

السياسة الرقمية في الجزائر بين التحول المنشود وتحديات السيادة الرقمية

Digital Policy in Algeria Between the Desired Transformation and the Challenges of Digital Sovereigntyبن بية عادل¹، بلقرشي إيمان²¹ مخبر البحث في السياسات العامة والتحديات التنموية والأمنية في بلدان المغرب العربي، المدرسة الوطنية

العليا للعلوم السياسية الجزائر، benbia.adel@enssp.dz

² مخبر البحث في السياسات العامة والتحديات التنموية والأمنية في بلدان المغرب العربي، المدرسة الوطنية

العليا للعلوم السياسية الجزائر، Belkorchi.imene@enssp.dz

تاريخ النشر: 2025/04/15

تاريخ القبول: 2025/04/10

تاريخ الاستلام: 2024/11/10

ملخص:

تهدف هذه الدراسة إلى تسليط الضوء على واقع السياسة الرقمية في الجزائر، تحليل مؤشري تنمية الحكومة الإلكترونية والأمن السيبراني، كما تستعرض استراتيجية الحكومة في تعزيز الأمن السيبراني، ثم العوامل الخارجية المهددة للسيادة الرقمية للدول، خلصت الدراسة إلى أن مؤشر نضج الحكومة الإلكترونية في الجزائر يبقى منخفض، ومؤشر الأمن السيبراني في مرتبة متدنية مقارنة بحجم الامكانيات البشرية والمادية المتوفرة، توصي الدراسة بضرورة رفع الجزائر من قدراتها الرقمية خاصة في مجال الأمن السيبراني لتحويل العوامل الخارجية المهددة للسيادة الرقمية إلى فرص و إلى نقاط قوة.

كلمات مفتاحية: السياسة الرقمية، السيادة الرقمية، التحول الرقمي، التحديات الخارجية.

Abstract:

This study aims to shed light on the reality of digital policy in Algeria, analyze the indicators of e-government development and cybersecurity, and review the government's strategy for enhancing cybersecurity, followed by the external factors that threaten the digital sovereignty of countries. The study concluded that the e-government maturity index in Algeria remains low, and the cybersecurity index ranks low compared to the size of the available human and material capabilities. The study recommends the need for Algeria to enhance its

digital capabilities, especially in the field of cybersecurity, and to transform the external factors that threaten digital sovereignty into opportunities and strengths.

Keywords Digital policy, digital Sovereignty, digital transformation, external challenges.

المؤلف المرسل: بن بية عادل، benbia.adel@enssp.dz

مقدمة:

برزت الرقمنة في العالم الحديث كشعار وحجر الأساس لنمو الإقتصادات الوطنية والدولية، كما أن مدى تقدم أو تخلف أي دولة يتحدد بمدى خضوع إقتصادها بالكامل للتحول الرقمي، وبسبب أهميتها في إطار التنمية الرقمية المستدامة والشاملة، فقد استحوذ مجال السياسات الرقمية أيضاً على قدر كبير من الإهتمام من قبل الباحثين الأكاديميين والممارسين وصناع القرار في مجال السياسات العامة، لما لها من دور مهم في السياسات الإجتماعية، فقد تولت العديد من المؤسسات الوطنية الرسمية وغير الرسمية، وكذلك المنظمات الدولية، مهمة تصميم وتنفيذ وتقييم السياسات الرقمية في ضوء التغيير الرقمي الذي شهدته الدول والشعوب والمنظمات.

ونتيجة لعملية التحول الرقمي، ظهرت سياقات جديدة وتشمل السيادة الرقمية والعمولة الرقمية المكثفة، وكلاهما له تأثير بارز على سيادة الدولة، ونظرا للتحديات الكبيرة التي تواجه مجال الأمن القومي حالياً فمن الضروري تقييم وتوجيه البحوث حول الأسس النظرية لتطوير السيادة الرقمية التي يتعين على الحكومات الإلتزام بها.

