

مجلة العلوم القانونية والاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

الذكاء الاصطناعي نحو مواجهة التحديات السيبرانية

Artificial intelligence towards addressing cyber challenges.

يحي راوية^{1*}، كرماش هاجر²

¹ جامعة باتنة 1 ، (الجزائر)، rawia.yahia@univ-batna.dz

² جامعة باتنة 1، (الجزائر)، hajar.kermeche@univ-batna.dz

تاريخ النشر: 2025/03/01	تاريخ القبول: 2025/01/01	تاريخ ارسال المقال: 2024/12/01
-------------------------	--------------------------	--------------------------------

*المؤلف المرسل

الملخص:

مع تقدم التكنولوجيا وتطور أنظمة الذكاء الاصطناعي زادت تحديات الأمن السيبراني، في الوقت الحالي يشهد الفضاء السيبراني الكثير من الهجمات المعقدة والمتطورة، وأصبح من الضروري دمج التكنولوجيا التي تعتمد أساساً على أنظمة الذكاء الاصطناعي، لتتفاعل بشكل فعال مع التهديدات السيبرانية وتتصدى لها، من خلال قدرتها الهائلة في اكتشاف التهديدات قبل حدوثها والوقاية منها، وتحديد الأنماط التي قد تشير إلى هجومات إلكترونية، والتصدي للتحديات التي تطرحها التهديدات السيبرانية، علاوة على أن هذا الاستعمال يجب أن يكون موجه وخاضع إلى مجموعة من الضوابط والأسس يتم اعتمادها من قبل الدول والمنظمات على المستوى الدولي والإقليمي من أجل تفادي إساءة استعمال الذكاء الاصطناعي وتوجيهه نحو خدمة البشرية.

الكلمات المفتاحية: الذكاء الاصطناعي ; الهجوم السيبراني ; شبكات الكمبيوتر ; هجمات التصيد.

Abstract :

With technology progress and the development of artificial intelligence systems increased the challenges of cyber security, Currently a lot of cyberspace is witnessing complex and advanced attacks, it is necessary to integrate technology that depends mainly on artificial intelligence systems, to effectively interact with cyber threats and confront them, through its enormous ability to discover the threats before they occur prevention, and identify patterns that may refer to an electronic attack, and address the challenges posed by cyber security threats in addition this use must be prompt and subject to a range of controls and foundations is adopted by states and organizations at the local and regional levels, to avoid the abuse of artificial intelligence and directed towards human service.

Keywords: cyber attack; artificial intelligence; security; Computer networks, Distinguish attacks.

مقدمة:

أثرت التهديدات السيبرانية على الأمن القومي والبنية التحتية الأساسية في جميع أنحاء العالم، أين يتم استخدام الأجهزة الذكية والأنظمة المعلوماتية والتكنولوجيا للتأثير على الوظائف الحيوية في الدول الأخرى، حيث تستهدف أنظمة الكمبيوتر الحكومية والشبكات المالية والبنية التحتية المدنية، إذ أنه وبعد انتشار التكنولوجيا المتقدمة يمكن أن تؤدي الهجمات السيبرانية إلى أحداث شلل في البنية التحتية الحيوية والحاق الضرر بالاقتصاد في الدول المستهدفة، فالتحديات السيبرانية ليست بالضرورة هجمات تهدد البرامج التقنية فحسب بل تمثل هجمات تهدد الأمن الداخلي للدول أين تستهدف البنية التحتية الصناعية الحيوية وبالتالي فهي تؤثر على كل شيء.

في العصر الرقمي اليوم أدى الاعتماد المتزايد على التكنولوجيا الى ارتفاع التهديدات السيبرانية وتحديات الأمن السيبراني، ذلك لأن الأشخاص والهيئات والمنظمات يقومون بتخزين عدد هائل من المعلومات الحساسة عبر الأنترنت، مما يجعل الحاجة الى تدابير قوية في مجال الأمن السيبراني أمراً ضروريا وملحا أكثر من أي وقت مضى، واستجابة لتلك التحديات ظهرت تقنية الذكاء الاصطناعي كأداة فعّالة في تعزيز جهود الأمن السيبراني والتخفيف من المخاطر السيبرانية

أولاً: أهمية الموضوع.

ترجع أهمية هذا الموضوع الى أن الاعتماد على الذكاء الاصطناعي قد أحدث تغييرا كبيرا في مجال الأمن السيبراني، من خلال توفير تقنيات متقدمة قادرة على اكتشاف التهديدات واحتواء الهجمات والاستجابة للحوادث بطريقة فعّالة، وما لا يقل أهمية عن سابقته هو أن الأنظمة التي تعمل بالذكاء الاصطناعي يمكنها تحديد الأنماط والحالات الشاذة التي تشير الى احتمال وجود انتهاكات أمنية بشكل استباقي مما يجعل الأفراد والمؤسسات جاهزين للاستجابة لتلك التهديدات في الوقت المناسب، وهو ما يخفف من حدة الهجمات الالكترونية وينقص من آثارها.

السيبراني، والأسس التي تم وضعها من أجل التحكم في الذكاء الاصطناعي، وتوجيهه لخدمة البشرية وتفادي الهجمات السيبراني.

ثانياً: طرح الإشكالية.

مما لا شك فيه أن عملية ادراج الذكاء الاصطناعي في مجال الأمن السيبراني وتوظيفه في مواجهة التهديدات السيبرانية يقودنا الى طرح الإشكالية التالية: ما مدى فعالية ادراج تقنية الذكاء الاصطناعي في التصدي للهجمات السيبرانية؟

ثالثاً: أهداف الموضوع.

نهدف من خلال هذا المقال الى تسليط الضوء على كيفية إدارة الذكاء الاصطناعي في مجال الأمن السيبراني من خلال الوقوف على واقع الذكاء الاصطناعي في المجال السيبراني من خلال بيان تقنياته في اكتشاف التهديدات والوقاية منها، وتعزيز قدرات الاستجابة للحوادث في حالة حدوث خرق أمني، ناهيك عن الأضرار والمخاطر التي أن تترتب عند إساءة هذا الاستعمال والآثار المترتبة عليه، كما نهدف الى التعرف على الجهود الدولية المبذولة في سبيل تحقيق الأمن السيبراني

رابعاً: المنهج المتبع.

