وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص:قانون إعلام آلي وأنترنت

الموسومة بـ

حفظ أمن المعلومات في ظل الذكاء الإصطناعي

إعداد الطلبة:

- عبدو رشيدة
- بلخضر رحاب

إشراف الدكتور:

*د.بكيس عبد الحفيظ

- لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة
بن داود حسين	أستاذ محاضر أ	رئيسا
عبد الحفيظ بكيس	أستاذ محاضر أ	مشرفا و مقررا
بلقسام مريم	أستاذ محاضر أ	عضوا مناقشا

السنة الجامعية 2024/2023

الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of higher education and scientific research
جامعة محمد البشير الإبراهيمي – برج بوعريريج
University Of Mohamed Al-Bashir Al-Ibrahimi - BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

إذن بالإيـــداع

أنا الممضي أسفله الأستاذ : بكيس عبد الحفيظ

الرتبة : أستاذ محاضر رتبة A

المشرف على مذكرة الماستر الموسومة بـ : الشكالية حفظ الأمن المعلومات في ظل الذكاء الاصطناعي

من إعـــداد :

الطالب الأول : بلحسن رحاب

الطالب الثاني : عبدو رشيدة

أوافق على إيداع الطالب (الطالبين) لمذكرة التخرج لدى الإدارة من أجل برمجتها للمناقشة.

إمضاء الأستاذ المشرف

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،

السيد(ة): بلحضر رحاب الصفة: طالب، أستاذ، باحث حالب

الحامل(ة) لبطاقة التعريف الوطنية رقم 107055609 والصادرة بتاريخ 2023-09-20

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم قانون خاص

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: إشكالية حفظ أمن المعلومات في ظل الذكاء الاصطناعي

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

التاريخ: .....

توقيع المعني (ة)

رئيس المجلس الشعبي البلدي
ملحق الإدارة الإقليمية
بن مراح مصطفى

*ملحق بالقرار رقم ....1082.... المؤرخ في 27 ديسمبر 2020 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله،

السيد(ة): عبد الوهاب رشيدة الصفة: طالب، أستاذ، باحث حالة

الحامل(ة) لبطاقة التعريف الوطنية رقم: 106345328 والصادرة بتاريخ 2017-09-20

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية تخصص القانون الخاص

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: استكشاف مخاطر تقنيات المعلومات على أعمال الذكاء الاصطناعي

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

التاريخ: .....

توقيع المعني (ة)

رئيس المجلس الشعبي البلدي
ملحق الإدارة الإقليمية
بن مراح مصطفى

شكر وتقدير

بسم الله الرحمن الرحيم

يقول عماد الدين الأصفهاني "إني رأيت أنه لا يكتب أحد كتاب في يومه إلا قال في غده لو غير هذا لكان أحسن ولو زيد هذا لكان يستحسن ولو قدم هذا لكان أفضل ولو ترك هذا لكان أجمل وهذا من أعظم العبر وهو دليل على استيلاء النقص على جملة البشر".

لذلك فالشكر والحمد والثناء لله تعالى على ما وهبنا من النعم فقد أحيانا من عدم وهدانا من ضلالة وعلمنا من جهالة وعافانا وأوانا وكسانا وبعث لنا رسولنا الكريم صاحب الفضل العظيم صلى الله وعليه وسلم.

فلله تعالى الحمد الكثير كما ينبغي لجلال وجهه وعظيم سلطانه الحمد لله الذي أعاننا على إتمام هذه الدراسة جعل الله فيها النفع والفائدة فنشكر الله تعالى على ما منه علينا ويسر لنا أمورنا في إعداد هذه الرسالة.

نخص بالذكر والشكر استاذنا "د. بكيس عبد الحفيظ" أولا لما قدمه لنا خلال مشورنا الدراسي وثانيا لما خصصه لنا من ثمين وقته وعلمه اعدادا لهذا البحث وتوجهنا بالصدر الرحب والخلق الطيب جزاه الله عنا خيرا وأدام عليه نعمة العلم وأمده بالصحة والعافية.

والشكر الجزيل لعميد الكلية" فرشة كمال" الذي طالما استقبلنا برحابة الصدر ولبا مطلبنا وسمع اهتماماتنا أيضا للأساتذة الكرام الذين أشرفوا على تدريسينا ومنوا علينا بالعلم والنصائح وكذا الطاقم الإداري للكلية الذي كان العون لنا في كل مرة التجأنا له.

إهداء

وآخر دعواهم أن الحمد لله رب العالمين

الحمد لله الذي بنعمته أتممت مسيرتي الدراسية فاللهم انفعني بعلمي وانفع بي

أهدي ثمرة جهدي إلى رفيق الدرب إلى كتفي الذي بتر في سبتمبر وزفته المنية لعالم الأموات صديقي في المحن ورضا قلبي في مهبات الحياة فل يحتسب الله أجري هذا لك وليشهد أني نويته صدقة جارية على روحك رحمك الله وأسكنك فسيح جناته "رياض بلحداد"

الى نفسي قبل كل شيء ممتنة لها على البقاء ثابتة رغم ما تصعف به الحياة وعلى مقامي هذا

إلى من أوصاني الله بهما خيرا لذان أفنى ثمرة شبابهما في تربيتي ومنا عليا بالعطاء والحب "أمي. أبي"

الى اليد التي تمد لي العون عندما اتعثر إلى أخواتي اللاتي وهبني الله إياهم دعما ونورا "رانيا – نور - نهاد - أسماء – خديجة"

الى صديقاتي الثابتات رغم تزعزع العالم "حبيبة – هاجر"

إلى الاتي جمعني بهم القدر حبا " ألفة -سهى – ريان- شيماء "

إلى صغاري حفظهم الله "أدم – يانيس - نوح - رسيم"

إلى زميلتي في هذا العمل رفيقة الخطوة الأولى والاخيرة "رشيدة"

رحاب

الإهداء

من قال أنا لها .. نالها وأنا لها وإن أبت رغما عنها أتيت بها الحمد لله حبا وشكرا وامتنان على البدء والختام

الحمد لله الذي ابتدأ الإنسان بنعمته وصوره في الأرحام بحكمته وعلمه ما لم يكن يعلم وكان فضل الله عليه عظيما

الحمد لله الذي يسر طريق العلم وأنار دروب الفهم وأسبغ علينا نعمة التوفيق

الحمد لله الذي لولاه ما كان علم ولا عمل الحمد لله أولا وأخرا

لا أحد يستحق الإهداء والإجلال والتعظيم مثلكما يا من ربيتماني صغيرة ورعيتماني كبيرة "أبي" يا صوتا يهمس في أذني بكل خير ويا نورا يشرق من داخلي لينير الطريق... أهديك ثمرة أعوام من الاجتهاد وسنين من المكابدة والتعب أهدي إليك عملي وعمري وروحي لعلي أوفي قطرة عرق أو أرد ساعة مشقة

إلى الإنسانة العظيمة إلى من أفضلها على نفسي إلى نبراس أيامي ووهج حياتي إلى الظل الذي آوي إليه في كل حين إلى جنتي وغاليتي "أمي"

إلى روح أخي الغالي ... رحمة الله عليه .

إلى ضلعي الثابت وأمان أيامي إلى من شددت عضدي بهم فكانو ينابيع ارتوي منها القوى والهمة إلى قرة عيني وصفوتها " إخوتي وأخواتي"

إلى رفيقة دربي في مشواري الدراسي ومشاركتي في هذا العمل غاليتي " رحاب "

ولكل من كان عونا وسندا في هذا الطريق وللأصدقاء الأوفياء ورفقاء السنين وأصحاب الشدائد والأزمات وإلى من أفاضني بمشاعره ونصائحه المخلصة

أهديكم هذا الإنجاز وثمرة نجاحي الذي لطالما تمنيته ها أنا اليوم أتممت ثمراته بفضل من الله عز وجل فالحمد لله على ما وهبني وأن يعينني ويجعلني مباركا أينما كنت

رشيدة

مقدمة

سمى هذا العصر بعصر تكنولوجيا الاتصال، وعصر الرقمنة وعصر الوسائط المتعددة والذكاء الاصـطناعي وغيرها من التسـميات الكثيرة الأخرى، وكلها تسـميات تشـير إليه من زاوية خاصـة، ويرجع إطلاق التسميات إلى ما يتسم به من تقنيات مستحدثة أدت بالضـرورة إلى تهديد الأمن السيبراني وأمن المعلومات وخصوصية الأفراد والمجتمعات، وإلى الكم الهائل من التكنولوجيات العالية الدقة والتعقيد الذي ظهرت، ونظرا للانفجار المعلوماتي الذي حصـل بفعل تسـخير هذه التكنولوجيات للإنتاج اللامحدود من البيانات التي تتحول بعد المعالجة إلى معلومات تحتويها أجهزة الحاسب بمختلف أنواعها والأجهزة المحمولة (Mobilephone).

من هنا بدأ القلق على أمن هذه المعلومات والأجهزة التي تعالجها وتخزنها وتنقلها فتم التفكير في حمـاية هذه الأجهزة وحمـاية المعلومـات الموجودة بهـا، وعنـدمـا ارتبطـت أجهزة الحاسـب بالأنترنت واعتمد الناس على الأنترنت في أعمالهم وتنمية تجارتهم، واسـتخدموها في التعليم والتواصل الاجتماعي (media Social) وفي مهام عديدة ومختلفة، أصبحت معلوماتهم الحساسـة البالغة الأهمية معرضـة للخطر والاختراق والإستيلاء، فنشأ مجال أمن المعلومات (Information Security)، وبات من أهم العلوم في عصـــر التكنولوجيا للحفاظ على هذه الثروة المعلوماتية المهمة لكل جهة سواء كانت حكومية أم أهلية.

بعد اعتمادها بشكل متنامي على حلول تقنية المعلومات في سير أعمالها وذلك لتحقيق أهداف المنظمة أو المؤسسة، وعندما نتحدث عن أمن المعلومات لابد أن نشمل الحديث عن الأمن السـيبراني (Cyber Security)، الذي يعد في الوقت الحالي أهم عناصـــر الأمن في الدول المتحضـرة وخاصـة مع التحول الكامل نحو السـيبرانية، في كافة جوانب الحياة وتقوم فكرة الأمن السـيبراني على تأمين البنية التحتية المعلوماتية للدول والتي تتمثل في المنشـآت الهـامـة وتظم المعلومـات الهـامـة ومنهـا نظم إدارة الحكومـات الالكترونيـة التي تـدار بهـا مؤسسات الدول الحيوية وكذلك النظم العسكرية والشرطية والقضائية والاقتصادية والصناعية والتجارية وغيرها.

ويعد ما يهددها هو تهديد للأمن القومي للدول حيث بات معلوما أن صـناع القرار في الدول الكبرى مثل (الولايات المتحدة الأمريكية، الإتحاد الأوروبي، روســيا، الصــين، الهند) وبعض الدول العربية وفي مقدمتها (المملكة العربية السعودية، مصر ولبنان) وغيرها أصبحوا يصنفون الأمن السيبيراني كأولوية في سياستهم الدفاعية الوطنية، بالإضـافة إلى ما تقدم فقد أعلنت أكثر ب 130 دولة حول العالم عن تخصـيص أقسـاما وسـيناريوهات خاصـة بالحرب السيبرانية ضمن فرق الأمن الوطني.

ومما لا شك فيه أن الأمن السيبراني في الأنظمة التصـنيفية يرتبط بشكل كلي بالذكاء الاصـطناعي، حيث تعتمد فكرة أنظمة الذكاء على استعمال أنظمة تكنولوجيا الحاسبات التي تبدو في أدائها الأقرب إلى الذكاء البشـري، ويعتبر الذكاء الاصــطناعي العنصــر الهام في تطوير أداء الحاسبات ويعتمد في نظام عمله على طريقة حل المشكلات، حيث توفر أنظمة الذكاء الاصـــطناعي دعم في البحث من خلال ملايين البيانات والقواعد والأنماط المثيرة للتوتر والقلق في وقت أقل من الوقت الذي يسـتخدمه العقل البشـري، بالإضـافة إلى معالجة كمية هائلة من البيانات يصعب على العقل البشري استيعابها.

أهداف الدراسة:

- إبراز العلاقة بين الأمن السيبراني وأمن المعلومات وشرحها.
- إلقاء الضوء على فعالية الذكاء الاصطناعي في حفظ أمن المعلومات والأمن السيبراني.
- توضــيح الأهمية التي يتمتع بها الذكاء الاصــطناعي وضــرورة الاهتمام به والســعي إلى استخدامه والاستفادة منه قدر الإمكان.

أهمية الموضوع:

- من المؤهل أن تســاعد هذه الدراســة ونتائجها المهتمين في المجال المعلوماتي وخاصــة جانب الذكاء الاصطناعي والأمن السيبراني.

– الذكاء الاصطناعي وسيلة لتعزيز الأمن السيبراني عبر الأتمتة العناصر الأساسية للعميل وتحويله إلى عملية مبســـطة ومســـتقلة تعمل على تســـريع المعالجة وزيادة أمن المعلومات والبيانات.

– الذكاء الاصطناعي ودوره في حماية الخصوصية والبيانات عن طريق تحليل كميات هائلة منها لتحديد الأنماط الشاذة والتهديدات المحتملة.

– الدور الحيوي الذي يلعبه الذكاء الاصطناعي في تعزيز الأمن السيبراني وأمن المعلومات، في ظل التطورات الحاصـــلة لذا يجب تطويره وتطبيق حلول الذكاء الاصـــطناعي لمواجهة التحديات الأمنية المتزايدة.

الأسباب والدوافع الموضوعية:

*** دوافع شخصية:**

– الشغف المتزايد بالتكنولوجيا واكتشاف الأفاق المتطورة لها.

– التطوير المهني في مجال الأمن السيبراني.

– محاولة كشف اللبس عن الكثير من الأسئلة التي تثير حيرتنا في هذا المجال.

*** دوافع موضوعية:**

– يعد أمرا حيويا فهم وتطبيق الذكاء الاصـــطناعي في حماية أمن البيانات والمعلومات خاصة في عصرنا هذا الذي ازدادت فيه التهديدات السيبرانية.

– نقص الخبرات البشرية في الأمن السيبراني والذكاء الاصطناعي.

– الذكاء الاصطناعي يمكن أن يسد الفجوة من خلال تحليل البيانات وكشف التهديدات.

– محاولة حل الكثير من الإشكاليات في هذا المجال من خلال اجراء دراسات عنه.

ومن بين الصعوبات التي واجهتنا خلال بحثنا هذا:

– جدة وحداثة الموضـوع إضـافة إلى نقص الكوادر البشـرية والمختصـين في هذا المجال وصعوبة التحكم فيه لمرونته.

– نقص المراجع العربية التي تساعد في دراسة الموضوع وفهمه، وصعوبة الوصول إلى الموارد والمراجع التعليمية الحديثة المختصة في المجال الذكاء الاصطناعي.

– نقص الخبرات التدريبية والتعليمية في مجال الذكاء الاصطناعي والأمن السيبراني وذلك بسبب جمود المناهج التعليمية المتبعة.

أهم المراجع السابقة:

– دراسة قامت بها بكوش رميساء في مذكرة ماستر، تحت عنوان انعكاسات التهديدات السيبرانية على الأمن الوطني الجزائري، تطرقت الطالبة فيه إلى جوانب الأمن السيبراني والمفاهيم المرتبطة به، وتناولت الأمن السيبراني في الجزائر كدراسة تحليلية والمناهج المستخدمة لمواجهة التهديدات السيبرانية.

– دراسة قام بها محمد حمداني في شكل مقال على مجلة الفكر القانوني والسياسي جامعة عمار ثليجي الأغواط، حيث يتناول مفاهيم حول الأمن السيبراني والذكاء الاصطناعي والعلاقة بينهما، إضافة إلى دور الذكاء الاصطناعي في حماية أمن المعلومات والأمان السيبراني.

الإشكالية:

– ما مدى ارتباط الذكاء الاصطناعي بتحقيق الأمن السيبراني وحفظ أمن المعلومات والبيانات ؟

المنهج المعتمد:

اعتمدنا لحل هذه الإشكالية على المنهج الوصفي والمنهج التحليلي، وذلك من خلال السعي إلى جميع المعلومات والحقائق والبيانات المتعلقة بالفضاء السيبراني وكذا الذكاء الاصطناعي و امن المعلومات، بالإضافة إلى ذلك تفسر مختلف المعطيات المتحصل عليها حول دور الذكاء الاصطناعي في حماية المعلومات لغرض إثراء الدراسة أكثر فأكثر من خلال .

تقسيم البحث:

الفصل الأول بعنوان: حفظ أمن المعلومات في الفضاء السيبراني والذي قسمناه الى **المبحث الأول:** أمن الفضاء السيبراني **المبحث الثاني:** الأمن السيبراني وحفظ أمن المعلومات.

الفصل الثاني بعنوان: واقع امن المعلومات والذكاء الاصطناعي **و**الذي قسمناه الى **المبحث الأول:** ماهية الذكاء الاصطناعي **المبحث الثاني:** اليات الذكاء الاصطناعي.

الفصل الأول:

حفظ أمن المعلومات في الفضاء السيبراني

بعد التطور الهائل الذي شهده عالم الاتصالات في مطلع الألفية الثالثة، تعاظمت الأنشطة التي تم أداءها عبر الفضاء السيبراني وتعاظمت أهميته، بالتالي ازدادت المخاطر التي يتعرض لها هذا الفضاء وأراء الاتجاه العالمي نحو تنظيمه والممارسات التي تجرى من خلاله، وإيجاد السبل القانونية والتقنية لتأمينه وتأسيس الخدمات التي تقدم عبره كان لابد من الوقوف على صيغة هذا الفضاء.

ونظرا لانتشـــار تكنولوجيا المعلومات الكبير والتطورات التقنية الراهنة مع ازدياد اعتمادنا عليها تصبح بياناتنا عرضة للخطر، مما يهدد أمن المعلومات ويشكل معضلة وتحدي للأفراد والمنظمات، ومع ارتباط الأمن السـيبراني بأمن المعلومات ارتباطا وثيقا ولاعتبارهما ممارستان تهدفان إلى حماية البيانات من المخاطر.

سنتطرق في هذا الفصل إلى:

المبحث الأول: يتمحور حول أمن الفضاء السبيراني .

المبحث الثاني: يتمحور حول الأمن السبيراني وحفظ امن المعلومات .

المبحث الأول:

أمن الفضـــــــاء السيبرانـــــــي

كانت ثورة المعلومات وظهور الانترنيت إيذ نا ببزوغ العصر السيبري، وخلق بنية جديدة هي الفضاء السيبراني، الذي أصبح يؤثر في النظام الدولي، خاصة مع بروز شكل جديد من القوة الا وهي القوة السيبرانية، التي توزعت وانتشرت بين عدد كبير من الفاعلين على المستوى الدولي والمحلي، ما جعل الفضاء السيبراني مجالا جديدا لصراع بين الدول

ولقد أحدث ظهور هذا الفضاء ثورة شاملة في جميع نواحي الحياة، اذ تزداد المخاطر السبيرانية في غالب الأحيان كلما ازدادت هيمنة تكنولوجيا الاتصالات و المعلومات على النسق العام لحياة، فأصبح امامنا جرائم حقيقية متكاملة الأركان، تمم عن طريق شبكة الانترنيت، فان البحث في قضايا التهديدات السيبرانية و التحديات الأمنية يقتضي الغموض في حيثيات العصر الرقمي الجديد [1].

وهذا ما دفع الباحثين الى إعادة صياغة مفهوم جديد، يعكس مدى قوة الدول في إمكانية حماية أمنها القومي الذي يتداخل ويترابط مع البيئة الجديدة، التي تفرض قوانينها وأمنها الخاص وهو الامن السيبراني[2]،

سنتطرق في هذا المبحث إلى:

المطلب الأول: مفهوم الفضاء السيبيراني

المطلب الثاني، الأمن السيبيراني.

[1] إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، جامعة محمد بوضياف المسيلة الجزائر، المجلد10، العدد01 أفريل 2019 ص 1016

[2] طمطامي سالم، الصحافة الالكترونية ولامن السيبراني، مذكرة ماستر، تخصص صحافة مطبوعة الكترونية، جامعة احمد دراية كلية العلوم الإنسانية والاجتماعية ولعلوم الإسلامية ادرار، 2022 ص 1

المطلب الأول:

مفهوم الفضـــــــاء السيبرانـــــي

بالرجوع إلى عام 1982 وهو تاريخ ظهور هذا المصطلح، صاغ كاتب الخيال العلمي "ويليام جيبسون"[1] تصورا غريبا "هلوسة جماعية يشترك فيها مليارات المستعملين يوميا في كل دولة، كتمثيل للبيانات المستخلصة من بنوك المعلومات في جميع أجهزة الكمبيوتر في العالم".

ولتسمية هذه الفكرة جمع جيبسون كلمة "السبرنطيقا"[2] (التي تعني علم التحكم الآلي) مع كلمة الفضاء **Space**، وسك منهما مصطلح الفضاء السيبراني **Cyberspace** الذي أصبح حقيقة مع انتشار شبكة الانترنيت على نطاق العالم[3]

فالفضاء السيبراني إذن مصطلح حديث ظهر نتيجة لثورة تكنولوجيا المعلومات، ويشمل جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام، أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الانترنت العامة.

فالفضاء السيبراني هو العالم المادي و المفاهيمي الذي توجد فيه جميع هذه الأنظمة.

---

[1] **ويليام جيبسون:** كاتب خيال علمي جندي معروف بكتابته للروايات التي تعتمد على مفهوم السايبربانك (أنظر ويكيبيديا المسوعة الحرة https://fr.wikepid.org).

[2] **السبرنطيقا:** مصطلح يشير إلى الفضاء السيبراني، يجمع بين العوامل الأفتراضية والحقيقية ويمثل هذا المصطلح تفاعل الأفراد مع التكنولوجيا والانترنت (أنظر ويكيبيديا المسوعة الحرة https://fr.wikepid.org).

[3] بيتر سينجر، دروس الحروب الماضية والاتجاهات التكنولوجيا المستقبلية في القرن الحادي والعشرين، ط1 مركز الامارات في الدراسات والبحوث الاستراتجية 2014ص38

و عليه يمكننا القول أن الفضـاء السـيبراني يعتبر مجالا حيويا وجيوسـتراتيجيا، تخاض فيه العديد من الحروب والهجمات الرقمية، وهو مجال مركب يشـمل عددا من العناصـر هي أجهزة الكمبيوتر، أنظمة الشـبكات والبرمجيات، حوسـبة المعلومات، نقل وتخزين البيانات ومستخدمو كل هذه العناصر، وعليه فمسألة تحديد مفهوم الفضاء السيبراني هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل دولة لأمنها القومي.[1]

الفرع الأول: تعريف الفضاء السيبراني

1- تعريف الفضاء

أ- لغة: مصدر مأخوذ من فعل ثلاثي (فضاء – يفضو – فضوا – فهو فاض) والفضاء هو المكان الواسع والفضاء الخارجي الواسع من الأرض.

ب- اصطلاحا: كل ما يقع على ارتفاع (10000 كلم) فوق سطح الأرض وكل ما يقع خلف الغلاف الجوي للأرض، ونظم سائر الأجرام السماوية في الكون. [2]

2- تعريف السبرانية

أ- لغة: الكلمة مشـتقة من My bernetes ويقصـد بها قيادة ربان السـفينة، مأخوذة من كلمة Cyber، وهي صـفة تطلق على كل ما هو مرتبط بفضـاء الإنترنيت من حواسـيب وتقنية معلومات وكذا المواقع الافتراضية. [3]

---

[1] علاء الدين فرحات، الفضاء السيبراني، تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، المدرسة الوطنية العليا للعلوم السياسية (الجزائر)، المجلد 10، العدد 03، ديسمبر 2019، ص 90-91.

[2] نورة عقون، "واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر"، مذكرة ماستر، تخصص دراسات أمنية وإستراتجية لكلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2019، ص 11-12.

[3] بكوش رميساء، "انعكاسات التهديدات السيبرانية على الأمن الوطني الجزائري"، مذكرة ماستر، تخصص دراسات إستراتجية وأمنية لكلية الحقوق والعلوم السياسية، جامعة العربي التبسي تبسة، 2019، ص 3.

كما عرفه المعجم الفرنسي Le petit Larousse العلم الذي يدرس آليات الاتصال والتحكم في الآلات والكائنات الحية الأخرى.[1]

عرفه معجم "Oxford" "دراسة فعالية العمل البشري بمصادرها بفعالية الآلات الحاسبة تتصل بسمات وخصائص الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي".[2]

ب- اصطلاحا: أصل كلمة "السيبرنتيك" يوناني قديم، مفهومه إدارة القوارب ولقد استعمله العالم الفرنسي أمبير[3] في العلم الخاص بالإدارة الإجتماعية السياسة.

ولقد كان هذا المصطلح مرتبط قبل هذا بالعالم الرياضي الأمريكي "**نوربرت وينر**"[4] الذي قدم تعريف "Cybernetics" من خلال كتابة المشهور عام 1948م تحت عنوان السيبرنيتك أو الإدارة والرابطة في الحيوانية والآلية.

ولقد تم إستخلاص العديد من التعاريف من خصائص السيبرنيك التي عرضها وينر.

1- تعريف أبريج Birg[5] قائم على الإدارة وضعه العالم السوفياتي "أبرج" مفاده أن السيبرنك هو علم الإدارة الجمل الديناميكية المعقدة، وهذا التعريف يعبر عن حقيقتها بشكل ملائم.

2- تعريف قائم على الإعلام حيث عرفته على أنه علم لعمليات إستلام وإرسال وتحليل وحفظ إستعمال المعلومات في الجمل الديناميكية المعقدة.[6]

---

[1] Dictionnaire français le petit Larousse (France. Edition 2001), P 104.

[2] English diction Oxford dictionaries language, P 299.

[3] **نوربرت وينر:** عالم رياضيات أمريكي من رواد علم التحكم الآلي، ويعتبر من الشخصيات المؤثرة في تاريخ التكنولوجيا ولقد مهدت أعماله لتطوير العديد من المجالات الحديثة، مثل الذكاء الاصطناعي (أنظر ويكيبيديا الموسوعة الحرة .)https://fr.wikepid.org

[4] **أندريه ماري أمبير** (1775-1836) عالم فزياء فرنسي يعتبر أحد مؤسسي الكهرومغناطيسية (أنظر تطبيق chatgpt https://chat.openai.com).