يبحث أغلب الباحثين والدارسين في مجال السياسات العامة الرقمية في السبل التي من خلالها الوصول إلى أبعد نقطة بلوغ من التحول الرقمي المنشود، لأنه مبتغى كل دول العالم من جهة، وتأمين السيادة الوطنية الرقمية من جهة أخرى والتي تشكل تحدياً وهاجساً أمام الدول من جهة أخرى، وانطلاقاً من كل هذه التحديات تولي الجزائر إهتماماً متزايداً بقطاعها الرقمية بصفة مستمرة إنطلاقاً من مشروع الجزائر الإلكتروني الذي انخرط فيه 2008-2013، وهو ما تؤكد مؤشرات تنمية الحكومة الإلكترونية ومؤشر الأمن السيبراني لتحقيق التمكين من الخدمات الرقمية، وبلوغ التحول الرقمي المنشود مع تأمين السيادة الوطنية الرقمية.

لتحقيق هذا المسعى تهدف هذه الورقة البحثية إلى معالجة الإشكالية التالية :

* إلى أي مدى نجحت الجزائر في إرساء تحول رقمي يأخذ بعين الاعتبار العوامل الخارجية المهددة

لسيادتها الرقمية؟

تنطوي تحت هذه الإشكالية الأسئلة الفرعية التالية:

- ما هو مفهوم السياسة الرقمية والمفاهيم ذات الصلة كالسيادة الرقمية الأمن السيبراني؟
- ما واقع السياسة الرقمية في الجزائر؟
- ماهي التحديات الخارجية المهددة للسيادة الرقمية للدول؟
- للإجابة عن الإشكالية المحورية والأسئلة الفرعية سيتم اختبار الفرضيات التالية:
- البيئة الرقمية الشائكة والمعقدة للتهديدات السيبرانية أدت إلى تدني مؤشرات الحكومة الإلكترونية والأمن السيبراني في الجزائر مقارنة مع العديد من الدول العربية والإفريقية.
- العوامل الخارجية المهددة للسيادة الرقمية قد تشكل فرصا ونقاط قوى لصالح السيادة الرقمية في الجزائر.
- وقصد الإلمام بجوانب هذه الدراسة، إرتأينا تقسيمها إلى المحاور التالية:
- السياسة الرقمية وعلاقتها بالسيادة الرقمية.
- واقع السياسة الرقمية في الجزائر واستراتيجية تعزيز الأمن السيبراني.
- التحديات الخارجية المهددة للسيادة الرقمية للدول.

أولا: الإطار النظري للدراسة

1. تحديد المصطلحات

1.1 السياسة الرقمية: يعتبر الكثيرون السياسة الرقمية على أنها مجموعة من المبادئ التوجيهية القانونية والإجرائية التي تستند إلى التطبيق التجاري المجدي للتكنولوجيات الرقمية، ووفقاً للباحثين والمؤلفين يشمل موضوع السياسة الرقمية ظواهر الإقتصاد الرقمي، و تحديد آثار الرقمنة، طبيعة وخصائص الفجوة الرقمية، الجوانب المختلفة والمتراطة للحياة الرقمية، والإشارة إلى التناقضات في الطرق التي تؤثر بها موارد المعلومات على العمليات الاجتماعية، والنمو الإقتصادي، والبنية الإقتصادية، والتطوير المنهجي للجودة في مجتمع

المعلومات، بالإضافة إلى ذلك، تم توضيح مكونات حاسمة لإنشاء السياسة الرقمية، أبرزها أن تتضمن السياسة الرقمية نوع تكنولوجيا المعلومات المستخدمة (التقنيات الخلوية على سبيل المثال)، الإعتماد على نموذج المجتمع الرقمي المختار، حيث توجد ثلاثة نماذج يمكن استخدامها لتشكيل إقتصاد المعلومات: مجتمع المعلومات، الرقمنة على نطاق واسع، الرقمنة على نطاق صغير، ربط التغييرات الحالية بطبيعتها الهيكلية و الابتكارية¹.

