول الجميع، مستندة إلى بنية تقنية متطورة تضمن حماية البيانات وتعزيز ثقة المستخدمين، على أن تضم في مرحلتها الأولى 52 خدمة عمومية رقمية ضمن رؤية وطنية شاملة للتحول الرقمي[2].

[1] البنية التحتية للشبكة الوطنية المؤمّنة المسماة بـ"IRIES", https://www.hcn.dz/projets/FondementTechnologique/IRIES , تاريخ الاطلاع الإثنين, 11 مايو 2026, 19:32.

[2] البوابة الوطنية للخدمات الرقمية, https://www.hcn.dz/projets/FondementTechnologique/Portail-unifi%C3%A9 , تاريخ الاطلاع الأحد, 10 مايو 2026, 17:22

تاسعاً: آليات مستحدثة موضوعة لدى وزارة الدفاع الوطني–المنظومة الوطنية لأمن أنظمة المعلوماتية:

تدخل المنظم بآليات مستحدثة ترعاها وزارة الدفاع الوطني بموجب أحكام المرسوم الرئاسي 20–05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية الذي يهدف إلى وضع منظومة وطنية لأمن الأنظمة المعلوماتية, وذلك وفقاً للمادة الأولى منه[1].

كما عرفت المادة 02 منه المنظومة على أنها "أداة الدولة في مجال أمن الأنظمة المعلوماتية, وتشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها"[2].

تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني حسب المادة 03 منه ما يأتي:

_مجلس وطني لأمن الأنظمة المعلوماتية، يدعي في صلب النص "المجلس" ويكلف بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة على‌ها وتوجيهها،

_ وكالة لأمن الأنظمة المعلوماتية تدعي في صلب النص الوكالة وتكلف بتنسيق تنفيذا لإستراتيجية الوطنية لأمن الأنظمة المعلوماتية،

ولممارسة مهامها يتوفر المجلس، بالإضافة إلى الوكالة على الهياكل المختصة لوزارة الدفاع الوطني في هذا المجال"[3] .

[1] المادة 01 ,المرسوم الرئاسي 20–05,المؤرخ في 20 جانفي 2020, المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية,الج.الر.2020,04,ص 06

[2] المادة 02, المرسوم الرئاسي 20–05, ص06

[3] المادة 03 ,المرسوم الرئاسي 20–05 , ص06

تضم وكالة أمن أنظمة المعلوماتية تشكيلة ثلاثية، تتألف من لجنة التوجيه التي تتولى تحديد السياسات والتوجيهات العامة، بالإضافة إلى مدير عام يشرف على سير العمل وتنفيذ القرارات، ولجنة علمية مختصة تتكفل بتقديم الخبرات الفنية والعلمية في معالجة وتحليل الحوادث السيبرانية التي تستهدف المؤسسات الوطنية.تقوم الوكالة بتنفيذ مهامها وفقاً لتوجيهات ومتابعة المجلس المختص, نظرا لأن قضايا الأمن السيبراني تعتبر من أهم الأولويات على الصعيد الدولي، حيث تتناول مسائل السيادة الوطنية و الأمن المعلوماتي, وتلعب دوراً حاسماً في تأمين البنى التحتية الرقمية للدولة وحمايتها من التهديدات السيبرانية المختلفة التي يمكن أن تعرض أمنها المعلوماتي للخطر من الداخل و الخارج[1].

وبالتالي وكالة أمن الأنظمة المعلوماتية هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية و الاستقلالية المالية وذلك ما نصت عليه المادة 17 من نفس المرسوم الرئاسي .

كما نصت المادة 38 و39 منه على أن هذه الوكالة تخضع لمختلف أنواع المراقبة المنصوص عليها في التشريع و التنظيم المعمول بهما, وتخضع أيضاً لمجموع الأحكام التشريعية و التنظيمية المطبقة في وزارة الدفاع الوطني[2].

نشرت وكالة أمن الأنظمة المعلوماتية لوزارة الدفاع الوطني، اليوم الثلاثاء 03 مارس 2026، الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة 2025-2029، في نسختها الأولى، والمصادق عليها من طرف السيد رئيس الجمهورية، القائد الأعلى للقوات المسلحة وزير الدفاع الوطني.

تمثل هذه الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، الإطار الشامل الذي يهدف إلى ضمان المرونة السيبرانية الوطنية وحماية البنية التحتية الرقمية للدولة وبياناتها، وكذا حماية

[1] تقية توفيق,رشيد بوبكر , مرجع سابق,ص138,139.

[2] المادة 38,39, المرسوم الرئاسي 20-05 , ص10

المواطنين من التهديدات التي قد تواجههم في الفضاء السيبراني، خاصة في ظل توجه السلطات العليا للبلاد الرامي إلى التسريع من وتيرة التحول الرقمي على مستوى كافة مؤسسات الدولة، كما تعد ورقة طريق من شأنها المحافظة على السيادة الرقمية الوطنية وضمان الخدمات العمومية الأساسية وتعزيز ثقة المواطن في بيئته الرقمية[1].

في الواقع، إن الهدف الرئيسي من هذه المنظومة يكمن في إعداد ووضع الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، من أجل تهيئة بيئة ملائمة لجميع الفاعلين الوطنيين المعنيين بالأمن السيبراني من خلال توفير كل الظروف اللازمة للمساهمة الناجعة في حماية السيادة الرقمية الوطنية والحفاظ عليها.

تتمثل الأهداف الإستراتيجية لهذه الإستراتيجية فيما يلي:

_بناء المرونة السيبرانية للأنظمة المعلوماتية الوطنية,

_العمل على وضع نظام بيئي وطني ملائم في مجال الأمن السيبيراني,

_إنشاء إطار وطني من أجل تطوير موارد بشرية مؤهلة في الأمن السيبيراني,

_تعزيز التعاون الدولي في الأمن السبيراني,

كما تتمثل المبادئ التوجيهية لاستراتيجية الوطنية لأمن الأنظمة المعلوماتية في:

_تعزيز السيادة الرقمية الوطنية,

[1] منشور وزارة الدفاع الوطني الجزائرية,WWW.MDN.DZ

#وزارة_الدفاع_الوطني_الجزائرية, تاريخ الاطلاع الثلاثاء, 12 مايو 2026 ,12:17

_مرافقة التحول الرقمي المباشر من طرف الدولة,

_ الحفاظ على المكاسب المحققة .تشجيع العمل التنسيقي الشامل,

_ تثمين تشارك الموارد,

_تحديد أهداف قابلة للتحقيق في آجالها المحددة وقابلة للقياس.[1]

المبادئ المذكورة أعلاه تعتبر كعناصر مرجعية في الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية.

عاشراً: التكامل المؤسساتي لحماية الأمن المعلوماتي للدولة_ إحداث مركز بيانات حكومي.

أفضت الطبعة الأولى لندوة الجزائر للرقمنة إلى تقديم توصيات بشأن تحقيق السيادة الرقمية بكل ما تحمله في طياتها من معاني، وبناءاً على ذلك خلصت الندوة إلى أن إرساء السيادة الوطنية في المجال الرقمي يقتضي تعاون وثيق مع القطاعات المعنية من أجل إنشاء شبكة انترنيت حكومية ومركز بيانات حكومي يهدف إلى تأمين البيانات .

يشكل مركز البيانات الحكومي الهيكل المؤسسي للدولة والبنية التحتية لبياناتها الذي يضم جميع أصول البيانات المتعلقة بمختلف العمليات الإدارية الرقمية التي تجريها الحكومة وجميع الخدمات الإلكترونية المقدمة والتي يتم تجميعها من خلال ربط البنية التحتية للدولة بأصول البيانات على مستوى الإدارات والمؤسسات العامة وفق آليتين أساسيتين هما التشغيل البيني الذي يتيح الوصول المادي للبيانات واستضافتها، والتزويد الذي يتيح تقديم الخدمات الرقمية؛ وعليه يعتبر مركز البيانات الحكومي مرفق مادي تستخدمه الدولة لإيواء التطبيقات والبيانات الهامة لمعالجتها ونشرها أو أرشفته ويعرف مركز البيانات من الناحية التقنية بأنه منشأة تقنية

[1] الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية, **https://www.mdn.dz/assi/nsiss_ar.pdf** , تاريخ الاطلاع الأحد, 10 مايو 2026 ,17:41

تأخذ غالباً شكل رفوف متماثلة داخل غرفة تعرف باسم خزانة الخادم بالإضافة المعدات الإضافية اللازمة لحفظ هذه الخوادم وتشغيلها والمتمثلة في إمدادات الكهرباء والطاقة الاحتياطية، الأسلاك والكوابل لتوصيل الخوادم بعضها البعض، وأجهزة و شبكات اتصال إضافية، وحدات تحكم ، معدات تبريد لحفظ درجة الحرارة المطلوبة التي تحول دون تلف هذه المعدات، أنظمة الكشف الحرائق والرطوبة، أجهزة المراقبة الأمنية والتي تمثل جميعا الأدنى من المعايير التقنية الواجبة التوافر عند إنشاء مراكز البيانات الحكومية .إن مركز البيانات الحكومي يوفر حلولا تقنية تدعم استمرارية العمل الحكومي كما تشكل بيئة آمنة إلى الوصول للخدمات الإلكترونية.وانجاز المعاملات الإلكترونية مع ضمان المحافظة على البيانات والمعلومات من حيث سريتها وسالمتها وحماية خصوصيتها.

