

الأطر القانونية لتعزيز السيادة الرقمية للدولة في مواجهة التحديات المتعلقة بالاستخدامات السلبية المحتملة للذكاء الاصطناعي

Legal frameworks to enhance the state digital sovereignty in the face of challenges related to potential passive uses of AI



د. توفيق تقيّة،¹ د. رشيد بوبكر²

¹ جامعة خميس مليانة-عضو مخبر نظام الحالة المدنية، t.teguia@univ-dbkm.dz

² جامعة تيبازة-عضو مخبر نظام الحالة المدنية، boubekeur.rachid@cu-tipaza.dz



تاريخ الإرسال: 2024/11/15 تاريخ القبول: 2024/11/18 تاريخ النشر: 2024/11/28

ملخص

تشكل السيادة عنصرا ومكونا أساسيا من مكونات الدولة، إلى جانب الإقليم والشعب والسلطة السياسية، إلا أن هذه السيادة أصبحت تواجه تحديات متزايدة في ظل التطورات السريعة لاستخدامات الذكاء الاصطناعي، حيث يفتح هذا التطبيق مخاطر في مجال الأمن القومي، عليه وجب البحث أكثر عن الآليات الكفيلة بالكشف عن مختلف المخاطر الناجمة عن الاستعمال السيء المحتمل لتقنيات الذكاء الاصطناعي والأطر القانونية لتعزيز السيادة الرقمية للدولة على الصعيد الوطني والدولي.

كلمات مفتاحية: السيادة. الرقمية، الذكاء. الإصطناعي.

Summary

Sovereignty is an essential element and component of the state, along with the region, the people and the political authority, but this sovereignty is facing increasing challenges in light of the rapid developments of artificial intelligence uses, as this application opens up risks in the field of national security, so it is necessary to search more

for mechanisms to detect the various risks resulting from the potential misuse of artificial intelligence technologies and legal frameworks to enhance the state's digital sovereignty at the national and international levels.

Keywords: Sovereignty; Digital; intelligence; Synthetic.

1- المؤلف المرسل: د. تقيّة توفيق ، الإيميل: t.teguia@univ-dbk.m.dz

مقدمة

يشير مفهوم السيادة الرقمية للدولة إلى القدرة والسيطرة التي تمتلكها الحكومة الوطنية على بياناتها وأنظمتها الرقمية في العصر الرقمي الحالي. تتضمن هذه السيادة القدرة على حماية البيانات الحساسة وضمان الأمن السيبراني، بالإضافة إلى القدرة على تطوير وتنفيذ التشريعات والسياسات التي تنظم استخدام البيانات والخدمات الرقمية داخل الحدود الوطنية. وبالمقابل تتعرض هذه السيادة لتحديات متزايدة في ظل التطورات السريعة لاستخدامات الذكاء الاصطناعي، حيث يفتح هذا التطبيق مخاطر في مجال الأمن القومي لاسيما في جانب السيادة الرقمية للدولة من خلال مواطن الضعف الناجمة عنه التي قد يستغلها الأعداء والخصوم لشن هجمات تستهدف نظم المختلفة للذكاء الاصطناعي لاسيما في مجال التجسس، والهجمات الإجرامية الالكترونية الضخمة للإضرار بالمصالح الاستراتيجية للدولة أو النيل من السيادة الرقمية لها.

وعلى هذا الأساس تسلط هذه الورقة البحثية الكشف عن مختلف المخاطر الناجمة عن الاستعمال السيء المحتمل لتقنيات الذكاء الاصطناعي والأطر القانونية لتعزيز السيادة الرقمية للدولة على الصعيد الوطني، والتعرف على الأطر الدولية المتخذة في هذا الشأن لحث المشرع على الإقدام نحو تقنين تشريعات حمائية لتعزيز هذه السيادة، حيث تنور إشكالية البحث حول: إلى أي

مدى وفق المشرع الجزائري في إرساء قواعد قانونية لتعزيز السيادة الرقمية للدولة في مواجهة التحديات المتعلقة بالاستخدامات السلبية المحتملة للذكاء الاصطناعي؟.

وللإجابة عن هذه الإشكالية نعلم النقاط البحثية التالية:

1. تحديد المصطلحات

تقتضي هذه الدراسة البحثية الوقوف على تحديد المصطلحات ذات الصلة:

1.1 مفهوم السيادة الرقمية

شهدت فكرة السيادة منذ ظهورها مجموعة من التحولات العميقة والتحورات، حيث إنتقلت من الإطلاق دون قيد أو شرط الى النسبية، نتيجة تحول النظام الدولي، ومع بداية عصر العولمة توقع بعض الدارسين أن السيادة الوطنية لن تزول دفعة واحدة وإنما ستسير نحو التآكل التدريجي بصورة أعمق مما عرفته خلال القرن العشرين، هذا التآكل الذي لن يرتبط بالعولمة الاقتصادية والاختراق الثقافي لخصوصيات المجتمع فحسب، ولكنه يرتبط أيضا بإعادة فهم الحدود انطلاقا من الفضاء السيبراني، مما يطرح إشكالية نطاق سريان سيادة الدولة على إقليمها.¹