[5] **ابريج (1876-1950):** عالم احياء وحيوانات بارز في الاتحاد السوفياتي ساهم في علم الاحياء التطوري والجغرافيا الحيوية وعلم الأسماك (انظر وكيبيديا الموسوعة الحرة https://fr.wikepid.org).

[6] نورة عقون، مرجع سابق، ص 12-13

تعريف الفضـــاء الســـيبراني: مجال علمي داخل بيئة المعلومات، يتكون من شـــبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنيت وشبكات الاتصالات، وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المدمجة، "كما يشـار إليه بوصـفه ليس مكانا عاديا بل أنه تحدي قياسـي في أي بعد مادي أو متواصـل في الفضـاء السـيبراني، مصـطلح مختصر يشير إلى البيئة المنشئة بواسطة إلتقاء الشبكات التعاونية من أجهزة كمبيوتر وأنظمة المعلومات والبنية التحتية للاتصالات المعروفة بشبكة ويب العالمية. [1]

عرفه الإتحاد الدولي للاتصـــالات "بأنه المجال المادي وغير المادي الذي يتكون وينتج عن عناصـر في أجهزة الكمبيوتر، شـبكات برمجيات، حوسـبة معلومات، محتوى معطيات النقل، والتحكم ومستخدمو كل هذه العناصر".

عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSST) "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية. [2]

الفرع الثاني: بنية الفضاء السيبراني

يتميز الفضـــاء السـيبراني عن المعلوماتي والإلكتروني بأنه يشـمل الاثنين بإعتباره بنية ذو ثلاث طبقات

أولا: الفضاء السيبراني والإلكتروني

[1] بوطلاعة وداد، بوكورو منال، صراع الفضاء السيبراني وتأثيره على سلم وأمن الدولتين تحديات وتهديدات جديدة وسبل مواجهة، مجلة العلوم القانونية والإجتماعية، جامعة الإخوة منتوري قسنطية(1)، المجلد 7، العدد 04، ديسمبر 2020، ص 813.

[2] متاح على الموقع الإلكتروني للوكالة الفرنسية لأمن نظم المعلومات:https://www.ssi.gov.fr/administration تاريخ الإطلاع: 2024/03/01 الساعة 10:08 صباحا.

مجال يتميز بإستخدام الإلكترونيات الكهرومغناطيسية لتخزين تأشيرات متحركة أو ساكنة ضد إشارات (الراديو وأجهزة الاتصال) ونقاط الربط وشبكات النظام الدفاعي، حيث يتم الوصول إلى الهدف بسرعة الضوء أو الصوت عند إستعمال قدرتها الفضائية الإلكترونية.

ويعمل الفضاء الإلكتروني تحت ظروف مادية غير تقليدية، حيث يكون وسيطا عبر العمل من خلال أجهزة الكمبيوتر وشبكات الاتصال.

فالفضاء الإلكتروني يهتم بالتفاعلات الداخلية للجهاز الإلكتروني، والأجهزة المرتبطة به في حين الفضاء السيبراني يهتم بالأنترنيت والأجهزة الإلكترونية والعنصر البشري[1].

ثانيا: الفضاء السيبراني والمعلوماتي

كل أنواع البيانات بطرق جمعها المختلفة، التي تمتاز بقابليتها للمعالجة بتقنيات الحاسوب لتتحول إلى خطاب ذو دلالة معرفية قابلة للتداول والتغير، بما يضمن اكتساب الجهات التي تستخدمها معارف وحقائق قابلة للإستثمار في شتى ميادين الأنشطة المعاصرة فالمعلوماتية هي عملية ترجمة البيانات داخل الحاسوب، وتحويلها إلى خطاب يحمل دلالات عديدة، حيث أن السيبرانية جمع البيانات وتحليلها وهو التفاعل الحاصل بين المعلومات المترجمة والعنصر البشري وكيفية التعامل مع المعلومة[2]. وتتمثل هذه الطبقات في:

– **الطبقة المادية:** تتكون من شقين الأول الأجهزة المادية كالكمبيوتر والشبكات والأسلاك وأجهزة التوجيه (Mouters)[3] وتقع ضمن ولاية السلطات القضائية، ويظهر أهمية هذا الأمر في البحث عن الأجهزة التي تم استعمالها في القيام بالجرائم السيبرانية مثلا.

---

[1] نورة عقون، مرجع سابق، ص 16 إلى 18.

[2] كريمة شافي جابر الكعبي، مجتمع المعلومات في العالم العربي، العراق نموذجا، مجلة كلية الأدب جامعة المستنصرية قصر المجتمع المدني العدد، 98، ص 718.

[3] **أجهزة التوجيه:** هي التي نستخدم لتوجيه حركة حزم البيانات بين الشبكات المختلفة، تعمل على تحديد أفضل طريقة لوصول البيانات إلى وجهتها المقصودة عبر الشبكة (أنظر ويكيبيديا الموسوعة الحرة https://fr.wikepid.org)

– **طبقة المعلومات:** تتمثل في إنشـــاء وتوزيع المعلومات والتعامل بين المســـتخدمين ويمكن لهم إنشاء هذه المعلومات من خلال مواقع الويب والربط بمواقع ويب أخرى، ونشر المعلومات على مواقع التواصل الاجتماعي وكما يمكن المستخدمين من الوصول إلى المعلومات

– **الطبقة المنطقية:** تعتبر الجهاز العصبي المركزي للفضاء السيبراني، وتكون مسؤولة عن توجه البيانات إلى محطتها النهائية بصورة أساسية عبر أنظمة أسماء النطاقات[1] (DNS) وبروتوكولات الإنترنيت، تعتمد على الكابلات الألياف البصرية والأسس المادية[2].

– **طبقة الأشـخاص:** الذين يشكلون شخصية الفضاء السيبراني، حسب الطرق التي تم إختيارها لاستخداماتهم وشخصياتهم المختلفة، التي تعتبر جزء مهم من بنية الفضاء السيبراني لهذا لا يمكن اعتبارهم مجرد مستخدمين سلبيين.

هذا التعريف يعتبر ناقص فالمختصين في هذا المجال يرون أن الأشخاص يساهمون في توليد وإستدامة الأنشطة المختلفة في الفضاء السيبراني، إلا أننا لا يمكن أن نعتبرها طبقة بل شرط لوجود وديمومة تلك البنية، ولكن لا يلتزم وجودها وجود باعتبار ذاتي وهذا ما يؤكده زيادة استعمال الذكاء الاصطناعي في هذه البيئة وخاصة مجال الأمن السيبراني، رغم هذا كل الطبقات تعتبر مهمة فلا يمكن التركيز على واحدة دون الأخرى إذا أردنا تأمين الفضـــاء السيبراني. [3]

---

[1] **أنظمة أسماء النطاقات (DNS):** نظام هرمي موزع، يستخدم لترجمة أسماء النطاقات التي يشمل ذكرها مثل Google.com إلى عنوان IP الرقمية التي تستخدمها أجهزة الكمبيوتر للاتصال ببعضها البعض، **انظر الملحق(1) ص 98**. **IP:** عنوان بروتوكول الأنترنيت، وهو معرف رقمي فريد يستخدم لتحديد جهاز معين على شبكة كمبيوتر، ويساعد في توجيه البيانات إلى الجهاز الصحيح **انظر الملحق(2) ص 98**. (أنظر chatgpt https://chat.openai.com).

[2] محمد خزعبل عباس، وليد مرزة، حمزة المخزومي، أمن الفضاء السيبراني، قراءة في المفهوم القانوني، مجلة العلوم القانونية، جامعة بغداد، المجلد 37، الجزء 2، شباط 2023، ص 9–10.

[3] David clark characterizing cyberspace: past present and future MIT CSAIL version 1.2 march 12-2010 pag 04.

الفرع الثالث: مخاطر الفضاء السيبراني

لقد قام الفضـــاء الســيبراني بتحويل الصــراع المادي إلى افتراضـــي بين الدول، وأعطى الحرب مفهوم جديد مما نتج عنه ظهور تهديدات حديثة ومتزايدة في الحجم والشدة.

هذه التهديدات لا تســتهدف الإضــرار بالبشــر بصــورة مباشــرة، بل يكون التأثير في الأنظمة والبيانات التي يســتخدمها الأفراد والدولة، مما يؤثر على أســلوب الحياة بشــكل يهدد أمن الدولة ككل، ومنه فإن المخاطر الناشئة عن الفضاء السيبراني تتسم بـ:

- اتساع النطاق وتعدد المستويات.
- عدم التمكن من إيقاف مخاطر تلك التهديدات كليا.
- تنوع المخاطر السيبرانية.

طبيعته جعلت المخاطر الأمنية الناتجة عن التفاعل فيه مختلفة كليا عن المخاطر التقليدية ذلك أنه عابر للحدود.

كما أن العولمة أصـــبحت حتمية واعتماد الدول عليها لا يمكن التراجع فيه، مما يزيد المخاطر بازدياد الإعتماد عليها، كما أن الفضـــاء الســيبراني مرن مما يترتب عن كل تطور ظهور مخاطر جديدة تهدد أمن الدولة، أي لا يتم التحكم بالديناميكية المتشابكة[1].

ويتمثل التحدي الأكبر في الفضـاء السيبراني في صـعوبة إسناد الهجوم لفاعل معين ما يمثل مصدر قوة الفواعل الدولية. [2]

وتأخذ هذه المخاطر السيبرانية عدة صور تعرف فيما يلي:

---

[1] **الديناميكية المتشابكة:** التفاعلات المعقدة والمترابطة بين عناصر مختلفة في نظام ما، وتتضمن هذه الديناميكيات التأثيرات المتبادلة بين مختلف العناصر التكنولوجية أو الاجتماعية أو البيئية، وكيفية تغيرها وتطويرها. (أنظر ويكيبيديا الموسوعة الحرة https://fr.wikepid.org).

[2] حازم محمود خليل، استعمال القضاء السيبراني في الحروب الغير التقليدية، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، القاهرة، المجلد 8، العدد 05، يناير 2023، ص 272-273.

- **الاختراق السيبراني:** يتمثل في عملية نسخ البرمجيات غير مصرح بها، أو إعادة إنتاجها أو استخدامها أو يضع نسخة غير شرعية، ونشرها وتوزيعها دون إذن أو تفويض، أو توصيل إلى المعلومات الشخصية أو السرية عبر اختراق المواقع أو صفحات التواصل الاجتماعي أو البريد الإلكتروني، وقواعد البيانات والقيام بتغيرها أو الاستيلاء عليها كأرقام وعناوين وأسماء المتعاملين وبيعها إلى جهات أمنية أو سياسية، وتوظيف اختراقات غالبا لأغراض سياسية.

مثال: اختراق البريد الإلكتروني لهلاري كلينتون 2016 تزامنا مع الانتخابات الرئاسية الأمريكية.

- **التجسس السيبراني:** أخطر الجرائم السيبرانية، حيث يتم بأحدث تكنولوجيات التصنت ذات القدرة والجودة والدقة العالية بهدف جمع مختلف المعلومات، (سياسية، اقتصادية...) أو اتفاقيات عالمية (كالأبحاث، الدراسات...) من خلال التجسس على المواقع والصفحات وما تحتويه من معلومات وبيانات (نصية، صوتيه أو مرئية) أو رسائل بريدية الكترونية، تتضمن ملفات برمجية لديها القدرة على الإرسال بشكل آلي للمعلومات المتوفرة على حاسوب المصمم وكلمة المرور واسم المستخدم.

مثال: الهجوم استهدف شركة Ecyceifix عام 2017 تم من خلاله سرقة معلومات شخصية حساسة لملايين الأفراد وتم استعمالها في العمليات احتيالية[1].

- **الإرهاب السيبراني:** كل نشاط إلكتروني يستعمل لإحداث الرعب وإرغام الأشخاص أو الدول أو الشعب، لأغراض سياسية أو دينية أو عنصرية، تهدف للسيطرة على الأفراد أو إفساد عقيدتهم لتحقيق مآرب تتعارض مع مصلحة المجتمع[2].

[1] بوطلاعة وداد، بوكورو منال مرجع سابق، ص 814-815.

[2] Hidden wiki، tor onion urls. Frorne: https:// thehiddenwiki.org
تاريخ الإطلاع الأربعاء: 8 ماي 2024ساعة: 9:50

مثال: تعطيل شبكة الكهرباء في مدينة إيفرت في أوكرانيا 2015 بواسطة هجوم سيبراني على شركة توزيع الكهرباء مما أحدث اضطرابات كبيرة.

- **الهجمات السيبرانية:** تتعرض الأنظمة المعلوماتية والمدنية والعسكرية لهجمات سيبرانية، تؤدي إلى تعطيل البنية التحتية الحرجة للمرافق العامة بهدف إرباك الخدمات والتلاعب بالبنيات. [1]

مثال: هجوم استهدف استونيا عام 2007 تم فيه إخراج الجيوش النظامية من سيطرة.

المطلب الثاني:

الأمـــــن السيبرانـــــي

مجموعة من الإجراءات والتقنيات المهمة لحماية أنظمة الحاسوب والشبكات والبيانات أو ما يدعى بالفضاء السيبراني من التهديدات الالكترونية (الاختراقات، البرامج الضارة، سرقة البيانات، الاحتيال الإلكتروني...)، ويتضمن عدة طرق ووسائل للحماية كالتشفير لضمان سلامة انظمة البيانات خاصة في عالمنا هذا المرتبط بواسطة الشبكة والذي يعتمد على الفضاء الالكتروني، وباعتباره مجالا خامسا للحروب فذهب الاهتمام بهذا الفضاء عن طريق تأمينه وحمايته.

الفرع الأول: تعريف الأمن السيبراني

يوجد هناك العديد من التعاريف أهمها:

- **ريتشارد كامر** [2] عبارة عن وسائل دفاعية من شأنها إحباط وكشف محاولات القراصنة.

---

[1] أحمد عبس نعيمة الفتلاوي، الهجمات السيبرانية، مفهومها والمسؤولية الدولية، الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العراق، العدد 04، السنة 2016، ص 619.

[2] **ريتشارد كامر:** عالم حاسوب وبرمجيات بريطاني قدم إسهامات في تطوير الذكاء الاصطناعي وأسس العديد من الشركات التقنية (أنظر تطبيق chatgpt https://chat.openai.com).

– **ادوارد أمورسو** "**Edward Amoroso**"[1] وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القراصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة. [2]

– عرفته **وزارة الدفاع الأمريكي** " **Pintagon** " أنه كافة الإجراءات التنظيمية التي تؤمن الحماية الكافية للمعلومات بجميع أنواعها وأشكالها، سواء كانت إلكترونية أو مادية من مختلف المخاطر والهجمات والجرائم وأفعال التخريب والتجسس والحوادث، بما أدرج الإعلان الأوروبي للأمن السيبراني معنى "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق، أو الحوادث غير المتوقعة التي تستهدف الآليات". [3]

– كما عرفته **صحيفة المرصد** بأنه سلاح استراتيجي في يد الحكومة والأفراد خاصة أن الحروب السيبرانية أصبحت جزء من الهجمات بين الدول.

– الأمن السيبراني هو المجال الجديد الخامس للحروب[4] الحديثة، بعد البحر الجو والفضاء الحقيقي، ويمثل جميع شبكات الحاسب الموجودة حول العالم، بما في ذلك الأجهزة الالكترونية المرتبطة من خلال شبكة الألياف البصرية والشبكات اللاسلكية، الفضاء السيبراني ليس انترنت فقط بل شبكات أخرى كثيرة متصلة.[5]

---

[1] **إدوارد أمورسو**: عالم حاسوب ومبرمج أمريكي معروف بدوره في تطوير شبكة الانترنيت، وكان له دور كبير في تطوير TCPوالTP (أنظر ويكيبيديا الموسوعة الحرة https://fr.wikepid.org).

[2] إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، دراسة منشورة، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي تبسة، 2019، ص 104.

[3] بوازدية جمال، الأمن السيبراني، محاضرات مقدمة لطلبة السنة ثالثة ماستر، تخصص دراسات استراتيجية وأمنية، جامعة الجزائر (3)، كلية العلوم السياسية والعلاقات الدولية، ص 13.

[4] **مجال الحروب الخامس**: المجال الإلكتروني الذي أصبح منافس للمجال البري والبحري والجوي والفضائي، في الحروب والشركات تعتمد على المجال الإلكتروني، لتخزين بياناتها التحتية مما جعلها عرضة لهجمات إلكترونية (أنظر تطبيق chatgpt (https://chat.openai.com)

[5] بكوش رميساء، مرجع سابق، ص 5–6.

يقصد بالأمن السيبراني حماية المعلومات من خلال ثلاث محاور رئيسية: محور المعلومات الشخصية، محور المعلومات داخل الشركات، ومحور المعلومات عبر الدول.

– كما **عرفه المشرع الجزائري في المادة 2 من قانون 04/03** بأن الأمن السيبراني يمثل مجموع الوسائل التقنية والتنظيمية والإدارية، التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستعمال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان التوافر واستمرارية عمل نظم معلومات، وتعزيز حماية وخصوصية البيانات الشخصية وإيجاد جميع التدابير لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. [1]

– عرفته **وكالة الأمن الرقمية الأروبية**[2] قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث الغير متوقعة التي تستهدف البينات المتداولة أو المخزنة وفق إطار قانوني. [3]

الفرع الثاني: أبعاد الأمن السيبراني

يرتبط الأمن السيبراني بعدة مجالات وذلك لتحقيق منظومة أمن متكاملة، تعمل على الحفاظ على أمن الدولة القومي من التهديدات السيبرانية المختلفة.

– **البعد العسكري:** تتميز القوة السيبرانية بقدرتها على الربط بين مختلف الوحدات العسكرية عبر شبكاتها في الفضاء الإلكتروني، مما يساعد في إنجاز مختلف المهام العسكرية بمرونة وسرعة فائقة كالأوامر العسكرية، وكذلك السهولة في تبادل المعلومات وإصابة الأهداف عن

---

[1] المادة 2 من قانون 04/03 المؤرخ في 2009/05/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (عرفت هذه الجريمة).

[2] **وكالة الأمن الرقمية:** هيئة مختصة بحماية الأنظمة الرقمية والبيانات الحساسة ،من التهديدات الإلكترونية وتطوير إستراتيجيات لتأمين الشبكات الالكترونية. (أنظر تطبيق chatgpt https://chat.openai.com).

[3] اتفاقية بودابيست معاهدة دولية، وقعت في بودابيست، عاصمة المجر، لمكافحة الجرائم الالكترونية سنة 2001.

بعد في حالة لم تكن الشبكة المستخدمة مؤمنة، فإن هذه المزايا تتحول إلى نقطة ضعف وتتسبب في هجمات إلكترونية مضادة على شبكات القوات المسلحة، وكذلك الاستخبارات وتدمير قواعد البيانات العسكرية، وتعطيل الدولة للنشر السريع لقدراتها وقواتها، وكذلك قطع أنظمة الاتصال بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن شل أنظمة الدفاع الجوي أو فقدان السيطرة على الوحدات القيادية من خلال التوجه الإلكتروني للخصم بالإضافة إلى فقدان الاتصال بالأقمار الصناعية. [1]

– **البعد الاقتصادي:** الغاية من الأمن السيبراني حماية الموارد الاقتصادية وليس ربح المال ان تقرير الربح الحاصل من المعلومات غير منتشر، وكذلك تقدير تكلفة الأمن (الميزانية المرصودة، تكلفة نواتج الأمن والتدريب، بناء مراكز السيطرة)، إذ أن حساب هذه التكاليف والخسارة الناتجة عن الأخطار والأعمال الخبيثة، أمر صعب جدا لأن احتياجات المؤسسة هي التي تحدد هذه التكاليف، وكذلك لا يمكن تحديد القيمة الاقتصادية للأمن المعلوماتي والمردودات المالية الناجمة عليه، ويجب فهم القيمة الاقتصادية بشكل واسع مع مراعاة تأثير التكنولوجيا الجديدة على الأفراد والمؤسسات والدول.[2]

– **البعد السياسي:** يتمثل البعد السياسي للأمن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها، والتي تقصد بها حقها وواجبها في تحقيق الرفاهية لشعبها فهي تؤثر موازين القوى داخل المجتمع نفسه، حيث أصبح الفرد يستطيع أن يكون اللاعب الأساسي في لعبة أساسية، كما أصبح بإمكانه الإطلاع على كل المعلومات الخاصة بالحكومة من خلفيات وقرارات ومبررات سياسية، ومن جهة أخرى يستفيد العاملون

---

[1] الأمن السيبراني وحماية أمن المعلومات، رابط الموقع: https://www.kutub.info.
تم الاطلاع عليه في: 2024/04/20 الساعة 12: 13PM

[2] سعيدة رشاش، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مذكرة ماستر، تخصص دراسات استراتيجية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة العربي تبسي تبسة، 2018، ص 4.

في السياسة من التكنولوجيا بالوصول إلى أكبر عدد ممكن من الأفراد، والترويج لأنفسهم وهذا يؤثر بشكل كبير على الأفراد بغض النظر على صحة السياسات. [1]

مثال: إختراق الشبكة الحاسوبية الفرنسية قبل الانتخابات الرئاسية عام 2017م المتعلقة بالمترشحين المحتملين وأحزاب سياسية في فرنسا.

- **البعد الاجتماعي:** يستخدم مواقع التواصل الاجتماعي أكثر من 4,35 مليار من أصل 5,35 مليار مستخدم للأنترنيت، مما يجعلها أكبر مجتمع لتفاعل الأفراد ويفتح أفق جديدة لتبادل الخبرات، ولكنه رغم هذا يعرض أخلاقيات المجتمع إلى الخطر لصعوبة مراقبة محتوى الأنترنيت، كما يهدد السلم الاجتماعي على الدولة ذلك بسبب عمليات الاختراق الخارجي، ولذلك وجب توعية المواطن لتحقيق الأمن السيبراني في البعد الاجتماعي.

مثال: اختراق الحسابات والملفات الشخصية.

- **البعد القانوني:** فرضت التطورات التكنولوجية الجديدة مواكبة التشريعات القانونية وهذا ما جعل العلاقة بين التكنولوجيا والقانون علاقة تبادلية، ولكن الجريمة السيبرانية تفتقر للتشريعات القانونية الصارمة للتعامل معها، وذلك عائد لطبيعة هذه الجريمة وصعوبة معرفة مرتكبيها أو تحديده، ولعدم تقيدها بحدود دولة الأمر الذي ألزم تفعيل تعاون دولي مشترك لمكافحتها،[2] ولقد وضعت الجزائر التشريعات الجزائية المتعلقة بالجرائم السيبرانية:

* 14-03 مكافحة الجرائم المعلوماتية وحماية الأنظمة القانونية.
* 09-03 حماية الأشخاص المادية والأنظمة الالكترونية ذات صلة بالمعلومات.
* 14-06 تنظيم الاتصالات الالكترونية.
* 02-03 حماية البيانات الشخصية.

[1] بكوش رميساء، مرجع سابق، ص 11-12.

[2] إسماعيل زروقة، مرجع سابق ص 1023.

الفرع الثالث: العلاقة بين الذكاء الاصطناعي والأمن السيبراني

هناك علاقة وثيقة بين الذكاء الاصـــطناعي والأمن الإلكتروني أو الســـيبراني، إذ يتم تطوير أنظمة الذكاء الاصطناعي التي يمكن استخدامها لتعزيز الأمن السيبراني، إلى جانب تنفيذ تدابير أمنية لحماية أنظمة الذكاء الاصطناعي من الاختراق أو التلاعب.

فبعد تزايد الجرائم الإلكترونية مثل سرقة البيانات والتصـيد الاحتيالي، لجأت المنظمات إلى عدة وسـائل لمكافحة تلك التهديدات، فاسـتعانت بفرق الأمن السـيبراني المؤهلة والمجهزة بأحدث التقنيات ومنها: تقنية الذكاء الاصـــطناعي التي تســـاعد على الكشـــف الســـريع عن الأنشطة الضارة ومواجهتها وتحمي الشبكات من الهجمات الإلكترونية. [1]

ومع ظهور تقنية الذكاء الاصـطناعي حيث تعد من أحدث التقنيات المسـتخدمة لتعزيز الأمن الســـيبراني وأمن المعلومـات، التجـأت الـدول إلى توظيف هـذه التقنيـة في المجـال السيبراني غير أن مثل هذه التقنيات تحتاج إلى قوانين تنظمها وضوابط.

لذلك وجب على الدول تطوير الأطر القانونية المتعلقة بهذه التقنية على الصـعيدين الإقليمي والدولي.

كما يمكن القول أن الذكاء الاصـــطناعي حقق تقدما هائلا في المجال التكنولوجي، كما أن لـه العديد من التطبيقات المحتملة وكذا الفوائد، ومع ذلك يجب أن يتم اســـتخدامه وفقا للقوانين والأخلاقيات بشـــكل مســـؤول، وأن يتم التركيز على حماية الخصـــوصـــية وتجنب التأثيرات الســـلبية المحتملة الناشـــئة منه وجعلها آلية فعالة لتحقيق الأمن الســـيبراني وأمن المعلومات وضمان فضاء رقمي أكثر أمنا. [2]

---

[1] الفرق بين الذكاء الاصطناعي والأمن السبراني: https://bakkah.com

تاريخ الإطلاع: 2024/03/29 الساعة: 10:00 AM

[2] محمد دحماني، الذكاء الاصطناعي كآلية لتعزيز الأمن السبراني، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي، الأغواط، مجلد 07، عدد 02، 2013، ص 607.

المبحث الثاني:

الأمن السيبراني وحفظ أمن المعلومات

يشـــير الأمن الســـبراني إلى حماية الأنظمة الحاســـوبية والشـــبكات من التهديدات الإلكترونية، بينما حفظ أمن المعلومات يتعامل بشـــكل واســـع مع حماية جميع أشـــكال المعلومات، بما في ذلك البيانات المطبوعة والمعلومات الحساسة الغير الرقمية، ويشمل حفظ أمن المعلومات سياسات الوصول والتخزين والتدمير لأمن المعلومات، بالإضافة إلى الأمن السيبراني الذي يرتكز على الحماية الرقمية في الجوانب العملية، يتشابه الإثنان في كثير من الجوانب ويتعاونان لضمان سلامة المعلومات بشكل عام.

الأمن الســـيبراني جزء من جهود حماية أمن المعلومات، بما في ذلك الاســـتراتيجيات والتقنيات التي تعمل على الحماية من التهديدات الإلكترونية لأمن المعلومات.