للإجابة على هذه الإشكالية ولتحقيق الأهداف المسطرة من هذه الورقة البحثية فقد قمنا باتباع المنهج التحليلي من خلال تحليل مختلف المعلومات والبيانات المتعلقة بموضوع الدراسة وإبراز دور الذكاء الاصطناعي في تحقيق الأمن السيبراني.

خامساً: هيكل الدراسة.

سوف نقوم بتقسيم الورقة البحثية الى محورين أساسيين، حيث يتعلق المحور الأول بتحديد المفاهيم الأساسية من خلال التعرف على المقصود بالذكاء الاصطناعي، وكذا تحديد المقصود بالهجمات السيبرانية، أما المحور الثاني فقد تناولنا من خلاله واقع الذكاء الاصطناعي في تعزيز الدفاع السيبراني من خلال التعرف على كيفية استغلال الذكاء الاصطناعي في التحول من الهجوم الى الدفاع، بالإضافة الى التطرق الى ضوابط استخدام هذه التقنية في المجال السيبراني.

المحور الأول: تحديد المفاهيم الأساسية.

ارتبط مؤخرا استعمال مصطلح الذكاء الاصطناعي بالهجمات السيبرانية، وفي هذا المحور سوف نقوم بتوضيح المقصود بالذكاء الاصطناعي، وكذا المقصود بالهجوم السيبراني.

أولاً: المقصود بالذكاء الاصطناعي.

بما أن نظم المعلومات تعرف ثورة هائلة فان وجود تطبيقات جديدة أصبح أمر حتمي، وهذا ما نراه من خلال تقنيات الذكاء الاصطناعي الذي يعدّ حقلاً جديداً، فالواقع يشير الى أن استخدامات الذكاء الاصطناعي تمتد لتدخل في كل المجالات التقنية التنموية والاقتصادية، الداخلية والخارجية التي لا يمكن حصرها أو عدّها. فالذكاء الاصطناعي يعتبر نقطة تحول كبيرة في تاريخ البشرية، ونظراً للأهمية المتزايدة لهذه التقنية سوف نحاول في هذا العنصر تعريف مصطلح الذكاء الاصطناعي وبيان أنواعه.

1/ تعريف الذكاء الاصطناعي.

مصطلح الذكاء الاصطناعي متكون من كلمتين، هما: الذكاء وكلمة الاصطناعي، وقبل الوقوف على تعريف الذكاء الاصطناعي، سوف نقوم بتقديم تعريف بسيط لمصطلح الذكاء، حسب قاموس Webster الذكاء: هو القدرة على فهم الظروف أو الحالات الجديدة والمتغيرة، والقدرة على ادراك وفهم وتعلم الحالات أو الظروف الجديدة، مما يعني أن الذكاء مرتبط بالإدراك وهو القدرة على الفهم والتعلم، أما كلمة الاصطناعي أو الصناعي، فهذا المصطلح مرتبط بالفعل يصنع أو يصطنع، بمعنى كل الأشياء التي تتميز وتختلف عن الأشياء الموجودة بالفعل والمولودة بصورة طبيعية خارج نشاط الانسان¹.

فيما يخص مصطلح الذكاء الاصطناعي فهناك عدّة تعاريف نذكر أهمها: الذكاء الاصطناعي Artificial Intelligence والذي يشار اليه باختصار (AI) يعتبر احدى الركائز التي تقوم عليها صناعة التكنولوجيا في العصر الحالي، ويعني قدرة الآلات والحواسيب الرقمية على القيام بمهام معينة تحاكي وتشابه تلك التي تقوم بها الكائنات الذكية، كالقدرة على التفكير والتعلم، ويهدف الذكاء الاصطناعي الى الوصول الى أنظمة تتمتع بالذكاء وتتصرف مثل البشر من حيث الفهم والادراك².

وقد عرّفه البعض بأنه: الذكاء الذي تبديه الآلات والبرامج، بما يحاكي القدرات الذهنية البشرية وأنماط عملها مثل: القدرة على التعلم والاستنتاج، ورد الفعل على أوضاع لم تبرمج في الآلة، كما أنه اسم لحقل أكاديمي يعني بكيفية صنع حواسيب وبرامج قادرة على اتخاذ سلوك ذكي³.

وقد عرفت المنظمة العالمية للملكية الفكرية (WIPO) بشأن الملكية الفكرية والذكاء الاصطناعي، الذكاء الاصطناعي: هو تخصص في علم الحاسوب يهدف الى تطوير آلات وأنظمة بإمكانها أن تؤدي مهامها ينظر إليها على أنها تتطلب ذكاءا بشريا سواء كان ذلك بتدخل بشري محدود أو بدون تدخل بشري ولأغراض هذه الوثيقة، الذكاء الاصطناعي يساوي عموما "الذكاء الاصطناعي الضيق"، ويقصد بذلك التكنولوجيات والتطبيقات المبرمجة لأداء مهام منفردة⁴.

من خلال التعاريف السابقة للذكاء الاصطناعي يتضح بأن هناك اجماع حول فكرة واحدة وهي أن الذكاء الاصطناعي هو مجموع القدرات الذهنية التي تحاكي الذكاء البشري والذي يتم تصنيعه من الانسان في الآلات والحواسيب بالشكل الذي يؤدي بالآلة الى الوصول الى نتيجة معينة بناء على المعطيات والبيانات والمعلومات التي يتم إدخالها دون التأثير بمؤثرات خارجية.

2/ أنواع الذكاء الاصطناعي.

يوجد ثلاث أنواع مختلفة للذكاء الاصطناعي تبعاً لما يتمتع به من قدرات نستعرضها فيما يلي:

أ/ الذكاء الاصطناعي المحدود أو الضيق: يعتبر الذكاء الاصطناعي المحدود أو الضيق أحد أنواع الذكاء الاصطناعي التي تستطيع القيام بمهام محددة وواضحة كالسيارات ذاتية القيادة، أو حتى برامج التعرف على الكلام أو الصور، أو لعبة الشطرنج الموجودة على الأجهزة الذكية، ويعتبر هذا النوع من الذكاء الاصطناعي أكثر الأنواع شيوعاً وتوافراً في وقتنا الحالي.