إضافة الى ذلك، فإن إنتشار الاستعمال الواسع لشبكة الانترنت، وفرض التكنولوجيا والرقمنة نفسها في جميع الميادين، وتخطيها الحدود الجغرافية والسياسية للدول، ساهم في بداية تكوين مفهوم جديد للسيادة، يجمع بين هذه الأخيرة ومصطلح الرقمنة وهو (السيادة الرقمية)، التي تقتضي ضرورة حمايتها من خلال إتخاذ الاجراءات القانونية والسياسية والعملية اللازمة، ومن بينها توطين التكنولوجيا؛² ونعني بهذا المصطلح المستجد: "قدرة الدولة على فرض إرادتها العامة وتطبيق قوانينها وولايتها القضائية خارج وداخل الفضاء

السيبراني، دون منافس أو منازع..."، والغاية من وراء ذلك حماية أمن الدولة ومؤسساتها، وإستقلّاليتها.

2.1. مفهوم الذكاء الاصطناعي

"علم يهدف إلى فهم طبيعة الذكاء الطبيعي للإنسان وعمل برامج للكمبيوتر قادرة على محاكاة القدرة الذهنية البشرية وخاصة القدرة على التعلم والاستنتاج ورد الفعل ووضعها في الأجسام غير الحية مثل الآلات والمعدات لجعلها قادرة على القيام بأعمال ووظائف تشبه الوظائف البشرية بطريقة ذاتية وبدون تدخل مسبق من الإنسان".³

كما ذهب البعض إلى تعريفه بأنه "ذكاء يظهر عند كيان غير طبيعي من صنع الإنسان ويشكل الذكاء الاصطناعي أحد فروع المعلوماتية التي تدرس تطوير خوارزميات وتقنيات ذكية لتطبيقها في الحواسيب والروبوتات بحيث تمتلك سلوكاً ذكياً في أداء المهام أو في حل المشكلات".⁴

عرفه آخرون بأنه "علم الحاسبات الذي يهتم بأنظمة الحاسوب التي تمتلك خصائص مرتبطة بالذكاء البشري والقدرة على اتخاذ القرارات بدرجة مشابهة إلى حد ما للسلوك الإنساني في مختلف المجالات".⁵

أصدرت منظمة التعاون الاقتصادي والتنمية (OECD) مدونة أخلاقيات استخدام تكنولوجيا الذكاء الاصطناعي وتعد هذه المدونة أول ميثاق شرف أو دستور أخلاقي أو مدونة أخلاقيات استخدام تكنولوجيا الذكاء الاصطناعي وتطبيقاته في بلدان العالم تهدف لضمان الاستخدام والتطبيق النزيه والعادل والأمن لمبتكرات الذكاء الاصطناعي والحيلولة دون تحويله إلى مهلكة للبشرية أو الانحراف به إلى ما لا يمكن السيطرة عليه وبخاصة، التطبيقات ذات الطابع العلمي الابتكاري.⁶

3.1. مفهوم الأمن السيبراني

كلمة سيبرانية في مفهومها الحديث استعملت لأول مرة من قبل عالم الرياضيات الأمريكي «نوربرت وينر Winer Norbert» وهو أستاذ الرياضيات في معهد ماساشوستس التقني MIT الذي أعطاها مفهومها الاصطلاحي الحديث وكان ذلك عام 1948 ومن أجل وصف نظام التغذية الراجعة Feedback للاستفادة من مخرجات الأنظمة out puts في ضبط مدخلاتها puts in وفي التحكم فيها وإستقرار أدائها.

ويمكن القول أن: "الأمن السيبراني مصطلح مركب من مصطلحين وهما الأمن والسيبراني، والذي يعني مجموعة الآليات والأدوات والوسائل القانونية والمادية والتنظيمية والتقنية والتكنولوجية التي تهدف لحماية الأمن الإلكتروني، بما في ذلك مكافحة الجرائم والاساليب غير القانونية التي تهدد هذا الفضاء"⁷ وعرفته الوكالة الفرنسية لأمن أنظمة الإعلام المكلفة بالدفاع السيبراني الفرنسي بأنه: "فضاء التواصل الرقمي بين الاشخاص عن طريق الروابط البينية العالمية وفقا لآليات معالجة البيانات الرقمية آليا"⁸.