و نظرا لأهمية مراكز البيانات الحكومية اتجهت بعض الحكومات إلى إنشاء مكان موحد للبيانات الحكومية والتي استحدثت بموجب قوانينها الداخلية، مهمتها تجميع البيانات المفتوحة من خلال نقل البيانات بطريقة دورية إلى هذه المراكز التأكد من تنظيفها من الشوائب و من مطابقتها وتحيينها على نحو مستمر، ثم توفيرها على الويب بغرض استفادة المبرمجين وشركات التكنولوجيا في بناء التطبيقات الذكية، وبالتالي إفادة المواطنين من خدمات الحكومة الرقمية بالشكل المطلوب ولتحقيق ذلك و جب العمل على بناء بوابة إنترنت مركزية في مراكز البيانات الحكومية، والعمل على إنشاء كتالوج لجميع البيانات الحكومية؛ من أجل معرفة البيانات التي يمكن الاستفادة منها، والعمل على تطوير تطبيقات بهذا الخصوص من قبل من شركات البرمجة،إضافة لإشراك المختصين في هذا المجال في مرحلتي تصميم و تنفيذ هذا المشروع، والعمل على بناء القدرات وتعزيز المهارات الرقمية لإدارة عمليات المركز[1].

[1] تقية توفيق ,رشيد بوبكر,مرجع سابق,ص139,140.

الفرع الثاني:الأطر الدولية للحفاظ على السيادة الرقمية .

إلى حد اليوم لا توجد قوانين دولية فعالة تتعلق بالأمن السيبراني والسيادة الرقمية للدول، وهذا بسبب حجم التعقيدات في هذا المجال التي تحول دون إيجاد تشريعات وقوانين واضحة ومحل توافق بين كيانات المجتمع الدولي، ومعه تتزايد الإشكالات القانونية وصعوبة الحلول لما يطفو على سطح الأحداث الدولية فيما يتعلق بالمشاكل السيبرانية، ومع كل هذا كذلك يتزايد تمسك الدول بمفهوم سيادتها الرقمية وأمنها التكنولوجي لتعزيز بسط سيطرتها على مكونات وجودها وأمنها بدءاً من حماية الاتصالات ووصولاً إلى عصرنة البنية التحتية المتعلقة باستعمال مختلف وجهات الانترنيت .

لكن وبالنظر في حيثيات هذا الموضوع يمكن القول أن السبب الذي يؤخر وجود قانون دولي فعال خاص بالفضاء السيبراني والرقمي ليس صعوبته فحسب، بل حجم لاختلافات الموجودة بين الدول[1].

تكمن الأطر الدولية لتعزيز السيادة الرقمية في المؤسسات الدولية الآتية:

1. **مقترح المفوضية الأوربية لأحكام لائحة لقانون الذكاء الاصطناعي:** تضمنت اللائحة 12 باباً بإجمالي 81 مادة، حيث ارتأت المفوضية الأوروبية عدم تعريف الذكاء الاصطناعي في حد ذاته ولكن تحديد أنظمته بدلاً من ذلك حيث قدمت تعريفا موسعا وغامضا إلى حد ما لهذه الأنظمة بموجب أحكام المادة 3 منه والذي قضت بأنه يعني البرنامج الذي تم تطويره باستخدام واحد أو أكثر من التقنيات والأساليب المدرجة في المرفق الأول والذي يمكن لمجموعة معينة من الأهداف التي يحددها الإنسان لتوليد مخرجات مثل المحتوى والتنبؤات أو توصيات أو قرارات تؤثر على

[1] سنوسي علي,مرجع سابق, ص 16.

البيئات التي يتفاعلون معها؛ أما القسم الأكبر من هذه اللائحة فقد اهتم بوضع الإطار القانوني المقترح على الاستخدام المحدد لأنظمة الذكاء الاصطناعي والمخاطر المرتبطة به؛ من خلال وضع تصنيف الأنظمة الذكاء الاصطناعي ذات المتطلبات والالتزامات المختلفة المصممة وفقا "لمعيار قائم على المخاطر". سيتم من خلاله حظر بعض أنظمة الذكاء الاصطناعي التي تقدم مخاطر "غير مقبولة".في حين سيتم الترخيص لمجموعة من أنظمة الذكاء الاصطناعي "عالية المخاطر" مقابل إخضاعها لمجموعة من المتطلبات والالتزامات للوصول إلى سوق الاتحاد الأوروبي .أنظمة الذكاء الاصطناعي هذه تقدم سوى " مخاطر محدودة " ستكون خاضعة لالتزامات الشفافية، في المقابل لا تطبق التزامات محددة بشأن أنظمة الذكاء الاصطناعي منخفضة ومحدودة الخطورة

2. **قوانين الذكاء الاصطناعي في الولايات المتحدة الأمريكية:** تم سن تشريعات محلية في بعض الولايات الأمريكية على غرار:

_ولاية كولورادو تم إنشاء فريق عمل لدراسة القضايا المتعلقة باستخدام الذكاء الاصطناعي في كولورادو للنظر على وجه الخصوص في خدمات التعرف على الوجه، وتقييد استخدام خدمات التعرف على الوجه من قبل الوكالات الحكومية الحكومية والمحلية، وحظر المدارس العامة مؤقتا من تنفيذ عقود جديدة لخدمات التعرف على الوجه واعتمادها[1].

_ ولاية كاليفورنيا تم تعديل القسم 5. 11547 من قانون الحكومة، المتعلق بالتكنولوجيا يحظر من خلال هذا التعديل على الشركات تقديم ادعاءات إعلانية كاذبة ومضللة، فضلا عن توجيه مجموعة العمل لتطوير آليات لتقليل وتحديد التزييف العميق والبالغ عن الاستخدامات الحالية ومخاطر التزييف العميق.

[1] تقية توفيق,رشيد بوبكر , مرجع سابق,ص140,141

_ولاية جورجيا إنشاء لجنة الشفافية والإنصاف في اتخاذ القرار الآلي، والتي ستراجع وتقدم تقارير علنية عن استخدام الدولة للذكاء الاصطناعي وأنظمة اتخاذ القرار المؤتمتة الأخرى وتضع توصيات الاستخدام هذه الأنظمة من قبل وكالات الدولة. وهي تحدد تركيبة اللجنة، وتضع متطلبات التأهيل، وتصف كيفية عمل اللجنة، وتتطلب من اللجنة إبلاغ النتائج التي تتوصل إليها إلى الهيئة التشريعية والجمهور.

3. **قانون الذكاء الاصطناعي الروسي:** صدر المرسوم رقم 490 عن الرئيس الاتحاد الروسي بتاريخ 10/10/2019 ،بشأن تطوير الذكاء الاصطناعي في الاتحاد الروسي إلى جانب الإستراتيجية الوطنية لتطوير الذكاء الاصطناعي إلى غضون عام 2030 التي تعتبر الأكثر شمولية حيث أرسى عدة أحكام متعلقة بمختلف جوانب الذكاء الاصطناعي، أهمها المبادئ الرئيسية التي تحمل الطابع الإلزامي بخصوص تطوير واستخدام تكنولوجيات الذكاء الاصطناعي تعلقت بالحقوق والحريات، والأمن، والشفافية، سلامة دورة الابتكار والتوفير المعقول، ودعم المنافسة والسيادة التكنولوجية التي تعد مبدءا سياديا لديها[1].

الفرع الثالث: تحديات السيادة الرقمية.

تثَير السيادة الرقمية والتحكم في الفضاء الرقمي للدولة مجموعة من الرهانات والتحديات من الصعب الفصل بينها بالرغم أن هذه التحديات تعد عراقيل ومشاكل البد على الدول مواجهتها لتحقيق السيادة الرقمية، في حين أن الرهانات هي تلك النتائج المحتملة للخطوات المتبعة من قبل الدول لتحقيق السيادة الرقمية، ويمكن إرجاع ذلك إلى طبيعة العلاقة المعقدة بين التكنولوجيا والسياسة يف العصر الرقمي، التي يجب تحديات ورهانات جديدة تتطلب استجابات سريعة وفعالة، كما أن التهديدات السيبرانية مثل الاختراقات الالكترونية تزيد من أهمية تطوير

[1] نفس المرجع,ص,142.

سياسات وإجراءات لضمان الأمان السيبراني، وهذه السياسات قد تشكل رهانات سياسية بالنسبة للدول.

بالإضافة إلى تداخل الأبعاد السياسية والاقتصادية والأمنية في مجال السيادة الرقمية مما يؤدي إلى تبعات تشكل رهانات كبيرة على الدول، دون أن ننسى التفاعل بين المجتمع المدني والقطاع الخاص من جهة، والجهات الفاعلة في الدول لتحديد سياساتها الرقمية. كل ذلك يجعل هنا تداخل يتعذر عزلها وعلى العموم تتمثل بالأساس في التحديات الإستراتيجية، القانونية، والسياسية الاجتماعية، والاقتصادية[1] .