ب/ الذكاء الاصطناعي العام: وهو النوع الذي يمكن أن يعمل بقدرته تشابه قدرة الإنسان من حيث التفكير، إذ يركز على جعل الآلة قادرة على التفكير والتخطيط من تلقاء نفسها وبشكل مُشابه للتفكير البشري، إلا أنه لا يوجد أيّ أمثلة عملية على هذا النوع، فكل ما يوجد حتى الآن مجرد دراسات بحثية تحتاج للكثير من الجهد لتطويرها وتحويلها إلى واقع، وتعد طريقة الشبكة العصبية الاصطناعية: من طرق دراسة الذكاء الاصطناعي العام، إذ تعني بإنتاج نظام شبكات عصبية للآلة مُشابهة لتلك التي يحتويها الجسم البشري.

ج/ الذكاء الاصطناعي الفائق: يُعتبر الذكاء الاصطناعي الفائق النوع الذي قد يفوق مستوى ذكاء البشر، والذي يستطيع القيام بالمهام بشكل أفضل مما يقوم به الإنسان المتخصص وذو المعرفة، ولهذا النوع العديد من الخصائص التي لا بد أن يتضمنها، كالقدرة على التعلم، والتخطيط، والتواصل التلقائي، وإصدار الأحكام⁵.

ثانياً: تحديد المقصود بالهجوم السيبراني.

نشاهد أنه في السنوات الأخيرة أصبح استعمال تكنولوجيا المعلومات بشكل كبير في الكثير من المجالات، وهذا الاستعمال يكون على المستويين الاقليمي للدولة والعالمي، وقد أصبحت تلك الاستعمالات كمتجهات لارتكاب جرائم الأنترنت، وفي الآونة الأخيرة ازداد حجم وقوة الهجمات السيبرانية بشكل سريع وملحوظ، وهذه الهجمات تستهدف أنظمة معلومات الكمبيوتر أو البنية التحتية أو شبكات الكمبيوتر، ومن خلال هذا العنصر سوف نحاول تعريف الهجوم السيبراني مع بيان أنواعه.

1/ تعريف الهجوم السيبراني.

حسب تقرير لمنظمة الصحة العالمية فإن الهجوم السيبراني هو محاولة لإلحاق الضرر عمدا بشخص (مجموعة أشخاص) أو مؤسسة عن طريق شن هجوم على نظمهم الرقمية مثل: أجهزة الحاسوب لسرقة البيانات و التطبيقات التي يعتبرونها سرية أو يعتمدون عليها، أو العبث بتلك البيانات أو التطبيقات أو تعطيل الوصول إليها أو تدميرها⁶.

أمّا بالنسبة للدكتور Jeetendra Pande فقد عرّف الهجوم السيبراني بناءً على أنواعه، واعتبر أن الهجوم السيبراني قد يكون داخلي وقد يكون خارجي، كما قد يكون منظم أو غير منظم، ولكن في كل الأحوال فإن هذه الهجمات تشكل جريمة سيبرانية، يتم تنفيذها من قبل مجرمين تستهدف المؤسسات المالية الكبيرة والمؤسسات الدفاعية والنووية⁷.

فالهجوم السيبراني عبارة عن عملية اقتحام لأنظمة الكمبيوتر والشبكات سواء خاصة بالأفراد أو شركات أو مؤسسات من قبل مخترقين مجرمين بهدف إحداث أضرار متعددة.

أمّا المهاجمون أو المخترقون يطلق عليهم اسم "مجرمو الأنترنت"، وهم الذين يهتمون بكسب المال عن طريق الاحتيال أو من بيع معلومات قيمة، المنافسون الصناعيون وأجهزة المخابرات الأجنبية، المهتمون بالحصول على ميزة اقتصادية لشركاتهم أو بلدانهم، نشطاء القرصنة الذين يرغبون في مهاجمة الدول لدوافع سياسية أو أيديولوجية⁸.

2/ أنواع الهجمات السيبرانية.

تتخذ الهجمات السيبرانية عدة أنواع نذكر أهمها وأكثرها خطورة.

أ/ الهجوم السيبراني من خلال استخدام البرامج الضارة: هذا الهجوم يتم من خلال برامج تصيب الأنظمة بطريقة خفية في الغالب لانتهاك سرية أو سلامة ودقة أو توافر البيانات أو التطبيقات أو نظم التشغيل⁹.

في هذه الحالة يجب توخي الحذر من قبل الأشخاص الذين يستعملون البرامج أو التطبيقات دون معرفة مصدرها، لأنها قد تكون برامج تجسس أو تطبيقات تحمل فيروسات يمكنها التكاثر والانتشار عبر الشبكات، بشكل يؤدي إلى تعطيل الأجهزة أو إيقافها أو إتلاف المعلومات الموجودة في أجهزة الكمبيوتر أو شبكات الكمبيوتر.

ب/ الهجوم السيبراني من خلال جمع ومراقبة معلومات الأعداء (التجسس): عادة ما تقوم دفاعات شبكات الكمبيوتر بمراقبة الأعداء والتجسس عليهم باستخدام أدوات اختراق الأنظمة¹⁰.

حيث يهدف من خلال هذه الهجمات الحصول على معلومات حساسة لأغراض ضارة وخبيثة.

ج/ الهجوم السيبراني من خلال الحرمان من الخدمات: تعمل هجمات الحرمان من الخدمات على اقتحام الأنظمة أو الخوادم أو الشبكات بهدف السيطرة على مواردها ومعدل نقل بياناتها، حيث يصبح النظام غير قادر على تلبية الأوامر اللازمة أو المطلوبة منه¹¹.

يتم من خلال هجمات الحرمان من الخدمات تعطيل النظام ومحاولة جعل الخدمة غير متوفرة.

المحور الثاني: واقع الذكاء الاصطناعي في تعزيز الدفاع السيبراني.

مع زيادة التحديات التي تواجه الأمن السيبراني، فبينما يوفر العصر الرقمي مزايا كبيرة إلا أنه قد فتح المجال أمام مخاطر عديدة وجديدة ومستحدثة تواجه الأفراد وتهدد الحكومات من قبل المحتالين والجرمين، زادت الضرورة إلى استخدام تقنيات متقدمة ومتطورة تعنى بحماية الأنظمة والبيانات تتمثل أساسا في تقنيات الذكاء الاصطناعي وفي هذا المحور سوف نتناول استغلال تقنيات الذكاء الاصطناعي من الهجوم إلى الدفاع، ثم نتطرق إلى ضوابط استخدام الذكاء الاصطناعي في المجال السيبراني.

أولا: استغلال الذكاء الاصطناعي في التحول من الهجوم إلى الدفاع.