2.1 تعريف التحول الرقمي هو الانتقال من استخدام الأساليب التقليدية إلى الإعتماد على التكنولوجيا داخل المؤسسات والقطاعات المختلفة، وذلك بهدف تعزيز الكفاءة التشغيلية وتحسين وتوسيع الخدمات المقدمة للأفراد ويشمل هذا التحول مواءمة التقنيات الرقمية مع استراتيجيات الأعمال، لتعزيز وتحسين كفاءة العمليات².

1.3 السيادة الرقمية: يجب أن تأخذ تعريف واسع يشمل السلطة السيادية للدولة في تنظيم ليس فقط تدفق البيانات عبر الحدود من خلال استخدام تقنيات تصفية الإنترنت وقوانين توطين البيانات، بل أيضاً أنشطة التعبير والوصول إلى التقنيات³.

4.1 الأمن السيبراني: إن مصطلح الأمن السيبراني ظهر عالمياً منذ 2013، ويعتبر مصطلح السيبرانية واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، ومعناها " الفضاء المعلوماتي"، ما يعني أن الأمن السيبراني أمن الفضاء السيبراني ويعرف كل من Neittaanmaki Pekka, Lehto Martti في كتابهما الموسوم بـ Cyber Security :Analytics, technology and automation حيث اعتبره " عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبهما، و يتضمن تنفيذ التدابير المضادة المطلوبة".

وقدمت وزارة الدفاع الأمريكية " البنتاغون " تعريفاً دقيقاً لمصطلح الأمن السيبراني باعتباره "جميع الإجراءات التنظيمية اللازمة لحماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم الهجمات، التخريب، التجسس والحوادث"، في حين اعتبر الإعلان الأوروبي الأمن السيبراني أنه "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات"⁴.

2. العلاقة بين السيادة والرقمية

تطور مفهوم السيادة، أي سلطة الكيان الحاكم على حكم نفسه دون تدخل خارجي، من المنظور التقليدي يركز على قدرة الحاكم على اتخاذ القرارات النهائية إلى رؤية تؤكد وتركز على السيادة الشعبية، حيث أصبحت السيادة اليوم تشير في المقام الأول إلى استقلال الدولة، أي السيادة الشعبية وتمتع المواطنين في حق تقرير المصير من خلال ممارسة حقوقهم غير القابلة للتصرف وقد أثر تراجع أهمية الدولة القومية خلال التسعينيات بشكل كبير على تطوير الإنترنت وحوكمتها، ثم تطور مفهوم سيادة الدولة من إطارين خطابين متميزين: الإستثنائية السيبرانية وحوكمة الإنترنت متعددة الأطراف.

بالنسبة للخطاب الأول، المسمى بالإستثناء السيبراني، أن المجال الرقمي يختلف اختلافاً جوهرياً عن المجال التناظري، مما يستلزم النظر إلى البيئات الرقمية بشكل مختلف عن جميع التطورات التكنولوجية السابقة وقد إكتسب هذا الإطار المفاهيمي أهمية ملحوظة خلال إنتشار الإنترنت التجاري في التسعينيات، إلا أنه لا يزال يتجلى في المناقشات العامة والأكاديمية وتستند أيديولوجية الإستثنائية السيبرانية إلى الاعتقاد بأن الأهمية المتزايدة لإتصالات الشبكات عبر الحاسوب تعني تآكل سيادة الدولة.

لا تزال الأطر النظرية للإستثنائية السيبرانية والليبرالية السيبرانية تتردد في الخطاب المعاصر، لا سيما في سياق العملات المشفرة ومع ذلك، فإن التأكيد الأساسي بأن انتشار الشبكات الرقمية سيؤدي حتماً إلى تآكل المفاهيم الإقليمية التقليدية للسيادة فقد تضاءل في قوته الإقناعية حيث شهدت البنية والآليات التنظيمية التي تحكم الإتصالات الرقمية تطوراً مستمراً، مما أتاح مراقبة المعاملات الرقمية وتنظيمها وقد تفاقمت هذه الظاهرة بسبب تسليع الإنترنت، مما أدى إلى إنتشار البيئات الرقمية المغلقة وظهور أصحاب مصلحة جدد يفضلون نهجاً هيكلياً دقيقاً يتميز بزيادة الشفافية وإطار عمل أكثر هرمية يسمح بالتدخل في مختلف المراحل.