أولاً:التحديات الإستراتيجية .

تتمثل في حماية البيانات من الوصول الغير مشروع لها، وعدم السماح بإساءة استخدامها أو تخريبها، وتستوجب الحماية السرية والتي تعني عدم السماح الإطلاع عليها إلا من قبل الأشخاص المصرح لهم بذلك، كما تتطلب تكامل المحتوى أي سلامتها من العبث أو التعديل أو الإفساد، وأخيراً توافر المعلومات وإتاحتها في الوقت المناسب من خلال الأشخاص المصرح لهم بذلك .غير أنه ومع تزايد استخدام الشبكة العنكبوتية أصبح مسألة الحماية معقدة وصعبة للغاية إذا لم نقول مستحلية .

ففي حين يشير تقرير نشره موقع "داتا بورت" أن هناك أكثر من 10مليارات جهاز متصل بالشبكة العنكبوتية، وثمة توقعات أن يصل هذا الرقم إلى 25مليار جهاز عام 2025 ،وأن عالم البيانات وصلت حجم مبيعاته إلى 100مليار دولار في عام 2017 ،وما يقارب 742مليار دولار عام 2020 , ومن المتوقع أن يصل إلى نحو 1,6 ترليون دولار بحلول عام 2025، بالإضافة إلى هذه الأرقام تأتي مسألة تخزين البيانات التي تعد أكبر معضلة تواجه

[1] إيجر أمينة,مرجع سابق, ص 77.

الدول بما فيها الدول الغربية المتطورة حيث أن 92 % من بياناتها مخزنة في الولايات المتحدة، وأن قانون الكلود الأمريكي (Cloud act)الذي دخل حيز التنفيذ عام 2018 في عهد الرئيس ترامب يسمح للحكومة الأمريكية بالولوج إلى البيانات المخزنة لدى الشركات التكنولوجية القائمة في الولايات المتحدة، عن طريق مذكرة أو استدعاء لتقديم البيانات المطلوبة المخزنة على الخوادم، بغض النظر عما إذا كانت البيانات مخزنة في الولايات المتحدة أو على أراضي أجنبية.

ويسمح قانون "كالود" للمدعي العام الأمريكي بإبرام اتفاقات خاصة تجعل للوكالات الأمنية الأمريكية، وشركائها في الخارج الحصول على البيانات الشخصية للمستخدمين المخزنة في الخارج من دون أمر من المحكمة. يشير مشروع القانون تحديداً إلى إسقاط مبدأ المعاملة بالمثل, ما يعني أن الاتفاقية المذكورة لن تنطبق على طلبات توفير بيانات شخصية للمستخدمين في الولايات المتحدة الأمريكية، وحتى يتجنب العالم أن يصبح مستعمرة رقمية للولايات المتحدة الأمريكية لابد تبني تشريعات حول الخدمات الرقمية والفضاء الرقمي[1].

ثانياً:التحديات السياسية و الاجتماعية.

تكمن أهمها في إعطاء الثقة للمواطنين للمشاركة في حماية بياناتهم الشخصية وحياتهم الشخصية, كما تسمح بحماية البنى التحتية بالنسبة للدول, أي تحقيق المواطنة الرقمية بتوجيه المواطن نحو منافع التقنيات الحديثة, وحمايتها من أخطارها وهي إذن التعامل الذكي مع التكنولوجيا و ذلك من خلال تربية الأجيال القادمة بالتحكم في الأدوات الرقمية, ومعرفة حقوقهم وحرياتهم و الاهتمام ببناء وحماية هويتهم الرقمية الناتجة عن الآثار المتبقية بشكل إرادي أو غير إرادي على الشبكات, كما يواجه الأفراد و المجتمعات تحديات في التعامل مع وسائل التواصل الاجتماعي ومنصات التواصل الرقمية, حيث يمكن أن يؤدي الاعتماد المفرط على

[1] نفس المرجع, ص,78.

هذه الوسائل إلى تأثيرات سلبية على الحصة النفسية والعلاقات الاجتماعية, كما يتعين عليهم التعامل مع التحديات المتعلقة بحماية الخصوصية الشخصية و التحكم في البيانات الرقمية الخاصة بهم, وهو أمر يشكل تحدياً في ظل الانتشار الواسع للمعلومات عبر الانترنت.

إلى جانب هذه التحديات يمكننا أن نذكر الوصول غير المتساوي للمعلومات و التكنولوجيا الرقمية بين الأفراد والمجتمعات, مما يمكن أن يزيد من الفجوات الاجتماعية و الاقتصادية, كما قد يؤدي التحول الرقمي إلى تغيرات في القيم و المعتقدات التي قد تنشأ نتيجة للتكنولوجيا الرقمية, بما في ذلك التأثير على التفاعلات الاجتماعية و العلاقات الإنسانية, وقد يساعد ذلك على ظهور ثقافة الرقمية مما يستوجب تحديد ماهيتها و تأثيرها على هوية المجتمعات و الأفراد , وكيفية الحفاظ على الهوايات الثقافية التقليدية في ظل التغيرات الرقمية, تتطلب هذه التحديات تفاعلاً وتكيفاً من المجتمعات و الأفراد للتعامل معها و المحافظة على الثقافة و القيم في عصر الرقمي. [1]

ثالثاً:التحديات الاقتصادية.

تشمل التحديات الاقتصادية مسألة المنافسة الغير شريفة التي تفرضها الشركات الكبرى العملاقة على الشركات الصغرى و المتوسطة وذلك باستغلال البيانات التي بحوزتها. فهي تتنافس مع الدولة على جذب الاستثمارات و المواهب وتطوير الابتكارات التقنية مما يشكل تهديد للدولة واقتصادها و يتطلب ذلك وضع التشريعات لمنع الاستغلال السيئ للبيانات, كما أن هذه المنافسة الغير شريفة تمتد إلى المجال الضريبي حيث لا تدفع الشركات الكبرى إلاّ ضريبة صغيرة على الأرباح حيث قدرت ب 9% مقابل 23% بالنسبة للشركات الأوروبية, ويتطلب تطوير الاقتصاد الرقمي استثمارات كبيرة في بنية التحتية الرقمية, مثل شبكات الانترنت عالية السرعة و التقنيات الحديثة, مما يشكل تحدياً مالياً وتنظيمياً للحكومات و الشركات, كما يتطلب

[1] نفس المرجع, ص,79.

أيضاً توفير القدرات و المهارات اللازمة للعمال في الاقتصاد الرقمي, وهو ما يشكل تحدياً للتعليم و تدريب القوى العاملة وتأهيلها لسوق العمل الرقمي المتطور[1]

رابعاً:التحديات القانونية.

تشمل مجموعة من القضايا والمسائل القانونية التي تؤثر على قدرة الدول المؤسسات للحفاظ على سيادتها وتحكمها في البيانات والنظم الرقمية، ومن بين هذه التشريعات تلك المتعلقة بحماية البيانات الشخصية وضمان الخصوصية, فهي تشكل تحدياً كبيراً للسيادة الرقمية، حيث تتطلب تلك القوانين التزامات صارمة من قبل الحكومات و المؤسسات لحماية بيانات المواطنين و العملاء, يمكن ذكر هنا بعض المحاولات التشريعية كلائحة الاتحاد الأوروبي لحماية البيانات الشخصية(RGPD) المعتمدة في 2018 .والجهود التي تبذلها كل من روسيا والصين لتطبيق التشريعات والسياسات التي تعزز السيادة الرقمية مثل قانون الانترنت السيادي Sovereign Law Internet الذي يجيز للحكومة الروسية حظر المواقع الأجنبية المناهضة لها م المتطرفة، وتشغيل انترنت مستقل في حالة انقطاع الاتصالات الأجنبية، أمّا الصين فقد وضعت جدار الصين الناري Firewall Great عبارة عن سلسلة من التنظيمات على شبكة الانترنت، وسياسات الرقابة على المواقع غير المرغوب فيها وحجبها. بالإضافة إلى الامتثال للقوانين الدولية المتعلقة بالأمن السيبراني والجرائم الإلكترونية التي شهدت تنسيقا فعالا بين الدول و المؤسسات الدولية، من أهمها اتفاقية بودابست لجرائم الحوسبة والجرائم السيبرانية في عام 2001 ، وقرارات الجمعية العامة للأمم المتحدة للأمن السيبراني كالقرار 237/70 ،التي دعت إلى تعزيز التعاون الدولي في مجال الأمن السيبراني ومكافحة جرائم الانترنت، واتفاقية الأمن السيبراني بين الولايات المتحدة والصين عام 2015 ،التي تهدف إلى تعزيز التعاون بين البلدين في مكافحة الجرائم السيبرانية وتبادل المعلومات وتعزيز الأمن السيبراني العالمي ، دون أن ننسى التشريعات المتعلقة بحقوق الملكية الفكرية والتأليف

[1] نفس المرجع,ص80.