2. مخاطر الذكاء الاصطناعي على الأمن القومي:

طرح نقاشنا الأول للمخاطر المرتبطة بالذكاء الاصطناعي في مجال الأمن القومي محاور مألوفة. إذ يمكن على سبيل المثال لعملية صنع القرار المؤتمتة بالكامل في مجال الأمن القومي أن تؤدي إلى أخطاء مكلفة ووفيات. إذ يكثر في الحكايات عن الحرب الباردة وقصص الأفلام ذكر بلدان وصلت إلى حافة الحرب النووية بسبب خلل في أنظمة دفاعها النووية المؤتمتة. وبيحث تقرير صدر مؤخرا عن موقع Defense One بقلم باحثين في مؤسسة RAND في المسألة الشائكة حول أسلحة الذكاء الاصطناعي التي تعمل بدون تدخل بشري.⁹

وتم تحديد الأمن الإلكتروني كمجال خصب بشكل خاص لمواطن الضعف الناجمة عن الذكاء الاصطناعي. فمن أبرز وظائف الأدوات الاصطناعية سواء

المعلوماتية أو الإلكترونية المادية منها التلاعب الفعال بالمعلومات. لذا فقد تلائم الأدوات الاصطناعية على نحو خاص حروب المعلومات وتطبيقات الأمن الإلكتروني.¹⁰

ويفتح تطبيق الذكاء الاصطناعي في مجال المراقبة أو الأمن الإلكتروني للأمن القومي وجهة على هذا الضعف في ماهية البيانات هجوم إلكتروني جديدة قائمة على هذا الضعف ويتعلم الخصوم كيفية تغذية نظم المراقبة العاملة بالذكاء الاصطناعي بمعلومات مضللة بشكل منهجي، فينشئون باختصار عميلاً مزدوجاً آلياً بشكل سري وعن غير قصد. وسبق أن بدأت الأعمال الحديثة تبين قابلية تنفيذ مثل هذه الهجمات السامة المستندة إلى التدريب لاستهداف نظم كشف البرامج الضارة القائمة على تعلم الآلة، ويقدم فساد خدمة الدردشة الذكية تشات بوت (bot-chat) القائمة على الذكاء الاصطناعي من ما يكروسوفت برهانا واسعا النطاق لهذا النوع من الهجمات على نظام ذكاء اصطناعي تجاري، ويمكن أن يفسح ذلك فرصة لعمليات مكافحة التجسس.¹¹

يصف تقرير منظمة برو بوبليكا (ProPublica) الصادر حول تحيز الآلات استخدام الخوارزميات في إجراءات العدالة الجنائية. ويناقش التقرير استخدام خوارزمية كومباس (COMPAS) تقدير العودة إلى الإجرام في نظام العدالة الجنائية في جلسات استماع إطلاق السراح المشروط. إذ تبين أن هذا النظام كان يعطي نتائج متحيزة على نحو منهجي، إلى جانب الاستخدام المضلل للنظام في إجراءات الكفالة وإصدار الأحكام أدى إلى أوجه تفاوت كبيرة في نتائج الأحكام الجنائية في المحاكم التي تستخدم هذه التكنولوجيا.¹²

ولقد أثبتت الدراسات أن الأسباب الرئيسية للتحيز والانحراف في اتخاذ القرار الخوارزمي تكمن في تحيز بيانات الإدخال بالأساس عن طريق الخطأ أو العمد أو من خلال اعتماد البيانات التاريخية، وكمثال بارز على ذلك نجد خوارزميات التوظيف التي طبقها أخصائيو التجارة الإلكترونية الأمريكية لدى شركة أمازون Amazon بخصوص توظيف مهندسي البرمجيات أين افترقت

بيانات الإدخال فيها إلى النزاهة إذ انحازت إلى توظيف الذكور على حساب الإناث بعد أن تم تدريبها على البيانات المتحيزة التاريخية ، ولقد أدت هذه الحادثة في نهاية الأمر إلى التوقف عن اتخاذ القرارات الخوارزمية المتعلقة بالتوظيف في Amazon¹³.

من الناحية الأمنية تمكن الشبكات التعلم الآلي الجهات الإجرامية من شن هجمات إلكترونية ضخمة دون استخدام موارد كبيرة أو مهارت متطورة أو أعداد كبيرة من المنفذين وذلك للإضرار بالمجتمع وعلى الصعيد الشخصي، و مثال على ذلك تطبيقات التزييف العميق "Fake Deep" وهي شكل من أشكال الذكاء الاصطناعي تستخدم خوارزميات التعلم العميق عند إعطائها مجموعات كبيرة من البيانات لمبادلة الوجوه في الفيديو والمحتوى الرقمي لإنشاء وسائط مزيفة تبدو واقعية، وهناك عدة طرق لإنشاء التزييف العميق، ولكن الأكثر شيوعا منها يعتمد على استخدام الشبكات العصبية العميقة التي تتضمن أجهزة التشفير التلقائي التي تستخدم تقنية تبديل الوجه. وهي تحتاج أولا إلى فيديو مستهدف لاستخدامه كأساس للتزييف العميق ثم مجموعة من مقاطع الفيديو للشخص المستهدف والمراد إدراجه في الفيديو الأول، ويمكن أن تسفر عن نتائج مقنعة للغاية، ويمكن غمر قنوات المعلومات بمحتوى مزيف يتم إنشاؤه تلقائيا، مما يؤدي إلى تآكل الثقة في صحة الوسائط الإلكترونية.¹⁴

3. الأطر القانونية لتعزيز السيادة الرقمية للدولة في الجزائر

تكمّن الأطر القانونية فيما يلي:

1.3. المنظومة التشريعية لأمن أنظمة المعالجة الآلية للمعطيات

حاول المشرع الجنائي الجزائري مواجهة المساس بالأمن القومي في شقه المتعلق بالمساس بأمن الأنظمة المعلوماتية من خلال حماية المعطيات والبيانات عند معالجتها بالطرق الإلكترونية عند إقدامه على تعديل وتنظيم الأمر 66-156 المتضمن قانون العقوبات بموجب القانون 04-15 القسم السابع مكرر منه بعنوان المساس بأنظمة المعالجة الآلية للمعطيات تناول ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 7.¹⁵

ونص القانون رقم 04-14 المتعلق بالاجراءات الجزائية على إمكانية تمديد الاختصاص في جرائم أنظمة المعالجة الآلية للمعطيات طبقاً للمادة 37-2 منه، واستبعد تطبيق الأحكام المتعلقة بعمليات التفتيش على الوجه المنصوص عليه بموجب نص المادة 45 المعدلة بالقانون رقم 06-22 إذا تعلق الأمر بهذه الجرائم، بينما إذا اقتضت ضرورات التحقيق الابتدائي في هذه الجرائم فإنه يجوز لوكيل الجمهورية المختص اعتراض المراسلات، ووضع الترتيبات التقنية اللازمة.....، طبقاً لأحكام المادة 65 مكرر 5 من القانون 06-22.¹⁶

2.3. تعزيز المنظومة التشريعية بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

نص القانون 09-04 على طائفة من الأحكام العامة لمكافحة الاعتداءات الواقعة على البيانات الشخصية مهما كانت الوسائط المتداخلة في تداولها سواء شبكات عامة أو خاصة، وبموجب المادة 13 من القانون 09-04 أعلاه أنشئت هيئة وطنية للوقاية من هذه الجرائم ومكافحتها، تحدد تشكيلتها وتنظيمها وكيفية تسييرها عن طريق التنظيم، حيث تأخر تطبيق أحكام هذه المادة إلى غاية 2019 بصدور المرسوم الرئاسي 19-172 المحدد لتشكيلتها وتنظيمها وكيفية تسييرها.

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

نص القانون رقم 18-07 في المادة 3 منه على أن المعطيات ذات الطابع الشخصي هي: "كل معلومة بغض النظر عن دعائها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه، "الشخص المعني" بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم".

وقد وضع القانون 18-07 ضمن الباب الثاني منه مبادئ أساسية لحماية هذه المعطيات من خلال الموافقة الصريحة للشخص المعني طبقاً لأحكام المادة 7

منه وما يليها، ومن خلال التصريح المسبق لدى السلطة الوطنية أو لترخيص منها طبقاً لأحكام المادة 12 منه وما يليها، هذا وقد أسندت صلاحية الرقابة للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي المنشأة بموجب أحكام الباب الثالث من هذا القانون.¹⁸

4.3. آليات مستحدثة موضوعة لدى وزارة الدفاع الوطني-المنظومة الوطنية لأمن أنظمة المعلوماتية:

تدخل المنظم بآليات مستحدثة ترعاها وزارة الدفاع الوطني بموجب أحكام المرسوم الرئاسي 05-20 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية حيث نصت المادة 3 منه على أنه: "تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني ما يأتي:

- مجلس وطني لأمن الأنظمة المعلوماتية، يدعي في صلب النص "المجلس" ويكلف بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها وتوجيهها،

- وكالة لأمن الأنظمة المعلوماتية تدعي في صلب النص الوكالة وتكلف بتنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية،

ولممارسة مهامه يتوفر المجلس، بالإضافة إلى الوكالة على الهياكل المختصة لوزارة الدفاع الوطني في هذا المجال".¹⁹

تضم وكالة أمن أنظمة المعلوماتية تشكيلة ثلاثية، تتألف من لجنة التوجيه التي تتولى تحديد السياسات والتوجيهات العامة، بالإضافة إلى مدير عام يشرف على سير العمل وتنفيذ القرارات، ولجنة علمية مختصة تتكفل بتقديم الخبرات الفنية والعلمية في معالجة وتحليل الحوادث السيبرانية التي تستهدف المؤسسات الوطنية. تقوم الوكالة بتنفيذ مهامها وفقاً لتوجيهات ومتابعة المجلس المختص، نظراً لأن قضايا الأمن السيبراني تعتبر من أهم الأولويات على الصعيد الدولي، حيث تتناول مسائل السيادة الوطنية والأمن المعلوماتي، وتلعب دوراً حاسماً في

تأمين البنى التحتية الرقمية للدولة وحمايتها من التهديدات السيبرانية المختلفة التي يمكن أن تعرض أمنها المعلوماتي للخطر من الداخل والخارج..