تطرقنا سابقا إلى أنواع الهجمات السيبرانية، ووجدنا أن هذه الهجمات تعتبر تهديدا للأمن السيبراني، حيث كانت تعتمد أساسا على تقنيات الذكاء الاصطناعي، وردا على هذه الهجمات السيبرانية وانطلاقا من مبدأ خلق الترياق من مادة السم نفسها، فقد سارعت الدول ومجتمع الأمن السيبراني إلى تسخير إمكانيات الذكاء الاصطناعي لتعزيز الدفاع السيبراني واستغلال تقنياته في التحول من الهجوم إلى الدفاع، وذلك من خلال الاعتماد على التقنيات الرقمية وتحويلها على نحو يتماشى مع الهجمات السيبرانية ويتصدى لها.

في الواقع فإننا نلاحظ تطور كبير في الأجهزة الذكية والأنظمة الرقمية والأنترنت التي يمكنها أن تتفاعل مع الهجمات السيبرانية التي أصبحت هي الأخرى أكثر تقدما وتعقيدا، حيث يسعى المهاجمون إلى البحث عن نقاط الضعف من أجل تلبية حاجاتهم واشباع رغباتهم المختلفة.

في البداية كان التصدي للهجمات السيبرانية يتم بشكل تقليدي وبسيط، حيث يتمثل في برامج مكافحة الفيروسات وغيرها من برامج توفير الحماية، إلا أنّ تطور تقنيات الذكاء الاصطناعي بات يشكل تهديدا فعليا على المجتمع الدولي، من خلال استغلاله في شن هجمات غير متوقعة ومعقدة يمكنها إحداث اضطراب هائل و رهيب، لذلك بات من الضروري الاعتماد على تقنيات الذكاء الاصطناعي ودمجه في مجال الأمن السيبراني، من أجل تطوير آليات الدفاع وتعزيز الجهود الأمنية له، وفي هذا السياق سوف نستعرض بعض التقنيات التي يتم الاعتماد عليها في مواجهة الهجمات السيبرانية، وسوف نذكرها على سبيل المثال وليس على سبيل الحصر، إلا أننا سوف نحاول التعرف على كيفية الانتقال من وضعية الهجوم إلى وضعية الدفاع باستغلال تقنيات الذكاء الاصطناعي.

1/ الكشف المسبق عن التهديدات والتخفيف من حدتها.

يمكن الكشف عن التهديدات والاختراقات بشكل مسبق من خلال استخدام تقنيات التعلم العميق وتحليل البيانات للكشف عن التهديدات السيبرانية والاختراقات المحتملة، كما يمكن للأنظمة التي تعمل بالذكاء الاصطناعي تحليل حركة مرور الشبكة وسلوك المستخدم لتحديد الأنماط غير العادية التي تشير إلى هجوم إلكتروني، والكشف المبكر للتهديدات والاستجابة السريعة¹².

حيث من خلال البرامج التي تعتمد على الذكاء الاصطناعي في عملها يتم اكتشاف الحالات التي تشكل تهديدا للأمن السيبراني بشكل مبكر وبذلك يمكن اتخاذ تدابير استباقية للتخفيف من الضرر وتعزيز جهود الاستجابة للحوادث.

2/ تحليل المعلومات ومعالجة البيانات المتعلقة بالأمن السيبراني.

يمكن للذكاء الاصطناعي تحليل كميات هائلة من البيانات والمعلومات والبرمجيات أثناء اتخاذ القرار مما يتيح الكشف المبكر عن نقاط الضعف غير المكتشفة والمخاطر الأمنية الخفية¹³.

3/ تعزيز القدرات الاستخباراتية والمعلوماتية.

يمكن توظيف تقنيات الذكاء الاصطناعي في عمليات التشخيص والاستطلاع والتحقق من الهوية من خلال جمع البيانات والمعلومات ورفع فاعلية التقنيات الحيوية وزيادة دقتها، وكذلك تطوير قدرات التشفير والأمان السيبراني، وذلك ما يحمي البيانات والمعلومات الحساسة من الاختراق¹⁴.

4/ تأمين الشبكات وتخفيض هجمات التصيد.

يعمل الذكاء الاصطناعي على تسريع عملية انشاء السياسات الأمنية وتحديد تصميم شبكات المؤسسات، بالإضافة الى ادارة عدد كبير من الأجهزة وتحديثها وتصحيح الأمان فيها تلقائيا¹⁵.

5/ التوفير والتقليل من التكاليف.

تتأثر المؤسسات ماليا بانتهاكات للبيانات كل عام لا يمكن تجاهلها ولا يمكن إيقاف الجرمين، حيث وجدت الدراسة فرقا شاسعا في توفير التكاليف للمنظمات التي تستخدم الذكاء الاصطناعي لأغراض الأمن السيبراني^{2.9} مليون دولار مقارنة بـ 671 مليون دولار للمرافق التي لا تستخدم الخدمة¹⁶.

ثانيا: ضوابط استخدام الذكاء الاصطناعي في المجال السيبراني.

أسفر نضوج عصر المعلومات على ضرورة تكييف قوانيننا ولوائحنا وسياساتنا وتطويرها بعض الشيء مع ما يتمشى وسرعة هذه المعلومات ومكانتها، حيث يمثل الذكاء الاصطناعي تحد جديد للقانون على عدة مستويات وهذا من حيث امكانية تطبيق القواعد القانونية الموجودة على جميع المسائل القانونية التي يمكن أن يثيرها الذكاء الاصطناعي في المجال السيبراني.

من الجدير بالذكر أن الذكاء الاصطناعي هو استخدام أنظمة الكمبيوتر، لتنفيذ مهام تتطلب إدراكا أو تخطيطا أو استدلالا أو تعلمًا، هذه المهام ترتبط عادة بالذكاء البشري، وكما ذكرنا سابقا أنه يتم عبر أنظمة الذكاء الاصطناعي ادخال مجموعة من البيانات، وتدريبها على التعلم والتعامل مع هذه البيانات، لتنتهي في الأخير الى اتخاذ مجموعة من القرارات، واتباع طرق تواجه وتعالج مجموعة هائلة من المتطلبات، فهي عبارة عن برمجيات أو خوارزميات ممكن تدريبها على العديد من المهام، الا أن استخدامها يترتب آثارا عديدة ممكن في غالب الأحيان أن تنطوي على خطورة خاصة عند اتخاذ قرارات خاطئة، بالإضافة الى أن فهمها من قبل الأفراد لا يزال منقوصا، لذلك لابد لهذه التقنية من ضوابط وأسس لاستعمالها، ولكن قبل الحديث عن أسس استخدام تقنية الذكاء الاصطناعي في المجال السيبراني، لابد من الحديث عن المخاطر التي تنطوي عليها هذه التقنية على المجال السيبراني.