والنشر التي تؤثر على قدرة التحكم في المعلومات الرقمية، وقد تؤدي إلى تحديات قانونية فيما يتعلق بنشر المحتوى وتبادل البيانات، و أيضاً التشريعات المتعلقة بمنافسة السوق، والحفاظ على المنافسة العادلة في البيئة الرقمية تعتبر تحدياً قانونياً, خاصة فيما يتعلق بالشركات التكنولوجية الكبيرة وسلطتها في السوق. وكذا النزاعات القانونية بين الدول حول السيادة الرقمية والقوانين الدولية المتعلقة بالانترنت و التجارة الالكترونية تشكل تحدياً قانونياً يتطلب حلولاً قانونية دولية فعالة, وعلى العموم تتطلب هذه التحديات استراتيجيات قانونية و تنظيمية فعالة للتعامل معها و حماية السيادة و الحقوق الرقمية للدول و المؤسسات[1].

خامساً:الذكاء الاصطناعي كأداة إستراتيجية لتعزيز السيادة الرقمية و صمود الأمن السيبراني.

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

مع تزايد حجم الأنشطة اليومية عبر الانترنت, يتم تبادل كميات هائلة من البيانات بين المستخدمين و البنية التحتية. هذا الكم الكبير يشكل تحدياً كبيراً لمحللي الأمن السيبراني في مراقبة حركة البيانات و تحليل سلوك الخوادم بدقة, مما يتيح له الكشف التلقائي عن التهديدات المحتملة فور ظهورها. نظراً للكم الهائل من المعلومات المتاحة على شبكة الانترنت, و تزايد حجم البيانات و انتشار البرمجيات المفتوحة المصدر, يواجه محللو الأمن السيبراني صعوبات كبيرة في رصد التهديدات الالكترونية 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 الالكتروني المهدد من المصادر العامة على الانترنت

[1] نفس المرجع, ص 80.

باستخدام تقنية متقدمة تعرف باسم Doc2Vec , والتي تمكن من تمثيل النصوص بشكل فعال لتحليلها و اكتشاف التهديدات بدقة أكبر.

إن 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 و التنبؤ بالهجمات المستقبلية . هذا يمكن الجهات الأمنية من اتخاذ إجراءات وقائية سريعة وفعالة, حيث يبقى الذكاء الاصطناعي في حالة تأهب مستمر لمواجهة أي تهديد محتمل لحماية البيانات و الأنظمة[1].

يمثل الكشف السريع عن التهديدات 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 حلاً لهذه التحديات عبر تحسين سرعة و دقة عمليات الكشف و الاستجابة.

فقد أدى التقدم التكنولوجي في العصر الحديث إلى توسيع استخدامات الذكاء الاصطناعي ليصبح أداة محورية في دعم الأمن و مكافحة الإرهاب, خاصة من خلال قدرته على التفاعل مع وسائل الاتصال الحديثة و شبكات التواصل الاجتماعي, مما أتاح للأجهزة الأمنية كشف التهديدات المحتملة و اعتراضها قبل وقوعها. يستخدم الذكاء الاصطناعي في جمع و تحليل كميات ضخمة من البيانات, وتتبع المعلمات الدقيقة, و التعرف على الوجوه, ما يساعد في تحديد منفذي العمليات الإرهابية و المروجين لها. كما يساهم في تقليل هامش الخطأ خلال

[1] وافي حاجة,مرجع سابق,ص,23,24.22

عمليات البحث و التحقيق والملاحقة, مما يعزز كفاءة الأجهزة الأمنية ويزيد من ثقة المواطنين بها. كذلك, يساعد الذكاء الاصطناعي في تصنيف الأفراد المعرضين للتأثير بالأفكار الهدامة و توجيههم عبر برامج وقائية مخصصة, كما يمكنه تحيل 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 كالفيسبوك, من خلال مطابقة و تحليل الصور.

سادساً:الذكاء الاصطناعي كأداة لتعزيز الأمن القومي.

يساهم الذكاء الاصطناعي بشكل فعال في تعزيز الأمن القومي من خلال عدة فوائد رئيسية, أبرزها القدرة على التنبؤ و الاستشعار المبكر للتهديدات عبر تحليل كميات ضخمة من البيانات و اكتشاف الأنماط المحتملة, ممّا يساعد على إصدار تحذيرات استباقية. كما يستخدم في التعرف على الوجوه وتتبع المطلوبين, وتحسين نظم المراقبة الحدودية باستخدام تقنيات متقدمة, فضلاً عن دوره في دعم الأمن السيبراني عبر رصد الهجمات الرقمية و التصدي لها بفعالية. ويعد الذكاء الاصطناعي أداة مهمة في دعم اتخاذ القرار الأمني, من خلال تقديم تحليلات وتوصيات دقيقة و سريعة, تسهم في مواجهة التحديات الأمنية بكفاءة أعلى[1].

سابعاً:أثر الذكاء الاصطناعي في تصاعد الهجمات السيبرانية وانتهاك السيادة الرقمية.

رغم أن أنظمة الأمن المبنية على الذكاء الاصطناعي صمت لحماية البنية التحتية الرقمية من التهديدات السيبرانية, إلاّ أن هذه الأنظمة قد تتحول إلى سلاح فعال في أيدي القراصنة, والمخترقين,وحتى بعض الأجهزة الإستخباراتية, حيث يمكن استغلال قدرات الذكاء الاصطناعي لشن هجمات احتيالية متقدمة , وتنفيذ تهديدات آلية, واستخدام الروبوتات الذكية في مهاجمة

[1] نفس المرجع,ص25,26.

البنى التحتية الرقمية, و التكيف مع أنظمة التشغيل لتفادي الاكتشاف من قبل برامج الحماية, بل وحتى مهاجمة أنظمة الكشف ذاتها.

في المقابل, تعاني أنظمة الأمن المتعددة على الذكاء الاصطناعي من محدودات تجعلها عرضة للخداع, لا سيما عند الاعتماد على بيانات تدريب غير دقيقة, أو مفرطة المعالجة ممّا يؤدي إلى اتخاذ قرارات خاطئة. هذه الثغرات قد تستغل لتنفيذ هجمات سيبرانية مدمرة تؤدي إلى خسائر مادية جسيمة, كما تقوّض قدرة الدولة على حماية فضائها الرقمي, بما يهدد سيادتها الرقمية ويضعف أمنها السيبراني في مواجهة التهديدات المتزايدة و المعقدة.

الفرع الرابع:العوامل المهددة للسيادة الرقمية للدولة .

يعد عصر الانترنت سلاح ذو حدين ولعل الحد السلبي منها هو تعريض السيادة الرقمية لتحديات وضغوط غير محمودة العواقب خاصة على الدول الهشة رقمياً، حيث تشكل السبل الجديدة للهجمات السيبرانية التطفل على الامتيازات السيادية للدول، وفي هذا الصدد عجز القانون على مواكبة التكنولوجيا العصرية بمفهومها الأمني، وحسب القانون الدولي فإن مسؤوليات الدول عن معاجلة الهجمات السيبرانية غير كافٍ وتتطلب التهديدات الخارجية التي حددت تشكيل السيادة الرقمية للدولة الحديثة إعادة الاعتبار لأم التحديات والتهديدات التكنولوجية والاقتصادية والسياسية والاجتماعية[1].

أولا:التهديدات الخارجية الناشئة.

كانت للهجمات التي شنها مجرمو الانترنت على البنية التحتية الحيوية وموارد المعلومات على مدى العقود القليلة الماضية نتائج كارثية، تسببت الجرائم الالكرتونية في خسائر تقدر بأكثر من 6000 مليار دولار على مستوى العامل في عام 2021 ،وهذا هو السبب الرئيسي في تطوير أساليب دولية وحكومية لمنع الهجمات الالكرتونية، وقد بدأت بعض البلدان بذلك

[1] بن بية عادل، بلقرشي إيمان,مرجع سابق,ص69

فعال، وبادرت في إنشاء كوادر مؤسسية على سبيل المثال، في عام 2013 ،أقر الإتحاد الروسي القانون الفيدرالي رقمFZ187 ،الذي "ينص على تعديل بعض القوانين التشريعية لإتحاد الروسي بشأن حماية الحقوق الفكرية على شبكات المعلومات والاتصالات""، أيضا قدمت الولايات المتحدة تدبيرين في عامي 2011 و2012 قانون منع التهديدات الحقيقية عبر الانترنت للإبداع الاقتصادي و سرقة الملكية الفكرية و قانون وقف القرصنة على الانترنت لكن بسبب العقوبات الصارمة, لم تحظى مشاريع القوانين هذه بالدعم بشأن الجرائم, يجب أيضاً حماية الأسرار التجارية و أسرار الإنتاج في الفضاء الإلكتروني, بالإضافة إلى حقوق النشر و براءات الاختراع من أجل توحيد القوانين في جميع الدول الأعضاء, قدم البرلمان الأوروبي التوجيه بشأن حماية الأسرار التجارية و المعرفة في الاتحاد الأوروبي في عام 2013, تعمل القوانين ضد المنافسة غير العادلة على حماية المعرفة هذه هي لوائح القانون العام في الولايات المتحدة و المملكة المتحدة يحكم القانون الاتحادي رقم FW98_ " بشأن الأسرار التجارية" والفصل 75 من القانون المدني[1].