5.3. التكامل المؤسساتي لحماية الأمن المعلوماتي للدولة-إحداث مركز بيانات حكومي

أفضت الطبعة الأولى لندوة الجزائر للرقمنة إلى تقديم توصيات بشأن تحقيق السيادة الرقمية بكل ما تحمله في طياتها من معاني، وبناء على ذلك خلصت الندوة إلى أن إرساء السيادة الوطنية في المجال الرقمي يقتضي تعاون وثيق مع القطاعات المعنية من أجل إنشاء شبكة انترنت حكومية ومركز بيانات حكومي يهدف إلى تأمين البيانات. فيما تم تجسيد هذا المطلب فعليا ضمن استراتيجية التحول الرقمي لسنة 2022.²⁰

يشكل مركز البيانات الحكومي الهيكل المؤسسي للدولة والبنية التحتية لبياناتها الذي يضم جميع أصول البيانات المتعلقة بمختلف العمليات الإدارية الرقمية التي تجريها الحكومة وجميع الخدمات الإلكترونية المقدمة والتي يتم تجميعها من خلال ربط البنية التحتية للدولة بأصول البيانات على مستوى الإدارات والمؤسسات العامة وفق آليتين أساسيتين هما التشغيل البيئي الذي يتيح الوصول المادي للبيانات واستضافتها، والتزويد الذي يتيح تقديم الخدمات الرقمية؛ وعليه يعتبر مركز البيانات الحكومي مرفق مادي تستخدمه الدولة لإيواء التطبيقات والبيانات الهامة لمعالجتها ونشرها أو أرشفته.²¹

ويعرف مركز البيانات من الناحية التقنية بأنه منشأة تقنية تأخذ غالبا شكل رفوف متماثلة داخل غرفة تعرف باسم خزانة الخادم بالإضافة المعدات الإضافية اللازمة لحفظ هذه الخوادم وتشغيلها والتمثلة في إمدادات الكهرباء والطاقة الاحتياطية، الأسلاك والكوابل لتوصيل الخوادم بعضها البعض، وأجهزة وشبكات اتصال إضافية، وحدات تحكم، معدات تبريد لحفظ درجة الحرارة المطلوبة التي تحول دون تلف هذه المعدات، أنظمة الكشف عن الحرائق

والرطوبة، أجهزة المراقبة الأمنية والتي تمثل جميعا الأدنى من المعايير التقنية الواجبة التوافر عند إنشاء مراكز البيانات الحكومية.

إن مركز البيانات الحكومي يوفر حولا تقنية تدعم استمرارية العمل الحكومي كما تشكل بيئة آمنة إلى الوصول للخدمات الإلكترونية. وانجاز المعاملات الإلكترونية مع ضمان المحافظة على البيانات والمعلومات من حيث سريتها وسالمتها وحماية خصوصيتها. و نظرا لأهمية مراكز البيانات الحكومية اتجهت بعض الحكومات إلى إنشاء مكان موحد للبيانات الحكومية والت استحدثت بموجب قوانينها الداخلية، مهمتها تجميع البيانات المفتوحة من خلال نقل البيانات بطريقة دورية إلى هذه المراكز التأكد من تنظيفها من الشوائب و من مطابقتها وتحديثها على نحو مستمر، ثم توفيرها على الويب بغرض استفادة المبرمجين وشركات التكنولوجيا في بناء التطبيقات الذكية، وبالتالي إفادة المواطنين من خدمات الحكومة الرقمية بالشكل المطلوب ولتحقيق ذلك و جب العمل على بناء بوابة إنترنت مركزية في مراكز البيانات الحكومية، والعمل على إنشاء كتالوج لجميع البيانات الحكومية؛ من أجل معرفة البيانات التي يمكن الاستفادة منها، والعمل على تطوير تطبيقات بهذا الخصوص من قبل من شركات البرمجة، إضافة لإشراك المختصين في هذا المجال في مرحلتي تصميم و تنفيذ هذا المشروع، والعمل على بناء القدرات وتعزيز المهارات الرقمية لإدارة عمليات المركز.²³

4. الأطر الدولية لتعزيز السيادة الرقمية للدول

تكمن هذه الأطر في المؤسسات الدولية الآتية:

1.4. مقترح المفوضية الأوروبية لأحكام لائحة لقانون الذكاء الاصطناعي

تضمنت اللائحة 12 بابا بإجمالي 81 مادة، حيث ارتأت المفوضية الأوروبية عدم تعريف الذكاء الاصطناعي في حد ذاته ولكن تحديد أنظمتها بدلا من ذلك حيث قدمت تعريفا موسعا وغامضا إلى حد ما لهذه الأنظمة بموجب

أحكام المادة 3 منه والذي قضت بأنه يعني البرنامج الذي تم تطويره باستخدام واحد أو أكثر من التقنيات والأساليب المدرجة في المرفق الأول والذي يمكن لمجموعة معينة من الأهداف التي يحددها الإنسان لتوليد مخرجات مثل المحتوى والتنبؤات أو توصيات أو قرارات تؤثر على البيانات التي يتفاعلون معها؛ أما القسم الأكبر من هذه اللائحة فقد اهتم بوضع الإطار القانوني المقترح على الاستخدام المحدد لأنظمة الذكاء الاصطناعي والمخاطر المرتبطة به؛ من خلال وضع تصنيف الأنظمة الذكاء الاصطناعي ذات المتطلبات والالتزامات المختلفة المصممة وفقا "لمعيار قائم على المخاطر". سيتم من خلاله حظر بعض أنظمة الذكاء الاصطناعي التي تقدم مخاطر "غير مقبولة". في حين سيتم الترخيص لمجموعة من أنظمة الذكاء الاصطناعي "عالية المخاطر" مقابل إخضاعها لمجموعة من المتطلبات والالتزامات للوصول إلى سوق الاتحاد الأوروبي. أنظمة الذكاء الاصطناعي هذه ال تقدم سوى " مخاطر محدودة " ستكون خاضعة لالتزامات الشفافية، في المقابل لا تطبق التزامات محددة بشأن أنظمة الذكاء الاصطناعي منخفضة ومحدودة الخطورة.²⁴