1/ مخاطر استخدام الذكاء الاصطناعي على المجال السيبراني.

على الرغم من الايجابيات التي يحققها استخدام الذكاء الاصطناعي في المجال السيبراني، إلا أن هناك عدة مخاطر تواجه هذا الاستخدام وهي:

أ/ التحيز في صنع القرار: في حال استخدام أنظمة الذكاء الاصطناعي القائمة على مجموعات البيانات التي تحتوي على معلومات أو خوارزميات متحيزة في مجال الأمن السيبراني، فقد يؤدي ذلك إلى قرارات تمييزية ضد جماعات أو أفراد معينين وأن تكون لها عواقب وخيمة على المنظمة.

ب/ الافتقار إلى القابلية للتفسير والشفافية: تتسم الخوارزميات المستخدمة لاتخاذ قرارات بشأن التهديدات الأمنية بعدم الشفافية في كل الأوقات، وهو ما يصعب من تفسير قرارات الذكاء الاصطناعي السيئة، ويُفقد القدرة على تحسينها، وبالتالي يتأثر أمن المنظمة بالسلب.

ج/ الاستخدام الضار للخوارزميات: على الرغم من أن خوارزميات الذكاء الاصطناعي تعمل على البحث في البيانات واكتشاف الأنماط بسرعة، إلا أن الجهات الضارة تستطيع استخدامها في الوصول إلى المعلومات الحساسة، أو مهاجمة البنية التحتية، كما يمكن للمهاجمين السيبرانيين أيضاً الاستفادة من الذكاء الاصطناعي في شن هجمات أكثر تعقيداً من خلال التعلم من البيانات لفهم الأهداف ونقاط الضعف المحتملة بشكل أفضل¹⁷.

د/ إساءة استخدام الذكاء الاصطناعي: قد يضر الذكاء الاصطناعي بالأمن السيبراني عندما يُستخدم في أغراض ضارة مثل إنشاء أخبار مزيفة أو نشر دعاية سلبية.

هـ/ انتهاك خصوصية البيانات: هناك العديد من المخاوف المثارة بشأن خصوصية البيانات التي تعالجها وتحللها تطبيقات الذكاء الاصطناعي في الأمن، إذ أن تلك التطبيقات قادرة على التعرف على تلك البيانات، وهو ما يفرض ضرورة الامتثال للوائح الخصوصية من خلال الفحص القانوني قبل نشر أنظمة الذكاء الاصطناعي¹⁸.

2/ أسس استخدام الذكاء الاصطناعي في المجال السيبراني.

يتم استعمال تطبيقات وأنظمة الذكاء الاصطناعي على الفضاء السيبراني الذي لا تحدّه ولا تحيط به حدود وبشكل متسارع، لذلك يجب تنظيم استعمال هذه التطبيقات بشكل كلي، لأنه توجد حافة كبيرة يتم السقوط منها إذا تم الاستمرار في حل كل مشكلة عند ظهورها، فالمشاكل تتطور بشكل تدريجي وبطريقة عشوائية مع تطور التكنولوجيا، بحيث تكون غير خاضعة للرقابة من قبل الدول، ولأن الاستعمال العشوائي لهذه التقنية قد ينتج عنه مخاطر وأضرار لا يمكن تداركها، ولأن الجريمة السيبرانية هي جريمة دولية عابرة للحدود أدّت الى خلق تحديات كبيرة لتقييم عدم المشروعية الدولية المحتملة للعمليات السيبرانية، كما أن الدول وحدها لا تستطيع تنظيم مجال استخدام تقنيات الذكاء الاصطناعي في الفضاء السيبراني بشكل فعال لأنه يتجاوز سيادتها الإقليمية، كما أن العديد من موارد الأنترنت الرئيسية غير خاضعة لسيطرة الدول، كان من الضروري وضع نظام شامل على المستوى الدولي يعني بتنظيم وتوجيه الذكاء الاصطناعي في الفضاء السيبراني.

أ/ الأمم المتحدة: تلعب الأمم المتحدة دوراً أساسياً في إطار مكافحة الجريمة السيبرانية وتحقيق العدالة عن طريق تعزيز تبادل المعرفة والخبرات بين الأخصائيين من مختلف الدول وإلى تدعيم التعاون الدولي والإقليمي في مكافحة الجريمة وقد كان لمؤتمر الأمم المتحدة الذي تم انعقاده في مدينة ميلانو الإيطالية عام 1985 دوراً في اتخاذ مجموعة من القواعد التوجيهية، التي تهدف إلى تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا في كل مكان

لصالح الجمهور وبالتالي لمنع الجريمة وأكد على أن تقنيات التكنولوجيا الجديدة قد تولد أشكالاً جديدة للجريمة فإنه ينبغي اتخاذ تدابير ملائمة ضد حالات إساءة الاستعمال¹⁹.

ومع التطور السريع لتقنيات الذكاء الاصطناعي في الآونة الأخيرة أصبح الفضاء السيبراني يشهد الكثير من الجرائم الخطيرة والمعقدة، لذلك أقر الأمين العام للأمم المتحدة "أنطونيو غوتيريش" بأن التطور السريع في التقنيات الرقمية وارتباطها بعدة مجالات يكشف عن نقاط ضعف، مما يعرض الأفراد والمؤسسات والدول إلى التهديدات السيبرانية، وفي إطار توجيه استخدام الذكاء الاصطناعي للدفاع السيبراني والوقاية من الهجمات السيبرانية، أكد على ضرورة تعزيز التعاون في مواجهة التحديات الحاسمة وإعادة تنشيط النظام متعدد الأطراف، وإعادة تأكيد الاجماع العالمي بشأن حماية البنية التحتية من ممارسات تكنولوجيا المعلومات والاتصالات الضارة، وفي سبيل ذلك تعمل الهيئة الاستشارية المعنية بالذكاء الاصطناعي على استكمال التقرير النهائي حول الكيفية التي يمكنها بها إدارة الذكاء الاصطناعي لصالح البشرية²⁰.