وسنتطرق في المبحث الى مطلبين:

المطلب الأول: مفهوم أمن المعلومات

المطلب الثاني: الأمن السيبراني كآلية لحفظ وسلامة أمن المعلومات

المطلب الأول:

مفهوم أمن المعلومات

قد ظهر مصطلح أمن المعلومات منذ بداية التواصل عن بعد، لاسيما في فترة الحروب ظهرت الحاجة لحماية المعلومات العســـكرية من اختراق العدو، والحصـــول على البيانات اللازمة فهذه كانت الغاية من أمن المعلومات، حتى تطورت لتشـــمل المعلومات الســـيبرانية والتقنيات الالكترونية كاملة، فبدأ بحمايتها بتشـــفير المعلومات وبتكار شـــيفرات ســـرية منعا لاختراقها وسرقتها بسهولة.

مع التقدم التكنولوجي في العالم، أصـبحت طرق الحماية أكثر تعقيدا بوسـائل تشـفير فعالـة، وهنـا كـان التواصـــل أكثر أمـانـا لكـافـة المعلومـات دون الخوف من العدو واختراقه للبيانات.

– تثبت المخابرات الأمريكية (CIA) مبدأ أمن المعلومات، فلم يتمكن ســـواء الأعداء أو الفضوليين من الوصول للمعلومات السرية.

– اتخذت السياسة المتبعة للحماية شكلها الحالي مع التطور التكنولوجي، وظهور الإنترنيت، واختراع الحواسيب بكافة أنواعها. [1]

الفرع الأول: تعريف أمن المعلومات

اختلف الباحثون والدارسون في هذا المجال على وضـع تعريف موحد لأمن المعلومات فمنهم من عرفه من زاوية أكاديمية، ومنهم من عرفه من زاوية تقنية، ويمكن إجمال هذه التعريفات فيما يلي:

– عرف فلاديمير قوان (Vladimir Guan) أمن المعلومات على أنه: جميع الوسـائل التي يتم توفيرها للحد من ضـــعف نظام المعلومات ضـــد مختلف التهديدات ســـواء المفاجئة أو المتعمدة، وبعبارة أخرى هي مجموع التقنيات التي تضـــمن لموارد نظام المعلومات ســـواء (الأجهزة أو البرامج) الاستخدام الأمثل وفي السياق المحدد.

[1] مؤمن محمد عيسى، بحث عن أمن المعلومات والبيانات والانترنيت رابط الموقع: https://qabila.net .
تم الإطلاع عليه في: 2024/04/8 الساعة 12: 17 AM

ويعرف آدم شوستاك (Adam Shostack)[1] أمن المعلومات على أنه: التأكد من أن نظم المعلومات يمكن أن تعمل بالشكل المطلوب، وعلى النحو المقصود في بيئة معادية. [2]

– أمن المعلومات هو مجموعة من المناهج والتقنيات والأدوات، التي تسمح بحماية موارد النظام المعلوماتي من أجل ضمان توافر المعلومات سريتها وسلامة محتواها.

– أمن المعلومات من زاوية أكاديمية: هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها

ومن زاوية تقنية هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.

ومن زاوية قانونية فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات، ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة[3].

كما يعرف بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها، أو الحاجز الذي يمنع الاعتداء عليها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية، المعايير والإجراءات

---

[1] **آدم شوستاك (Adam Shostack):** مدير أول للبرنامج في مجموعة هندسة الأمان والمجتمع، في Microsoft وهو جزء، من فريق دورة حياة تطوير الأمان من، Microsoft حيث يكون مسؤولا عن تقنيات تحليل تصميم الأمان (انظر وكيبيديا الموسوعة الحرة https://fr.wikepid.org).

[2] بغداد محمد، الأمن المعلوماتي وسبل حمايته في الجزائر، مذكرة مكملة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة سعيدة،2018/2017، ص 30–31.

[3] نوفيل حديد، كربيط حنان، أمن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة، المؤسسة LENTREPRISE كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، العدد 3، 2014، ص 197.

المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين، عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات[1].

– يمكن تعريفه بتفصيل أكثر بأنه "المفاهيم والتقنيات والتدابير التقنية والإدارية المستخدمة لحماية أصول المعلومات من الوصول غير المأذون به عمدا أو سهوا أو حيازتها أو الإضرار بها أو كشفها أو التلاعب بها أو تعديلها أو فقدها أو إساءة استخدامها".

– تعرف لجنة الأمن القومي الأمريكية (NSC)[2] أمن المعلومات بأنه "حماية المعلومات وعناصرها المهمة (الحرجة)، بما في ذلك الأنظمة والأجهزة التي تستخدم هذه المعلومات وتخزنها وترسلها".[3]

الفرع الثاني: عناصر أمن المعلومات

حدد بعض الباحثين والمهندسين بأمن المعلومات ثلاثة عناصر ينبغي توافرها والاهتمام بها لفهم وتوفير أمن المعلومات، وجاءت هذه العناصر تحت مسمى ثالوث أو مثلث أمن المعلومات (the CIA Triad) وهذا سنة 1987.

ويمكن تعريف هذه العناصر على أنها: مجموعة من المكونات الواجب توفرها للحفاظ على المعلومات الثابتة والمنقولة من أي نوع من أنواع الاستغلال والاعتداء، بحيث لا يطلع عليها سوى الأشخاص المصرح لهم، حيث أن كل عنصر من هذه العناصر مهم للإبقاء

---

[1] الموسوعة الحرة ويكيبيديا، أمن المعلومات رابط الموقع: https://ar.wikipedia.org
تاريخ الاطلاع 2024/05/08 الساعة 01:45 PM.

[2] **لجنة الأمن القومي الأمريكية:** يعرف باختصار بـ NSC هو مجلس تابع للرئاسة الأمريكية، يختص بقضايا الأمن القومي، وهو جزء من المكتب التنفيذي للولايات المتحدة (انظر تطبيقCHATGPT https://chat.openai.com(

[3] ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية فهرسة مكتبة الملك الوطنية أثناء النشر، الرياض، 2015م، ص 58..

على سرية وسلامة البيانات، وأن أي نقص في عنصر من هذه العناصر سيؤدي حتما إلى المساس بسرية وسلامة المعلومات.

هذه العناصر هي:

1- سرية المعلومات(Data confidentiality) : الغاية من هذا العنصر هو التأكد من أن المعلومات السرية والحساسة لا تكشف، ولا يتم الاطلاع عليها من قبل الأشخاص غير المخولين أو غير المصرح لهم بذلك، وهذا يعني أن المعلومة مؤمنة ولا يطلع عليها إلا من طرف الأشخاص أو الأقسام الذين لهم صلاحيات الاطلاع، ومن هنا يجب الحرص على درجة السرية وتقسيم المعلومات حسب درجة أهميتها وحساسيتها، وفي المقابل يتم تصنيف الأشخاص الذين يحق لهم الوصول لهذه المعلومات، وكذلك نوع هذا الوصول هل هو للاطلاع فقط أو للنسخ والتعديل، كما أن هؤلاء الأشخاص الذين يطلعون على معلومات معينة قد لا يكون لديهم الحق في الاطلاع على معلومات أخرى[1].

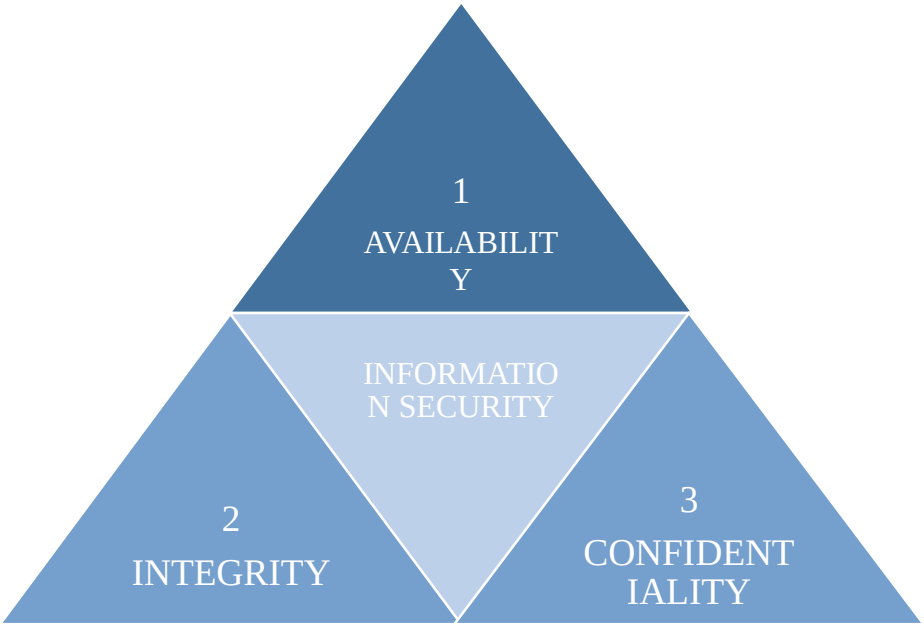
2- توفر المعلومات(Data Availability) : يشير هذا العنصر إلى وجوب ديمومة وتوفر المعلومات، أي أن تكون المعلومات متوفرة ومتاحة لدى الطلب من قبل الأشخاص المخولين بالاطلاع، وبمعنى آخر حماية المعلومة من أي خطر من أخطار الهجوم أو التعدي وبأي أسلوب كان هذا التعدي.

3- سلامة المعلومات وتكاملها(Data Integrity): ويقصد بهذا العنصر أن تكون المعلومات سليمة في محتواها ولم تتعرض لأي محاولة للإتلاف أو التغيير، سواء كانت المحاولة مقصودة أو غير مقصودة، ويوضح الشكل في الأسفل نموذج مثلث أمن المعلومات[2].

[1] عصامي نور الدين، دور أمن المعلومات في الحماية من أخطار التجسس الالكتروني،بحث، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة 20 أوت 1955، سكيكدة، 2019-2020، ص 3-4.

[2] بغداد محمد، مرجع سابق ص 37-38.

شكل رقم 01: يوضح نموذج مثلث أمن المعلومات(The CIA Triad)



Source: https://www.marianowo.orgpage255consulter le 2024/04/07 À 19: 23

إضافة إلى هذه العناصر الثلاثة هناك عناصر أخرى وجب توفرها هي:

1- **الحيازة (possession):** يعتبر عنصر الحيازة او إمتلاك التحكم واحد من إضافات باركر للنموذج السابق، وتممت إضافة هذا العنصر انطلاقا من فرضية مفادها أن المعلومات يمكن أن يتحكم فيها فرد أو مجموعة من الأفراد لا يمتلكون الحق في ذلك.

2- **المنفعة (utility):** يساعد هذا العنصر في الإشارة الى المعلومات ذات الفائدة والقيمة وهو عنصر من سداسي بارك[1]ر لأمن المعلومات، ويركز هذا العنصر على مفهوم يتم إغفاله تماما، أو الخلط بينه وبين عنصر التوافر، وهو فائدة هذه البيانات[2]

[1] **دون باركر**:باحث ومستشار في امن المعلومات، وضع وجهة نظر جديدة حول عناصر امن المعلومات (أنظر التطبيق https://chat.openai.com).

[2]Umesh hodeghtta and umeshaa nayak ,the info sec handbook an introductioni to informations se curity apress open ,new york, p 52

3- التحكم بالوصـول (Access Control): هو طرق أو وظائف الحماية التي تتحكم بوصـول المسـتخدمين أو الأنظمة إلى موارد المنشـأة، أو بعبارة أخرى منع الاسـتخدام غير مرخص به للموارد.

4- التحقق من الهوية(Authentication): أي التحقق من هوية الشـخص أو الجهة وأنه الشـخص المعني لا غيره، بعبارة أخرى فإن التحقق من الهوية هو التحقق من المستخدم لنظام ما هو بالفعل من ادعى أنه ذلك المســـتخدم، وفي حالة نقل المعلومات فإنه يجب التحقق من هوية المرسـل لضـمان أن المعلومة قادمة من مصـدرها الحقيقي، وكذلك يجب التحقق من هوية المستلم لضمان أن المعلومة ذاهبة إلى وجهتها الصحيحة[1].

الفرع الثالث: تهديدات أمن المعلومات

التهديد هو كل تصرف يمكن أن يؤثر سلبا على عناصر الأمن.

1- مصادر التهديدات

أ- التهديدات الطبيعية: كل التهديدات الخارجة عن الإرادة ومنها:

- **الكوارث الطبيعية** مثل الزلازل والفيضـــانات والنيران، إضـــافة إلى درجة الحرارة العالية والرطوبة العالية التي تلحق الضرر بالحاسوب والأجهزة الإلكترونية.

- **التهديدات التقنية:** كل المشـــاكل التي توقف الأعمال لمدة معنية، مما ســـبب خســـائر للمؤســـســـات، كانقطاع التيار الكهربائي للإنترنيت، حدوث أعطال في المكونات تنظم المعلومات.

[1] ذيب بن عايض القحطاني مرجع سابق ص 80 إلى 98.

ب- التهديدات البشرية: وتتمثل في مصادر خارجية تصدر من أعوان خارجية (المنافسين، الحكومات ،جماعات الضغط[1]) أو داخلية أو أجراء غير راضين أو أجراء قدماء متذمرين، وحتى نهاية القرن العشرين مصدر المعلوماتية الأكثر خطورة كانت الجرائم ذات مصدر داخلي صادرة من عمال نظرا لامتلاكهم المعارف وقدرتهم من الوصول إلى الأنظمة.[2]

2- أنواع التهديدات على المعلومات ونظم المعلومات

أ- التهديدات الناتجة عن الاعتداء: ومن تقنيات الاعتداء نجد:

- **البرامج الضارة:** كل برنامج يدخل في النظام ويكون عمله ضار منها (الفيروسات، الديدان، حصان طروادة، القنابل المنطقية).

- **القرصنة المعلوماتية (التجسس على أنظمة المعلومات):** القرصنة تعمل على كشف نقاط ضعف نظم حماية الأنظمة المعلوماتية، وغالبا ما يتم استعمال مختلف وظائف الأنترنت التي تحوله إلى نظام مفتوح يشمل الاختراق، وعليه هذا النوع من تقنيات الاعتداء يتمثل في محاولة اقتحام أنظمة المعلومات، والحصول على المعلومات السرية بأي طريقة وسنقوم بذكر أكثر الطرق انتشار (التنصت، سرقة الهوية، رفض الخدمة، تزوير أو تعديل).

- **التهديدات المادية:** التهديدات التي تمس الأجهزة المعلوماتية، تعني تهديد أمن المعلومات التي تحتويها ومنها (السرقة، الوصول والتدمير المادي).

ب- التهديدات الناتجة عن ثغرات أمنية: تعتبر الثغرة الأمنية[3] عبارة عن فجوة أو ضعف على مستوى نظام المعلومات، ومن الممكن استغلالها من طرف عناصر مهددة باستعمال

---

[1] **جماعات الضغط:** هي مجموعات منظمة تهدف الى التأثير على السياسة العامة وعملية صنع القرار من قبل الحكومة او المؤسسات الأخرى (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org).

[2] فيلالي أسماء، شليل عبد اللطيف، تهديدات أمن المعلومات وسبل التصدي لها، مجلة البشائر الاقتصادية، جامعة أبو بكر بلقايد تلمسان (الجزائر)، مجلد 4، عدد 3، تاريخ القبول 2019، ص 166.

[3] **ثغرات أمنية:** هي نقاط ضعف في نظام الحماية او التصميم او التنفيذ للتطبيقات او الأنظمة الحاسوبية (أنظر التطبيق chatgpt https://chat.openai.com).

مختلف طرق الهجوم العالية، الثغرة الأمنية هي عبارة عن ضعف أو خطأ في نظام معين أو طريقة حماية معينة يتم استغلالها من قبل المهاجم لإحداث أضرار مختلفة وتكون الثغرة الأمنية على ثلاث مستويات: (- ثغرات أمنية على مستوى تنظيمي (الإدارة)- الثغرات الأمنية على المستوى المادي- الثغرات الأمنية على المستوى التكنولوجي). [1]

المطلب الثاني:

الأمن السيبراني كآلية لحفظ أمن المعلومات

الأمن السبيراني هو حماية الشبكة والأنظمة التقنية للمعلومات، وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات والحماية من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع ويشمل مفهوم الأمن السبيراني أمن المعلومات والبيانات والأمن الإلكتروني والأمن الرقمي.

الفرع الأول: حفظ أمن المعلومات

إن أمن المعلومات والحفاظ عليه يستوجب مجموعة من الإجراءات الوقائية التي تستخدم للمحافظة على المعلومات وسريتها من السرقة أو التلاعب أو الاختراق غير المشروع

متطلبات تحقيق أمن المعلومات

وجب وضع سياسات وإجراءات لحماية المعلومات بشكل كافي لعدم الإطلاع عليها من قبل الأشخاص غير مصرحين بالدخول، ويرى المختصين في هذا المجال أنه يجب أن يكون هناك تعدد في المستويات للحماية والمرور، أو وضع نظام حماية فعال يقلل قدر المستطاع المشكلة كشف المعلومات ذات الأهمية القصوى من الإجراءات هذه:[2]

[1] فيلالي أسماء، شليل عبد اللطيف، نفس المرجع السابق، ص من 167 إلى 169.

[2] قذايفية أمينة، استراتيجية أمن المعلومات، مجلة الأبعاد الاقتصادية، جامعة أحمد بوقرة بومرداس الجزائر، العدد 06 جزء 1، 2016، ص 165.

– النسخ الاحتياطية للملفات المهمة لحمايتها من الفقدان.

– تطبيق وسائل حماية إضافية مثل (مفتش كابلات[1]، محلل البروتوكول[2]).

يؤكد (Markfathers) أن من متطلبات أمن المعلومات وضـــع قوانين ولوائح وتشـــريعات المسؤولة عن أمن المعلومات، لتحديد الأدوار الرئيسية والحد الأدنى لضوابط أمن المعلومات ويوجد طرق مهمة لتقليل المخاطر منها:

– البناء الصحيح لنظام المعلومات.

– تدريب المستخدمين في مجال أمن المعلومات، أمن قواعد البيانات، أمن الشركات.

– وضع إجراءات حازمة عند البوابة لتشغل النظام. [3]

وتعتبر الجزائر من الدول الساعية إلى تكثيف إطارها القانوني في إطار أمن المعلومات حيث سن المشرع الجزائري نصين يجرمان الجرائم الالكترونية.

1- قانون العقوبات: المعدل بـــــــموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 المتعلق بالمساس بالشبكة المعلوماتية والتي تضمن 3 أصناف:

– التزوير المعلوماتي والمساس بالمعطيات.

– الجرائم المتعلقة بالبحث والجمع والحيازة أو بث أو تجارة المعطيات.

– الجرائم المتعلقة بالمساس بالسرية ووحدة وأمن المعطيات في نظامها.

2- القانون المتضـمن القواعد الخاصـة للوقاية من الجرائم المتصـلة بتكنولوجيا الإعلام والاتصـال ومكافحتها: قانون 09-04 المؤرخ 5 أوت 2009 ويحتوي على 19 مادة موزعة

---

[1] **مفتش الكابلات:** فحص التوصيلات واختيار الأسلاك (أنظر التطبيق chatgpt https://chat.openai.com)

[2] **محلل البروتوكول:** شخص مختص في تحليل البروتوكولات، بين الأجهزة على الشبكة وفقا لمعايير محددة http/TCP/TP (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org) **اظر ملحق(3)** ص 98

[3] سلمى عبد الرحمان الدوسري، جبريل حسن محمد، دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع، مجلة مكتبة الملك فهد الوطنية، المجلد 24، العدد 2، أفريل-سبتمبر، 2017، ص 11.

عل 6 فصـول ومسـتمد من بنود الاتفاقيات الدولية خاصـة إتفاقية (بودابسـت) حول الجرائم المعلوماتية، كما اصدر قوانين أخرى لحماية أمن المعلومات:

- قانون الإجراءات الجزائية المعدل بموجب 04-14 مؤرخ في 10-2004.
- قانون 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة صدر في 19 يوليو 2003.
- المرسـوم التنفيذي 98-256 المؤرخ 25 أوت 1998 المعدل والمتمم للجزء التنظيمي من الأمر 75-89 المؤرخ 30-12-1975.

بالإضافة إلى استحداث هيئات وطنية لتقصي الجريمة الإلكترونية وحماية أمن المعلومات. [1]

أساليب ومبادئ حماية أمن المعلومات:

- استخدام برامج مكافحة الفيروسات والتجسس وتحديثها بشكل دوري.
- إنشاء حسابات شخصية متعددة منفصلة بصلاحيات منوعة والحذر من الحصول على حساب مدمر لنظام.
- تشفير [2] المعلومات المهمة بشكل صحيح.
- الحذر من الملفات المتعددة مثل (bmp-exe).
- تحميل البرامج والملفات من المواقع الموثوقة.
- استخدام كلمة مرور نظام قوية مع ضبط إعدادات المتصفح الأمنية.
- استخدام أجهزة مودم الموثوقة والآمنة مع تعطيل خاصية التشغيل عن بعد.
- اختبار خطط الطوارئ بشكل دوري.[3]

---

[1] بوميلة بوضياف، أمينة حمراني، أمن المعلومات في الجزائر، المجلة الجزائرية للأمن والتنمية، المجلد 09، العدد 16 جانفي 2020، ص 182-184.

[2] **التشفير**: تحويل البيانات من شكلها الأصلي إلى شكل مشفر، باستخدام خوارزميات معينة مما يجعلها غير قابلة للقراءة لأي شخص غير مخول بالوصول (أنظر التطبيق chatgp https://chat.openai.com)

[3] سلمى عبد الرحمان الدوسري، جبريل حسن محمد العشري، مرجع سابق، ص 11-12 .

الفرع الثاني: علاقة الأمن السبيراني وأمن المعلومات

بعد إرتفاع نسبة إستخدام الإنترنيت والأجهزة المحسوبية بنسب عالية، مع تطور السنوات وتوسع مجال استخدامها في كل مجالات الحياة من الحياة الاجتماعية لبناء صفقات تجارية وأعمال بين مؤسسات وشركات عبر الشبكة العنكبوتية، وصولا إلى تصريحات الدول الرسمية وموافقتها من أحداث دولية وعالمية.

كل ذلك يشكل أهمية كبيرة لاستخدام الأنترنيت، ولكن يشكل أهمية أكبر في معرفة مخاطر الأنترنيت وأساليب الاستخدام الصحيح للشبكات الاجتماعية ووسائل التواصل الاجتماعي، لكي يستطيع المستخدم تحقيق أكبر عدد ممكن من متطلباته مع أقل نسبة للتعرض للخطأ، والوقوع في المشاكل الإلكترونية، وعرضة للعصابات الإلكترونية التي تقود الأشخاص إلى الخضوع لعمليات الابتزاز الإلكتروني التي تؤدي بلا شك إلى خسارة الكثير إن كان على الصعيد المالي أو الاجتماعي، والنفسي والشخصي لذلك وجب التعرف على الأمن السيبيراني وأمن المعلومات .

1- يعرف الأمن السيبيراني أنه نظام حماية أنظمة الحاسوب المتصلة مباشرة بالإنترنيت وحماية البيانات والبرامج ضد أي هجمات إلكترونية دون الحاجة إلى تنظيم خطة أمنية .

2- يعرف أمن المعلومات بأنه نظام حماية المعلومات الرقمية، ويمكن من خلاله تشفير البيانات وتوفير الشبكات والبنية التحتية التي تحتوي على معلومات شخصية ومعلومات مادية وبيانات خاصة بالشركات ،وتكون كلها محمية بشكل مكثف ضد أي اختراقات[1] .

كما أن العلاقة بين أمن المعلومات والأمن السبيراني هي علاقة جزئية، حيث يتضمن أمن المعلومات حماية المعلومات من الوصول غير المصرح به، وقد تكون المعلومات في

[1] فتحي حسن عامر، الميتافيريس ثورة الاعلام الآلي الرقمي، طبعة 2، العربي للناشر والتوزيع، القاهرة 2023، ص 151 .

شـكل مسـتندات ورقية أو مخزنة على وسـائط الإلكترونية، ولكن لا يمكننا أبدا ان نقول أن أمن المعلومات يشمل أمان الشبكة تماما، كما لا يمكننا القول ان أمان الشبكة يتضمن أمان المعلومات ويشـــمل الأمن الســـبيراني أمن المعلومات المنقولة أو المخزنة أو المعالجة في أنظمة تكنولوجيا الاتصـالات والمعلومات، هذا صـحيح لكنه يشـمل أيضـا الحفاظ على توفير وأمن الخدمات المقدمة عبر الفضـاء السبيراني، مثل الطاقة الكهربائية ووسائل الاتصال لذلك لا يصـح القول أن امن المعلومات يشـمل الأمن السـبيراني والعكس، لأنه لا علاقة له بأمن المعلومات المكتوبة على المستندات ورقية وذلك لأنه لا ينتمي إلى نطاق الفضاء السبيراني .

إذن العلاقة بين أمن المعلومات والأمن السـبيراني هي التقاطع من حيث الاهتمام بأمن المعلومـات الموجودة بـالســـايبر، ويختلفـان فيمـا تبقى من الاهتمـامـات في نفس الوقـت لا نستطيع استخدام مصطلح الأمن السبيراني وأمن المعلومات كمصطلحين مترادفين تماما[1].

الفرع الثالث: آليات الأمن السبيراني في حفظ وسلامة أمن المعلومات

لا شـــك في أن الأمن الســـبيراني يمثل الدرع الرقمي الذي يحمي عالمنا المتصـــل بالإنترنيت، وفي عصـــر تكنولوجيا المعلومات حيث تتداخل حياتنا مع الشـــبكة العنكبوتية يصـبح الأمن السـبيراني أمرا حيويا للحفاظ على خصـوصـيتنا وأمان بياناتنا، ويشـمل الأمن السبيراني مجموعة من السياسات والتقنيات التي تستهدف الوقاية من الهجمات والحفاظ على سـلامة الأنظمة الرقمية، وبناء حاجز ضـد التهديدات السـبيرانية المتزايدة من خلال اسـتخدام برامج مكافحة الفيروسات وجدران الحماية وتحديثات البرمجيات.