تُعَدّ حوكمة الإنترنت متعددة الأطراف تهديداً ثانياً أقل مباشرة للسيادة بالمعنى التقليدي، وينصبّ التركيز هنا على المسؤوليات العديدة غير السيادية التي يجب على الحكومات الإضطلاع بها ضمن إطار تنظيمي حيث يرى حوكمة الإنترنت مسؤولية المتأثرين بها بشكل مباشر، بدلاً من التركيز على قصور الدول في إدارة الشؤون الرقمية وقد تطورت منذ بدايات المجتمع التقني العديد من العمليات اللامركزية، التي اتسمت بالكفاءة واتخاذ القرارات القائمة على الجدارة وتهدف هذه العمليات إلى دعم واستخدام معايير وإرشادات وبروتوكولات مشتركة لصيانة الإنترنت وتطويره.

تتسم حوكمة الإنترنت المتعددة الأطراف بعدد من النزاعات، على الرغم من أنها أصبحت مجاًلاً مستقلاً إلى حد ما في الساحة السياسية العالمية. وتتبع هذه النزاعات الخارجية غالباً من استمرار رفض نموذج حوكمة الإنترنت متعدد الأطراف للمؤسسات الدولية الحالية التي تهيمن عليها الحكومات، ومحاولة استبدالها بمفهوم العولمة⁵.

3. عودة السيادة كمبدأ لصنع السياسات الرقمية

لا يزال الإعتقاد السائد بأن الاتصالات الرقمية تُعيق سيادة الدولة قائماً من جوانب عديدة، ولا يزال إرساء السيادة في المجال الرقمي يُشكل صعوبات عملية إلا أن مبررات معارضة سيادة الدولة أصبحت أضعف وبدلاً من ذلك، ولأسباب متعددة، بدأ العديد من الجهات الفاعلة يُجادلون بأن الحفاظ على السيادة في المجال الرقمي أمرٌ ضروري.

أولاً، يُقال كثيراً إن النفوذ الواسع للشركات الفاعلة التي تزدهر في بيئة الإنترنت التجارية، والتي تمتلك القدرة المالية والأخلاقية على التحكم في الهياكل المجتمعية الأساسية، يُشكل الآن تهديداً أكبر لسيادة الدولة من الخصائص التنظيمية الغامضة للشبكات اللامركزية وقد تحول التركيز التجاري للإنترنت إلى استغلال تأثير الشبكة والإعلانات⁶ تلعب المنصات الرقمية دوراً كبيراً في توفير المحتوى لدرجة أن بروتوكولات الإنترنت المفتوحة التي تعتمد عليها الاتصالات الرقمية أصبحت بلا معنى واليوم، لا يقتصر الأمر على الموارد الهائلة التي يسيطر عليها هؤلاء الوسطاء فحسب، بل أيضاً على الطريقة التي يمارسون بها السيطرة، مما يجعلهم أحد أكبر التحديات لمفهوم السيادة الديمقراطية⁷ من نواحٍ عديدة، لا يزال التصور السائد بأن الاتصالات الرقمية مُعادية لسيادة الدولة قائماً، ولا تزال التحديات العملية لتأكيد السيادة في المجال الرقمي قائمة ومع ذلك، فقد تضاعفت الحجج الداعية إلى رفض سيادة الدولة بشكل ملحوظ بل بدأت جهات فاعلة مختلفة تدعو إلى ضرورة ترسيخ السيادة في المجال الرقمي، بمبررات متعددة.

أولاً، غالباً ما يُقال إن التحدي الحقيقي لسيادة الدولة لم يعد يكمن في السمات التنظيمية غير الواضحة للشبكات اللامركزية، بل في النفوذ الهائل للشركات الفاعلة التي تزدهر في بيئة الإنترنت التجارية وتمتلك القوة المادية والمعنوية للاستحواذ على هياكل مجتمعية حيوية أصبح التركيز التجاري للإنترنت مُنصباً على الإعلان واستغلال تأثيرات الشبكة⁸.