ب/ المجلس الأوروبي: بالنسبة للمجلس الأوروبي فقد أدى التطور السريع في مجال الحاسبات وتقنية الإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجنائية، الشيء الذي عجل إلى إصدار التوصية رقم 13 / 95 بتاريخ 11 / 09 / 1995 بخصوص مشاكل الإجراءات الجنائية المتعلقة بالتكنولوجيا وتكنولوجيا المعلومات، وعقوبات تتناسب مع التنمية في هذا المجال، ومواكبة لتطور تقنيات الكمبيوتر، فقد أبرم المجلس الأوروبي اتفاقية بودابست في: 8 / 11 / 2001 التي تعتبر أولى المعاهدات الدولية في مكافحة جرائم الإنترنت، ووضعت للمصادقة بتاريخ: 23 / 11 / 2001 والتي تضمنت التعريف بأهدافها ووضعت قائمة للجرائم التي يجب على الدول المصادقة عليها أن تحرمها في قوانينها الداخلية²¹.

ج/ الاتحاد الأوروبي: أما فيما يخص الاتحاد الأوروبي فقد كان له دور فعال في مجال الأمن السيبراني، فقد تم انشاء وكالة الاتحاد الأوروبي للأمن السيبراني **European Union Agency for Cybersecurity** والتي تعرف اختصاراً **ENISA** هي وكالة تابعة للاتحاد الأوروبي، تم إنشائها عام 2004 بموجب لائحة الاتحاد الأوروبي رقم 460/2004 تعمل منذ 01 سبتمبر 2005، تعمل الوكالة بشكل وثيق مع الدول الأعضاء في الاتحاد الأوروبي وأصحاب المصلحة الآخرين لتقديم المشورة والحلول بالإضافة إلى تحسين قدرات الأمن السيبراني لديهم، كما أنها تدعم تطوير استجابة تعاونية لحوادث أو أزمات الأمن السيبراني واسعة النطاق عبر الحدود، ومنذ عام 2019 تقوم بوضع خطط لإصدار شهادات الأمن السيبراني.

تساعد وكالة الاتحاد الأوروبي للأمن السيبراني المفوضية الأوروبية والدول الأعضاء، في تلبية متطلبات الشبكة وأمن المعلومات، بما في ذلك تشريعات الاتحاد الأوروبي الحالية والمستقبلية، كما تسعى الوكالة في النهاية إلى العمل كمركز خبرة لكل من الدول الأعضاء ومؤسسات الاتحاد الأوروبي لطلب المشورة بشأن الأمور المتعلقة بأمن الشبكات والمعلومات، تدعم الوكالة تنظيم تمارين الأمن السيبراني لكافة دول أوروبا "Cyber Europe" منذ عام 2010، وقد تم تحديد سبعة تهديدات رئيسية للأمن السيبراني خلال الأشهر الماضية من سنة 2024،

وتصدّرت التهديدات ضد التوافر القائمة، تليها برامج الفدية والتهديدات ضد البيانات، ويقدم التقرير نظرة متعمقة ذات صلة بكل منها من خلال تحليل عدّة آلاف من أحداث الأمن السيبراني المبلغ عنها علناً²².

نظمت أكاديمية القانون الأوروبي الحدث الثالث عشر لشبكة خبراء حماية البيانات التابعة لليوروبول (EDEN) بالتعاون مع الأكاديمية الأوروبية للقانون، وتناول الحدث الآثار المترتبة على حماية البيانات والأمن السيبراني على إنفاذ القانون وما بعده.

وفي إطار توجيه استعمالات تقنيات الذكاء الاصطناعي في مواجهة الجريمة السيبرانية تم عقد مؤتمر "حماية البيانات والأمن السيبراني كأعمال أساسية لإنفاذ القانون"، يومي 16 و 17 سبتمبر 2024 في مقر اليوروبول في لاهاي، أين تم التركيز على الفرصة المتاحة لإنفاذ القانون للاستفادة من التقنيات المتقدمة مع الحفاظ على المعايير الأخلاقية وتلبية المتطلبات القانونية، وقد تضمن المؤتمر العلاقة الحاسمة بين قانون الذكاء الاصطناعي ولوائح حماية البيانات، وخاصة في سياق التحقيقات القائمة على البيانات وإنفاذ القانون، كما تم تسليط الضوء على الأهمية المتزايدة للتعاون بين أجهزة إنفاذ القانون، والأكاديميين والعلماء، للتنقل بفعالية في المشهد الرقمي المتطور، حيث تتطور المخاطر باستمرار، الشيء الذي يتطلب وضع الأسس والضوابط من خلال التصميم والتطبيق منذ البداية. والتنقل عبر تعقيدات إدارة المعلومات الحساسة بطريقة تحافظ على الثقة العامة وسيادة القانون²³.

د/ الاتحاد الافريقي: لقد تزايد الاهتمام بالمجال السيبراني الشيء الذي أدّى الى اصدار المشروع الأولي لاتفاقية الاتحاد الافريقي حول الثقة والأمن في الفضاء الرقمي، وقد تم وضعه للنقاش سنة 2013 بالتعاون بين مفوضية الاتحاد الافريقي ولجنة الأمم المتحدة الاقتصادية لافريقيا "CEA" وقد اعتمده رؤساء الدول والحكومات المجتمعين في مالابو بغينيا الاستوائية خلال الدورة العادية رقم 23 لمؤتمر الاتحاد الإفريقي يومي 26 و 27 جوان 2014، وبالتالي أصبح المشروع اتفاقية مفتوحة للمصادقة مع تعديل تسميتها، لتصبح اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية البيانات ذات الطابع الشخصي، والتي تسمى اختصاراً "اتفاقية مالابو"، حيث تشكل الاتفاقية نص قانوني استراتيجي في مجال مكافحة الجرائم الالكترونية في افريقيا، بحيث تعالج مسألة الأمن السيبراني بتوسع²⁴.

هـ/ المشرع الجزائري: ركزت الجهود الجزائرية على تحقيق الأمن السيبراني من خلال اتخاذ مجموعة من التدابير التشريعية والمؤسسية، وفي سبيل ذلك فقد تم اصدار القانون رقم 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها²⁵، كما استحدثت قسم في قانون العقوبات تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات ونص من خلاله على الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، وقد جاء ذلك نتيجة تأثر المشرع الجزائري بما ورد في اتفاقية بودابست التي وضعت للمصادقة بتاريخ: 23 / 11 / 2001 ومن ويمكن ذكر الجرائم التي نص عليها المشرع الجزائري بموجب قانون العقوبات في المواد من 394 مكرر الى غاية المادة 394 مكرر 7 من قانون رقم 15/04 مؤرخ في 10 نوفمبر 2004 يعدّل ويتمم الأمر رقم 156/66 يتضمن قانون العقوبات²⁶، فيما يلي:

- جريمة المساس بأنظمة المعالجة الآلية للمعطيات عن طريق الغش والتدليس.