[1] قطاف سليمان، بوقرين عبد الحليم، الأمن السبيراني والمضامين المفاهيمية المرتبطة به، جامعة الاغواط (الجزائر)، مجلة طيبة للدراسات العلمية الأكاديمية، مجلد 05، عدد 02، 2022، ص 66 .

وتمثل تحقيق التوازن بين التقدم التكنولوجي والحفاظ على الأمن تحديا مستمرا يتطلب تطويرا وتبني استراتيجيات فعالة للدفاع عن العالم الرقمي الذي نعيش فيه، حيث يلعب الأمن السيبراني في هذا العالم الرقمي المعقد دورا حيويا في حماية معلوماتنا الشخصية وضمان استمرارية العمليات الأساسية للشركات والحكومات. [1]

أهم أدوات الأمن السيبراني لحماية وحفظ أمن المعلومات

1- **جدار الحماية[2]: firewall** أو ما يعرف بالجدار الناري وهو جهاز أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب كما يراقب حركة المرور الشبكة بالإضافة إلى محاولات الاتصال مما يساعد في حماية الأنظمة من التسلل.

وله عدة أنواع هي: utm firewall / stateful inspection firewall / proxy firewall / Next-generation firewall

2- برامج مكافحة الفيروسات: Antivirus Software حيث تقوم هذه البرامج بالتنبيه في حالة الإصابة بالفيروسات، والبرامج الضارة كما ستقدم خدمات إضافية مثل فحص رسائل البريد الالكتروني للتأكد من خلوها من المرفقات الضارة أو روابط الواب كما تقدم هذه البرامج إجراءات وقائية مفيدة مثل عزل التهديدات المحتملة وإزالتها.

3-خدمات البنية التحتية للمفاتيح العمومية: PKI Services هي إطار عمل يستخدم لإنشاء اتصالات آمنة، وسلامة البيانات والمصادقة في المعاملات الرقمية داخل شبكات

[1] تقنيات الأمن السيبراني والتحديات المستقبلية: https://www.aljazeera.net
2023/12/04 تاريخ الاطلاع: 03/25/ 2024 الساعة 3:00

[2] **جدار الحماية:** يعمل كبوابة دخول بين شبكة واخرى لتطبيق معين خوادم البروكسي يمكنها تزويد وظائف إضافية كتخزين المحتوى المؤقت وكذلك الامن عبر منع الاتصالات المباشرة من خارج الشبكة (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org). **أنظر الملحق (4) ص 99.**

الكمبيوتر، والخدمات المستندة الى الإنترنيت لأنها تلعب دورا حاسما في ضمان الأمن والامتثال في عالم رقمي متزايد.

يربط العديد من الأشخاص PKI[1] فقط بـ SSL[2] أو TLS وهي التقنية التي تقوم بتشفير اتصالات الخادم والمسؤولة عن HTTPS[3] والقفل الذي تراه في أشرطة عناوين متصفحك.[4]

4- خدمات الكشف المدارة: نظرا لأن مجرمي الإنترنيت والمتسللين أصبحوا أكثر تعقيدا وأصبحت التقنيات والبرامج التي يستخدمونها أكثر تقدما فقد أصبح من الضروري وجود أشكال دفاعية أكثر قوة وتكون استباقية وقادرة على تحديد الهجمات الإلكترونية قبل أن تتسبب في حدوث مشكلات، حيث شهد الأمن السيبراني تحولا من الاستثمار في التقنيات التي تحاول منع احتمال وقوع هجوم نحو الخدمات المتقدمة، التي تتفاعل مع مشكلات الأمان المحتملة وتكتشفها وتستجيب لها بأسرع وقت ممكن.

---

[1] **PKI** أو ما يعرف بعلم التعمية والتشفير للبنية التحتية للمفاتيح العامة، والتي بواسطتها يتم الربط بين المفتاح العام والمستخدم بواسطة مصدر الشهادة، يتم ذلك عن طريق برمجيات خاصة من الممكن أن تكون تحت إشراف بشري جنبا إلى جنب مع برمجيات منسقة ،في مواقع مختلفة ومتباعدة(أنظر التطبيق chatgpt.)https://chat.openai.com

[2] **SSL** : وهو اختصار لـ Secure Sockets Layer وهو بروتوكول أمان، يستخدم لتأمين اتصالات بتشفير البيانات التي يتم نقلها بين متصفح الويب وخادم الويب، مما يحمي البيانات من التسلل أو الاستيلاء عليها من قبل المتطفلين(أنظر موقع ويكيبيديا الموسوعة الحرة)https://fr.wikepid.org

[3] **TLS** : هو اختصار لـ Transport Layer Security وهو بروتوكول يستخدم لتأمين إتصالات الإنترنيت بين العميل والخادم ،عن طريق تشفير البيانات وتأمينها ضد الاختراق والتلاعب، مثل المعاملات المصرفية عبر الإنترنيت(أنظر موقع ويكيبيديا الموسوعة الحرة)https://fr.wikepid.org. **انظر الملحق (5) ص 9**

[4]البنية التحتية للمفتاح PKI على الموقع: https://Appmaster.io

تاريخ الاطلاع 2024/04/11 الساعة12:57 AM

5- اختبار الاختراق: يحاول اختبار Pen Test محاكاة نوع الهجوم الذي قد تواجهه الشركة من المتسللين المجرمين، بدءا من اختراق كلمة المرور وحقن الشفرة وحتى التصيد الاحتيالي[1].[2]

6- قيد الوصول: عند عدم قدرة المهاجم على الوصول إلى الشبكة فلن يكون الضرر كبيرا كما أن أي شخص مخول له الوصول إلى الشبكة قد يشكل خطرا أيضا، فمن الأفضل أن تقوم بتقييد وصول المستخدم والموارد إلى الشبكة، وهنا تكون قد رفعت من نسبة الأمان للشبكة والتي مسؤوليتها تقع على عاتقك.

7- تقنيةDLP : تقدم هذه التقنية المساعدة في حسن استخدام البيانات المهمة، والتي قد يُخطئ الموظف في استخدامها بشكل سيء، وهذا يعرضها لخطر بالغ، فمن المهم الاعتماد على تقنيات وسياسات DPL للتخلص من هذه النقطة الضعيفة في الاستخدام، وهذا ما سنتعرف عليه عند دراسة أساسيات تحليل البيانات وتخزينها.

8- أمان نقطة النهاية: للأسف أصبح لا يوجد فارق بين أجهزة الحاسوب الشخصي والأجهزة التي تستخدم في الأعمال، وهذا زاد من احتمال حدوث هجمات اختراق للأجهزة الشخصية بسبب عدم التمييز بينها، لأن المهاجم قد يخترق حاسوبك الشخصي، ظنا منه أنه حاسوب تجاري، لذلك لابد من وجود حماية تساعد على التمييز بين الإثنين، وهذا ما يقوم به تأمين نقطة النهاية.

---

[1] التصيد الاحتيالي: نوع من الهجمات عبر الأنترنيت يستهدف خداع الأشخاص للكشف عن معلوماتهم الحساسة (أنظر موقع ويكيبيديا الموسوعة الحرةhttps://fr.wikepid.org).

[2] الحماية من الهجمات الالكترونية عبر ستة أدوات للأمن السيبراني: https://www.rmg-sa.com
تم الاطلاع عليه في: 2024/03/28 ساعة2:15 pm

9- أنظمة منع التطفل: تقوم هذه الأنظمة بمراقبة حركة مرور الشـــبكة، وتتعرف على أنواع عديدة من الهجمات الإلكترونية، وتقوم بصدها ومحاربتها، وتعتمد في ذلك على قاعدة بيانات الأساليب الهجومية المعروفة.

10- أمان الويب: إن أمان الويب يحمي الشـبكة بشـكل شـامل، وتعتمد عليه الشـركات)من أجل إضـافة الأمان عند اسـتخدام الشـبكة الداخلية للويب، وهذا يسـاعد على منع اسـتخدام صفحات الويب كطريقة لاختراق الشبكة.

كانت هذه أفضـل الممارسـات والتقنيات في مجال الأمن السـيبراني والتي معظمها تعمل وفق نظام الذكاء الاصـطناعي، وبالتالي تسـاعد المؤسـسـات على الكشـف والوقاية من عمليات اختراق الشبكات وسرقة المعلومات الرقمية التشغيلية. [1]

11- التشـفير: تهدف هذه التقنيات إلى حماية البيانات والمعلومات الحسـاسـة من الوصـول غير المصـرح به، تعتمد تقنيات التشـفير المتقدمة على اسـتخدام خوارزميات رياضـية معقدة لتحويل البيانات إلى شـكل غير قابل للقراءة، يتم اسـتخدام مفتاح سـري لتشـفير البيانات وفك تشـفيرها، واحدة من أهم تقنيات التشـفير المتقدمة هي تقنية التشـفير بالمفتاح العام[2] والمفتاح الخاص، تعتمد هذه التقنية على اسـتخدام مفتاحين مختلفين لتشـفير وفك تشـفير البيانات، يتم استخدام المفتاح العام لتشفير البيانات ويتم استخدام المفتاح الخاص لفك تشفيرها، يعتبر هذا النوع من التشفير آمنا وفعالا في حماية البيانات الحساسة. [3]

---

[1] تقنيات الأمن السبيراني إدارة المخاطر في عصر المعلومات: https://ar.lpcentre.com
تم الاطلاع عليه في: 2024/03/28 ساعة pm3:15

[2] **التشفير بالمفتاح العام:** هو نظام يستخدم مفتاحين عام وخاص، يستخدم العام لتشفير البيانات والخاص لفك التشفير ويعتبر، هذا النوع متاحا للعامة ويمكن توزعيه بشكل عام (أنظر التطبيق chatgpt https://chat.openai.com).

[3] تقنيات الأمن المتقدمة لمكافحة الاختراق والتهديدات السيبرانية، مدونة أمرنا: ae.linkedin.com
تم الاطلاع عليه في: 2024/03/28 ساعة pm 3:15

اقتراحات الفصل الأول:

_ تطوير البنية التحتية السبرانية لتعزيز الأمان السبيراني، وحمايته من المخاطر عن طريق تحسين البنية الرقمية، وتفعيل التعاون الدولي إضافة الى تطوير الكوادر الوطنية.

_ تعزيز الأمن السبيراني في مختلف المجالات المرتبطة به، من خلال توظيف الذكاء الاصطناعي الذي يلعب دورا حيويا في تعزيز أمان الأنظمة والمعلومات.

_ دعم عناصر أمن المعلومات لأن لها دورا أساسيا في حماية البيانات والمعلومات الحساسة من الهجمات الالكترونية والتهديدات، وذلك بتعميق السرية وتكريس النزاهة، إلى جانب تعزيز الوصول.

_ التوعية بمخاطر الهجمات والجرائم الإلكترونية، من خلال الحملات الإعلامية وإدراج مواد توعوية في مجال أمن المعلومات والأمن السيبراني في المناهج الدراسية.

الفصل الثاني:

واقع أمن المعلومات والذكاء الاصطناعي

في ظل التحول الرقمي الحاصل في ظل الثورة الصناعية الرابعة واندماج التكنولوجيا التي تشمل إنترنيت الأشياء، والحوسبة الحاسبة، وتحليلات البيانات الضخمة، والذكاء الاصطناعي، وجدت الشركات التجارية والمجتمعات نفسها أمام فرص وتحديات غير مسبوقة، هذه التحديات زادت حدتها بانفجار تداول وانتشار معلومات والبيانات حيث أصبح لازما على المجتمعات حمايتها وفقا لآليات عديدة، فبرز الأمن السيبراني للحفاظ على أمن المعلومات ومنع الوصول للبيانات الحساسة، وأصبحت حتمية توظيف الذكاء الاصطناعي لتحقيق الأمن السيبراني، وهذا بسبب الاعتماد المتزايد لأنظمة الكمبيوتر على الإنترنيت والشبكات اللاسلكية لتخزين المعلومات وتبادلها.

سنتطرق في **المبحث الأول:** إلى ماهية الذكاء الاصطناعي

أما **المبحث الثاني:** آليات الذكاء الاصطناعي في حماية أمن المعلومات وتحدياته. [1]

[1] خليل سعيدي، مرزوق بن مهدي، الذكاء الاصطناعي كتوجه حتمي لحماية الأمن السيبراني، مجلة دراسات في حقوق الإنسان، جامعة العربي تبسي، تبسة، مجلد 6، عدد 1 جوان 2022، ص 26.

المبحث الأول:

ماهية الذكاء الاصطناعي

تم استخدام مصطلح الذكاء الاصطناعي لأول مرة عام 1955 من قبل أستاذ الرياضيات في كلية دارتموث **جون مكارثي**، والذي أشار إليه باسم "**علم وهندسة صنع الآلات الذكية**" منذ ذلك الحين انتشرت الأبحاث حول الذكاء الاصطناعي في مجالات المعرفة المختلفة، إذ يناقش علماء الاجتماع الآثار الأخلاقية والقانونية للذكاء الاصطناعي في حين يطور علماء الكمبيوتر خوارزميات التعلم العميق المتقدمة، بينما يدرس الباحثون في إدارة الأعمال آثار الذكاء الاصطناعي على العملاء والمؤسسات، وأصحاب المصلحة في عالم مترابط بشكل متزايد، إذ يعتمد التوصيف على المكان الذي يقف فيه الباحث، كما أن التعريف يميل إلى التغيير اعتمادا على السياق المحدد للبحث والتطبيق. [1]

سنتطرق في هذا المبحث إلى:

المطلب الاول: مفهوم الذكاء الاصطناعي.

المطلب الثاني: تقييم الذكاء الاصطناعي

[1] سناء أرطباز، أثر استخدام تطبيقات الذكاء الاصطناعي على تحسين أداء المؤسسة، جامعة أم البواقي، مجلة العلوم الإنسانية لجامعة أم البواقي، مجلد 09، عدد 03 ديسمبر 2022، ص 1250.

المطلب الأول:

مفهوم الذكاء الاصطناعي

يعد الذكاء الاصطناعي دراسة للسلوك الذكي (في البشر والحيوانات والآلات)، كما أنه يمثل محاولة لإيجاد السبل التي يمكن بها إدخال مثل هذا السلوك على الآلات الاصطناعية علاوة على ما سبق يعد الذكاء الاصطناعي من أصعب الموضوعات وأكثرها إثارة للجدل للبشرية بأسرها.

قد لا تتضح صعوبة هذا الموضوع في بادئ الأمر، ولكن يتم إدراكها بعد ذلك بشكل كبير، ففي بعض الأحيان يتشابه البحث في مجال الذكاء الاصطناعي مع استكشاف الفضاء البعيد في مستوى الصعوبة، ولكن تتجلى حقيقة مهمة تتمثل في أن البحث في هذا المجال أصعب بكثير من استكشاف الفضاء، ففي مجال استكشاف الفضاء تكون لدينا على الأقل معرفة بالمشكلات الفنية الرئيسية، ولكن لسوء الحظ في الذكاء الاصطناعي يكون الأمر مختلفا عن ذلك. [1]

– الذكاء الاصطناعي هو مجال يهتم بتطوير أنظمة الكمبيوتر القادرة على أداء المهام التي تتطلب تفكيرا وتحليلا بشريا ذكيا، وهو تطور هائل في مجال التكنولوجيا يسمح للأنظمة الذكية بالتعلم والتكيف والتفاعل مع البيئة المحيطة. [2]

– وفقا **SOLANKI AND ALL** فإن**artificial inteligence AI**، هو ذكاء تظهره الآلات أو أجهزة الكمبيوتر، والذي يطلق عليه أحيانا ذكاء الآلة لمحاولة محاكاة الذكاء البشر

[1] بلاي ويتباي، الذكاء الاصطناعي، دار الفاروق للاستثمارات الثقافية، الجيزة، مصر، 2003، الطبعة العربية 2008، ص 15.

[2] محمد دحماني، مرجع سابق، ص 599.

أحيانا التفوق عليه، أي أن الذكاء الاصـطناعي هو المحتوى الإبداعي المكتوب عن طريق الدردشة بصيغة السؤال بواسطة العنصر البشري، والإجابة بواسطة الذكاء الاصطناعي. [1]

– هو علم مبني على القواعد الرياضـــية والأجهزة والبرامج التي تم تجميعها في الحاســـبات الآلية، التي تقوم بدورها بالعديد من المهام والعمليات التي يمكن للإنســـان أن يقوم بها، غير أنها تختلف عليه من حيث السرعة والدقة في إيجاد الحلول للمشاكل المعقدة.

نجد بعض الأمثلة البارزة للذكاء الاصـــطناعي، من بينها المركبات ذاتية القيادة والطائرات بدون طيار في مجال المركبات، والتشخيص الطبي والرعاية الصحية عن بعد في مجال الرعاية الصـحية، وأنظمة اكتشـاف البرامج الضـارة والفيروسـات البرمجية في مجال الأمن السبيراني، ومعالجة الصور في مجال تقنيات الإبصار الحاسوبي وغير ذلك. [2]

الفرع الأول: تعريف الذكاء الاصطناعي

يعرفه **راسل بيل**[3]: الذكاء الاصطناعي هو علم بناء الآلات العادية، هذه محاولة لجعل الآلات تعمل كما رأينا في أفلام الخيال العلمي، مما يسمح لهم بالتفكير والتعلم والقيام بأشياء كانت حتى وقت قريب غير إنسانية.

يعرفه **ســيمون**[4]: الذكاء الاصـــطناعي بأنه مرتبط بعلم النفس والعلوم المعرفية، وغيرها من العلوم التي تمكن أجهزة الكمبيوتر من أداء المهام بكفاءة، وتقليد القدرات البشـــرية وجعل أجهزة الكمبيوتر تفكر بذكاء.

---

[1] لحول بن علي، بريكي خالد، الذكاء الاصطناعي في المجال العلمي بين الحتمية في التطبيق والمخاطر في الإنتاج، مجلة التراث، المجلد 14، العدد مارس 2024، ص 70.

[2] بن علي إحسان، أهمية الذكاء الاصطناعي في إدارة الأزمات في ظل كوفيد 19 – تجربة الإمارات العربية المتحدة– مجلة آفاق علوم الإدارة والاقتصاد، جامعة زيان عاشور الجلفة، الجزائر، المجلد 06، العدد 02، 2022، ص 467.

[3] **راسل بيل:** رجل أعمال ومبرمج شهير، مؤسس شركة مايكروسوفت (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org).

[4] **سيمون:** عالم ذكاء اصطناعي شهير، حاصل على جائزة نوبل في علم الاقتصاد (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org).

– ويعرفه **ريتش وكينج:** الذكاء الاصـــطناعي هو دراســـة كيف يمكن لأجهزة الكمبيوتر أداء المهام بشكل أفضل من البشر.

– ويعرفه **مجلس صناعات المعلوماتITI** : الذكاء الاصطناعي بأنه "مجموعة من التقنيات القادرة على التعلم واســـتخدام المنطق، والتكيف وأداء المهام بطرق مســـتوحاة من العقل البشري". [1]

– يعتبر **العالم الأمريكي جون مكارثي john mcCarthy**[2] هو الذي صـك مصـطلح الذكاء الاصـطناعي في عام 1956 وقد عرفه بأنه علم وهندسـة صـناعة الآلات الذكية أو "the science and engineering of making intelligent machines وخاصـــة برامج الحاســوب الذكية، أو هو فرع علوم الحاسوب الذي يهدف إلى إنشاء الآلات الذكية.

والذكاء intelligence كمفهوم يصـــعب تعريفه بدقة، ويمكن اعتباره الجزء الحســـابي الذي يعطينا القدرة على تحقيق الأهداف في العالم من حولنا، ولدى الناس مختلف الدرجات من الذكاء، وكذلك الحيوانات وبعض الآلات وفق هذا التعريف.[3]

كما أننا نستطيع تعريف الذكاء الاصطناعي بأكثر من تعريف:

---

[1] محمد دحماني، إستخدامات الذكاء الاصطناعي في المجال البيئي، مجلة القانون والعلوم البيئية، جامعة عمار ثليجي الأغواط، المجلد 02، العدد 03، 2023، ص 483.)

[2] **جون ماكثي:** عالم حاسوب أمريكي، ساهم بشكل كبير في تطوير لغة البرمجة (انظر تطبيق copilot على الموقع https://copilot.microsoft.com

[3] الذكاء الاصطناعي ويكيبيديا على الموقع: https://ar.wikepid.org

تاريخ الاطلاع 2024/05/06 الساعة 11:11 AM

– الذكاء الاصـــطناعي AI هو دراســـة القدرات الذهنية من خلال اســـتخدامه للنماذج الاحتسابية[1] computational models .

– الذكاء الاصـطناعي AI هو دراسـة كيفية جعل الحواسـيب تقوم بأشـياء يقوم بها الإنسـان بشكل أفضل في الوقت الحالي.

– الذكاء الاصـطناعي AI هو دراسـة وتصـميم العملاء الأذكياء intelligent agents، حيث أن العميل الذكي، هو نظام يدرك بيئته ويقدم أفعالا تزيد من فرصة نجاحه في أهدافه.[2]

– كما عرف بأنه "دراسة وتصميم أنظمة ذكية بطريقة مستقلة تستوعب بيئتها مع اتخاذ كافة التدابير اللازمة من أجل تحقيق أهداف محددة".

– كما يعرف الذكاء الاصـــطناعي على أنه "نظام معلوماتي يتمتع بقدرات فكرية مماثلة لتلك التي توجد لدى الإنسـان، أو هو تطبيق حاسـوبي أو آلة تؤدي العمليات التي يقوم بها الذكاء البشري".

من خلال التعاريف الســابقة يمكن القول بأن الذكاء الاصـــطناعي هو "أحد علوم الحاســب الآلي الحديثة، التي تبحث عن أســاليب متطورة لبرمجته للقيام بأعمال واســتنتاجات تشــابه الأساليب التي تنسب لذكاء الإنسان، من خلال فهم العمليات الذهنية الشائكة التي يقوم بها العقل البشـــري أثناء التفكير، ثم ترجمتها إلى ما يوازيها من عمليات حســـابية تزيد من قدرة الحاسب على حل العمليات الشائكة".[3]

مما ســبق من التعريفات نســتنتج أن الذكاء الاصـــطناعي يهدف إلى تطوير أنظمة تحقق مستوى من الذكاء شبيه بذكاء البشر، أو أفضل منه وصممت تطبيقات الذكاء الاصطناعي

---

[1] **النماذج الاحتسابية:** النماذج الحاسوبية التي تستخدم لحاسب أو تنبؤ الظواهر.

[2] فهد آل قاسم، مدخل الى علم الذكاء الاصطناعي، موقع الرابط: https:// www.alarabimag.com تاريخ الاطلاع: 29-04-2024، ساعة 10:17

[3] بدري جمال، الذكاء الاصطناعي، المجلة الجزائرية للعلوم القانونية والسياسية، كلية الحقوق، جامعة الجزائر 1، المجلد 59، العدد 4، 2022، ص 175.

لتكون تقليدا لتصرفات العقل البشري، وحتى يتم ذلك فقد حددت جوانب تفوق الذكاء البشري في طريقة الاستنتاج، والتفكير وحصرها في خمس نقاط أو خطوات: التصنيف (**Categirization**)، تحديد القوانين (**Specific Rules**)، التجارب (**Heuristics**)، الخبرة السابقة (**Past Experience**)، التوقعات (**Expectation**).

فالهدف هو وضع المعارف البشرية داخل الحاسوب ضمن ما يعرف بقواعد المعرفة ومن ثم يستطيع الحاسوب عبر الأدوات البرمجية البحث في هذه القواعد، والقيام بالمقارنة والتحليل، من أجل استخلاص واستنتاج أفضل الأجوبة والحلول للمشكلات المختلفة، وهذا ما يشبه ما يقوم به الإنسان عندما يحاول حل مشكلات جديدة تصادفه في حياته اليومية إعتماد على خبراته وتجاربه السابقة، وعبر توقعاته للنتائج المحتملة، ومن خلال مهاراته في الاستنتاج والمفاضلة بين أحسن الحلول المتاحة. [1]

الفرع الثاني: خصائص الذكاء الاصطناعي

يتسم الذكاء الاصطناعي بالعديد من الخصائص منها:

- استخدام الذكاء في حل المشاكل المعروضة مع غياب المعلومات الكاملة.
- القدرة على التفكير والإدراك.
- القدرة على اكتساب المعرفة وتطبيقها.
- إمكانية التعلم والفهم من التجارب والخبرات السابقة.
- استخدام الخبرات القديمة وتوظيفها في مواقف جديدة.
- القدرة على استخدام التجربة والخطأ لاكتشاف الأمور المختلفة.
- الاستجابة السريعة للمواقف والظروف الجديدة، التعامل مع المواقف الغامضة.

[1] أسماء بليليطة، التكريس القانوني والتنظيمي للذكاء الاصطناعي في الجزائر، المجلة الدولية للذكاء الاصطناعي في التعليم والتدريب، جامعة الجزائر 1، ص 19-20.

– القدرة على تمييز الأهمية النسبية لعناصر الحالات المعروفة.[1]

بعبارة أخرى فإن الذكاء الاصطناعي يتسم بمجموعة أخرى من الخصائص هي:

1– إمكانية تمثيل المعرفة: استخدام هيكلة خاصة لوصف المعرفة تتضمن الحقائق والعلاقات بين هذه الحقائق، والقواعد التي تربط هذه العلاقات في الأخير هذه الهياكل تكون فيما بينها قاعدة المعرفة[2]، والتي توفر أكبر قدر من المعلومات عن المشكلة المراد حلها.

2– استخدام الأسلوب التجريبي المتفائل: أي التركيز على الحلول الوافية، وليس على الحلول المثلى والدقيقة.

3– قابلية التعامل مع المعلومات الناقصة: قابليتها لإيجاد الحلول حتى ولو كانت المعلومات غير متوافرة بأكملها في الوقت الذي يتطلب فيه الحل.

4– القابلية على التعلم: من الخبرات والممارسات السابقة، إضافة إلى قابلية تحسين الأداء مع أخذ الاعتبار الأخطاء السابقة.

5– قابلية الاستدلال: القدرة على استنباط الحلول الممكنة لمشكلة معينة، ومن واقع المعطيات المعروفة والخبرات السابقة ولاسيما المشكلات التي لا يمكن معها استخدام الوسائل التقليدية المعروفة الحل. [3]

الذكاء الاصطناعي سيلغي الكثير من الوظائف التي تدعى بـــ low skiled jobs مثل تحليل بيانات ضخمة data analysis لصنع تصميمات الإكترونية، والذي يحتاج إلى مراقبة وتحليل قبل اتخاذ قرارات حساسة وسريعة في أثناء التصميم وبسبب خطأ صغير جدا، كانت

---

[1] زعموكي سالم، مرزق فتيحة حيالي، مجلة التراث، جامعة زيان عاشور بالجلفة (الجزائر)، المجلد 13، العدد 04، ديسمبر 2023، ص 39–40.