عند دراسة ردود الفعل المتضاربة للدول تجاه كشف إدوارد سنودن عن عمليات المراقبة العالمية واسعة النطاق التي تقوم بها أجهزة الاستخبارات الأمريكية وحلفاؤها، تتضح الحجة الثانية لتعزيز السيادة الرقمية ودعمها فقد كشف سنودن عن القدرات الهائلة التي تتمتع بها وكالات الاستخبارات وشركات التكنولوجيا في الولايات المتحدة ودول غربية أخرى في جمع البيانات وتحليلها والتحكم فيها، بالإضافة إلى الاستخدام المفرط للقوة المهيمنة ومن المثير للإهتمام أنه لم يُوجَّه انتقاد كبير لهذه الكتلة القوية ككل نتيجة اختيارها العمل كمنظمات ذات سيادة دون أن تكون إقليمية⁹.

ثانيا: واقع السياسة الرقمية في الجزائر

تعد الجاهزية الإلكترونية محددًا هامًا لنجاح المشاريع الرقمية، وفي هذا الصدد نحاول تحليل الجاهزية الرقمية في الجزائر من خلال المؤشرات التي تعتمد عليها بعض المنظمات الدولية لتصنيف الدول حسب استعدادها للتحويل الرقمي الحقيقي.

1. دراسة تحليلية لمؤشر تنمية الحكومة الإلكترونية في الجزائر

تم التركيز في هذه الدراسة على سنوات 2012 - 2022 لأن بداية مشروع الحكومة الإلكترونية في الجزائر بدأ سنة 2012 - 2013، ويفترض بداية نتائج تطبيق الحكومة الرقمية.

الجدول (01): تصنيف الجزائر العالمي وفق مؤشر التنمية للحكومة الإلكترونية من 2012-2022

المؤشر - السنة	2012	2014	2016	2018	2020	2022
مؤشر الخدمات عبر الانترنت	0.2549	0.0787	0.0652	0.2153	0.2765	0.3743
مؤشر رأس المال البشري	0.6463	0.6543	0.6412	0.6640	0.6966	0.6956
مؤشر البنى التحتية	0.1812	0.1989	0.1934	0.3889	0.5787	0.6133
مؤشر تنمية الحكومة الإلكترونية	0.3608	0.3106	0.2999	0.4227	0.5173	0.5611
الترتيب العالمي من 193 دولة	132	136	150	130	120	112

المصدر: الأمم المتحدة

من خلال الجدول أعلاه نلاحظ تراجع مؤشر تنمية الحكومة الإلكترونية في الجزائر في الفترة بين(2012-2016)، وهذا مرتبط أساسا بانخفاض في مؤشر الخدمات عبر الأنترنت مع استقرار نسبي في المؤشرين الفرعيين الآخرين.

في الفترة ما بين (2018-2022) نلاحظ تحسن واضح في مؤشر تنمية الحكومة الإلكترونية الإجمالي طبعاً هذا مرتبط بارتفاع مؤشر البنى التحتية للإتصالات وارتفاع في الخدمة عبر الأنترنت مع تحسن طفيف في مؤشر رأس المال البشري.

1.1. تحليل مؤشر الحكومة الإلكترونية في الجزائر لسنة 2012-2022 وفق المؤشرات الفرعية مؤشر الخدمة عبر الأنترنت

الجدول 02: ترتيب الجزائر في مؤشر الأمم المتحدة للخدمات عبر الانترنت خلال الفترة 2012-2022

السنوات	2012	2014	2016	2018	2020	2022
قيمة المؤشر	0.25	0.07	0.06	0.21	0.27	0.37

Source:UNE-gouvernement knowlodge base.available on the site bit.ly/3irna_msa.