2.4. قوانين الذكاء الاصطناعي في الولايات المتحدة الأمريكية

تم سن تشريعات محلية في بعض الولايات الأمريكية على غرار:

- ولاية كولورادو تم إنشاء فريق عمل لدراسة القضايا المتعلقة باستخدام الذكاء الاصطناعي في كولورادو للنظر على وجه الخصوص في خدمات التعرف على الوجه، وتقييد استخدام خدمات التعرف على الوجه من قبل الوكالات الحكومية والمحلية، وحظر المدارس العامة مؤقتا من تنفيذ عقود جديدة لخدمات التعرف على الوجه واعتمادها.²⁵
- ولاية كاليفورنيا تم تعديل القسم 11547.5 من قانون الحكومة، المتعلق بالتكنولوجيا يحظر من خلال هذا التعديل على الشركات تقديم ادعاءات إعلانية

كاذبة ومضللة، فضلا عن توجيه مجموعة العمل لتطوير آليات لتقليل وتحديد التزييف العميق والبالغ عن الاستخدامات الحالية ومخاطر التزييف العميق.²⁶

- ولاية جورجيا نشاء لجنة الشفافية والإنصاف في اتخاذ القرار الآلي، والتي ستراجع وتقدم تقارير علنية عن استخدام الدولة للذكاء الاصطناعي وأنظمة اتخاذ القرار المؤتمتة الأخرى وتضع توصيات الاستخدام هذه الأنظمة من قبل وكالات الدولة. وهي تحدد تركيبة اللجنة، وتضع متطلبات التأهيل، وتصف كيفية عمل اللجنة، وتتطلب من اللجنة إبلاغ النتائج التي تتوصل إليها إلى الهيئة التشريعية والجمهور.²⁷

2.4. قانون الذكاء الاصطناعي الروسي

صدر المرسوم رقم 490 عن الرئيس الاتحاد الروسي بتاريخ 2019/10/10، بشأن تطوير الذكاء الاصطناعي في الاتحاد الروسي إلى جانب الاستراتيجية الوطنية لتطوير الذكاء الاصطناعي إلى غضون عام 2030 التي تعتبر الأكثر شمولية حيث أرسى عدة أحكام متعلقة بمختلف جوانب الذكاء الاصطناعي، أهمها المبادئ الرئيسية التي تحمل الطابع الإلزامي بخصوص تطوير واستخدام تكنولوجيات الذكاء الاصطناعي تعلقت بالحقوق والحريات، والأمن، والشفافية، سلامة دورة الابتكار والتوفير المعقول، ودعم المنافسة والسيادة التكنولوجية التي تعد مبدءا سياديا لديها.²⁸

الخاتمة

تنبني فلسفة الذكاء الاصطناعي على مسألتين هامتين للغاية، الخوارزميات وكتلة البيانات التي تعتبر عمودها وهو ما يصطلح عليه بدستور الذكاء الاصطناعي عند التطبيق خاصة في المسائل المتعلقة بالسيادة الرقمية والأمن السيبراني والخصوصية والإشراف وهو ما يصطلح عليه في هذا العلم بالثقة الرقمية وعلى ضوء هذه الدراسة نخلص إلى جملة النتائج والتوصيات التالية:

- 1- **وضع التشريعات واللوائح:** يمكن للدول وضع قوانين ولوائح تنظم استخدام التكنولوجيا والذكاء الاصطناعي لحماية البيانات وضمان الخصوصية، وتقديم إطار لمسؤولية الشركات والمؤسسات التي تستخدم التكنولوجيا الرقمية.
 - 2- **تعزيز البحث والتطوير:** يمكن للدول الاستثمار في البحث والتطوير في مجالات الذكاء الاصطناعي والأمن السيبراني لتطوير حلول تقنية تساهم في تعزيز السيادة الرقمية وحماية البيانات.
 - 3- **تشجيع التعاون الدولي:** من خلال التعاون مع الدول الأخرى والمنظمات الدولية، يمكن للدول تبادل المعرفة والخبرات وتطوير استراتيجيات مشتركة لمواجهة التحديات المتعلقة بالسيادة الرقمية والذكاء الاصطناعي.
 - 4- **تعزيز الوعي والتثقيف:** يمكن للدول تعزيز الوعي بين المواطنين والشركات حول أهمية الأمن السيبراني وحماية البيانات الشخصية، وتوفير التدريب والتثقيف حول كيفية تقليل مخاطر استخدام التكنولوجيا والذكاء الاصطناعي.
- التهميش و الإحالات**