ثانياً:الأجندة السياسية الدولية.

لقد أدى التحول في النظام السياسي العالمي من عالم ثنائي القطب إلى عالم أحادي القطب بعد انهيار الاتحاد السوفييتي, وتشكل عدة أقطاب للقوة ما ينبئ بإعادة تشكيل خارطة العلاقات بمبادئ جديدة في المستقبل القريب من الطبيعي و المتوقع أن يشكل رفض العولمة السابقة حدثاً هاماً, لكنه يمثل تهديداً كبيراً للمجتمع العالمي و المنافسة على مناطق النفوذ, وتصعيد الصراعات العسكرية الإقليمية, من ناحية أخرى, أدت المنافسة بين الدول و الشركات الناجمة عن المناخ الجيوسياسي الحالي إلى تسريع تطوير التكنولوجيا الرقمية بشكل كبير ومع ذلك, فإنها تجعل بعض الدول و المنظمات أكثر تقدماً من الناحية التكنولوجيا من غيرها في المنافسة

[1] نفس سابق,ص69.

على الموارد, وفي نهاية المطاف, على الزعامة السياسية العالمية, على الأمم المتحدة أن تأخذ زمام المبادرة في إنشاء إطار لتحقيق المساواة الرقمية العالمية و الدعوة إلى استخدام البيانات التكنولوجيا الرقمية لإنشاء استراتيجيات سياسية أكثر مرونة, سيساعد التعاون بين الدول في الفضاء الرقمي على تقليل التوترات الجيوسياسية و إنشاء معايير عالمية عادلة في مجال الأمن واحترام حقوق الإنسان وترد هذه في تقارير الفريق الرفيع المستوى المعني بالتعاون الرقمي و إستراتيجية الأمم المتحدة بشأن التكنولوجيات الجديدة[1].

ثالثاً:الصراع من أجل الريادة التكنولوجية العالمية.

لقد شهدت السنوات العشر الماضية تحولاً في دور الزعامة التقنية العالمية في السياسة الاقتصادية, الأمر الذي أثر على تفضيلات الاسترداد و التصدير لدى اتحادات الدول و الأمم, إن إحدى الطرق التي يمكن للدول من خلالها تعزيز استقلالها التقني هي التنافس على التفوق التكنولوجي, لقد اتخذ مفهوم تحقيق الاستقلال التقني دور نموذج العولمة الذي اعتمد على التعاون في مجال العلوم والتكنولوجيا, إن التهديدات التي تشكلها التكنولوجيا المتقدمة تتسبب في تدهور السيادة الرقمية للدول الفقيرة لذلك, فإن استخدام التكنولوجيا المتقدمة في العديد من المجالات, وخاصة تلك ذات الأهمية الوطنية, يضمن القدرة التنافسية للدول الفقيرة, وفقاً لمؤشر الابتكار العالمي, يجري الآن سباق بين الدول الرائدة لتطوير التقنيات في مجال الذكاء الاصطناعي.

وفي عام 2017 قدمت الصين خطة لتطوير خطة لتطوير الذكاء الاصطناعي بحلول عام 2030 بتمويل إجمالي قدره 150 مليار دولار.

[1] نفس سابق,ص69.

رابعاً:بنية تحتية رقمية عالمية موحدة.

توفر العناصر الحالية للبنية التحتية الرقمية, في شكل خطوط اتصالات الألياف الضوئية وأرباح الهاتف المحمول (G3, G4, G5) الوصول إلى الانترنت العالمي لجزء فقط من سكان العالم إنشاء وصاية البنية التحتية في المناطق النائية و الريفية (وخاصة مناطق القطب الشمالي) مهمة صعبة تتطلب استثمارات مالية جادة وفي العقد الماضي, ظهرت طريقة بديلة, وهي الانترنت عبر الأقمار الصناعية عالية الجودة و السرعة من مدار أرضي منخفض, مما سيسمح لمطوري تقنيات الفضاء و الأقمار الصناعية بتغطية العالم كله و مع ذلك, وروسيا و الصين و اليابان و الهند و فرنسا و المملكة المتحدة هي الرائدة في عدد المركبات الفضائية و عمليات إطلاقها وتحاول دول أخرى أيضاً الدخول في سباق الفضاء الجديد , لكن الافتقار إلى البنية التحتية اللازمة لإطلاق الأقمار الصناعية, والتطورات العلمية و التكنولوجية الخاصة بها في صناعة الفضاء, والموارد الأخرى, تحد من قدراتها[1].

خامساً:الحمائية الرقمية.

لقد أجبرت رقمنة الاقتصاد العالمي العديد من البلدان على تنفيذ سياسات الحماية الرقمية بسبب ضبابية و غياب الوضوح في الحدود الوطنية للأسواق الرقمية, وطرق الاتصال ونقل البيانات عبر الحدود وضعف البنية التحتية الرقمية وحمايتها من المخاطر, إلى جانب القيود الاصطناعية على استيراد التقنيات و السلع و البيانات و الخدمات الرقمية, هذه السياسات لها آثار إيجابية و سلبية على السيادة الرقمية للدولة إحدى الطرق التي قد تساعد بها سياسة استبدال الواردات العدوانية الأمة في بناء تقنياتها الرقمية الخاصة هي من خلال الترويج لاستخدامها ومع ذلك, فإن غياب المنافسة من السلع المستوردة يمكن أن يشجع أيضاً الابتكار ويخفض جودة السلع المحلية, مما يفوض السيادة الرقمية وفي هذا الصدد, تحاول الدول

[1] نفس المرجع, ص 70.

الفردية(المجموعات أو النقابات) ضمان أمن الفضاء الرقمي الوطني الخاص بها عندما وضعت العديد من الدول متطلبات إلزامية للشركات الرقمية العالمية لتحديد قواعد البيانات الخاصة بمواطنيها في أراضيها لقد تطورت الحاجة ألى تحديد وحماية البيانات الشخصية للمواطنين تدريجياً إلى الحمائية الرقمية في قطاع التجارة ومع إطلاق الأسواق العالمية الكبيرة, أصبح من الممكن شراء الفردية (المجموعات و النقابات) ضمان أمن الفضاء الرقمي الوطني الخاص بها عندما وضعت العديد من الدول متطلبات إلزامية للشركات الرقمية العالمية لتحديد قواعد البيانات الخاصة بمواطنيها في أراضيها لقد تطورت الحاجة إلى تحديد وحماية البيانات الشخصية للمواطنين تدريجياً إلى الحمائية الرقمية في قطاع التجارة ومع إطلاق الأسواق العالمية الكبيرة, أصبح من الممكن شراء البضائع من وفي أي مكان في العالم[1].

سادساً:الشركات العابرة للحدود.

إن التوسع الجغرافي للشركات عبر الوطنية لها تأثير إيجابي على النظم الاجتماعية و الاقتصادية للبلدان التي تعمل فيها حيث ترتبط التغيرات الايجابية بنقل المعرفة و إدخال تقنيات وأساليب إدارية جديدة تعمل الشركات عبر الوطنية كمصدر للاستثمارات الأجنبية المباشرة في المناطق و الصناعات تنتقل العديد من الشركات عبر الوطنية إلى تصميم الأعمال الرقمية تتزايد حصة الشركات الرقمية التي تقدم الخدمات من خلال منصاتها الخاصة (Google, Amazon, Apple, Microsoft, bay ,Airbnb) وتدخل بلداناً جديدة ليس فقط من خلال التنويع الجغرافي ولكن أيضاً من خلال التوسع الرقمي(جمع البيانات وتخزينها ومعالجتها) يتزايد عدد المستخدمين تدريجياً وتتوسع تغطية بيانات المستخدم تصبح هذه البيانات مورداً جديداً في السوق الرقمية و التكنولوجيا الفائقة بامتلاكها مجموعة فريدة من البيانات, بما في ذلك البيانات الشخصية, يمكن للشركات التأثير على العمليات الاجتماعية و الاقتصادية و السياسية في

[1] نفس المرجع,ص71,72.

المناطق التي تعمل فيها و بالتالي, فإن التهديد الرئيسي هو انتقال بعض وظائف الدولة إلى منطقة نفوذ الشركات عبر الوطنية.

قد تنشأ اتجاهات سلبية أخرى أثناء التوسع الاستثماري والتكامل الرأسي من خلال اندماج الشركات المحلية الصغيرة و المتوسطة الحجم التي إمّا تتنافس مع الشركات في محاولات تطوير وتنفيذ تقنيات مبتكرة أو تقديم خدمات أخرى لنفس المستهلكين[1].

[1] نفس المرجع ,ص,73.

الخاتمة

الخاتمة

وفي ختام دراستنا, تبين أن للذكاء الاصطناعي دور فعال في تحقيق الأمن السيبراني وتعزيز السيادة الرقمية يظهر ممّا سبق, أن الذكاء الاصطناعي يعد فاعلاً محورياً في تشكيل معالم السيادة الرقمية وتعزيز الأمن السيبراني. لقد ساعد الذكاء الاصطناعي في تحسين الدول قدرتها في الرصد و التنبؤ بالهجمات السيبرانية, وساهم في تطوير استراتيجيات متقدمة لحماية الفضاء الرقمي,إلاّ أن هذا التطور يطرح من جهة أخرى تحديات قانونية وأمنية معقدة, ترتبط بتقويض سيادة الدول, وتصاعد الهجمات السيبرانية, واحتكار التكنولوجيا من قبل كيانات غير خاصة للرقابة الدولية في عصر الذكاء الاصطناعي.