[2] * **قاعدة المعرفة:** نوع من أنواع قاعدة البيانات، لإدارة المعرفة وتكون للاستخدام البشري فقط، (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org).

[3] أبو بكر خوالد، تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات الأعمال، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، الطبعة الأولى، جامعة عنابة، الجزائر، 2019، ص 13–14.

سـابقا تنفذ من قبل خبير أو مصـمم يراقب ويحلل، ومع العلم أنه أصـبح يسـتثمر وقته في وظائف أهم وهي high skilled jobs[1] والتي تعزز صفاتنا الإنسانية ،ويصعب على الذكـاء الاصطناعي محاكاتها مثل الذكاء العاطفي والإبداع Intelligent intelligent creativity [2]

وكذا تحسين الرعاية الصحية:

إن تطبيق الذكاء الاصـطناعي سـاهم في العديد من العمليات الصـحيةhealthcare automation كالتشخيص، الجراحة الدقيقة، الصناعات الدوائية.[3]

وكذا إحداث دورة في الزراعة:

لـه أثر بـالغ في التطور الزراعي مثلا تقوم أحد أنواع الروبوت بزراعة البذور، كما تقوم Drones [4] بمراقبة الزراعة وإضافة المبيدات الحشرية وتحليل بيانات المحاصيل.

كما يقوم الذكاء الاصطناعي بإلغاء المهام المملة والمكررة: يقوم بإعادة تشكيل فئات العمل بحيث يقلل الـــ low skilled jobs ،والتي تحتاج إلى وقت وجهد وقوة عاملة production lines ،مع دخول الذكاء الاصـطناعي أصـبحت مهام العامل تقتصـر على تفعيل مهاراته الإنسانية

---

[1] **high skilled jobs**: وظائف ذات مهارات عالية، تكون نادرة وغالبا ما تكون لتشغيل أعمال ناجحة مثل متخصص أمان المعلومات(أنظر موقع ويكيبيديا الموسوعة الحرة)https://fr.wikepid.org

[2] رؤى حسن الدين هاني قطيشات، الذكاء الاصطناعي المستقبل الجديد، ص 4

[3] دور الذكاء الاصطناعي يزداد في القطاع الطبي على الموقع: https://cnnbusinessararbic.com تاريخ الاطلاع 01/05/2024 الساعة 13:12 AM

[4] **الدرون:** طائرة مصممة بحجم اصغر، تعمل بالتحكم عن بعد بدون طيار انظر تطبيق copilot على الموقع https://copilot.microsoft.com

وكذا تحسين السلامة المرورية ،حاليا تسعى المدن للتحول إلى Smart cities[1]، بحيث يتم إدارة السير والمرور بناء على Trafic pattern[2]، وعليه تقوم Desision Making algorithm بتعديل إضاءة الإشارات المرورية ومدتها وإصدار المخالفات.[3]

* **إنشـــاء قاعدة بيانات معرفية منظمة:** بحيث يتم تخزين المعلومات بشـــكل فعال، حيث يتمكن العاملون في المؤسسة من الحصول على المعرفة، وتعلم القواعد التجريبية

* **خزان المعلومات والمعرفة المرتبطة بالذكاء الاصطناعي:** حيث يمكن المؤسسة من حماية المعرفة الخاصة بها من التسرب والضياع.

* **إنشـاء آلية لا تكون خاضـعة للمشـاعر البشـرية:** خاصـة عندما يتعلق الأمر بالأعمال المرهقة ذهنيا.

* **توليد إيجاد الحلول للمشاكل المعقدة:** وتحليل هذه المشاكل ومعالجتها بشكل فعال. [4]

الفرع الثالث: التمييز بين الذكاء الاصطناعي وما يشابهه

الذكاء الاصـــطناعي كعلم واســـع الانتشـــار، فإنه كثيرا ما يتشـــابك ويختلط مع غيره من المصـطلحات والعلوم، لذا سـنقوم بتمييز الذكاء الاصـطناعي عما يشـابهه من مصـطلحات لإزالة أي لبس:

---

[1] **smart cities**: هي المدينة الذكية، حضرية حديثة، هيئة تستخدم أنواعا مختلفة من الأساليب الإلكترونية ، وطرق تنشيط الصوت وأجهزة الاستشعار (انظر تطبيق copilot على الموقع) https://copilot.microsoft.com

[2] **traphic pattenrn**: المسار القياسي الذي يشبه الطائرات عند الإقلاع والهبوط (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org)

[3] رؤى حسن الدين هاني قطيشات، مرجع سابق ص 5

[4] بلكحل راضية، الذكاء الاصطناعي ودوره في تطوير الإدارة الإلكترونية، مذكرة ماستر، تخصص إدارة أعمال، جامعة أحمد دراية، أدرار، 2022/2021، ص7.

أولا: التمييز بين الذكاء الاصطناعي والذكاء البشري

عند اكتشاف الإنسان وتطويره لأنظمة الكمبيوتر، دفعه الفضول إلى التساؤل هل يمكن للآلة التفكير والتصرف مثل البشر لذا طور الذكاء الاصطناعي بهدف إنشاء ذكاء مشابه للذكاء البشري

– **تعريف الذكاء البشري:** هو قدرة الإنسان على استنباط حقائق جديدة والوصول لحلول مبتكرة لمسائل معقدة، عن طريق المعلومات والخبرات الكامنة لديه التي اكتسبها من خلال التعلم والتجربة، بالإضافة إلى القدرة الذهنية التي يتمتع بها مكننا أن نبين ذلك في الجدول التالي: [1]

جدول رقم 01: الفرق بين الذكاء البشري والذكاء الاصطناعي

الذكاء البشري	الذكاء الاصطناعي
خلق بالذكاء الإلهي	من صنع الذكاء البشري
قد يكون ذاتيا	موضوعي للغاية
ربما أقل دقة	أكثر دقة
يمكنه التكيف مع التغييرات بشكل جيد	لا يمكنه التكيف مع التغييرات بشكل جيد
يمكنه بسهولة تعدد المهام	لا يمكن أن تعدد المهام بشكل جيد
مهارات اجتماعية ممتازة	المهارات الاجتماعية أقل من متوسط
الوعي الذاتي الجيد	مازال يعمل من أجل الوعي الذاتي

المصدر: بوقجار إسمهان، بن قاجة نور الهدى، التكريس القانوني والتنظيمي للذكاء الاصطناعي في الجزائر، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2023، ص21.

[1] بوقجار إسمهان، بن قاجة نور الهدى، التكريس القانوني والتنظيمي للذكاء الاصطناعي في الجزائر، مذكرة مقدمة لإستكمال متطلبات شهادة ماستر أكاديمي، تخصص قانون الإعلام الآلي والإنترنيت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022–2023، ص 20–21.

انطلاقا من الجدول نلاحظ أهم الفروقات التي تميز الذكاء الاصـــطناعي عن الذكاء الإنساني تتمثل في:

– يـدرك البشـــر من خلال الأنمـاط بينمـا تـدرك الآلات من خلال مجموعـة من القواعـد والبيانات.

– الإنســان قادر على اسـتخدام عدة عمليات ذهنية، كالتفكير والاسـتنتاج والابتكار في حين اقتصـــار برمجيات الذكاء الاصـــطناعي على اســـتنتاجات محدودة، طبقا لبديهيات وقوانين متعارفة على أن يتم برمجتها في الذكاء الاصـــطناعي من قبل البشـــر الباحثين في الذكاء الاصطناعي والقائمين على تطويره.[1]

– إمكانية توثيق الذكاء الاصـطناعي، وتوثيق قرارات الحاسـوب بسـهولة عن طريق متابعة نشاطات ذلك النظام أما في الذكاء البشري فصعب.

– جمود الذكاء الاصطناعي عكس الذكاء الإنساني الخلاق.

– ديمومة الذكاء الاصطناعي على عكس الذكاء الطبيعي الأكثر قابلية للتلف.

– يمكن للبشـــر معرفة الكائن بالكامل حتى لو كان جزء منه مفقودا أو مشـــوها في حين أن الآلة لا تستطيع بشكل صحيح.

– الفارق الآخر متصـل بالنطاق حيث يعد الذكاء البشري شـاملا ومطلقا في جميع المواقف، بخلاف ذكاء الآلة الذي يوصـف بأنه خاص، نسـبي أي مقصـور على مهمة معينة أو مجال معين، فهو بعبارة مختصـرة ذكاء محدود النطاق أو الأهداف، ولم نصـل بعد إلى حد الحديث عن ذكاء اصطناعي عام. [2]

[1] غادة المنجم وأخرون، الذكاء الاصطناعي، بحث مقدم في مادة نظم مساندة القرارات، كلية العلوم الإدارية، فجامعة الملك سعود، الرياض ،2009 ص 9

[2] بوقجار إسمهان، بن قاجة نور الهدى، مرجع سابق، ص 22.

جدول رقم 02: الفرق في الخصائص بين الذكاء البشري والذكاء الاصطناعي

الخاصية	الذكاء الإنساني	الذكاء الاصطناعي
الحصول على حجم كبير من المعلومات الخارجية	مرتفعة	منخفضة
القدرة على أن تكون خلاقا وتخيليا	مرتفعة	منخفضة
القدرة على التعلم من الخبرة	مرتفعة	منخفضة
التسامح	مرتفعة	منخفضة
إعداد عمليات حسابية معقدة	منخفضة	مرتفعة
استخدام مصادر مختلفة للمعلومات	مرتفعة	منخفضة
التكيف	مرتفعة	منخفضة
القدرة على تحمل تكلفة اكتساب الذكاء	مرتفعة	منخفضة
القدرة على نقل المعلومات	منخفضة	مرتفعة
القدرة على استخدام الحواس	مرتفعة	منخفضة

المصدر: نبيل محمد مرسي، نظم المعلومات الإدارية، دور دار النشر، جامعة الإسكندرية 2006ص368

إذن وحسب الجدول نجد أن:

– البشـــر أفضـــل من الآلة من ناحية: القدرات الإدراكية، المرونة، القدرة على الارتجال التحفيز، الحكم.

– أما عن الآلة فهي أفضـــل من البشـــر في: النزعة والقوة، اليقظة، الاســـتشـــعار، العمل الروتيني، الحساب، التخزين والأنشطة المتزامنة. [1]

[1] دداش حسين، شيحي هشام، دور الذكاء الاصطناعي في تحسين أداء المؤسسة الاقتصادية، مذكرة ماستر في علوم التسيير، تخصص إدارة أعمال، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2021-2022، ص 28.

ثانيا: تمييز الذكاء الاصطناعي عن الأتمتة

مصـطلح الأتمتة قريب جدا من الذكاء الاصـطناعي لدرجة الخلط بينهما، فالأتمتة تعمل من خلالها الآلة وفق مصـــفوفة فكرية وبيانات ومعلومات يضـــعها المبرمج وتكون تحت سيطرته بالكامل، أما الذكاء الاصطناعي فيقصد به معنى أوسع من مجرد مهام أتمتة عامة أي أن تطبيقاته تجمعها كلها سـمة مشـتركة(تجمع البيانات وتحللها وتصـنفها بنفسـها لتتخذ القرار) حيث أن أهم ما يميز الذكاء الاصـــطناعي هو محاكاة الأنشـــطة الإدراكية رفيعة المستوى المرتبطة بالذكاء البشـري، مما يجعل من قراراته لا يمكن التنبؤ بها، ومن هنا يمكن استخلاص أهم نقاط التباين بين المصطلحين:

1- الذكاء الاصـــطناعي يتخذ قرارا غير معلوم ويعمل وفق مجموعة من القواعد تتيح له التصـــرف بأكثر الطرق عقلانية، أما في الأتمتة فإن الآلة تقوم بعملية "مقاســـة" ومحددة ومتوقعة وفق برنامج معد مسبقا.

2-الذكاء الاصطناعي يتميز بالإستقلالية التامة، أما الأتمتة فهي ما تزال تابعة للإنسان.

3- الهدف من الذكاء الاصطناعي هو إنشاء آلات لتنفيذ المهام التي تتطلب تفكيرا ذكيا مثل البشر، أما الأتمتة فهي هندسة وعلم صنع أجهزة تحاكي الذكاء البشري

أما عن التشابه بين كل من الأتمتة والذكاء الاصطناعي فيشتركان في عنصر البيانات حيث تقوم الأجهزة الآلية بجمع البيانات لتفهمها أنظمة الذكاء الاصطناعي ولو تم الجمع بين الذكاء الاصـطناعي والأتمتة فسـينتج برنامج لا يتطلب أي تدخل بشـري وبدقة عالية وامتثال قانوني للعملية المطلوبة منه. [1]

[1] مصطفى أبو مندور موسى عيسى، مدى كفاية القواعد العامة للمسؤولية المدنية في تعويض أضرار الذكاء الاصطناعي دراسة تحليلية تأصيلية مقارنة، مجلة حقوق دمياط للدراسات القانونية والاقتصادية، كلية الحقوق، جامعة دمياط، مصر، يناير 2022، العدد 5، ص 239 إلى 249.

ثالثا: تمييز الذكاء الاصطناعي عن الروبوت

يوجد نوع من التداخل فيما يخص مصطلحات الذكاء الاصطناعي والروبوتات، فهما مجالان منفصلان للتكنولوجيا والهندسة، ومع ذلك عند الدمج تحصل على روبوت ذكي اصطناعي حيث يعمل الذكاء الاصطناعي كعقل وتعمل الروبوتات كجسم لتمكين الروبوتات من المشي والرؤية والتحدث والشم وغير ذلك. [1]

فالروبوت هو جهاز ميكانيكي متطور قابل للبرمجة، يتميز بالقدرة على التفاعل مع البيئة الخارجية ، يستخدم الروبوت في المهام التي تتطلب تحريك الأشياء أو تنفيذ أعمال محددة.

أما الذكاء الاصطناعي هو قدرة الأنظمة الكمبيوترية على تعلم البيانات، وتحليلها واتخاذ قرارات الذكاء المشابهة للبشر، يستخدم الذكاء الاصطناعي في مجموعة متنوعة من التطبيقات مثل: التجارة الإلكترونية، الطب، والتحكم في الروبوتات.

وبالتالي يمكننا تلخيص الفرق بين الروبوت والذكاء الاصطناعي، بأن الروبوت هو جهاز ميكانيكي برمجي قادر على الحركة والتفاعل، بينما الذكاء الاصطناعي هو قدرة الأنظمة الكمبيوترية على تعلم البيانات واتخاذ قرارات ذكية.[2]

كما أن الروبوتات تتضمن تصميم وبناء واستخدام الآلات لأداء مهام معينة يقوم بها البشر، أما الذكاء الاصطناعي فيشير إلى قدرة الحاسوب أو الآلة الرقمية على تمكينه من أداء المهام والوظائف التي يؤديها على الكائنات الحية. [3]

---

[1] الفرق بين تقنية الذكاء الاصطناعي والروبوتات.: https://www.youm7.com
تاريخ الاطلاع: 2024/04/29، ساعة 13:00 AM

[2] ما هو الفرق بين الروبوت والذكاء الاصطناعي:https://bawabaai.com
تاريخ الإطلاع: 2024/04/29، ساعة 14:00

[3] هل هناك فرق بين الروبوتات والذكاء الاصطناعي:https://whatsbot.me
تاريخ الإطلاع: 2024/04/29، ساعة 14:30

فالذكاء الاصـــطناعي هو عقل الآلة وهو من يوجهها وعلى الرغم من أن الروبوتات تستخدم تطبيقات الذكاء الاصطناعي لتنفيذ بعض المهام، لكن الروبوتات بطبيعتها لا تتمتع بالذكاء الاصطناعي، حتى أن هناك بعض الروبوتات التي لا تستخدم أي مكون من مكونات الذكاء الاصطناعي مثل الصرفات الآلية.

في الأخير يبقى القول أن فهم الفرق بين الروبوت والذكاء الاصـــطناعي يســـاعدنا في اســتخدام هذه التكنولوجيات بشــكل أفضــل، وفهم أعمق لإمكاناتها وقدراتها، فهو يمكننا من اتخاذ القرارات السليمة بشأن الاستثمار في هذه التقنيات، وتوجيه الأبحاث والتطورات في هذا المجال. [1]

المطلب الثاني:

تقييم الذكاء الاصطناعي

الذكاء الاصطناعي مجال علمي خاضع للتطور المستمر، لذا نجده مرنا وتتغير وتيرته مما يجعل أنواعه واستخداماته تختلف استنادا إلى القدراته، وهذا ما سنتطرق له خلال مطلبنا إضافة إلى الأخطار التي تنشأ عن جراء استخدام الذكاء الاصطناعي.

الفرع الأول: أنواع الذكاء الاصطناعي

يمكن تقســـيم أنواع الذكاء الاصـــطناعي إلى ثلاث أنواع رئيســـية، تتراوح من رد الفعل البسيط إلى الإدراك والتفاعل الذاتي وذلك على النحو التالي:

- **الذكاء الاصطناعي الضيق أو الضعيف (Narrow AI or weak AI)**

يبرمج الذكاء الاصـــطناعي للقيام بوظائف معينة في بيئة محددة، وهو أبســـط أشـــكال الذكاء الاصطناعي ويعتبر تصرفه بمرتبة رد فعل على موقف محدد ولا يمكنه العمل سوى في البيئة المناسبة والخاصة به.

---

[1] الفرق بين تخصص الذكاء الاصطناعي وتخصص الروبوتات:https://ar.quora.com .
تاريخ الإطلاع: 2024/04/29، ساعة 14:30،

مثال: "ديب بلو"[1] الذي صـــنعته شـــركة (IBM) والذي هزم جاري كاســـباروف بطل الشطرنج العالمي.[2]

– الذكاء الاصطناعي القوي أو العام (General AI or Strong AI)

يتميز بالقدرة على التعامل مع مجموعة واسعة من المهام والمواقف بشكل ذكي، والقدرة على جمع المعلومات وتحليلها، وعمل تراكم خبرات من المواقف التي يكســـبها وهذا ما يؤهله إلى اتخاذ قرارات صحيحة مستقلة وذاتية.

مثال: مساعدات الذكاء الاصطناعي الشخصية مثل "Siri" من أبل و"Alexa" من أمازون.[3]

– الذكاء الاصطناعي الخارق (Super AI)

يسعى هذا النوع لمحاكاة عقل الإنسان، ولكنه لا يزال قيد التجربة وينقسم إلى نمطين:

النمط الأول: يملك قدرة محدودة على التفاعل الاجتماعي، ويحاول فهم الأفكار البشـــرية إضافة إلى الانفعالات المؤثرة على سلوك الإنسان.

---

[1] **ديب بلو Deep Blue**: كمبيوتر صممته شركة IBM تغلب على بطل العالم في شطرنج، أندارك غاري كاسباروف في مباراة تاريخية عام 1997، وتم تصميمه خصيصا للعب الشطرنج واستخدام تقنيات الذكاء الاصطناعي، والحسابات الضخمة لتحليل المواقف واتخاذ القرارات(انظر تطبيق copilot على الموقع https://copilot.microsoft.com)

انظر ملحق (6) ص99

[2] إيهاب خليفة، الذكاء الاصطناعي تأثيرات تزايد دور التقنيات الذكية في الحياة اليومية للبشر، العدد 20، مجلة إتجاهات الأحداث، أبو ظبي مارس – أفريل2017، ص 63.

[3] جيلالي سارة، تركي سميرة، برازوم عبد القادر، "تطبيقات الذكاء الاصطناعي في إدارة المكتبات الجامعية"، مذكرة ماستر، كلية العلوم الإنسانية والاجتماعية، جامعة ابن خلدون، تيارت، 2022، ص 22.

النمط الثاني: يهدف إلى فهم مشـــاعر الآخرين ومواقفهم وفق نموذج نظرية العقل، وكذا التفاعل معهم وهذا ما يعتبر الجيل المقبل من الآلات فائقة الذكاء[1].

كما يمكن تقسيم الذكاء الاصطناعي إلى نوعين، من حيث المهام والوظائف كما يلي:

النوع الأول: وظائف حياتية ذكية، وتعني جُل المهام التي تقوم بها بشـــكل دوري لتفاعل مع العالم وتتضمن:

* الرؤية وفهم ما نراه.

* اللغة الطبيعية.

* التخطيط والحركة.

النوع الثاني: يتمثل في الوظائف الخبيرة المهام التي تتطلب تدريبا شـــاملا في حالة وجود نقص في الخبراء مثل: **التشخيص الطبي.** [2]

الفرع الثاني: تطبيقات الذكاء الاصطناعي

من غير الممكن دراســـة كل مجالات تطبيق الذكاء الاصـــطناعي في بنية الأعمال الإلكترونية على الوجه الخاص، ولكن يمكن دراســـة أهم المنظومات في مجال الذكاء الاصـــطناعي، التي تســـتخدم في دعم القرارات الإدارية من خلال نوع الإســـناد الذي تقدمه لصناع القرار ومستوى القرار الذي يناسبه، وكذا طبيعة المجال التطبيقي الذي يسانده.

---

[1] **الألات فائقة الذكاء:** يشير الى الذكاء الفائق، أي انه لم يتم تحقيقه بعد وهو الذي يتجاوز قدرة الذكاء البشري **(**انظر تطبيق copilot على الموقع https://copilot.microsoft.com**)**

[2] عبد الرازق مختار محمود، تطبيقات الذكاء الاصطناعي: مدخل لتطوير التعليم في ظل تحديات جائحة فيروس كورونا، المجلة الدولية للبحوث في العلوم التنموية، المجلد 03، العدد 04، جامعة أسيوط، مصر، 15-08-2020، ص 192.

1- الشبكات العصبية: شهدت الشبكات العصبية تطورات هائلة منذ نشأتها في الأربعينيات من القرن المنصرم إلى أن وصلت لما هي علي اليوم.

وهي النظم مصممة لمحاكاة عقل الإنسان في القيام بمهمة معينة بنفس العمق، ويعتبر معالج ضخم موزع على التوازي ومكون من وحدات معالجة بسيطة، وتعتبر عناصر حسابية يطلق عليها مصطلح العصبونات[1]، أو عقد ذات خاصية عصبونية حيث تقوم بتخزين المعرفة العملية والمعلومات التجريبية لتجعلها متاحة للمستخدم، وذلك عن طريق ضبط الأوزان[2]. [3]

2- الرجل الآلي أو الإنسان الآلي: هو الجهاز أو الآلة الكهروميكانكية[4]، تقوم بتلقي التعليمات أو الأوامر من حاسوب تابع لها ليقوم بأداء أعمال ووظائف معينة، فالإنسان الآلي أو الروبوتات يتم عادة إعطاءه القدرة على التحرك والتعامل مع محيطه بواسطة التفهم ومن ثم الاستجابة إلى عدد من العوامل الخارجية والقيام بوظائف محددة.

فالإنسان الآلي يلقن باتجاه القيام بوظائف محددة مكررة، ويستخدم طريقة التحسس المشابه لطريقة تحسس الإنسان الحقيقي بالنسبة إلى اللمس والنظر والسمع ،وتستخدم بعض من الروبوتات في مجالات قد تكون خطرة أو مملة ومتعبة بالنسبة للإنسان الحقيقي كالحراسة، والأمن في مستودعات البضائع، والمواد والإنسان الآلي يغذى بخارطة للموقع

---

[1] **العصبونات:** الوحدات الأساسية في الجهاز العصبي للكائنات الحية (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org) **انظر الملحق (7) ص 100**

[2] **ضبط الأوزان:** ضبط معاملات أو وزن الاتصالات بين العناصر داخل نموذج معين باستخدام خوارزميات(انظر تطبيق copilot على الموقع) https://copilot.microsoft.com

[3] جيدة سعاد، كادي سليمة، "استخدامات تطبيقات الذكاء الاصطناعي في تحسين عملية اتخاذ القرار في المؤسسة الاقتصادية"، مذكرة لاستكمال شهادة ماستر العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة أحمد دراية، أدرار، 2020، ص 13.

[4] **الكهروميكانيكية:** دراسة التفاعلات بين الحركة الميكانيكية، والتأثيرات الكهربائية في سياق العصبونات (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org)

الذي يقوم بحراسته ويقوم بالإصغاء للأصوات غير الطبيعية وغير المألوفة، وكذلك يراقب أي من الدخلاء غير المرغوب بوجودهم أو الحرائق التي قد تحدث

وإذا ما وجد الروبوت[1] مثل هذه الأشياء فإنه يجري اتصال وتحذير للجهات المسؤولة، وباستطاعة الروبوت أو الإنسان الآلي التقاط النفايات والعلب من البناية، لكي يؤدي عمله على أحسن وجه. [2]

- **العميل الذكي:** ظهرت فكرة العميل الذكي في منتصف الخمسينات في معهد (massachustts) [3] لالتكنولوجيا، وعلى الرغم من أن الفكرة تعود للستينات فلم يتفق الباحثون في الذكاء الاصطناعي حتى الآن على تعريف مشترك له، بل حتى تسميته لم تستقر على مصطلح واحد.

عرفته باتي ماس"[4]نظام حاسوبي يسكن بيئة ديناميكية معقدة، يستشعر ويعمل بشكل مستقل من خلال هذا العمل مجموعة من الأهداف والمهمات التي صمم لأجلها. [5]

- **النظم الخبيرة:** نظام يعتمد على تحديد مهمة من خلال استخدام الحاسب الآلي في محاكاة المعلومات، وكذا القرارات للمختصين في مجالات محددة وذو خبرة عالية ،وكذا برمجة

---

[1] **الروبوتات:** أجهزة آلية مصممة لتنفيذ مجموعة من المهام بشكل(نظر موقع ويكيبيديا الموسوعة الحرة (https://fr.wikepid.org

[2] غسان العمري، عبد الساتر العلي، عامر القنديلجي، المدخل إلى إدارة المعرفة، دار المسيرة للنشر والتوزيع، طبعة 2، عمان، الأردن، 2009، ص203.