تحليل مؤشر البنية التحتية للاتصالات

الجدول 03: ترتيب الجزائر في مؤشر الأمم المتحدة للبنية التحتية للاتصالات خلال الفترة 2012-2022

السنوات	2012	2014	2016	2018	2020	2022
قيمة المؤشر	0.57	0.38	0.19	0.19	0.18	0.12

Source:UNE-gouvernement knowlodge base.available on the site bit.ly/3irna_msa.

مؤشر رأس المال البشري في الجزائر

الجدول 04: ترتيب الجزائر في مؤشر الأمم المتحدة لرأس المال البشري خلال الفترة 2012-2022

السنوات	2012	2014	2016	2018	2020	2022
قيمة المؤشر	0.69	0.66	0.64	0.65	0.64	0.73

Source:UNE-gouvernement knowlodge base.available on the site bit.ly/3irna_msa.

حسب القيم الموجودة في الجداول أعلاه فالجزائر لم تتمكن من تسجيل قيم محفزة على التحول الفعلي نحو النماذج الإلكترونية للخدمة العمومية فالقيم متذبذبة وليست ثابتة، ما يجعل من إمكانية التحول الرقمي صعبة مقارنة بدول أخرى لا تملك إمكانيات الجزائر لا من حيث البنى التحتية ولا مستوى رأس المال البشري ولا من حيث خدمات الأنترنت التي يمكن تطويرها لأن تذبذب الأنترنت راجع إلى ظروف مقصودة ومعروفة لدى السلطة تحول دون الرفع من تدفق الأنترنت.

مؤشر المشاركة الإلكترونية

الجدول 06: ترتيب الجزائر في مؤشر الأمم المتحدة للمشاركة الإلكترونية خلال الفترة 2012-2022

السنوات	2012	2014	2016	2018	2020	2022
الترتيب	124	172	167	165	183	148
قيمة المؤشر	0.05	0.07	0.11	0.20	0.15	0.22

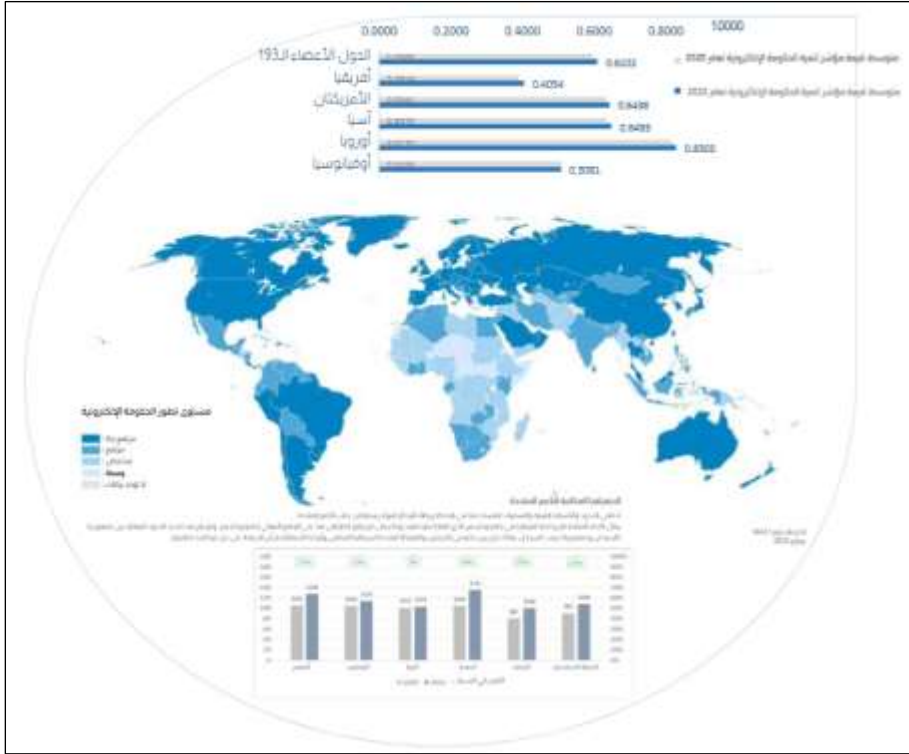
Source: UNE-government knowledge base. available on the site bit.ly/3irna_msa.