- 1- علاء الدين فرحات، عمارة عمرو، الفضاء السيبراني وتآكل مفهوم السيادة الوطنية، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، المجلد 8، العدد 2، 2021، ص 112.
 - 3- فايق عوضين، استخدامات الذكاء الاصطناعي بين المشروعية وعدم المشروعية، الجزء الأول: ماهية الذكاء الاصطناعي ومجالات استخداماته الأمنية، المجلة الجنائية القومية، المجلد 65، العدد 01، الشارقة، الإمارات العربية المتحدة، مارس 2022، ص 8.
 - 4- فايق عوضين، المرجع السابق، ص 8.
 - 5- المرجع نفسه، ص 8.
 - 6- مدحت أبو لنصر، الذكاء الاصطناعي في المنظمات الذكية، المجموعة العربية للتدريب والنشر، القاهرة، ط 1، 2020، ص 156.
 - 7- منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، مايو 2012، ص 16.
- 8 kempf, olivier. (2015). introduction à la cyber stratégie, paris: economica, p 09.

9- يستعمل مصطلح الأمن القومي باعتباره مصطلحا عاما لمناقشة المخاطر التي تفرضها الجئات الخارجية الحكومية وغير الحكومية على البلاد، بينما يستخدم مصطلح الأمن الداخلي باعتباره مصطلحا عاما للإشارة إلى المخاطر على الاستقرار التي تنشأ من داخل الدولة القومية.

راجع: أوسوندي أ. أوسوبا، ويليام ويلسر الرابع، مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل، مؤسسة راند ص 5، على الموقع الإلكتروني:

https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE237/RAND_PE237z1.arabic.pdf

تعتبر مؤسسة **RAND** منظمة غير ربحية وخليّة تفكير أمريكية تأسست سنة 1948 من قبل شركة طائرات دوغلاس لتقديم تحليلات وأبحاث للقوات المسلحة الأمريكية تساعد على تحسين السياسات وعملية اتخاذ القرار من خلال البحث والتحليل من أهم إصداراتها التصميم الأولى لمركبة فضائية تجريبية تدور حول العالم، وبناء جهاز كومبيوتر **JOHNNIAC** على اسم عالم الرياضيات جون فون نيومان، حيث يعتبر هذا الجهاز من أوائل أجهزة الكمبيوتر المخزنة ذات الذاكرة المخزنة.

10- المرجع نفسه، ص 6.

11- أفادت وكالات الاستخبارات الأمريكية أنها تعتقد أن دورة الانتخابات الأمريكية التي انعقدت عام 2016 تعرضت لتدخل أجنبي تجاوز حده من خلال هجمات إلكترونية خارجية تمثلت في شكل إصدارات عامة انتقائية لبيانات خاصة مسربة في محاولة للتأثير في آراء الناخبين. وفي حين أن هذا النوع من الهجمات يمكن الكشف عنه والتعرف إليه متى توفرت المعلومات الملائمة، يمكن للأدوات الاصطناعية الأكثر تقدماً أن تزيد من كفاءة أي جهات ذات نوايا وأن تجعلها أقل قابلية ليتم اكتشافها في هذه العملية.

12- المرجع نفسه، ص 7.

13-Köchling Alina, Marius Claus Wehner, Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development, Ibid, p796.

14- ممدوح عبد الحميد عبد المطلب، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، دار النهضة العربية الجديدة، الإسكندرية، مصر، 2018، ص 10.

15- قانون رقم 15-04 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر عدد 71.

16- قانون رقم 04-14 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتم الأمر 66-155 المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية العدد 71.

17- قانون رقم 09-04 مؤرخ في 2714 شعبان عام 30 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47.

أمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق 25 غشت سنة 2021، يتم الأمر رقم 66-155 المتضمن قانون الاجراءات الجزائية، ج ر العدد 65.

18- قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439، الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية العدد 34.

أمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق 25 غشت سنة 2021، يتم الأمر رقم 66-155 المتضمن قانون الاجراءات الجزائية، ج ر العدد 65.

19- مرسوم رئاسي رقم 20-05 مؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر عدد 04.

20- انعقدت هذه الفعالية بتاريخ التاسع من شهر ماي 2022م تحت رعاية وزارة الرقمنة و الإحصائيات، و بإشراف كل من الكنفدرالية الجزائرية لأرباب العمل المواطنين وهذا بالتنسيق مع النقابة الوطنية لأرباب العمل المواطنين في الرقمنة ولقد حملت هذه الفعالية عنوان: "الرقمنة: ركازة للتنمية و التنافسية، حيث شكلت هذه الفعالية مؤتمرا يضم الفاعلين الأساسيين والذي يهدف إلى إنجاح وتسريع عملية التحول الرقمي في الجزائر مع ضرورة ترقية الإطار الوظيفي و ضمان بيئة متماسكة لدعم التكنولوجيا الرقمية، حيث ثمن وزير الرقمنة والإحصائيات "حسين شرحبيل" هذه الفعالية و ثمن شعارها الواعد مشيرا إلى أن هذه الخطوة قد تم التأكيد عليها مسبقا في خطابات رئيس الجمهورية في العديد من المناسبات، كما دعى الوزير المنظمات النقابية المهنية للعمال المجتمع المدني إلى إدراك حجم مسؤولياتها و ثقل دورها في كسب الرهان و خوض غمار الرقمنة واقتصاد المعرفة.