وعليه توصلت الدراسة للنتائج التالي:

- أصبح الذكاء الاصطناعي أداة مزدوجة, تجمع بين التمكين السيبراني و التهديد للسيادة الرقمية,
- عجز الإطار القانوني الدولي عن مواكبة تسارع التطورات التقنية, ممّا يخلق فراغاً تنظيمياً في الفضاء السيبراني,
- يمكن أن تتحول أدوات الذكاء الاصطناعي إلى وسائل هجومية في أيدي الفاعلين غير الحكوميين والتنظيمات الإرهابية,
- يؤدي الاعتماد المفرط على تقنيات مستوردة إلى تهديد السيادة التقنية و الرقمية للدول,
- الذكاء الاصطناعي يحدث تحولاً في البنية الاقتصادية و الاجتماعية للدول, ما يستلزم تكيفاً تشريعياً وهيكلياً مستمراً,
- 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 التحكم في فضائها وإقليمها الرقمي,
- أهم التحديات التي تواجهها الدول في تحقيق سيادتها الرقمية, غياب الصفة القانونية و المعنوية لشبكة الانترنت إضافة على انتشارها الواسع و اللامحدود,

- أدت هيمنة الأجهزة الإلكترونية وبرامج الذكاء الاصطناعي إلى ظهور جرائم وتهديدات سيبرانية بدوافع متعددة مفوضة للسيادة الرقمية للدول,
- أسهم الذكاء الاصطناعي في تحسين القدرة على اكتشاف الهجمات المتقدمة و الأنشطة غير الطبيعية بسرعة أكبر مقارنة بالأساليب التقليدية,
- من خلال الأتتمة , أصبح من الممكن استجابة الأنظمة للهجمات الالكترونية بشكل أكثر سرعة وفعالية, ممّا يقلل من الأضرار الناتجة,
- تمكن تقنيات الذكاء الاصطناعي من معالجة وتحليل كميات ضخمة من البيانات في وقت قصير, ممّا يعزز القدرة على التنبؤ بالهجمات المستقبلية,
- ساعد الذكاء الاصطناعي في تطوير استراتيجيات أمنية أكثر تطوراً ومرونة, ممّا يساهم في تعزيز دفاعات الأنظمة ضد الهجمات المتزايدة التعقيدة.

قائمة المصادر والمراجع

قائمة المصادر و المراجع:

أولاً: باللغة العربية.

أ): القوانين.

1. من القانون 18-04 المتضمن القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، المؤرخ في 10-05-2018، الجريدة الرسمية، العدد 03، الصادرة بتاريخ 13-05-2018.
2. القانون رقم 18_07, المؤرخ في 10يونيو 2018, المعدل والمتمم بالقانون رقم 25_11, المؤرخ في 24 يوليو 2025, المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي,الصادر في الجريدة الرسمية.2018,34
3. القانون رقم24_06, المؤرخ في 28 أبريل 2024, يعدل ويتمم الأمر رقم 66_156 والمتضمن قانون العقوبات, الصادر في الجريدة الرسمية,العدد2024,30.
4. القانون رقم 25_11, المؤرخ في 24 يوليو 2025, يعدل ويتمم القانون رقم 18_07 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي, الصادر في الجريدة الرسمية,العدد 2025,48.
5. القانون رقم 25_14 , المؤرخ في 03 أوت 2025.المتعلق بالإجراءات الجزائية الجزائري, الصادر في الجريدة الرسمية,العدد2025,54

ب)_النصوص التنظيمية:

1. المرسوم الرئاسي 20-05,المؤرخ في 20 جانفي 2020, المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية,الصادر في الجريدة الرسمية,العدد.2020,04.
2. المرسوم الرئاسي رقم 23_314 المعدل بمقتضى المرسوم الرئاسي رقم 25-320 المؤرخ في 30 ديسمبر سنة 2025، والمتضمن وضع منظومة وطنية لحوكمة البيانات, الصادر في الجريدة الرسمية الجزائرية, الصادرة في 10 سبتمبر 2023,العدد59.

3. المرسوم الرئاسي رقم 25_320 المؤرخ في 30 ديسمبر 2025 المتضمن وضع المنظومة الوطنية لحوكمة البيانات, الصادر في الجريدة الرسمية ,العدد87, 2025

ج):التقارير.

1. تقرير الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات، 2011-2015 .

د):المؤلفات.

1. أحمد سعيد فرحات السرجاني، *التحول الرقمي في تحقيق الأمن السيبراني*، دار العلم والإيمان، جمهورية مصر العربية، محافظة كفر الشيخ، 2025.

2. أحمد طارق محمد، *البيانات المتوافقة في الشبكات والهجمات الأمنية السيبرانية*، الطبعة الأولى، مؤسسة الوراق للنشر والتوزيع، الأردن،2024.

3. أماني يحيى عبد المنعم النقيب, الذكاء الاصطناعي وآثاره على المجتمع, دار الفكر الجامعي,2024.

4. بلباي إكرام, الذكاء الاصطناعي في القانون الدولي.دراسة في المفهوم و الأطر و التطبيقات,ابن النديم للنشر و التوزيع و مؤسسة الكتاب القانوني, الطبعة الأولى,2024.

5. بتشيم بوجمعة,الذكاء الاصطناعي في منظومة العدالة الحديثة على ضوء أحداث أحكام التشريع والقضاء المقارن إلى غاية سنة 2022,الناشر ألفا للوثائق,الطبعة الأولى,2023.

6. حسين مصيلحي، *التحول الرقمي: الإطار المستقبلي لنظم وتكنولوجيا المعلومات*، دار الكتب والوثائق، الطبعة الأولى، 2024.

7. دحان حزام ناصر القربطي، *الأمن السيبراني وحماية أمن المعلومات*، دار الفكر الجامعي، الإسكندرية، 2024.

8. شريفة كلاع، *الأمن السيبراني وأشكال التهديد: تحديات عالمية*، ألفا للوثائق للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2023.

9. صدام حسين قيراد، *الإرهاب السيبراني وتداعياته الرقمية*، Edition Best Book، الجزائر، 2025.

10. علاء عبد الرزاق سالمي، *مدخل إلى الذكاء الاصطناعي السيبراني*، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية,2022 .

11. عفيفي حافظ محمد، *الشبكات العنكبوتية السيبرانية العالمية المبرمجة*، الطبعة الأولى، مؤسسة الرواق للنشر والدار الجزائرية للكتاب زموري، الجزائر، والتوزيع بالأردن، 2025.

12. فارس محمد العمارات، إبراهيم الحمامصة، *الأمن السيبراني: المفهوم وتحديات العصر*، دار الخليج للنشر والتوزيع، الأردن، الطبعة الأولى، 2022.

13. محمد سعادي، *القانون الإنساني الدولي*، المصرية للنشر والتوزيع، 25 فبراير 2020.

14. نريمان فتيئية، خولة هاني، *الحرب السيبرانية من منظور القانون الدولي والتنظيم الدولي وسبل المواجهة*، المكتبة الوطنية الجزائرية، جوان 2023.

15. وافي حاجة، *استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني*، منشورات دار لامية، الجزائر، 2025.

م):المجلات العلمية.

1. أحمد حاتم جبار عطية، "الأبعاد القانونية والاجتماعية للأمن السيبراني"، *مجلة الشرق الأوسط للدراسات الفقهية والقانونية*، المجلد 05، العدد 03، 2025 .

2. أحمد السيد النجار، محمد عبد الهادي علام, "حروب المعلومات من يواجهها؟"، مجلة الأهرام, العدد 139,يوليو2015.

3. أحمد محمد، "دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني"، *مجلة العلوم الإنسانية والطبيعية*، المجلد 06، العدد 10، 2025 .

4. إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، مجلة اتجاهات الأحداث، ع 22,أوت 2017

5. إيجر أمينة، "السيادة الرقمية في العالم المعولم: التحديات والرهانات"، *مجلة الدراسات القانونية والسياسية*، جامعة الجزائر 3، المجلد 10، العدد 02، جوان 2024 .

6. الشيماء مخالفية، كريمة لعيساوي، "السيادة الرقمية: تكيف العقيدة الدفاعية الجزائرية مع التهديدات الأمنية الجديدة"، *المجلة الجزائرية للعلوم الاجتماعية والإنسانية*، المجلد 13، العدد 02، 2025.

7. السبتي آسيا، بوقريط عمر، "دور الذكاء الاصطناعي في تحقيق الأمن السيبراني"، *المجلة الدولية للبحوث القانونية والسياسية*، المجلد08، العدد03، 2024.

8. بلحاج خالدية، فرعون محمد، "السيادة الرقمية"، *مجلة البحوث في الحقوق والعلوم السياسية*، المجلد 11، العدد 01، 2025 .