نتائج القيم المؤشرات الفرعية في الجزائر تسجل انخفاضا واضحا وبهذا فإن مؤشر تطور الحكومة الإلكترونية بناء على هذه القيم فهي ضعيفة وليست في مستوى تطلعات الحكومة، فبطبيعة الحال فهذا الضعف يؤثر على عملية التحول الرقمي على مستوى الإدارة العامة ويؤثر على جودة الخدمات العمومية.

تبين القيمة الضعيفة المسجلة في مؤشر المشاركة الإلكترونية فجوة التواصل والمشاركة بين كل القطاعات وأبعاد المواطن من المشاركة في صناعة القرار وتعزيز الديمقراطية التشاركية وهو عنصر مهم في عملية التحول الرقمي.

يبرز الشكل 01 متوسطات مؤشر تطور الحكومة الإلكترونية العالمية والإقليمية، وتصنيفات الدول حسب مستويات مؤشر تطور الحكومة الإلكترونية، وتقديم الخدمات عبر الأنترنت في قطاعات مختارة، 2020 و2022.

الشكل (01): مسح الحكومة الإلكترونية العالمية و الإقليمية



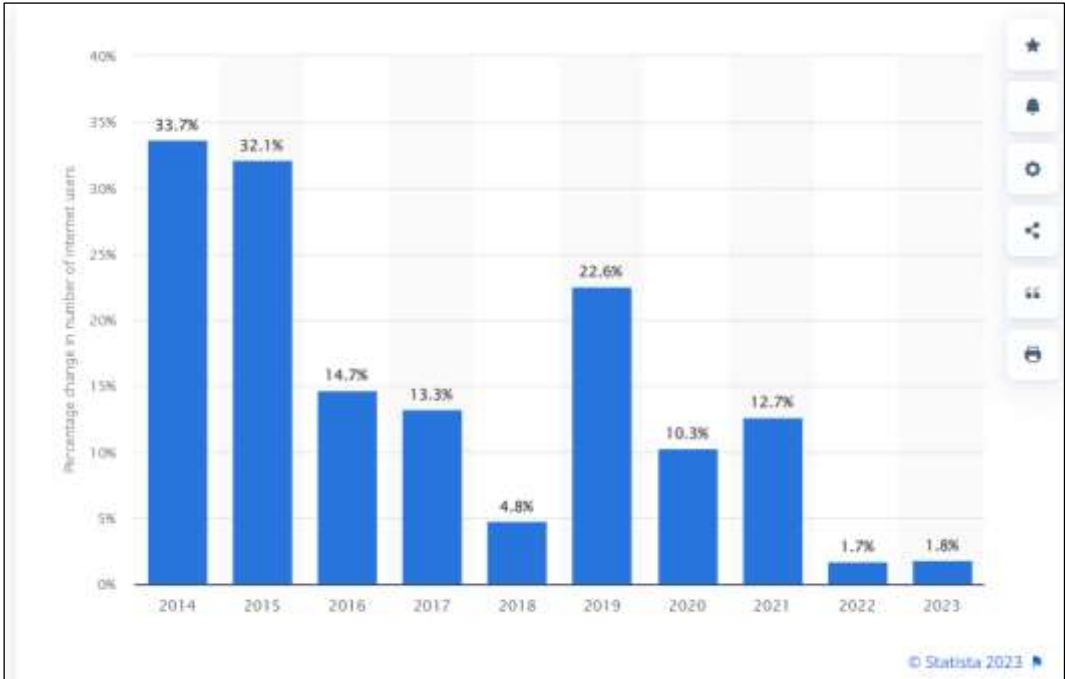
المصدر : الأمم المتحدة، مسح الحكومة الإلكترونية 2022، مستقبل الحكومة الرقمية نيويورك 2022 ص.27
بناءً على الشكل المذكور أعلاه يتضح أن الجزائر تعاني انخفاض واضح في مؤشرات نضج الحكومة الإلكترونية رغم الجهود الإصلاحية للحكومة الجزائرية المقترنة بالتحول الرقمي إلا أن هذا التحول غير كافٍ لرفع قيمة مؤشر تنمية الحكومة الإلكترونية خلال الفترة بين 2020-2022.