[3] **معهد ماساتشوستس MIT:** معهد بحثي، وجامعة خاصة تقع في كامبريدج، ويعتبر أهم وأبرز معاهد التكنولوجية(انظر تطبيق copilot على الموقع) https://copilot.microsoft.com

[4] **باتي ماس:** عالمة حاسوب وأستاذة في معهد ماساتشوستس للتكنولوجيا، تعمل في مجالات الذكاء الاصطناعي ووسائل التواصل البشرية والحوسبة التقنية (انظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org)

[5] Pattie maes, Softwar agents tutorial.available at. http://www.mediamit.edu/pattie.1997 الإطلاع: 2024/05/13، 03:00

الخبراء لمعرفتهم داخل النظام والاســـتفادة منهم في هذا النظام الآلي، ويصـــل من خلاله المستخدم العادي إلى القرار السليم دون الرجوع إلى الخبير، ومن الأمثلة الشائعة للنظام نجد:

* **PXDES** نظام خبير في تحديد نوع ومستوى سرطان الرئة.

* **Cadet** نظام خبير يمكنه اكتشاف السرطان في مرحلة مبكرة جدا، كما أن لها عدة سمات أساسية:

- ✓ **المعرفة الذاتية:** تحدد قوة النظم الخبيرة المبينة في قاعدته، ومنها يستطيع هذا النظام الاستدلال المنطقي عن عملياته التي يقوم بها.
- ✓ **الخبرة:** قدرة النظام الخبير في تحقيق نفس المستوى الذي يحققه الخبير البشري، مع توفير السرعة والكفاءة العاليين.
- ✓ **العمق في المعالجة:** يأتي من واقع تحديد المشكلة تحديدا جيدا لحلها.
- ✓ **الاســـتنتاج المنطقي المرمز:** اختيار مجموعة من الرموز لتمثل المفاهيم لحل الإشكالية.[1]

– **معالجة اللغات الطبيعية:** تطوير نظم وبرامج لها القدرة على فهم اللغة البشرية، وينقسم إلى جزئيين رئيسيين:

* **فهم اللغات الطبيعية:** طرق تسمح للحاسب فهم لغة الإنسان.

* **إنتاج اللغات الطبيعية:** الطرق تسمح للحاسب بإنتاج لغة طبيعية.

– **التعرف على الكلام:** تبحث تطبيقات الذكاء الاصطناعي على طريقة تجعل الحاسب يفهم لغة الإنسان، ويتلقى الأوامر منه شفهيا حتى تقوم بتنفيذها. [2]

[1] بوقجار اسمهان، بن قاجة نور الهدى، مرجع سابق، ص 23.

[2] سعاد بوبحة، "الذكاء الاصطناعي: تطبيقات وانعكاسات"، مجلة اقتصاد المال والأعمال، المركز الجامعي عبد الحفيظ بوالصوف، المجلد 6، العدد 4، ديسمبر 2022، ص 98.

- **البرمجية الآلية:** اســـتخدام الخوارزميات والتقنيات لكتابة البرمجيات التي تمكن أنظمة الحاسـوب من تعلم اتخاذ القرارات تتضـمن الأسـاليب مثل تعلم الآلة والشـبكات العصـبية[1] الاصطناعية.

الفرع الثالث: مخاطر الذكاء الاصطناعي

1- العمل والتوظيف:

دعت رئيسـة صـندوق النقد الدولي "كريسـتالينا جورجيفا"[2] الحكومات إلى معالجة الاتجاه المثير للقلق، واتخاذ خطوات اســـتباقية لمنع التكنولوجيا من زيادة تأجج التوترات الاجتماعية حيث قالت نحن على شـــفا حفرة من ثورة تكنولوجية يمكنها تحفيز الإنتاجية، وتعزيز النمو العالمي، وزيادة الدخل في جميع أنحاء العالم، ومع ذلك يمكن أن تحل محل الوظائف وتعمق عدم المساواة. [3]

وجاء في تقرير وظائف المســـتقبل 2040 أنه من المتوقع اختفاء عدد من الوظائف الحالية مع ظهور الأتمتة، ودخول الروبوتات مجالات مختلفة كما أكد كذلك أنه في المقابل سيكون هناك أكثر من 157 وظيفة شاغرة حتى عام 2040 وفقا لدراسة المعهد "ماكينزي"[4]

---

[1] **الشبكات العصبية الاصطناعية:** نماذج جوسسة مستوحاة من الجهاز العصبي للكائنات الحية، تتألف من مجموعة من الوحدات المعروفة بالعصبونات. (نظر تطبيق copilot على الموقع https://copilot.microsoft.com).

[2] **كريستينا جورجيفا:** سياسية بلغارية، والمدير العام لصندوق النقد الدولي منذ 1 أكتوبر 2019، أول مديرة من الاقتصادات ناشئة تشغل هذا المنصب، شغلت منصب الرئيس التنفيذي للبنك (انظر تطبيق copilot على الموقع https://copilot.microsoft.com

[3] تحذير هام الذكاء الاصطناعي يهدد الوظائف في جميع أنحاء العالم https://arabic.rt.com
تاريخ الإطلاع: 13-05-2024، 12:22

[4] **ماكينزيMcKinsey** : معهد أمريكي يقوم بإجراء تحليل نوعي وكمي ،لتقييم قرارات الإدارة عبر القطاعين العام والخاص وتنشر منذ 1964 (أنظر موقع ويكيبيديا الموسوعة الحرةhttps://fr.wikepid.org)

العالمي، ويتوقع أن يفقد أكثر من 800 مليون موظف حول العالم وظائفهم وهو ما تعادل خمس القوى العاملة. [1]

2- الأمن القومي:

في دراسة أجراها الباحثون في جامعة "هارفارد كيندي سكول" الأمريكية عام 2017 تحت عنوان "الذكاء الاصطناعي والأمن القومي" جاء في نتائجها أنه من المحتمل أن يصبح التقدم المستقبلي في الذكاء الاصطناعي تقنية تحويلية[2] للأمن القومي، مثلها مثل الأسلحة النووية والطائرات وأجهزة الحاسوب والتكنولوجيا الحيوية.

وفي تقرير نهائي للجنة الأمن القومي للذكاء الاصطناعي الأمريكية، والذي صدر مع مطلع عام 2021 جاء فيه أن تقنيات الذكاء الاصطناعي تؤدي إلى تفاقم تحديين الحاليين للأمن القومي.[3]

أ- تأثيره على أمن المعلومات: تتعدد مخاطر وتهديدات الذكاء الاصطناعي للدول، وإذ يزيد من انتشار المعلومات المضللة قد يولد معلومات خاطئة، من شأنها أن تزعزع استقرار الدولة ويثير الذكاء الاصطناعي التوليد في مخاوف من الزيادة المحتويات الزائفة عبر الانترنيت، ما يدفع صناع القرار في مجال الأمن القومي إلى اتخاذ إجراءات، فعلية بناء على معلومات خاطئة مما يؤدى إلى أزمات أو أسوء من ذلك اتخاذ قرار الحرب.

---

[1] مجدي نارمين، الذكاء الاصطناعي وتعلم الآلة، الإمارات، صندوق النقد العربي، (2022)، ص 22.

[2] **التقنيات التحويلية:** تكنولوجيات الحديثة الرقمية المعتمدة على الشبكات، وخاصة شبكة الانترنيت مثل انترنيت الأشياء(انظر تطبيق copilot على الموقع)https://copilot.microsoft.com

[3] Greg, Allen, Tanial, Chan (2017) Artificial Intelligence and national Security. USA. Harvard University. Retrieved form: https://www.belfencenter.org/
on 13-05-2024 at 5:48 AM P.1

ب- تأثيره على الأمن السيبراني: يمكن من خلال استغلال بعض العيوب أو الثغرات في أنظمة الذكاء الاصطناعي شن الهجومات الالكترونية، تؤدي إلى تعطيل البنية التحتية الحيوية[1] للدول المتقدمة، أو سرقة البيانات الحساسة لها في 11 يونيو 2023 تكون العمليات السيبرانية المعتمدة على الذكاء الاصطناعي أكثر عدوانية مستقبلا، واستهدافا وفعالية بشكل ملحوظ سواء، في هجمات الحرمان من الخدمات والبرمجيات الخبيثة[2] أو البرمجيات الفدية[3] أو التصييد الاحتيالي،

بالإضافة إلى التسلح بالذكاء الاصطناعي.[4]

3_الأسلحة الفتاكة ذاتية التشغيل: يتمثل أحد أهم تطبيقات الذكاء الاصطناعي العسكرية في ظهور الأسلحة ذاتية التشغيل (autonomous wenpon System) والتي تعرف بأنها أي نظام تسليحي يتمتع بالاستقلالية في القيام بوظائفه الحيوية، أي أنه يستطيع اتخاذ القرارات التي تتعلق بالقيام بالبحث والرصد وتحديد وتعقب واختيار ومهاجمة الأهداف من دون تدخل البشر.

وتستطيع الأسلحة ذاتية التشغيل التي تعرف أيضا باسم الروبوتات المستقبلة الفتاكة أو الروبوتات القاتلة "البحث عن الأهداف وتحديدها ومهاجمتها، بما في ذلك البشر من دون تدخل من أي إنسان في توجيهها ويؤكد البرلمان الأوروبي في أحد تقاريره حول مخاطر

---

[1] **البنية التحتية الحيوية:** الأصول والنظم والشبكات، سواء مادية أو اعتبارية وهي حيوية جدا لأي دولة، حيث تدميرها أو عجزها يوثر على الأمن والاقتصاد القومي(انظر تطبيق copilot على الموقع https://copilot.microsoft.com)

[2] **البرمجيات الخبيثة:** برامج تم تصميمها لتسبيب الضرر عمدا لانظمة الكمبيوتر، او المستخدمين مثل الفيروسات (انظر تطبيق copilot على الموقع https://copilot.microsoft.com)

[3] **برمجيات الفدية:** فيروس يعمل على حجب الوصول الى النظام، او يقوم بتشفير البيانات الموجودة يطلب المجرمين الالكترونيون مبلغا فدية من ضحاياهم مقابل فك التشفير(أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org).

[4] "الأمن القومي وتأثير الذكاء الاصطناعي على الأمن القومي. https://www.europavabet.com تاريخ الاطلاع 09/05/2024 الساعة 12:13 PM

الذكاء الاصطناعي على السلامة والأمن بأن "الاستخدام السيئ لتنظيم الذكاء الاصطناعي في مجال الأسلحة، يمكن أن يؤدي إلى فقدان السيطرة البشرية على الأسلحة الخطيرة. [1]

المبحث الثاني:

آليات الذكاء الاصطناعي في حماية أمن المعلومات وتحدياته

الذكاء الاصطناعي يلعب دورا حيويا وحاسما في تعزيز أمان المعلومات والسبرانية لحمايتها من الاختراقات والأخطار التي تهددها، لذلك وتم إدراج الذكاء الاصطناعي في مجال الأمن السيبراني لضمان حماية عالية للمعلومات والبيانات، من خلال جملة من الاستخدامات التي تساهم بشكل ملحوظ في تطوير وتعزيز هذا المجال، ووجب ضبط وتكريس أخلاقيات لاستعمال الذكاء الاصطناعي ذلك عائد الى جدة الموضوع.

تعتبر أحد التحديات التي واجهتنا في هذا المجال نقص التشريعات القانونية، إلى جانب التحديات التقنية وهذا ما سنتطرق إليه في:

المطلب الأول: الذكاء الاصطناعي كألية لحفظ أمن المعلومات.

المطلب الثاني: تحديات الذكاء الاصطناعي.

المطلب الأول:

آليات وأخلاقيات الذكاء الاصطناعي في حفظ أمن المعلومات

في حين ان أدوات الذكاء الاصطناعي تقدم تشكيلة من الوظائف جديدة، فإن استخدامه يثير مسائل أخلاقية، حيث يمكن إدراجه في أمور غير أخلاقية او غير قانونية، حيث أنه

[1] الأسد صالح الأسود، الذكاء الاصطناعي الفرص والمخاطر والواقع في الدول العربية، مجلة إضافات اقتصادية، المركز الجامعي تيبازة الجزائر مجلد 07 العدد01 2023 ص178.

مهما كانت الألة ستنوب عن الإنسان في القيام بهذه الوظائف، إلا أنها تظل محصورة في ذكاء البيانات التي يتم تقديمها في التدريب، وبما أن الإنسان من يختار طبيعة هذه البيانات فان هناك احتمال كبير لتحيز التعلم الألي، وهو ما يلزم وضع أخلاقيات لهذا الذكاء الاصطناعي، تبرز أهمية الذكاء الاصطناعي في تحقيق الأمن السيبراني والحفاظ على البيانات والمعلومات المعرضة للاختراق .

الفرع الأول: أخلاقيات الذكاء الاصطناعي

الذكاء الاصطناعي هو الحدود الجديدة للإنسانية بمجرد عبور هذه الحدود سيؤدي الذكاء الاصطناعي إلى شكل جديد من الحضارة الإنسانية.

المبدأ التوجيهي للذكاء الاصطناعي ليس باستقلاليته، ولا بكونه يحل محل الذكاء البشري، ولكن يجب ضمان حقوق الإنسان وقيمه خلال تطويره، كما يجب على العالم أن يضمن استخدامات التكنولوجيات الجديدة لصالح مجتمعاتنا وتنميتها المستدامة[1].

ولقد دعت العديد من الجهات الفعالة إلى الإطار الأخلاقي لتطوير الذكاء الاصطناعي.[2]

من بين الاقتراحات المقدمة من قبل الدراسات والبحوث في الميدان، كمبادئ للاستخدام الأخلاقي للذكاء الاصطناعي ما يلي:

- **عدالة أنظمة الذكاء الاصطناعي:** يجب أن تجنب الخوارزميات التحيز، بالإضافة إلى وجوب تمثيل الفئة المتأثرة قدر الإمكان من قبل البيانات التي يتلقاها نظام الذكاء

[1] **التنمية المستدامة:** تأخذ بعين الاعتبار الأبعاد الاجتماعية والبيئية، إلى جانب الأبعاد الاقتصادية لحسن استغلال الموارد المتاحة لتلبية حاجيات الأفراد، مع الاحتفاظ بحق الأجيال(أنظر موقع ويكيبيديا الموسوعة الحرة (https://fr.wikepid.org)

[2] نحو أخلاقيات الذكاء الاصطناعي للأمم المتحدة https://www.un.org.
تاريخ الإطلاع: 3:19AM، 10 mai 2024.

الاصـــطناعي، وكذلك اتخاذ القرارات والإجراءات التي تســـمح بالحد أو تقيم إلى انحياز من البنيات وإثبات عدالتها.

– **شفافية أنظمة الذكاء الاصطناعي:** اعتماد على شفافية البيانات، والخوارزميات[1] المتاحة في الأنظمة في حدود الخصوصية وحماية الملكية الفكرية. [2]

– **خصوصية وأمن الذكاء الاصطناعي:** يتم تطوير أنظمة الذكاء الاصطناعي لتكون محمية بطريقة آمنة، وتراعي المتطلبات النظامية ذات العلاقة، ومن ذلك المتطلبات النظامية المتعلقة بحماية خصوصية أصحاب البيانات الشخصية[3]، ومعايير الأمن السيبراني بهدف منع الوصول الغير مشروع.

– **المساءلة والمسؤولية:** يحمل مبدأ المساءلة والمسؤولية المصممين والمطورين ومسؤولي ومقيمي أنظمة الذكاء الاصـــطناعي، المســـؤولية الأخلاقية من القرارات والإجراءات التي قد تؤدي إلى مخاطر المحتملة وآثار ســـلبية على الأفراد والمجمعات، ويجب تطبيق الإشـــراف البشري والحكومة والإدارة المناسبة عبر دورة حياة نظام الذكاء الاصطناعي، لضمان وجود آليات مناسبة لتجنب إساءة استخدام هذه التقنية. [4]

– **أنظمة قابلة للشـــرح تقنيا:** إجبارية شـــرح المفهوم للقرارات والمنهجيات التي تقوم عليها أنظمة الذكاء الاصطناعي، للمجتمع وفقا لما تسمح به التكنولوجيا المتوفرة.

---

[1] **الخوارزميات:** مجموعة الخطوات الرياضية والمنطقية والمتسلسلة، اللازمة لحل مسألة ما(انظر تطبيق copilot على الموقع) https://copilot.microsoft.com

[2] وسيلة سعود، "الذكاء الاصطناعي وتحديات الممارساتية الأخلاقية"، جامعة البويرة، الجزائر، مخبر السياسات التنموية والدراسات الإستشراقية، مجلة نماء للاقتصاد والتجارة، المجلد 07، العدد 02 ديسمبر 2023، ص 10

[3] **المتطلبات النظامية :** القوانين و اللوائح التي يجب على الأفراد و المؤسسات الإلتزام بها، و تختلف هذه المتطلبات بإختلاف القطاعات و النشاطات على سبيل المثال في مجال الأعمال التجارية على الشركات الالتزام بالتراخيص. (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org)

[4] مبادئ وأخلاقيات الذكاء الاصطناعي، الهيئة السعودية للبيانات والذكاء الاصطناعي. https://sdara.gov.sa تاريخ الاطلاع 10 mai 2024 03: 18 AM

- **الإنسانية في أنظمة الذكاء الاصطناعي:** تزويدها بالقيم الإنسانية حيث تجعلها أكثر إفادة للبشر عن طريق تمويل الأبحاث الخاصة[1] للاستخدامات المفيدة للذكاء الاصطناعي، مع تطويره وفقا على هذه القيم وعدم الخروج عنها. [2]

- **التعاون العالمي في مجال حوكمة الذكاء الاصطناعي:** قال بول دوجيرتي[3] كبير مسؤولي الابتكار التكنولوجي من شركة أكسنتشر[4]، يتميز الذكاء الاصطناعي بتسارع تطوره الكبير على مدى الوقف مما يجعل تعاون القطاعين الحكومي والخاص أولوية لتبادل الأفكار وأفضل الممارسات، لبناء أنظمة الذكاء الاصطناعي مسؤولية، وأخلاقية وتوسع نطاقه بشكل كبير. [5]

- **توعية المجتمع بمزايا ومنافع الذكاء الاصطناعي:** حيث يتم تنسيق تطوير أنظمة الذكاء الاصطناعي، عن طريق الاستجابة الانعكاسيه[6] على التوظيف مع استخداماتها في مساعدة البشر على معرفة ذاتهم وتوفير التدريب والفرص والأدوات للجميع، مع ضرورة تطوير التعليم بها، بتكيفها مع استخدامات الذكاء الاصطناعي وحسب المتغيرات المجتمعية.

---

[1] **تمويل الأبحاث الخاصة:** الدعم المادي الذي تتلقاه الشركات الناشئة من مصادر الغير الحكومة، ويمكن أن يوفر العديد من الفوائد لهذه الشركات مثل المرونة في شروط التمويل . (أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org)

[2] وسيله سعود، "الذكاء الاصطناعي وتحديات الممارسة الأخلاقية، مرجع سابق، ص 10.

[3] **بول دوجيرتي:** فيلسوف وعالم إجتماع فرنسي شهير، يعتبر أحد أبرز الفلاسفة في القرن العشرين وترك بصمة كبيرة في الفلسفة الحديثة والنقد الاجتماعي(أنظر موقع ويكيبيديا الموسوعة الحرة https://fr.wikepid.org)

[4] **شركة أكسنتشر(Accenture)** : شركة عالمية للخدمات الاستشارية الإدارية والتكنولوجية ،والتحول الرقمي والحلول الذكية والخدمات مالية وصناعية (انظر تطبيق copilot على الموقع) https://copilot.microsoft.com.

[5] حوكمة الذكاء الاصطناعي مركز الاتحاد للأخبار https://www.alet.had.de
تاريخ الاطلاع 10:32 PM 15-05-2024،

[6] **الاستجابة الانعكاسية:** رد فعل فوري ينشأ عادة نتيجة لتحقير الخارجي، وهو عملية غير واعية تحدث دون تفكير مسبق. انظر تطبيق copilot على الموقع https://copilot.microsoft.com)

– **موافقة الأعراف والمعايير الدولية من قبل أنظمة الذكاء الاصطناعي:** خاصة ما يرتبط بالحقوق والقيم الإنسانية للأفراد، والسلوكات المقبولة مع ضرورة احتفاظ البشرية بقدرتها على التحكم بنفسها.[1]

الفرع الثاني: أليات الذكاء الاصطناعي لحماية أمن المعلومات السيبرانية

تعد السيبرانية تخصصا متعدد المخططات، فشمل مفهومها عدة مجالات منها أمن المعلومات والأمن السيبراني ... ، ويهدف كل هذا العمل المتعلق بالسيبرانية إلى توفير أنظمة معلومات آمنة والحفاظ على خصوصية البيانات وسلامتها، ويؤدي الذكاء الاصطناعي دورا هاما في مجال الأمن المعلوماتي، ويمتد لمجموعة واسعة للاستخدامات التي تخص الأمن. [2]

التعلم الآلي والتكييف: التعلم الآلي هو علم تطوير الخوارزميات التي تستخدمها أنظمة الحاسوب لأداء المهام بدون تعليمات واضحة، اعتمادا على أنماط والاستدلال بدلا من ذلك وتستخدم أنظمة الحاسوب لوغاريتمات[3] التعلم الآلي لمعالجة كميات كبيرة من البيانات السابقة، والتعرف على أنماط البيانات هذا ما يسمح لها بتوقع النتائج بصورة أدق،[4] أما فيما يخص التكيف فهو التكيف مع التهديدات المتغيرة.

التعامل مع كميات كبيرة من المعلومات: هناك الكثير من الأنشطة الجارية على خوادمنا[5] وهذا ما يعني أنه يتم نقل عدد هائل من البيانات والمعلومات بين عمالتنا ومنشأتها وبين

---

[1] وسيلة سعود، مرجع سابق، ص 11.

[2] الذكاء الاصطناعي وتحسين أمن المعلومات السيبرانية https://www.annajah.net

تاريخ الإطلاع: 15-05-2024 الساعة 05:48 PM

[3] **اللوغريتمات:** مجموعة التعليمات من التعليمات، أو القواعد تمكن الآلات من التعلم والتحليل البيانات واتخاذ القرارا

[3] ما المقصود بتعلم الآلة شرح (تعلم الآلة المؤسسي) https://www.amazon.com

تاريخ الإطلاع: 15-05-2024 الساعة 06:00 PM

[5]* **الخوادم:** جزء من الحاسوب يوفر برامج، أو وظائف لأجهزة أخرى تسمى "العملاء(انظر تطبيق copilot على الموقع https://copilot.microsoft.com).

أجهزتها وشـــبكاتها كل يوم، هذا يصـــعب علينا الكشـــف عن مخاطر محتملة، والذكاء الاصـطناعي صـار الخيار الأفضـل لاكتشـاف هذه التهديدات، بالإضـافة إلى فحص كمية كبيرة من البيانات حيث يمكنه مراقبة حركة المرور تلقائيا، بتحليل نشـاط الخادم بدقة وتحديد المخاطر المحتملة في حركة مرور المعلومات.[1]

توقع التهديدات المســـتقبلة: يمكن للذكاء الاصـــطناعي تحليل البيانات التاريخية، والتنبؤ بالتهديدات المحتملة والثغرات الأمنية المحتملة، ويمكنه أن يســـاعد على تحديد النقاط الضعيفة في الأنظمة وتوجيه الجهود لتعزيز الأمان وتقبل المخاطر. [2]

إن كمية البيانات التي تمر عبر محللي الأمن الســـيبراني، تجعل من الصـــعب التنبؤ بالتهديدات المستقبلة، لكن الذكاء الاصـطناعي يمكنه معالجة كميات كبيرة من البيانات في وقت واحد مما يتيح الكشف المبكر عن الأنشطة الضارة، ويمكن أن يؤدي تحديد الإجراءات الوقائية والتهديدات المحتملة إلى تقليل الوقت الضائع.

تقليل وقت اكتشـــاف التهديد: القدرة على اكتشـاف التهديدات بسـرعة أمر بالغ الأهمية حيث أبلغ 42% من المنظمات عن زيادة في التهديدات الحساسة للوقت والناس بطيؤون في تبنيها وهم دون المســـتوى الأمثل، ومن الناحية الأخرى يمكن للذكاء الاصـــطناعي فحص كميات كبيرة من البيانات في وقت واحد لاكتشـــاف التهديدات الســـيبرانية، وبالتالي تســـهيل الأمن وأفادت 23 في المائة منهم بأنهم غير قادرون على التحقيق بشكل فعال من التهديدات المحددة. [3]

[1] محمد دحماني، مرجع سابق، ص 604-605.

[2] مرجع سابق https://www.annajah.net

تاريخ الإطلاع: 15-05-2024 الساعة 05:00 PM

[3] محمد دحماني، مرجع سابق، ص 605.

الذكاء الاصـــطناعي يلعب دورا هاما في تقليل وقت اكتشـــاف التهديدات الإلكترونية يستخدم الذكاء الاصطناعي الأتمتة مهام للأمان. [1]

التوفير في التكاليف: تتأثر العديد من المؤسسات ماليا بإنتهاكات البيانات كل عام، ولا يمكننا تجاهلها ولا يمكننا إيقاف المجرمين حيث وجدت الدراسة فرقا بنسبة 80 % في توفير التكاليف للمنظمات التي تستخدم الذكاء الاصطناعي لأغراض الأمن السيبراني، وحفظ أمن المعلومات. 2.9 مليون دولار مقارنة 6.71 مليون دولار للمرافق التي لا تستخدم الخدمة. [2]

لعل من أهم تقنيات الذكاء الاصـــطناعي التي لها تأثير فعال نجد ChatGPT[3] وعلى الرغم من المخاوف له فوائد عديدة، ومع ذلك فإنه يحلل بشـــكل نقدي المخاوف المشـــروعة بشـــأن التحيز العنصـــري، وبعض مقاييس التي تم التحقق من صـــحتها واســـتغلال جرائم الإنترنيت، ونقاط الضعف والاستغلال وقضايا الخصوصية والهندسة الاجتماعية والمعلومات المضللة.

[4]تقليل تكاليف باستخدام الذكاء الاصطناعي في تخزين من خلال:

1- تحسين موارد التخزين وتحليل أنماط الاستخدام.

2- تقليل استهلاك الطاقة عن طريق إدارة استخدام الطاقة بذكاء الاصطناعي.