9. بن أحمد فاطمة الزهراء، صحراوي بن شيحة، "الذكاء الاصطناعي وتحسين الأمن السيبراني للمنظمات: دراسة حالة شركة مايكروسوفت"، المجلد 11، العدد 01، 2025 .

10. بن بية عادل، بلقرشي إيمان، "السياسة الرقمية في الجزائر بين التحول المنشود وتحديات السيادة الرقمية"، *مجلة الناقد للدراسات السياسية*، المجلد 09، العدد 01، 2025 .

11. بن قطاط خديجة، "تداعيات الحروب السيبرانية على السيادة الرقمية"، *مجلة القانون العام الجزائري والمقارن*، المجلد 10، العدد 02، ديسمبر 2024 .

12. بوالديار نوال، بوالديار فوزي، "الذكاء الاصطناعي والأمن السيبراني: المدلول والتحديات"، مداخلة في ملتقى وطني بعنوان *تحديات الأمن السيبراني في عصر الذكاء الاصطناعي: علاقة تأثر وتأثير*، جامعة الشهيد الشيخ العربي التبسي، تبسة، كلية الحقوق والعلوم السياسية، 30-11-2025 .

13. بوخنفر زوليخة، "الشبكات المعلوماتية العملاقة على الويب GAFAM والدولة: تحديات السيادة الرقمية"، *مجلة الدراسات الإعلامية والاتصالية*، المجلد 03، العدد 01، مارس 2023 .

14. تقية توفيق، رشيد بوبكر، "الأطر القانونية لتعزيز السيادة الرقمية للدولة في مواجهة التحديات المتعلقة بالاستخدامات السلبية المحتملة للذكاء الاصطناعي"، *مجلة صوت القانون*، المجلد 11، العدد 01، 2024 .

15. حمد عبد الله علي النيادي، "الدليل السيبراني المستمد من الذكاء الاصطناعي"، *المجلة القانونية*، المجلد 14، العدد 04، 2022 .

16. هاشم عبد الله الحاتم علي وآخرون، "توظيف تقنيات الذكاء الاصطناعي في التحقق من المحتوى الإخباري بالتطبيق على عينة من الأخبار بموقع جمنة الإخباري"، *مجلة بحوث ودراسات في الميديا الجديدة*، المجلد 05، العدد 03، 2024 .

17. هبة عبد المجيد، عبد الحافظ العودة، "التحديات التي تواجه الأمن السيبراني"، *مجلة* Humanities Natural Sciences Journal (HNS) ، المجلد 06، العدد 07، 2025

18. هيثم رزق فضل الله، "دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني: دراسة تحليلية للتحديات والحلول المستقبلية"، *المجلة المصرية للدراسات المتخصصة*، المجلد 13، العدد 46، الجزء 05، أفريل 2025 .

19. هناء رشيد محيسن كزار، "التهديدات السيبرانية وأثرها على العلاقات الأمريكية الصينية"، *مجلة كلية القانون والعلوم السياسية*، الجامعة العراقية، العدد 28، 2025.

20. نور الدين حامد علي إبراهيم، "الفضاء السيبراني: المفاهيم والأبعاد"، *المجلة العلمية للبحوث والدراسات التجارية*، جامعة حلوان، المجلد38، العدد02، 2024

21. سامية بوشوشة، حياة سلماني، "التجسس الإلكتروني وطرق مكافحته"، *مجلة العلوم الاجتماعية والإنسانية*، جامعة تبسة، المجلد 16، العدد 01، 2023.

22. سعداوي عمر، "السيادة الرقمية في ظل العولمة التكنولوجية والرهانات الجيوسياسية"، *المجلة الجزائرية للحقوق والعلوم السياسية*، المجلد 10، العدد 02، 2025 .

23. سارة بخوش، "الذكاء الاصطناعي والأمن السيبراني: الوظائف والتحديات"، *المجلة الجزائرية للعلوم الإنسانية والاجتماعية*، المجلد 09، العدد 01، 2025 .

24. سمير بارة، "الأمن السيبراني في الجزائر: السياسات والمؤسسات"، *المجلة الجزائرية للأمن الإنساني*، المجلد 02، العدد 04، 2017 .

25. سنوسي علي، "السيادة الرقمية والاستقلال التكنولوجي بين تحديات الظروف الوطنية والدولية"، *المجلة الجزائرية للحقوق والعلوم السياسية*، المجلد 09، العدد 02، 2024 .

26. شحيرط أحمد، قريبيز مراد، "تحديات الإنترنت لسيادة الدول (السيادة الرقمية")، *مجلة البحوث القانونية والاقتصادية*، المجلد 05، العدد 01، 2022 .

27. شريفة كلاع، "الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني"، *مجلة الحقوق والعلوم الإنسانية*، جامعة الجلفة، المجلد 15، العدد 01، 2022 .

28. عبد العالم حسين الفقيه وآخرون، "الذكاء الاصطناعي: السلبيات والإيجابيات وفق رؤية شرعية وقانونية وسبل المواجهة (دراسة تحليلية"(، *مجلة جامعة البيضاء*، المجلد 07، العدد 02، أفريل 2025 .

29. فاطمة علي إبراهيم، رحاب يوسف، وليد محمود السيد، "الأمن السيبراني والنظافة الرقمية"، *المجلة المصرية لعلوم المعلومات*، المجلد 09، العدد 02، 2022 .

30. قطاف سليمان، بوقريت عبد الحليم، "الأمن السيبراني والمضامين المفاهيمية المرتبطة به"، *مجلة طبنة للدراسات العلمية الأكاديمية*، المجلد 05، العدد 02 .

31. كريم رقولي، لخضر نويوة، "الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية"، *مجلة طبنة للدراسات العلمية الأكاديمية*، المجلد 02، العدد 02، 2019 .

32. محمد حسن المهندي، "الإطار القانوني للأمن السيبراني في المحافظة على الصحة العامة في القانون القطري: دراسة مقارنة"، *مجلة الدراسات الإنسانية والاجتماعية*، جامعة وهران 08، المجلد 14، العدد 02، 2025 .

33. محمد دحماني، "الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني"، *مجلة الفكر القانوني والسياسي*، المجلد 07، العدد 02، 2023 .

34. محمد مختار، "الأمن السيبراني: مفاهيم المستقبل"، *مجلة اتجاهات الأحداث*، العدد 02، 2025، ص06 .

35. محمود علي عبد الرحمان، أسامة فاروق مخيم، "الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية"، *مجلة كلية السياسة والاقتصاد*، جامعة محمد البشير الإبراهيمي، برج بوعريريج، المجلد 06، العدد 05 .

ه) مذكرات التخرج:

1. بوعلام فتيحة، *الأمن السيبراني في الجزائر*، مذكرة ماستر في القانون الخاص، تخصص قانون خاص، جامعة مستغانم، السنة الجامعية 2024-2025 .

2. بوحفص راوية، *الجريمة الإلكترونية في التشريع الجزائري*، مذكرة ماستر، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، تخصص قانون جنائي، السنة الجامعية 2017-2018.

3. حنين جميل أبو حسن، *الإطار القانوني لخدمات الأمن السيبراني: دراسة مقارنة*، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2024 .

4. شاري خيرة، صادقي إيمان، *الأمن السيبراني وأثره في تحقيق الأمن القومي*، مذكرة ماستر، جامعة محمد البشير الإبراهيمي، برج بوعريريج، كلية الحقوق والعلوم السياسية، تخصص إعلام آلي وإنترنت، 2023-2024 .

5. صمودي كريمة، برقعي سمر، *الأمن السيبراني في الجزائر*، مذكرة ماستر، جامعة 08 ماي 1945 قالمة، كلية الحقوق والعلوم السياسية، تخصص قانون أعمال، السنة الدراسية 2024-2025 .

6. عيش موسى، خيمود محمد، *الأمن السيبراني*، مذكرة ماستر، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، تخصص قانون جنائي والعلوم الجنائية، الجزائر، 2023 .

7. عبد الباسط عيساوي, سفيان زيتوني,آثار الذكاء الاصطناعي على الأمن السيبراني,مذكرة ماستر, جامعة الشهيد حمة لخضر – الوادي,كلية الحقوق والعلوم السياسية, السنة الجامعية2024/2023.

8. لعياشي حمزة، قعفر محمد الأمين، *الأمن السيبراني وحماية البيانات الرقمية في الجزائر*، مذكرة ماستر، جامعة محمد البشير الإبراهيمي، برج بوعريريج، كلية الحقوق والعلوم السياسية، تخصص قانون الإعلام الآلي والإنترنت، 2023-2024 .

9. معمري حفيظة، مجيدي يحيى، ركابي صدام، *آثار الذكاء الاصطناعي على الأمن السيبراني: دراسة حالة الجزائر*، مذكرة ماستر، تخصص سياسة عامة، جامعة الشهيد حمة لخضر، الوادي، كلية الحقوق والعلوم السياسية، 2023-2024 .

10. سلاوي بشرى وآخرون، *مستقبل السيادة الرقمية في ظل التكنولوجيات الحديثة: دراسة تحليلية استشرافية*، مذكرة ماستر، جامعة 08 ماي 1945، كلية العلوم الإنسانية والاجتماعية، السنة الجامعية 2019-2020.