الكنفدرالية الجزائرية لأرباب العمل المواطنين، معرض الصحافة: خاصة بفعاليات الطبية الأولى لندوة الجزائر للرقمنة: ركيزة للنمو والتنافسية، 08 شارع سيلفان فوريستييه المرادية، الجزائر العاصمة، 10 ماي 2022م، ص 4.

راجع: كوثر منسل، تفعيل دور الإدارة الإلكترونية في الجزائر: نحو بروز قانون للإدارة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في الطور الثالث، قانون عام، كلية الحقوق والعلوم السياسية، جامعة 08 ماي 1945 قالمة، الجزائر، 2023، ص 45.

21- المرجع نفسه، ص 391.

- 22- كوثر منسل، المرجع السابق، ص 392.
- 23- المرجع نفسه، ص 392.
- 24-European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts of 21 April 2021, COM(2021) 206 final. 2021/0106(COD).
- 25-Georg Borges, A Legal Framework for Autonomous Systems, Law and Technology in a Global Digital Society, Springer, Cham, 2022 ,p8.
- 26 -STATE OF CALIFORNIA, Senate Bill No. 1216, CHAPTER 885, An act to add and repeal Section 11547.5 of the Government Code, relating to technology, [Approved by Governor September 30, 2022. Filed with Secretary of State September 30, 2022.].
- 27-GEORGIA GENERAL ASSEMBLY, HB 1651, Transparency and Fairness in Automated Decision-Making Commission; create, 04/04/2022.
- 28-Decree of the President of the Russian Federation No. 490 of 10 October 2019 "On the Development of Artificial Intelligence in the Russian Federation". 2019.

قائمة المراجع:

المؤلفات

- 1- أبولنصر (2021)، الذكاء الاصطناعي في المنظمات الذكية ، مصر، المجموعة العربية للتدريب والنشر ، .
- 2- جبور منى الأشقر(2012)، الأمن السبراني: التحديات ومستلزمات المواجهة، مصر، المركز العربي للبحوث القانونية والقضائية.
- 3- ممدوح عبد الحميد عبد المطلب، (2018)، الإسكندرية، مصر ، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، دار النهضة العربية الجديدة.

4 -kempf, olivier. (2015). introduction à la cyber stratégie, paris: economica.

5-Köchling Alina, Marius Claus Wehner, Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development, Ibid.

6-European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts of 21 April 2021, COM(2021) 206 final. 2021/0106(COD).

7-Georg Borges, A Legal Framework for Autonomous Systems, Law and Technology in a Global Digital Society, Springer, Cham, 2022, p8.

8-STATE OF CALIFORNIA, Senate Bill No. 1216, CHAPTER 885, An act to add and repeal Section 11547.5 of the Government Code, relating to technology, [Approved by Governor September 30, 2022. Filed with Secretary of State September 30, 2022.].

9-GEORGIA GENERAL ASSEMBLY, HB 1651, Transparency and Fairness in Automated Decision-Making Commission; create, 04/04/2022.

10 -Decree of the President of the Russian Federation No. 490 of 10 October 2019 "On the Development of Artificial Intelligence in the Russian Federation". 2019.

الأطروحات:

1- منسل كوثر، (2023)، تفعيل دور الإدارة الإلكترونية في الجزائر: نحو بروز قانون للإدارة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في الطور الثالث، قسم القانون عام، كلية الحقوق والعلوم السياسية، جامعة 08 ماي 1945 قالمة، الجزائر.

المقالات:

1-فرحات علاء الدين، عمروس عمارة (2021)، الفضاء السيبراني وتآكل مفهوم السيادة الوطنية ، المجلة الجزائرية للدراسات السياسية، المجلد 08، العدد 02، 112 الصفحة ؛

2- عوضين، فايق (2022)، استخدامات الذكاء الاصطناعي بين المشروعية وعدم المشروعية، الجزء الأول: ماهية الذكاء الاصطناعي ومجالات استخداماته الأمنية، المجلة الجنائية القومية، المجلد 65، العدد 01، الصفحة 08.

المداخلات: الاسم الأخير، ثم الاسم الأول للمؤلف(ة)، (تاريخ انعقاد المؤتمر)، عنوان المداخلة، عنوان المؤتمر، الجامعة، البلد؛

مواقع الانترنت:

1- أوسوندي أ. أوسوبا، ويليام ويلسر الرابع، مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل، مؤسسة راند ، على الموقع الالكتروني:

https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE237/RAND_PE237z1.arabic.pdf