---

[1] تهديد الذكاء الاصطناعي الهجومي وكيفية الحماية منه https://www.unite.ai
تاريخ الإطلاع: 16-05-2024 الساعة 07:11 PM،

[2] فوائد استخدام الذكاء الاصطناعي في الأمن السيبراني https://www.thakaa.as
تم الإطلاع: 16-05-2024 الساعة 10:05 PM

[3] **ChatGPT:** نموذج لغة اصطناعي هو قادر على إنشاء نص يشبه الإنسان، استنادا إلى OpenAL للمحادثات المثيرة واكتساب الرؤى وتلقين المهام (انظر تطبيق copilot على الموقع https://copilot.microsoft.com)
انظر ملحق (8) ص 100

[4] أوبانلا أوبيهي مزايا واهتمامات ChatGPT في الأمن السيبراني: https://toxcare.com.
تم الإطلاع: 16-05-2024 الساعة 11:00 PM، .

* **تقليل تكاليف الصـــيانـة والدعم:** من خلال تنفيذ حلول التخزين التي تعتمد على الذكاء الاصـــطناعي، يمكن أتمتة العديد من هذه المهام، وهذا يقلل من الحاجة للموظفين المتفانين ويقلل من تكاليف الصيانة والدعم.

تحليل البريد الالكتروني: يمكن للذكاء الاصـــطناعي فحص رســـائل البريد الإلكتروني والاتصـالات الأخرى للكشـف عن رسـائل البريد الالكتروني الاحتيالية، والهجمات الاحتيالية الأخرى.

تصـنيف البرامج الضـارة: يمكن للذكاء الاصـطناعي اسـتخدام تقنيات التعلم العميق لتحليل السلوكيات والخصائص للتعرف إلى البرامج الضارة وتصنيفها بدقة عالية.[1]

المطلب الثاني: تحديات الذكاء الاصطناعي

التعريف المبسـط لمصـطلح الذكاء الاصـطناعي (AI)، يشـير إلى الأنظمة أو الآلات التي تحاكي الذكاء البشـري والمصـممة لأداء المهام وحل المشـكلات، ويقدم الذكاء الاصـطناعي مزايا هائلة للمجتمع الإنســـاني في كثير من المجالات، خاصـــة في العلوم الطبية والتعليم والإعلام وإنتاج الغذاء وتوفير وســـائل نقل عامة أكثر كفاءة، ومن هنا يرى الخبراء أن نمو استخدامات الذكاء الاصطناعي سيجعل حياة معظم الناس أفضل حالا خلال العقود المقبلة.

في السـياق الآخر ظهر خبراء آخرون لديهم كثير من المخاوف بشـأن تأثير التقدم في الذكاء الاصطناعي على المجتمع الإنساني، ويشيرون إلى العديد من التحديات لعل أبرزها هي[2]:

الفرع الأول: التحديات التقنية

[1] الذكاء الاصطناعي وتخزين البيانات: فحص التكاليف وتحسين قابلية التوسع.https://www.astera.com
تم الإطلاع 16-05-2024، 03:30 AM،

[2] تحديات الشركاء الاصطناعي الخمسة.https://elaph.com
تاريخ الإطلاع: 2024/05/12، الساعة 13:00 AM

1- تحدي تنفيذ تقنية الذكاء الاصـــطناعي: حيث يجب وضـــع خطة عمل اســـتراتيجية للاستفادة من هذه التقنية خاصة فيما يتعلق بضمان وسلامة الذكاء الاصطناعي، إضافة إلى الجدوى المالية أين يجب تقدير التكاليف والإيرادات المالية، ضف إلى ذلك التحديات المتعلقة بالمهارات مثل نقص المعرفة حول مجالات الذكاء الاصـــطناعي، ونقص المواهب وندرة الخبراء والفجوات في التعليم لاكتساب مهارات تقنية عالية المستوى. [1]

2- البنية التحتية: يتطلب تحديد وتنفيذ الذكاء الاصـــطناعي بنية تحتية قوية ،بما في ذلك أجهزة الكمبيوتر، وأجهزة التخزين، وشـــبكات الاتصـــالات يمكن أن تكون هذه البنية باهظة الثمن، إضافة إلى عامل السرية والنزاهة حول البيانات التي يتم معالجتها ليست مضمونة. [2]

3- العديد من خوارزميات التعلم لا تتســم بالمرونة في وظائفها: قبل اســتخدام التطبيقات الذكية لابد أولا من تدريب الخوارزميات الأســـاســـية، ومع ذلك تؤدي عملية التدريب مع مجموعات البيانات الممثلة، إلى تخصـــص خوارزميات التعلم تلك، وهذا يعني أنه بمجرد تغيير اللون أو تغيير قاعدة في لعبة ما أو حذف الأحرف في النصوص سيؤدي إلى معالجة غير صـحيحة للآلة، ولكن بالنسـبة للبشـر فإن التكيف مع مثل هذه التغيرات سـيكون سـهلا للغاية.

---

[1] عادل إنزارن، حوكمة السياسات العامة في عصر الذكاء الاصطناعي، المكاسب والتحديات، المجلة الجزائرية للأمن الإنساني، المجلد 09، العدد 01، جانفي، 2024، ص 487.

[2] بن ناصر سعيد، الذكاء الاصطناعي والاقتصاد الرقمي، الغرض والتحديات، المجلد 8، العدد 1، ديسمبر 2023، ص 40.

*برنامج Cyber Security watson fo : برنامج تحسين أمان المعلومات السيبرانية، ويعزز قدرة محللي الأمان على اكتشاف التهديدات المعقدة، من خلال الاستفادة من البيانات غير المهيكلة (انظر تطبيق copilot على الموقع https://copilot.microsoft.com)..

*برنامجintelligence for tiguard Artificial: أحد الحلول المقدمة في fortiguard Ips، برنامج في مجال الأمن السيبراني، يستخدم الذكاء الاصطناعي وتقنية التعلم العميق للكشف عن التهديدات، ومنعها قبل أن تصل fortinet security. (انظر تطبيق copilot على الموقع https://copilot.microsoft.com)

4- بناء تطبيقات آمنة يكاد يكون مستحيلا: حتى الآن ليس من الممكن العثور على جميع الشوائب(Bugs) في رموز البرمجة سواء كان ذلك بمساعدة البشر أو عبر الوسائل التكنولوجية، وهذا يعني أن تقنيات الذكاء الاصطناعي ستكون عرضة لأشكال معينة من الهجمات الحاسوبية بطريقة أو بأخرى، فمن ناحية يتم استخدام التطبيقات الذكية نفسها بشكل متزايد لمنع الهجمات واكتشافها واتخاذ إجراءات دفاعية تحول دون وقوعها

5- محدودية الكفاءات التكنولوجية: إن الأشخاص القادرين على البحث وتطوير تطبيقات الذكاء الاصطناعي نادرون في الوقت الحالي مقارنة مع مجالات أخرى، ذلك أن هذه العمليات لا تتم عن طريق استخدام برنامج معين بحد ذاته، بل ينبغي تكيف البرامج الذكية مع مجموعة بيانات معدة يتم جمعها واستخدامها في سياق معين، ولذا وجب توفر مهارات ومواهب معينة لا يملكها سوى عدد قليل نسبيا من الناس حول العالم.

6- نقص التنوع في مجال بحوث الذكاء الاصطناعي: حيث أن 80% من العاملين في هذا المجال من أساتذة في جامعات العالم الرائدة مثل ستانفورد أو أكسفورد، وغيرها هم من فئة الذكور وفي الولايات المتحدة على سبيل المثال، يشكل الرجال أكثر من 70 % من المتقدمين لوظائف الذكاء الاصطناعي، مما يؤكد الحاجة إلى زيادة عاجلة في نسبة مطوري البرمجيات من الإناث، من أجل تمثيل مصالحهن وقيمهن بشكل أفضل وتقليل فجوة النقص.

7- عدم توافق البيانات المستخدمة في أنظمة الذكاء الاصطناعي مع الواقع بين جمع البيانات والمخرجات المتأتية من البرامج الذكية(outputs)[1] : ذلك أنه ينطوي على خطر أن تؤدي عمليات جمع البيانات ومعالجتها إلى بناء شخصية افتراضية مجزأة أو مشوهة أو غير صحيحة من جوانب معينة، فقد تم تزييف البيانات بسبب أخطاء الجهاز أو بواسطة حسابات وهمية أو برامج روبوت أخرى، والنتيجة في هذه الحالة ستكون بيانات مجزأة

[1] **Outputs** : وحدات برمجية مهمة للتشغيل على الأجهزة الذكية(أنظر موقع ويكيبيديا الموسوعة الحرة (https://fr.wikepid.org)

ومشـــوهة يتم جمعها ومعالجتها ودمجها في أنظمة التعلم، وهذا شـــيء نادرا ما يفكر فيه الناس.[1]

الفرع الثاني: التحديات القانونية

1- نقص التأطير المحترف: مادام الذكاء الاصـــطناعي قائم على التكنولوجيا الحديثة فهو يحتاج إلى الاسـتثمار في الأشـخاص والمهارات اللازمة لبناء تطبيقات الذكاء الاصـطناعي وفي الوقت الحاضـــر تعاني أغلب الدول وأبرزها الجزائر من نقص المهندســـين والتقنيين المختصـــين في هذا المجال، ومن جهة أخرى وليتم اعتماد تقنيات الذكاء الاصـــطناعي في المعاملات القانونية والمحاكمات لابد من تدريب الكوادر القانونية على هذه التقنيات، وهذا الأمر الذي تفتقر إليه الجزائر التي أغلب موظفيها لا يملكون خبرات في المجال التكنولوجي الأمر الذي يصعب مهمة استخدام الذكاء الاصطناعي في المجال القانوني.

2- غياب الإســـتراتيجية والتخطيط: أهم عائق يقف في وجه الانتقال لمجتمع قائم على تقنيات الذكاء الاصـــطناعي، هو غياب خطة عمل وحوكمة رشـــيدة للأهداف والمتطلبات وغياب التشـــريعات المنظمة لهذا النوع من التكنولوجيا، فنجد أن المشـــرع الجزائري لم ينص على أي تعريف للذكاء الاصـطناعي بل أشـار له بصـفة عرضـية في قانون حماية الملكية الفكرية، وهذا يؤدي لغياب الابتكار والإبداع كنتيجة لغياب الحماية القانونية. [2]

3- التنظيم التشـريعي للذكاء الاصـطناعي: عدم التناغم بين القانون والتكنولوجيا من شـأنه أن يخلق فجوة بين الإطار القانوني النظري، والتطبيقي التقني مما يترتب عليه عرقلة التطور التقني، فضلا عن ظهور ممارسات سلبية تلحق الضرر، وبالرجوع إلى أبرز التشريعات لبيان

[1] اجهاد عبد ربه محمد تركي، التحديات التي تواجه تطبيق الذكاء الاصطناعي في تعليم الموهوبين وآفاقه المستقبلية، المجلة التربوية، كلية العلوم التربوية، جامعة الطفيلية التقنية، الأردن، عدد 110، ج 1، 2023، ص 13-16.

[2] بوقجار اسمهان، بن قاجة نور الهدى، مرجع سابق، ص 54.

موقفها من برامج الذكاء الاصطناعي، نجد أن هذه التشريعات لم تتضمن أي معالجة شاملة للجوانب المختلفة لتقنية الذكاء الاصطناعي. [1]

أولا: التشريع الأمريكي

على الصـــعيد الأمريكي تطرق قانون المعاملات الالكترونية الموحد (UETA) إلى الوكلاء الالكترونيين واعترف بصـــحة العقود التي يبرمها الوكيل الالكتروني دون أي علم أو تدخل بشري لكن في الوقت عينه اعتبر مجرد أداة ليس لديها إرادة مستقلة خاصة بها وبالتالي فان الشـــخص الذي يوظفها مســـؤول بشـــكل مطلق عن النتائج التي تترتب على أعمال الوكيل الالكتروني.

ثانيا: على الصعيد الأوروبي

فإن التوجيه رقم EC/31/200[2] بشأن التجارة الالكترونية لم يتضمن أي إشارة مباشرة أو صريحة إلى برامج الذكاء الاصطناعي ذلك أنه اعتبر أن برامج الذكاء الاصطناعي على الرغم من خصائصها الفريدة ليست سوى وسائل الكترونية عادية لا تحتاج إلى قواعد خاصة أو الإشـــارة إليها على وجه الخصـــوص على اعتبار أن الإطار التنظيمي الحالي يكفي لتنظيمها واستيعاب جوانبها المختلفة.

[1] حمادي العطرة، نون زازة الزهرة، تحديات الذكاء الاصطناعي للقانون، مذكرة ماستر، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2021/2020، ص 38.

[2] **قانون المعاملات الالكترونية الموحد(UETA)** : قانون يهدف إلى تنظيم المعاملات الالكترونية وتحديد الأحكام المتعلقة بالتوقع الالكتروني والتبادل الآمن للمعلومات الرقمية ويساهم في تعزيز أمان المعلومات وتطوير البيئة الرسمية. انظر تطبيق copilot على الموقع https://copilot.microsoft.com.) .

بالإضـــافة إلى ذلك فإن التوجه الأوروبي بشـــأن التجارة الالكترونية لم يتطرق إلى حماية المســـتخدم من التصـــرفات غير المتوقعة للبرامج الذكية ولم ينظم على وجه التحديد كيفية التعامل مع الأخطاء التي تسببها الآلة أو البرامج الإلكترونية. [1]

ثالثا: التشريع الجزائري

بالنســـبة للجزائر وفي خضـــم القوانين التي صـــدرت مؤخرا في إطار تنظيم المعاملات الإلكترونية لاســـيما قانون التجارة 05/18، لم يشـــر المشـــرع الجزائري تماما إلى الذكاء الاصطناعي وتطبيقاته مباشرة أو غير مباشرة.

رابعا: التشريع الدولي

على الصعيد الدولي نجد أن **قانون الاونسترال** النموذجي بشأن التجارة الإلكترونية، لم يتطرق صراحة إلى برنامج الذكاء الاصطناعي أو الوكلاء الالكترونيين.

وفي المادة 12[2] **من اتفاقية الأمم المتحدة** المتعلقة باســـتخدام الخطابات الإلكترونية في العقود الدولية، بجوار تكوين العقود نتيجة لأفعال قام بها وكلاء إلكترونيين حتى ولم يقم بها شـــخص طبيعي بيد أن هذه الاتفاقية وعلى غرار قانون الاونســـترال النموذجي، ركزت فقط على العقود الأوتوماتيكية التي يتم إنشاؤها آليا بواسطة أنظمة برمجية.

[1] عماد عبد الرحيم الدحيات، نحو تنظيم قانوني للذكاء الاصطناعي في حياتنا، إشكالية العلاقة بين البشر والآلة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة الإمارات العربية المتحدة، مجلد 8، عدد 5، 2019، ص 24-25.

[2] المادة 12 من اتفاقية الأمم المتحدة: تهدف إلى تسهيل استخدام الخطابات الإلكترونية، تتضمن اليقين القانوني للعقود المبرمة، والخطابات المتبادلة إلكترونيا، اطلع على القانون الأونسترال النموذجي.

ولكنها لم تنص على إمكانية تكوين العقود بشكل مستقل بواسطة أنظمة برمجية ذكية كما لم تتضـــمن هذه الاتفاقية أي أحكام للأخطاء الآلية، بل تناولت فقط الأخطاء التي يرتكبها شخص طبيعي. [1]

4- عدم وجود تنظيم قانوني خاص بالذكاء الاصـــطناعي: واقع ممارســـات الذكاء الاصطناعي في حياة الأفراد المتجسد من خلال الاستعمال المتكرر والممتد للسيارات الذكية والروبوتات، وكذا الأنظمة المبرمجة في مجال الصـحة والاقتصـاد والقانون، دفع مصـممي ومالكي ومسـتعملي الذكاء الاصـطناعي للمطالبة بنظام قانوني خاص به، قصـد تجنيبهم تحمل المسؤولية القانونية عن قرارات وأفعال هذه التكنولوجيا، بـــحكم أنها قد أصبحت تقوم بمهامها بعيدا تماما عن ســيطرتهم وبالاســتقلالية، كما أن بعضـــهم دعا الإعتراف بحقوق الملكية الفكرية لهذا الذكاء الذي أصبح قادرا على الإبداع والاختراع، لكن هذا التوجه وإن كان قد بدا فعال فإنه خلق خوفا وقلقا كبيرين من حيث أثاره التي يرى الأغلبية أنها لا تتوافق والمنطق القانوني[2].

5- **المســـؤولية والملكية الفكرية:** التحدي القانوني الأول الذي قد يواجه القانون متعلق بالمسؤولية القانونية عن سلوك الذكاء الاصطناعي، باعتباره وصل إلى مرحلة اتخاذ قرارات مستقلة بعيدة تماما عن إرادة البشر، وهذا من خلال إحداث ضرر للغير في إطار المسؤولية المدنية، أو بارتكاب جرائم تحت لواء المســؤولية الجزائية، وبالتالي فإن أســاس المســؤولية للتعويض عن الضــرر الذي يلحق بالغير، هو اكتســاب الشــخصــية القانونية التي يمنحها القانون للشخص الطبيعي والشخص المعنوي وفق أسس وشروط معينة، هناك مجموعة من

[1] حمادي العطرة، نون زازة الزهرة، مرجع سابق، ص 42 إلى44.

[2] بن عثمان فريدة، الذكاء الاصطناعي (مقاربة قانونية)، دفاتر السياسة والقانون، جامعة لونيسي علي، البليدة 2 الجزائر، المجلد 12، عدد 02، 2020، ص 162-163.

فقهاء القانون الذين حاولوا البحث عن أساس المسؤولية المدنية للذكاء الاصطناعي، فاتجه جانب منهم إلى إسقاط قواعد المسؤولية التقليدية للوصول إلى الطرف الذي يتحمل التعويض عن كل ضرر قد يلحق الغير جراء الذكاء الاصطناعي، مع بعض التعديلات الطفيفة على تلك القواعد واستبعادهم لفكرة شخصنة الذكاء الاصطناعي، للتعلم والقياس ثم الاستنتاج لاتخاذ قراراته، كذلك لا يمكن أبدا أن يتخذ الذكاء الاصطناعي قرارات معينة إلا بعد تشغيله من طرف البشر.[1]

واعتبر **ريان ابوت:** وهو محام مختص ببراءات الاختراع أنه يمكن اعتبار الذكاء الاصطناعي مخترعا، ولقد قدم في الولايات المتحدة الأمريكية طلبات لبراءتي اختراعين متعلقين بالضوء التحذيري ومستوعب غذائي، لكن تلك الطلبات سجلت باسم ذكاء اصطناعي اسمه دبوس ايه أي[2]، وهو ذكاء اصطناعي ابتدعه ستيفن ثيلر، أي أن هذا الأخير صمم هذا الذكاء وزوده بخوارزميات عامة ومعلومات ، لكن لم يكن أبدا بوسع ثيلر الوصول لهذا الابتداع لأنه لا علاقة له بالأضواء والمستوعبات.

يري البعض أنه لا يمكن اعتبار الذكاء الاصطناعي مخترعا ،لأن المخترع في حقيقة الأمر فرد ينتسب لشركة معينة كموظف، وملكية البراءة تعود للشركة ولا يمكن للذكاء أن يكون موظفا أو متعاقدا، هذا بغض النظر على أن براءة الاختراع تنسب للأشخاص الطبيعية، كما أن هناك من يرى أنه لا يمكن أبدا للذكاء الاصطناعي العمل دون مساعدة بشرية حتى، ضف على ذلك أن اعتبار الذكاء الاصطناعي مخترعا يفرض عليه مجموعة من الالتزامات لعل من أهمها توقيع العقود، الترخيص ورفع الدعاوي، وهذا غير ممكن عمليا

---

[1] سالم المطروشي، المسؤلية القانونية لمنظومة الذكاء الاصطناعي https://wwwalkhaleej.ae تاريخ الاطلاع 01/06/2024 الساعة 12:01pm

[2] **دابوس ايه أي:** هو جهاز مبتكر تقنية (Alpin) دبوس الذكاء الاصطناعي، ويثبت على الملابس، يعمل بالذكاء الاصطناعي، ويمكن التحدث إليه وطرح الأسئلة عليه. (انظر تطبيق copilot على الموقع https://copilot.microsoft.com **انظر ملحق (9) ص 100**

في نظرهم، يرى أبوت[1] أنه يجب إيجاد حل لهذه المعضـــلة حيث أنه من المعلوم أن للذكاء الاصطناعي علاقة بالعديد من الأطراف التي جعلته قادرا علي التعلم وتطوير نفسه، والقياس الاسـتنتاج بداية بمصـممه ونهاية بمسـتعمليه، وعليه قد يكون من الصـعوبة تحديد الطرف الجدير ببراءة الاختراع في حالة ابتداع الذكاء الاصطناعي لاختراع معين. [2]

6- **تعارض المنطق القانوني وحقيقة الذكاء الاصـطناعي:** إن منح الشـخصـية القانونية للذكاء الاصطناعي يعني خلق منظومة قانونية خاصة بغير البشريين، وهذا ما يعني مجتمعا آخر في موازاة المجتمع البشري وهذا قد ينم عن الوقوع بالضـرورة في إشـكالات عديدة فيما بين المجتمعين قد يؤدي في النهاية إلى إنصـــاف أحد عن الآخر، وهذا ما يتعارض تماما والكرامة الإنســـانية التي خلق القانون أصـــلا لحمايتها والمحافظة عليها، إذا كان منشـــأ الاعتراف للذكاء الاصطناعي بالشخصية القانونية، هو إسناد المسؤولية عن الضـرر الذي يســببه، فهل ســيكون ذلك منصــفا فعال للمضــرور، كما أن الشــخص الإلكتروني ليس باســتطاعته إبرام بعض العقود كالهبة والزواج، فهي تعتمد على الإدراك والعاطفة الإنســانية كما أنه لا يمكنه وإن تم منحه الشــخصــية القانونية أن يرفع الدعاوي، وبغض النظر عن لا ماديته فهو لا يمكن له أن يقدر مدى تضرره خاصة إن كان الضرر معنويا.

إن الشخصية القانونية للذكاء الاصطناعي تستوجب قيام مسؤوليته حيال الغير، وهذا يعني البحث في المراحل التي اتبعها وكذا خوارزمياته لمعرفة حقيقة اتخاذه القرار الذي تســبب في الضــرر، وهذا ما قد يتعارض مع أهم مقومات الذكاء الاصــطناعي، ألا وهو الكشــف عن أسرار عمل نظامه، وهذا ما يمثل مساسا بحقوق الملكية الفكرية. [3]

---

[1] **ريان ابوت:** هو فنان لبناني مشهور ومؤلف أغاني، حامل درجة دكتوراه في الطب والفقه القانوني (انظر تطبيق copilot على الموقع) https://copilot.microsoft.com

[2] بن عثمان فريدة، مرجع سابق، ص 164-165.

[3] بن عثمان فريدة، مرجع سابق، ص 166.

اقتراحات الفصل الثاني

– الإلمام بالجانب التقني لذكاء الاصـطناعي، وتأهيل الكوادر المتخصـصـة في هذا المجال بالإضافة إلي تطبيق الذكاء الاصطناعي في كافة الميادين.

– عمل الباحثين وصناع السياسات على التخفيف من مخاطر الذكاء الاصطناعي والتصدي لتهديداته، عن طريق تطوير طرق أمنة وموثقة لتصميم ونشر أنظمة الذكاء الاصطناعي.

– ضرورة وحتمية توفير إطار أخلاقي متكامل، يضبط تطبيق واستخدام الذكاء الاصطناعي في الواقع، أين يتم تضـــمين الأخلاق والقيم في كل العمليات التي تضـــمن تســـير وبرمجة والتحكم في الذكاء الاصطناعي.

_ وضـــع إطار قانوني متكامل في إطار الذكاء الاصـــطناعي، لمحاولة التقليل من الثغرات الناتجة عن إنعدام التشريعات بالإضافة الى التصدي للتحديات التقنية.

الخاتمة

من أجل تحقيق توازن بين التطور التكنولوجي والقيم الإنسانية الأساسية وجب التعمق أكثر في المواضيع ذات الصلة بالذكاء الاصطناعي، والأمن السبيراني وضرورة توظيف هذه التقنيات الحديثة خاصة في ظل البيئة الرقمية وانتشار المنصات عبر مواقع التواصل الاجتماعي، وبالتالي ضمان حماية خصوصيات الأفراد والمستخدمين.

ونظرا لأن الفضاء الإلكتروني متاح للجميع دون استثناء، فقد أدى ظهور الهجمات السبيرانية التي تتخذ أشكالا وألوانا عديدة وخاصة الجرائم الإلكترونية والإرهاب السبيراني والصراع السبيراني بين الدول، ومع ظهور تقنية الذكاء الاصطناعي حيث تعد من أحدث التقنيات المستخدمة لتعزيز الأمن السبيراني، سارعت العديد من الدول إلى توظيف هذه التقنية في مجال الأمن السبيراني ،غير أن مثل هذه التقنيات تحتاج إلى ضوابط وقوانين تنظمها لذلك وجب على الدول تطوير الأطر القانونية الخاصة باستخدامات هذه التقنية على الصعيدين الإقليمي والدولي.

يمكن القول أن الذكاء الاصطناعي يمثل تقدما هائلا في مجال التكنولوجيا وله العديد من الفوائد والتطبيقات المحتملة، ومع ذلك يجب أن يتم استخدامه بشكل مسؤول وفقا للقوانين والأخلاقيات، وأن يتم التركيز على حماية الخصوصية وتجنب التأثيرات السلبية المحتملة لاستخدام هذه التكنولوجيا الجديدة وجعلها آلية فعالة لتحقيق الأمن السبيراني وفضاء رقمي أكثر أمانا.

2_ النتائج:

ومن خلال دراستنا توصلنا إلى النتائج التالية:

– يعتبر الأمن السبيراني بمثابة شريان حياة بالنسبة للعديد من الدول التي تعتمد على التكنولوجيا الرقمية، سواء على الصعيد الأمني والعسكري والاقتصادي والاجتماعي والثقافي.

– يعد الأمن السبيراني أداة هامة للحفاظ على خصوصية المعلومات، بالإضافة إلى تحسين أمن المعلومات وتحسين طريقة حفظ البيانات والمعلومات خاصة بالنسبة للشركات والبنوك.

– الأمن السـبيراني يوسـع إمكانية العمل بأمان دون أي مخاطر أمنية لاختراق المعلومات وقطع الطريق على مسـتخدمي برامج التجسـس واختراق أجهزة الحواسـيب وأجهزة الهواتف النقالة، وهذا يترك أثرا رائعا في مختلف المجالات لأنه يحافظ على الخصوصية والسرية إلى أقصى درجة.