و):المواقع الالكترونية:

1. أنواع الاختراقات الالكترونية أبرز الهجمات السيبرانية,https://routesa.ap
2. أسامة بوعرفة,مفاهيم الأمن السيبراني,https://www.noor-book.com .
3. ايجابيات وسلبيات الذكاء الاصطناعي-https://bakkah.com/ar/knowledge-center/
4. الجزيرة نت,"الأمن السيبراني": مفهومه وتاريخه,19 سبتمبر 2024 , https://www.aljazeera.net/
5. الجزائر تسعى إلى تعزيز سيادتها الرقمية من خلال الإستراتيجية الوطنية للتحول الرقمي,**https://www.aps.dz/algerie/actualite-nationale/mhutp24i-**
6. الجزائر تسعى إلى تعزيز سيادتها الرقمية,https://www.entv.dz/ar/news
7. الذكاء الاصطناعي والأمن السيبراني: العلاقة والفرق بينهما وتحدياتهما, https://bakkah.com/ar/knowledge-center
8. الذكاء الاصطناعي في الأمن السيبراني: الفوائد الرئيسية , واستراتيجيات الدفاع والاتجاهات المستقبلية,https://www.fortinet.com/resource .
9. الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية , https://www.mdn.dz/assi/nsiss_ar.pdf

10. المنظومة الوطنية لحوكمة البيانات,
https://www.hcn.dz/projets/juridique/GouvernanceDonnees

11. البوابة الوطنية للخدمات الرقمية,
https://www.hcn.dz/projets/FondementTechnologique/Portail-unifi%C3%A9.

12. النظام الوطني للتشغيل البيني,
https://www.hcn.dz/projets/FondementTechnologique/Datashiring

13. البنية التحتية للشبكة الوطنية المؤمّنة المسماة بـ"IRIES",
https://www.hcn.dz/projets/FondementTechnologique/IRIES

14. بورحيل, حوكمة البيانات ركيزة أساسية لنجاح التحول الرقمي,
https://www.aps.dz/algerie/actualite-nationale/mo8qjidz

15. بيان لوزارة الدفاع الوطني, وكالة أمن الأنظمة المعلوماتية لوزارة الدفاع الوطني تنشر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029,
https://www.mdn.dz/site_principal

16. جو لي ,ما المقصود بالسيادة الرقمية؟,
https://www.trendmicro.com/ar_sa/what-is/data-sovereignty/digital-sovereignty.html

17. جميل حسين طويلة, تاريخ الأمن السيبراني, .https://www.noor-book.com/

18. حوكمة البيانات في الجزائر: وضع الحجر الأساس للسيادة الرقمية وإدارة متطورة,
https://www.entv.dz/ar/news

19. نشر المرجعين,المحافظة السامية للرقمنة,
https://www.hcn.dz/projets/juridique/PublicationR

20. شرح معنى "الأمن السيبراني",https //hbrarabic.com

21. عطية السحاتي, الأمن السيبراني ودوه في حماية الأمن القومي,
https://www.noor-book.com._

22. عطية السحاتي, الأمن السيبراني ودوره في حماية الفضاء السيبراني للمؤسسات التي تعمل في المجال الجوي الوطني, https://www.noor-book.com

23. قاسم دنش,السيادة الرقمية: معركة الدول لحماية بياناتها في عصر الذكاء الاصطناعي,https://www.almayadeen.net/reports

24. كلمة الوزير الأول خلال إشرافه على وضع المنظومة الوطنية لحوكمة البيانات حيز الخدمة,https://www.premier-ministre.gov.dz/ar/post

25. منشور وزارة الدفاع الوطني الجزائرية,WWW.MDN.DZ

26. مريم بن مولود, كلمة السيدة ,الاستراتيجية الوطنية للتحول الرقمي 2025-2030,https://www.hcn.dz/projets/juridique/SNTN

27. مجدل القحطاني, ماهي السيادة في البيانات؟,https://www.linkedin.com/posts/dr-mejdal

28. هجوم سيبراني,https://ar.wikipedia.org/wiki .

29. يعقوب حرتم,السيادة الرقمية في الجزائر: بين التحديات الراهنة وآفاق الاستقلال التكنولوجي,https://tkawen.online/ .

ثانياً: باللغة الأجنبية.

1. DJABALLAH Hakima , AHADDAD Mourad, Applications of Artificial Intelligence in Enhancing Cybersecurity A Study of Opportunities and Challenges, Herodotus' Journal of the Human and Social Sciences, Volume: 9 / N°: 5 (2025)

2. Hajar KERMECHE , Rawia YAHIA, Technical Protection of Digital Intellectual Works ,Banta 01 University Algeria, Revue des Sciences Humaines, Vol –36 N°4, December 2025.

3. Gideon Mekonnen ,Iris Reychav,Digital Sovereignty in the Global South : Autonomy in a connected World,Procedia Computer Science 278(2026).

4. Lee, Robert M., Michael J. Assante & Tim Conway. 2016. 'Analysis of the Cyber Attack on the Ukrainian Power Grid.' SANS & E-ISAC, 18 March. As of 21 October 2020: https://ics.sans.org/ media/EISAC_SANS_Ukraine_DUC_5.pdf, Accessed on: September 01, 2024

5. Salah Ghechir , Digital Sovereignty and Cyber Security:Legal and Strategic Implication For Algeria,university of Algiers1,journal of the Human and Sociall Sciences,volume 09,N:05(2025).

الفهرس

الفهرس

المقدمة 1

الفصل الأول: الدور القانوني والتقني للذكاء الاصطناعي في تحقيق الأمن السيبراني 6

المبحث الأول: ماهية الأمن السيبراني و نشأته. 8

المطلب الأول: مفهوم الأمن السيبراني و أبعاده المختلفة. 8

المطلب الثاني: أهمية و أهداف الأمن السيبراني. 21

المبحث الثاني: أطر حماية الأمن السيبراني في ظل أنظمة الذكاء الاصطناعي. 29

المطلب الأول: الدور للذكاء الاصطناعي في حماية الأمن السيبراني..... 30

المطلب الثاني: العوائق التي تواجه الذكاء الاصطناعي في ضمان الأمن السيبراني..... 47

الفصل الثاني: أثر الذكاء الاصطناعي في تعزيز السيادة الرقمية 57

المبحث الأول: الإطار المفاهيمي للسيادة الرقمية..... 59

المطلب الأول:ماهية السيادة الرقمية. 59

المطلب الثاني: أهمية السيادة الرقمية و معالمها. 73

المبحث الثاني: أطر حماية السيادة الرقمية في ظل الذكاء الاصطناعي. 78

المطلب الأول: الهجمات السيبرانية.....78

المطلب الثاني:الآليات الإقليمية والدولية للحفاظ على السيادة الرقمية. 88

الخاتمة 126

قائمة المصادر و المراجع:.....129

الفهرس 141

الملخص

يشهد العالم اليوم ثورة رقمية و تقنية يرى الكثيرون أنها قد تقضي على الكثير من حقوق التي يتمتع بها الإنسان, وفي مقدمتها الحق في الخصوصية خاصة في عصر الذكاء الاصطناعي, إلّا 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 إلاّ أنه لا يمكن إنكار آثاره الإيجابية على حفظ سيادة الدولة و تحقيق أمنها السيبراني, فأصبح بذلك الذكاء الاصطناعي أداة مزدوجة تجمع بين التمكين السيبراني و التهديد للسيادة الرقمية, الأمر الذي يستوجب سن التشريعات وطنية واضحة و متكاملة لتنظيم استخدام الذكاء الاصطناعي بما يضمن الأمن السيبراني و يحافظ على السيادة الرقمية, و كذا تعزيز التعاون الدولي من أجل وضع قواعد قانونية ملزمة لحوكمة الذكاء الاصطناعي في الفضاء السيبراني.

الكلمات المفتاحية:

1/_الذكاء الاصطناعي،2/_ الخصوصية، 3/_السيادة الرقمية،

4/_ الأمن السيبراني، 5/_الفضاء السيبراني، 6/_حوكمة الذكاء الاصطناعي.

The world today is witnessing a digital and technological revolution that many believe may undermine numerous rights enjoyed by individuals, foremost among them the right to privacy, especially in the era of artificial intelligence. However, the matter may go beyond infringing upon individual privacy to violating the digital sovereignty of states in a way that threatens their cybersecurity. Despite the negative impacts of artificial intelligence, its positive role in preserving state sovereignty and achieving cybersecurity cannot be denied. Artificial intelligence has thus become a dual-use tool that combines cyber empowerment with threats to digital sovereignty. This situation necessitates the enactment of clear and comprehensive national legislation to regulate the use of artificial intelligence in a manner that ensures cybersecurity and preserves digital sovereignty, as well as strengthening international cooperation to establish binding legal rules for the governance of artificial intelligence in cyberspace.

Keywords:

1/_Artificial Intelligence,2/_ Privacy, 3/_Digital Sovereignty,

4/_Cybersecurity,5/_ Cyberspace, 6/_Artificial Intelligence Governance