- جرائم نشر أو حيازة أو الاتجار بالمعطيات المخزنة أو المعالجة.
 - جرائم المعالجة الآلية الماسة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام.
 - الجرائم المعلوماتية لمشخص المعنوي.
 - جريمة تكوين جمعية أشرار المعلوماتيين لغرض التحضير للجرائم الماسة بأنظمة المعالجة الآلية.
- بالإضافة الى تسخير مجموعة من الهيئات والأجهزة التي تعنى بمكافحة الجريمة السيبرانية وتوفير الأمن السيبراني والتي تتمثل فيما يلي:

- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.
 - مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة.
 - المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.
 - مركز الوقاية من جرائم الاعلام الآلي والجرائم المعلوماتية التابعة للقيادة العامة للدرك الوطني.
 - المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني التابع للقيادة العامة للدرك الوطني²⁷.
- وبما أن الجريمة السيبرانية ذات أبعاد دولية وعالمية، ومن أجل تعزيز التعاون الدولي في مجال مكافحة الجريمة السيبرانية . فقد انضمت الجزائر الى العديد من الاتفاقيات الدولية التي نصت على ضرورة التعاون الدولي من أجل مواجهة هذه الجرائم بما فيها التعاون القضائي والأمني، على غرار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات²⁸، وكذا الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية²⁹.

الخاتمة:

لقد أصبح استعمال تقنية الذكاء الاصطناعي في المجال السيبراني مغيرا لقواعد اللعبة، نظرا لاستعماله في مواجهة التحديات والتهديدات السيبرانية، الشيء الذي يجعله ضرورة لا مفر منها، خاصة وأنه يوفر إمكانيات متقدمة وفعالة في اكتشاف التهديدات والاستجابة للحوادث وإدارة المخاطر، فمن خلال تلك التقنيات يمكن للمؤسسات أن تكوّن جدار لحماية المعلومات والبيانات الحساسة وتمنع عملية اختراقها، كما يمكنها تعزيز دفاعات الأمن السيبراني من الهجمات المتطورة والمعقدة.

بالرغم من كل ذلك تجدر الإشارة الى أن استعمال الذكاء الاصطناعي قد يشكل في حدّ ذاته خطرا على تلك المؤسسات عند إساءة استعماله أو خروجه عن السيطرة، أين يجب المضي قدما بحذر تجاه هذه التقنية من أجل ضمان استخدامه لصالح البشرية بشكل مسؤول ومفيد، ومن خلال هذه الورقة البحثية توصلنا الى مجموعة من التوصيات من أجل معالجة الآثار الجانبية التي يمكن أن تترتب على استعمال الذكاء الاصطناعي في المجال السيبراني وتحقيق الغاية من استعماله في مواجهة التحديات السيبرانية:

- مراقبة وتفحص أنظمة الذكاء الاصطناعي عند عملية اتخاذ القرار لتفادي اتخاذ قرارات تمييزية وعنصرية والتي تكون لها عواقب وخيمة.
- التطور السريع للذكاء الاصطناعي يجعله يساهم في تعزيز قدرات الهجمات السيبرانية، لذلك يجب توجيه هذا الاستعمال من أجل رفع إمكانيات مواجهة تلك التهديدات والهجمات.

- بالرغم من أن دمج الذكاء الاصطناعي في المجال السيبراني يعتبر فعالاً في مواجهة التهديدات السيبرانية إلا أنه يجب أن تكون هناك ضوابط وأسس لهذا الاستخدام وهذا الدمج لأنه قد يتم إساءة استعمال الذكاء الاصطناعي من قبل جهات خبيثة بشكل يؤدي الى مخاطر وأضرار كبيرة.
- تتميز أنظمة الذكاء الاصطناعي المدمج في المجال السيبراني بالاستقلالية الا أنه يجب خلق التوازن بين الاستقلالية والاشراف البشري من أجل تفادي المسؤولية عند اتخاذ الذكاء الاصطناعي قرار تنتج عنه عواقب وخيمة وغير مقصودة.
- الحاجة الى تدريب وتكوين أفراد على المستوى الدولي من أجل خلق قوة عاملة وماهرة ومتمكنة من كل تعقيدات الأمن السيبراني وكذا تعقيدات الذكاء الاصطناعي.
- اتلاع نهج شامل للأمن السيبراني من خلال تعزيز التعاون بين الدول والمنظمات والمؤسسات على المستوى العالمي ووضع قوانين دولية للذكاء الاصطناعي وتوجيه استخدامه في مجال الأمن السيبراني للاستجابة بفعالية لمشهد التهديدات المتطورة.
- بما أن الهجمات السيبرانية عابرة للحدود الدولية يجب على الدولة الجزائرية تكثيف الجهود على جميع المستويات، التشريعية والتنظيمية والمؤسسية، وتعليم وتدريب أشخاص ورفع المهارات لتزويد المتخصصين في المجال السيبراني بالخبرة والمعرفة لتسخير الذكاء الاصطناعي بشكل فعال.

الهوامش:

- 1 خالد زواتين، الذكاء الاصطناعي وحقوق الملكية الفكرية أي علاقة ترابطية؟، مجلة حقوق الانسان والحريات العامة، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد ابن باديس، مستغانم، مجلد 07، عدد 02، 2022، ص-ص 137-163، ص 142
- 2 خليل سعيد، مرزوق بن مهدي، الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبراني، مجلة دراسات في حقوق الانسان، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، 2022، ص-ص 25-37، ص 29.
- 3 دليلة العوفي، الحرب السيبرانية في عصر الذكاء الاصطناعي ورهائتها على الأمن الدولي، مجلة الحكمة للدراسات الفلسفية، كلية الحقوق والعلوم السياسية، جامعة الجزائر 03، مجلد 09، عدد 02، 2021، ص 08.
- 4 المنظمة العالمية للملكية الفكرية، محادثة الويبو بشأن الملكية الفكرية والذكاء الاصطناعي، الذكاء الاصطناعي والملكية الفكرية، 2020/06/09، متوفر على الموقع الالكتروني: www.wipo.int ، تاريخ الاطلاع: 2024/09/06 على الساعة: 13 و 17د.
- 5 خليل سعيد، مرزوق بن مهدي، مرجع سابق، ص 29.
- 6 منظمة الصحة العالمية، الهجمات السيبرانية على البنية التحتية الصحية الحيوية، 2024/02/06، متوفر على الموقع الالكتروني: www.who.int تاريخ الاطلاع: 2024/09/06 على الساعة 21 و 35د.
- 7 Pand jeetendra, Introduction to cyber security, uttarahkand university, India, 2017, p.p 16.17
- 8 , disponible sur le site : 2016 National cyber security centre, cyber attacks white paper, 16/01/2016, www.sans.org date de consultation : 22h26m.
- 9 المركز الوطني الارشادي للأمن السيبراني، الهيئة الوطنية للأمن السيبراني، ماهو الهجوم السيبراني؟، 2020/02/16، متوفر على الموقع الالكتروني: www.cert.gov.sa تاريخ الاطلاع: 2024/09/20 على الساعة: 16 و 45د.
- 10 إيمان علام أحمد، الهجمات السيبرانية (الحرب الالكترونية) واستخدام القوة المسلحة في القانون الدولي العام (الاستغلال السيبراني)، مجلة الدراسات القانونية والاقتصادية، جامعة بنها، مصر، مجلد 05، عدد 04، 2023، ص-ص 446-480، ص 456.

- ¹¹ شركة تقنين للمحاماة والاستشارات القانونية، أنواع الهجمات السيبرانية وكيفية الوقاية منها، 2024/04/20، متوفر على الموقع الإلكتروني : www.ae.linkedin.com تاريخ الاطلاع: 2024/08/12 على الساعة 23 و 47د.
- ¹² فيصل بن عبد العزيز الفوزان، دور الذكاء الاصطناعي في تطوير استراتيجيات الأمن السيبراني، 08 سبتمبر 2023 متوفر على الموقع الإلكتروني: www.maal.com تاريخ الاطلاع 2024/08/16، على الساعة 23 و 20د.
- ¹³ Hu,ied Ismail, Improving cybersecurity systems using artificial intelligence techniques, International journal of artificial intelligence and mechatronics, yamen, volume11, issue05, 2023, p60.
- ¹⁴ مركز المستقبل للأبحاث والدراسات المتقدمة، كيف يدير الذكاء الاصطناعي دقة الحروب الحديثة؟ 20 ماي 2024 متوفر على الموقع الإلكتروني: www.futureuae.com تاريخ الاطلاع 10/سبتمبر 2024 على الساعة 14 و 40د.
- ¹⁵ الهيئة الوطنية للأمن السيبراني، تطبيقات الذكاء الاصطناعي في الأمن السيبراني، 26 أكتوبر 2021، متوفر على الموقع الإلكتروني: www.cert.gov.sa تاريخ الاطلاع: 2024/09/26 على الساعة 23 و 32د.
- ¹⁶ محمد دحماني، الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي، الأغواط، 2023، ص-ص 597-608، ص 606.
- ¹⁷ بكة، الذكاء الاصطناعي والأمن السيبراني: العلاقة والفرق بينهما وتحدياتهما، تحديات الأمن السيبراني في عصر الذكاء الاصطناعي، 25 جوان 2024 متوفر على الموقع الإلكتروني: www.bakkah.com تاريخ الاطلاع: 2024/09/22 على الساعة 15 و 15د.
- ¹⁸ سكاى نيوز عربية، ماهي أبرز تحديات الأمن السيبراني مع تقدم الذكاء الاصطناعي، الأمن السيبراني يثير قلقاً، 20 أكتوبر 2023، متوفر على الموقع: www.skynezsarabia.com تاريخ الاطلاع 2024/09/26 على الساعة 22 و 10د.
- ¹⁹ سليمان قطاف، عبد الحليم بوقرين، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، مجلد 05، عدد02، 2022، ص-ص 62-87، ص74.
- ²⁰ تقرير أنطونيو قوتريش، الأمين العام للأمم المتحدة بشأن التصدي للتهديدات الناشئة في الفضاء الإلكتروني، الأمم المتحدة، 20 جويلية 2024، متوفر على الموقع الإلكتروني: www.webtv.un.org تاريخ الاطلاع: 2024/09/22 على الساعة 22 و 20د.
- مراد مشوش، الجهود الدولية في مكافحة الاجرام السيبراني، مجلة الواحات للبحوث والدراسات، كلية الحقوق والعلوم السياسية، جامعة غرداية، مجلد12، عدد 02، 2019، ص-ص 703-726، ص 25. ²¹
- ²² European union agency for cyber security, enisa 2024 enisa threat lands cap 2024, 19 septembre 2024, available on the website: www.enisa.europa.eu, date viewed 26/09/2024, in the time 22h15m.
- ²³ الاتحاد الأوروبي، شبكة حماية البيانات التابعة لليوروبول، 20 سبتمبر 2024، متوفر على الموقع الإلكتروني: www.ungeneva.org تاريخ الاطلاع عليه: 2024/09/27 على الساعة 22 و 24د.
- ²⁴ مريم لوكال، قراءة في اتفاقية الاتحاد الافريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة2014، مجلة الدراسات القانونية والاقتصادية، مجلد 04، عدد03، 2021، ص-ص 657-673، ص 651.
- ²⁵ القانون رقم 04/09 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الصادر في الجريدة الرسمية عدد 47 الصادرة بتاريخ: 16 أوت 2009.
- ²⁶ القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 يتضمن قانون العقوبات الصادر بموجب الجريدة الرسمية عدد 71 الصادرة بتاريخ 10 نوفمبر 2004.
- ²⁷ آسيا لعمراني، التعاون الدولي في مواجهة الجرائم السيبرانية: الجزائر نموذجا، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، مجلد 03، عدد02، 2010، ص.ص 18.19.
- ²⁸ المرسوم الرئاسي رقم 14-252 المؤرخ في 08 سبتمبر 2014 المتضمن انضمام الجزائر الى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الصادر بموجب الجريدة الرسمية عدد 57 المؤرخة في 08 أوت 2014.
- ²⁹ المرسوم الرئاسي رقم 14-251 المؤرخ في 08 أوت 2014 المتضمن انضمام الجزائر الى الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، الصادر بموجب الجريدة الرسمية عدد56 المؤرخة في 09 أوت 2014.