– مسألة تحقيق الأمن المعلوماتي لازالت من المواضيع التي تثير إشكالات كبيرة سواء على الصعيد العالمي أو الإقليمي أو الداخلي، خاصة مع تزايد التهديدات الأمنية الإلكترونية سواء على الدول أو الأفراد، بالرغم من إبرام العديد من المعاهدات والاتفاقيات الدولية في مجال الأمن السيبراني.

– يعتبر الذكاء الاصـطناعي تجسـيدا للعقل البشـري في شـكل آلي في صـورة آلة تامة كالروبوتات، أو في شـكل أنظمة وبرامج وتطبيقات تكنولوجية حاسـوبية هدفها الأول محاكاة العقل البشري في القيام بالعديد من الأعمال والوظائف.

– أثبت الذكاء الاصطناعي فعالية كبيرة في العديد من المشاكل والمجالات من حيث السرعة في التصـرف ومسـتوى الدقة والجودة العالية، أين أصـبحت معدلات الخطأ منخفضـة نسـبيا عما كانت عنه سـابقا بالاسـتعمال البشـري البحت، وهو ما كان له أثر إيجابي على أنماط الحياة المتنوعة.

– تحكم الإنسـان في الذكاء الاصـطناعي ولد قضـية طبيعة اسـتخدام هذا الذكاء، أين يرتبط ارتباطا مطلقا بما برمج عليه من قبل العقل البشري، والذي يمكن أن يستخدم في نطاق غير شـرعي وغير أخلاقي أين أتاح الذكاء الاصـطناعي إمكانيات هائلة للقرصـنة والهجومات الإلكترونية، واسـتخدامات المعلومات المتحصـل عليها في جرائم إلكترونية متنوعة أو في تظليل الرأي العام وتغيير وجهات نظره وغيرها.

2-الإقتراحات:

- رصـــد التجارب والممارســـات الناجحة الدولية والعربية منها، فيما يخص إدارة نظام أمن المعلومات بهدف دراســـتها والاســـتفادة منها، والوقوف على عوامل نجاحها والصـــعوبات والمعوقات التي تواجهها والعمل على وضع آلية قابلة للتطبيق.

- العمل على بناء بنية تحتية معلوماتية (infrastructure information) كمطلب أولي لابد منه، من أجل استخدام أنظمة المعلومات الرقمية (Digital information) بكفاءة وفعالية.

- وجود منهجيات تســتند على ثقافة المعلومات كســلوك، والتي تعني فهم وإدراك المعلومات كثروة في مجتمع المعلومـات والمعرفـة لضـــمـان النجـاح المســـتمر في أداء منظمـاتنـا لعملهاوإعطاء مكانة متميزة لقطاع المعلومات وأمنه في البلد.

- تنمية رأسمال الفكري خاصة للعاملين في مجال النظم المعلوماتية الحاسوبية، والعمل على إشراك العاملين في مجال الحاسبات ببرامج تدريبية في مجال أمن المعلومات.

- ضــرورة ديمومة المراجعة والرقابة والتقويم لنظم المعلومات، ومجابهة حالات الاختراق أول بأول والعمل على تحديث النظام.

-وجوب تطوير اســـتراتيجية بيانات تعزز الابتكار، وتحمي مســـتخدمي مختلف المنصـــات المتاحة عبر وسائط الإعلام الجديد.

- تشجيع الوصول إلى البيانات بشكل أكبر للباحثين، دون المساس بالخصوصية الشخصية للمستخدمين باعتماده تقنيات الذكاء الاصطناعي.

- الترويج لنمـاذج جـديـدة من التعليم الرقمي وتطوير القوى العـاملـة في مجـال الـذكـاء الاصطناعي.

- فرض العقوبات على ســوء اســتخدام الذكاء الاصــطناعي، وتعزيز الأمن الســبيراني في الحفاظ على خصــوصــيات رواد ومســتخدمي تطبيقات الذكاء الاصــطناعي مهمة جدا في مختلف المنصات في البيئة الرقمية الحديثة.

قائمة المصادروالمراجع

I/المصادر:

- **الاتفاقيات الدولية:**

اتفاقية بودابيست معاهدة دولية وقعت في بودابيست عاصمة المجر لمكافحة الجرائم الالكترونية سنة2001

- **القوانين:**

1- القانون 04/09 المؤرخ في 2009/05/09 المتضـــمن القواعد الخاصـــة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

2- التوجيه رقم EC/31/200 : قانون أوروبي يعالج بعض الجوانب التوجيه لخدمات المجتمع المعلوماتي وبشكل خاص التجارة الالكترونية.

II/المراجع باللغة العربية:

- **الكتب:**

1- بيتر ســينجر، دروس الحروب الماضــية والاتجاهات التكنولوجيا المســتقبلية في القرن الحادي والعشرين، ط1 مركز الامارات في الدراسات والبحوث الاستراتجية 2014ص.

2- بلاي ويتباي، الذكاء الاصـطناعي، دار الفاروق للاسـتثمارات الثقافية، الجيزة، مصـر، 2003، الطبعة العربية 2008.

3- ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية فهرسة مكتبة الملك الوطنية أثناء النشر، الرياض، 2015.

4- رؤى حسن الدين هاني قطيشات، الذكاء الاصطناعي المستقبل الجديد

5- غســـان العمري، عبد الســـاتر العلي، عامر القنديلجي، المدخل إلى إدارة المعرفة، دار المسيرة للنشر والتوزيع، طبعة 2، عمان، الأردن، 2009

6- فتحي حســـن عامر، الميتافيرس ثورة الإعلام الرقمي، ط2، العربي للنشـــر والتوزيع، القاهرة، 2023.

7_ مجدي نارمين، الذكاء الاصـــطناعي وتعلم الآلة، الإمارات، صـــندوق النقد العربي، 2022.

- **المذكرات والأطروحات:**

1- نورة عقون، واقع الفضـــاء الســـيبراني وإشـــكالية الدفاع الوطني في الجزائر، مذكرة ماستر، تخصص دراسات أمنية وإستراتيجية لكلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2019.

2- حمادي العطرة، نون زازة الزهرة، تحديات الذكاء الاصطناعي للقانون، مذكرة ماستر، تخصـــص قانون أعمال، كلية الحقوق والعلوم الســـياســـية، جامعة قاصـــدي مرباح، ورقلة، 2021/2020.

3- بكوش رميساء، انعكاسات التهديدات السيبرانية على الأمن الوطني الجزائري، مذكرة ماستر، تخصص دراسات إستراتيجية وأمنية لكلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، 2019.

4- ســعيدة رشــاش، مكانة الأمن الســيبراني في منظومة الأمن الوطني الجزائري، مذكرة ماستر، تخصص دراسات إستراتيجية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة العربي التبسي، 2018.

5- بغداد محمد، الأمن المعلوماتي وسـبل حمايته في الجزائر، مذكرة مكملة لنيل شـهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة سعيدة، 2018/2017.

6- بلكحل راضـــية، الذكاء الاصـــطناعي ودوره في تطوير الإدارة الالكترونية، مذكرة ماستر، تخصص إدارة أعمال، جامعة أحمد دراية، أدرار، 2022/2021.

7- بوقجار اســـمهان، بن قاجة نور الهدى، التكريس القانوني والتنظيمي للذكاء الاصطناعي في الجزائر، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي، تخصص قانون الإعلام الآلي والانترنيت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2023/2022.

8- دداش حسين، شيحي هشام، دور الذكاء الاصطناعي في تحسين أداء المؤسسة الاقتصادية، مذكرة ماستر في علوم التسيير، تخصص إدارة أعمال، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022/2021.

9- جيلالي ســـارة، تريكي ســـميرة، تطبيقات الذكاء الاصـــطناعي في إدارة المكتبات الجامعية، مذكرة ماســـتر، كلية العلوم الإنســـانية والاجتماعية، جامعة ابن خلدون، تيارت، 2022.

10- جيدة سعاد، كادي سليمة، استخدام تطبيقات الذكاء الاصطناعي في تحسين عملية اتخاذ القرار في المؤسسة الاقتصادية، مذكرة لاستكمال شهادة ماستر، علوم اقتصادية وتجارية وعلوم التسيير، جامعة أحمد دراية، أدرار، 2020.

11- غادة المنجم واخرون، الذكاء الاصـــطناعي، بحث مقدم في مادة نظم مســـاندة القرارات، كلية العلوم الإدارية، فجامعة الملك سعود، الرياض ،2009

- **المقالات:**

1- علاء الدين فرحات، الفضاء السيبراني، تشكيل ساحة المعركة في القرن الحادي والعشـــرين، مجلة العلوم القانونية والســـياســـية، المدرســـة الوطنية العليا للعلوم السياسية (الجزائر)، المجلد 10، العدد 03، ديسمبر 2019.

2- نوفيل حديد، كربيط حنان، أمن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة، المؤسسة lentreprise، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، العدد 3، 2014.

3- عصـــامي نور الدين، دور أمن المعلومات في الحماية من أخطار التجســـس الالكتروني، كلية العلوم الاقتصـــادية والتجارية وعلوم التســـيير، جامعة 20 أوت 1955، سكيكدة، 2020/2019.

4- سلمى عبد الرحمان الدوسري، جبريل حسن محمد، دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع، مجلة مكتبة الملك فهد الوطنية، المجلد 24، العدد 02، أفريل 2017.

5- ســهيلة بوضــياف، أمينة حمراني، أمن المعلومات في الجزائر، المجلة الجزائرية للأمن والتنمية، المجلد 09، العدد 16، جانفي 2020.

6- ســناء أرطباز، أثر اســتخدام تطبيقات الذكاء الاصــطناعي على تحســين أداء المؤســســة، جامعة أم البواقي، مجلة العلوم الإنســانية، جامعة أم البواقي، مجلد 09، عدد 03، ديسمبر 2022.

7- محمد دحماني، الذكاء الاصــطناعي كآلية لتعزيز الأمن الســبيراني، مجلة الفكر القانوني والســـياســـي، جامعة عمار ثليجي، الأغواط، مجلد 07، العدد 02، 2023.

8- لحول بن علي، بريكي خالد، الذكاء الاصـطناعي في المجال العلمي بين الحتمية في التطبيق والمخـاطر في الإنتـاج، مجلـة التراث، مجلـد 14، العـدد مـارس 2024.

9- بن علي إحسان، أهمية الذكاء الاصـطناعي في إدارة الأزمات في ظل كوفيد 19 – تجربـة الإمارات العربية المتحدة، مجلة آفاق علوم الإدارة والاقتصـــاد، جامعة زيان عاشور الجلفة (الجزائر)، المجلد 06، العدد 02، 2022.

10- خليل سعدي، مرزوق بن مهدي، الذكاء الاصطناعي كتوجه حتمي لحماية الأمن السيبراني، مجلة دراسات في حقوق الإنسان، جامعة العربي تبسي (تبسة)، مجلد 6، عدد 1، جوان 2022.

11- محمد دحماني، استخدامات الذكاء الاصطناعي في المجال البيئي، مجلة القانون والعلوم البيئية، جامعة عمار ثليجي الأغواط، مجلد 02، عدد 03، 2023.

12- بوطلاعة وداد، بوكورو منال، صراع الفضاء السيبراني وتأثيره على سلم وأمن الدولتين تحديات وتهديدات جديدة وسبل مواجهة، مجلة العلوم القانونية والاجتماعية، جامعة الإخوة منتوري قسنطينة (1)، المجلد 07، العدد 04 ديسمبر 2020.

12- بدري جمال، الذكاء الاصطناعي، المجلة الجزائرية للعلوم القانونية والسياسية، كلية الحقوق، جامعة الجزائر 1، مجلد 59، العدد 4، 2022.

13- أسماء بليليطة، التكريس القانوني والتنظيمي للذكاء الاصطناعي في الجزائر، المجلة الدولية للذكاء الاصطناعي في التعليم والتدريب، جامعة الجزائر 1

14- زعموكي سالم، مرزق فتيحة حبالي، مجلة التراث، جامعة زيان عاشور بالجلفة (الجزائر)، المجلد 13، العدد 04، ديسمبر 2023.

15- أبو بكر خوالد، تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات الأعمال، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، الطبعة الأولى، جامعة عنابة، الجزائر، 2019.

16- مصطفى أبو مندور موسى عيسى، مدى كفاية القواعد العامة للمسؤولية المدنية في تعويض أضرار الذكاء الاصطناعي، دراسة تحليلية تأصيلية مقارنة، مجلة حقوق دمياط للدراسات القانونية والاقتصادية، كلية الحقوق، جامعة دمياط، مصر، يناير 2022، العدد 5

17- إيهاب خليفة، الذكاء الاصطناعي تأثيرات تزايد دور التقنيات الذكية في الحياة اليومية للبشر، مجلة اتجاهات الأحداث، أبو ظبي، العدد 20، مارس – أفريل 2017.

18- عبد الرازق مختار محمود، تطبيقات الذكاء الاصطناعي: مدخل لتطوير التعليم في ظل تحديات جائحة كورونا، المجلة الدولية للبحوث في العلوم التربوية، المجلد 03، العدد 04، 2020.

19- سعاد بوبحة، الذكاء الاصطناعي. تطبيقات وانعكاسات، مجلة اقتصاد المال والأعمال، المركز الجامعي عبد الحفيظ بوالصوف، المجلد 6، العدد 4، ديسمبر 2022.

20- الأسد صالح الأسد، الذكاء الاصطناعي. الفرص والمخاطر والواقع في الدول العربية، مجلة إضافات اقتصادية، المركز الجامعي تيبازة (الجزائر)، مجلد 07، عدد 01، 2023.

21- وسيلة سعود، الذكاء الاصطناعي وتحديات الممارسة الأخلاقية، مجلة نماء للاقتصاد والتجارة، جامعة البويرة (الجزائر)، مجلد 07، عدد 02، ديسمبر 2023.

22- محمد خزعبل عباس، وليد مرزة، حمزة المخزومي، أمن الفضاء السيبراني، قراءة في المفهوم القانوني، مجلة العلوم القانونية، جامعة بغداد، المجلد 37، الجزء 2، شباط 2023.

23- عادل إنزارن، حوكمة السياسات العامة في عصر الذكاء الاصطناعي المكاسب والتحديات، المجلة الجزائرية للأمن الإنساني، مجلد 09، عدد 01، جانفي 2024.

24- بن ناصر سعيد، الذكاء الاصطناعي والاقتصاد الرقمي، الفرص والتحديات، إدارة مراجعة مغاربة للمنظمات، مجلد 8، عدد 1، ديسمبر 2023.

25- جهاد عبد ربه محمد تركي، التحديات التي تواجه تطبيق الذكاء الاصطناعي في تعليم الموهوبين وآفاقه المستقبلية، المجلة التربوية، كلية العلوم التربوية، جامعة الطفيلية التقنية، الأردن، عدد 110، ج 1، 2023.

26- كريمة شاني، جير الكعبي، مجتمع المعلومات في العالم العربي، مجلة كلية الأدب، جامعة المستنصرية، قسم المجتمع المدني، العدد 98.

27- أحمد عيبس نعيمة القتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولة المعاصرة، مجلة المحقق الحلبي للعلوم القانونية والسياسية، العراق، العدد 4، 2016.

28- بارة سميرة، الأمن السيبراني في الجزائر، السياسات والمؤسسات، جامعة قاصدي مرباح، ورقلة، المجلة الجزائرية للأمن الإنساني، العدد 4، جويلية 2017.

29- قطاف سليمان، بوتريش عبد الحليم، الأمن السيبراني والمضامين المفاهيمية المرتبطة به، جامعة الأغواط (الجزائر)، مجلة جنية للدراسات العلمية الأكاديمية، مجلد 05، عدد 02، 2022.

30- عماد عبد الرحيم الدحيات، نحو تنظيم قانوني للذكاء الاصطناعي في حياتنا، إشكالية العلاقة بين البشر والآلة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة الإمارات العربية المتحدة، مجلد 8، عدد 5، 2013.

31- بن عثمان فريدة، الذكاء الاصطناعي (مقاربة قانونية)، دفاتر السياسة والقانون، جامعة لونيسي علي، البليدة 2 (الجزائر)، مجلد 12، عدد 02، 2020.

32- حازم محمود خليل، استعمال الفضاء السيبراني في الحروب الغير التقليدية، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، القاهرة، المجلد 08، العدد 05، يناير 2023.

33- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، دراسة منشورة، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، 2019.

34- بوازدية جمال، الأمن السيبراني، محاضرات مقدمة لطلبة السنة ثالثة ماستر، تخصص دراسات إستراتيجية وأمنية، جامعة الجزائر (3)، كلية العلوم السياسية والعلاقات الدولية.

35- إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، جامعة محمد بوضياف المسيلة، مجلد 10، عدد 01، أفريل 2019.

36- دلال صادق الجواد، حميد ناصر الفتال، أمن المعلومات، دار البازوري العلمية للنشر والتوزيع، المملكة الأردنية، 2019.

37- فيلالي أسماء، شليل عبد اللطيف، تهديدات أمن المعلومات وسبل التصدي لها، مجلة البشائر الاقتصادية، جامعة أبو بكر بلقايد تلمسان (الجزائر)، مجلد 04، عدد 03، 2019.

38- طمطامي سالم، الصحافة الالكترونية ولامن السيبراني، مذكرة ماستر، تخصص صحافة مطبوعة الكترونية، جامعة احمد دراية كلية العلوم الإنسانية والاجتماعية ولعلوم الإسلامية ادرار،2022

- **المواقع الالكترونية:**

1- https://www.ssi.gov.fr الوكالة الفرنسية لأمن نظم العلومات:

2- https://www.kutub.info الأمن السيبراني وحماية امن المعلومات:

3- https://www.youn7.com الفرق بين تقنية الذكاء الاصطناعي والروبوتات:

4- https://bakkah.com الفرق بين الذكاء الاصطناعي والامن السيبراني:

5- https://kabila.net عن امن المعلومات والبينات والانترنيت:

6- https://ar.wikipedia.orgأمن المعلومات:

7- www.myreaders.info الذكاء الاصطناعي:

8- https://bawabaai.comها هو الفرق بين الروبت والذكاء الاصطناعي :

9- https://watsbot.meهل هناك فرق بين الروبوتات والذكاء الاصطناعي :

10- https://ar.quora.com الفرق بين تخصص الذكاء الاصطناعي وتخصص الروبوتات:

11- https://arabic.rt.com تحذير هام الذكاء الاصطناعي يهدد الوظائف في جميع انحاء العالم:

12- https://www.europavabet.com الأمن القومي وتأثير الذكاء الاصطناعي عليه:

13- https://www.un.org: نحو اخلاقيات الذكاء الاصطناعي للأمم المتحدة

14- https://sdara.gov.sa مبادئ واخلاقيات الذكاء الاصطناعي:

15- https://aletiltad.aeحوكمة الذكاء الاصطناعي :

16- https://www.anhajab.net الذكاء الاصطناعي وتحسين امن المعلومات السيبرانية

17- https://www.amazon.comما المقصود بتعلم الالة :

18- https://www.unite.ai تهديد الذكاء الاصطناعي الهجومي وكيفية الحماية منه:

19- https://www.thakaa.as فوائد استخدام الذكاء الاصطناعي في الامن السيبراني:

20- https://toxcare.com مزيا واهتمامات chat GPT في الامن السيبراني

21- https://www.astera.comالذكاء الاصطناعي وتخزين البيانات :

22- https://www.aljazeera.net تقنيات الامن السيبراني والتحديات المستقبلية:

23- https://www.rmg-sa.com الحماية من الهجمات الالكترونية عبر ستة أدوات للأمن السيبراني

24- https://ar.lpecentre.com تقنيات الامن السيبراني إدارة المخاطر في عصر المعلومات

25-https://www.mediamit.edo/pattie Pattie maes, Softwar agents tutorial .available

26- linkedin.com مدونة اميرنا تقنيات الامن المتقدمة لمكافحة الاختراق والتهديدات السيبرانية :

27- https://ar.wikepid.org الذكاء الاصطناعي ويكيبيديا على الموقع:

28- https://alarabimag.com: فهد آل قاسم، مدخل الى علم الذكاء الاصطناعي

29-https://cnnbusinessararbic.com دور الذكاء الاصطناعي يزداد في القطاع الطبي

30–https://wwwalkhaleej.ae: المسؤولية القانونية لمنظومة الذكاء الاصطناعي

III/المراجع بالغة الأجنبية:

- **المعاجم بالغة الاجنبية:**

1- Dictionnaire français. Le petite Larousse (France Edition 2001).

2- English diction Oxford dictionaires Languag

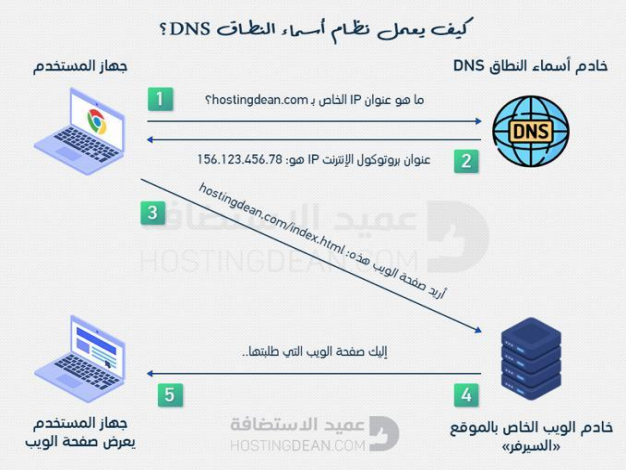
- **الكتب باللغة الأجنبية:**

1-David clark, characterizing cyberspace past present and future, MIT CASAIL, Version 1. 2 of March 2010

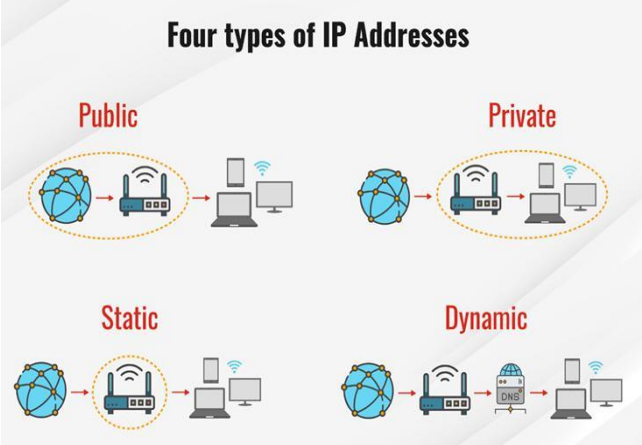
2-Umesh hodeghtta and umeshaa nayak ,the info sec handbook an introductioni to informations se curity apress open ,new york,

ملاحق

الملحق (1): نظام أسماء النطاقات DNS



الملحق(2): عنوان البرتكول IP



الملحق(3): محلل البرتكول

الملحق(4): جدار الحماية

الملحق (5): TLS

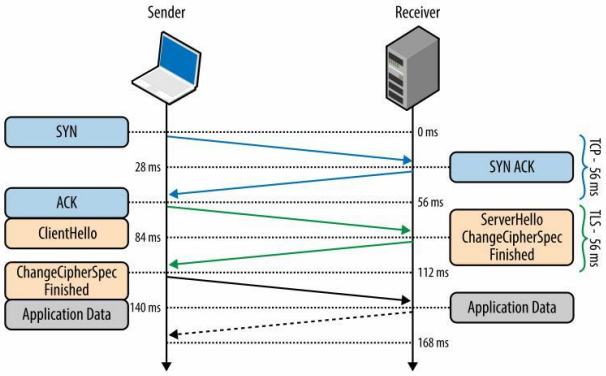
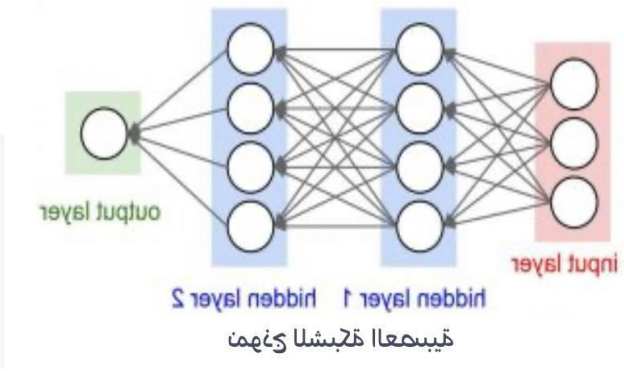


Figure 4-3. Abbreviated TLS handshake protocol

الملحق (6): DEEP BLUE

ملحق(7): العصبونات



ملحق(8): CHAT GPT

ملحق(9): دبوس أي ايه

فهرس المحتويات

فهرس المحتويات:.....

ملخص:.....

تهدف الدراسة إلى حل إشكالية حفظ أمن المعلومات في ظل الذكاء الاصطناعي وتم التطرق إلى:

– الفضاء السيبراني وأمنه كتمهيد لحل الإشكالية المطروحة من خلال التعرف على المفاهيم الأساسية للفضاء السيبراني والتي شملت تعريفه وبنيته وأخطاره، إضافة إلى الأمن السيبراني الذي تم تعريفه ودراسة أبعاده وعلاقته بالذكاء الاصطناعي.

وبناء على هذا تم ربط الأمن السيبراني وحفظ أمن المعلومات بالتطرق لمفهوم أمن المعلومات وكذا الأمن السيبراني كآلية لحفظ أمن وسلامة هذه المعلومات، هذا ما هيكلناه في الفصل الأول.

وقد توصلنا في الفصل الثاني إلى أن الذكاء الاصطناعي يحمي أمن المعلومات وفق جملة من الآليات والتحديات وذلك لاعتباره عنصرا فعالا في المجال التكنولوجي وباعتباره مجالا واسعا وبارزا في العصر الحديث.

summary

The study aims to solve the problem of maintaining information security in light of artificial intelligence, and it addressed:

- Cyberspace and its security as a prelude to solving the problem at hand through identifying the basic concepts of cyberspace, which included its definition, structure, and dangers, in addition to cybersecurity, which was defined and its dimensions and relationship to artificial intelligence studied.

Based on this, cybersecurity and preserving information security were linked by addressing the concept of information security, as well as cybersecurity as a mechanism for preserving the security and integrity of this information. This is what we structured in the first chapter.

In the second chapter, we concluded that artificial intelligence protects information security according to a number of mechanisms and challenges, as it is considered an effective element in the technological field and as a broad and prominent field in the modern era.