وفقاً لأحدث البيانات الصادرة في أوائل عام 2023، بلغ عدد مستخدمي الإنترنت في الجزائر 32.09 مليون جزائري، بنسبة انتشار بلغت 70.9٪. في يناير 2023، بلغ عدد مستخدمي وسائل التواصل الاجتماعي حوالي 23.90 مليون، أي ما يعادل 52.9٪ من إجمالي السكان في الأشهر الأولى من عام 2023، بلغت نسبة مستخدمي الإنترنت في الجزائر 70.9٪ ووفقاً لتحليل أجرته شركة كيبوس، فقد نمت قاعدة مستخدمي الإنترنت في الجزائر بمقدار 553 ألف مستخدم، أي بنسبة 1.8٪، بين عامي 2022 و 2023⁹.

في غضون سنوات قليلة، ارتفعت نسبة السكان المتصلين بالإنترنت تدريجيًا وقد ارتفع عدد مستخدمي الإنترنت بين عامي 2014 و2023، وشهد عام 2015 أعلى معدل نمو بنسبة 32.1%. تجدر الإشارة إلى أنه خلال العام، وفقًا للرسم البياني المرفق¹⁰.

و حسب Statista يتوقع أن ترتفع حصة السكان الذين لديهم إمكانية الوصول إلى الإنترنت في الجزائر بشكل مستمر بين عامي 2024 و 2028 بإجمالي 15.3 نقطة مئوية¹¹.

الشكل (02): مستخدمي الانترنت في الجزائر من 2014-2023



Source: Saifaddin Galal, Percentage change in the number of internet users in Algeria from 2014 to 2023 Jun 29, 2023

وفقًا لبيانات aokla، بلغ متوسط سرعة الإنترنت في الجزائر عام 2023 11.01 ميجابت في الثانية لاتصالات الإنترنت الثابتة، و 13.40 ميجابت في الثانية لاتصالات الإنترنت عبر الهاتف المحمول كما ارتفع متوسط سرعة الإنترنت عبر الهاتف المحمول في الجزائر بمقدار 1.97 ميجابت في الثانية (+17.2%) خلال الاثني عشر شهرًا التي سبقت بداية عام 2023 ووفقًا لبيانات أوكلا، ارتفعت سرعة الإنترنت عبر الهاتف الثابت في الجزائر بمقدار 1.23 ميجابت في الثانية (+12.6%) خلال الفترة نفسها.

2.1. تحليل مؤشر الأمن السيبراني في الجزائر

حسب مؤشر الأمن السيبراني الذي يصدره الاتحاد الدولي للاتصالات (ITU)، التابع للأمم المتحدة، فإن الجزائر تحتل المرتبة 104 عالميا من مجموع 182 بلد ، 93 من 160 أمة حسب تصنيف الأمم (NCSI)، والمرتبة 23 أفريقيا، و 12 عربيا من مجموع 22 بلد عربي، ويأتي تصنيف البلدان الأفريقية، التي تحقق أفضل أداء فيما يتعلق بالأمن السيبراني كما يلي:

- موريشيوس مؤشر رقم 100/96.86 | الأولى على المستوى الأفريقي .

- تنزانيا مؤشر رقم 100/90.58 | الثانية على المستوى الأفريقي

- غانا مؤشر 100/86.69 | الثالثة على المستوى الأفريقي .

يأتي تصنيف بلدان المغرب العربي ضمن شروط الأمن السيبراني كآتي:

- تونس : مؤشر رقم 100/.86.23 | الخامس على منطقة المينا

- المغرب : مؤشر رقم 100/.82.41 | السابع المستوى على منطقة المينا .

- الجزائر : مؤشر رقم 100/33.93 | الثالث والعشرين على منطقة المينا

- ليبيا : مؤشر رقم 100/28.78 | السادس والعشرين على منطقة المينا..

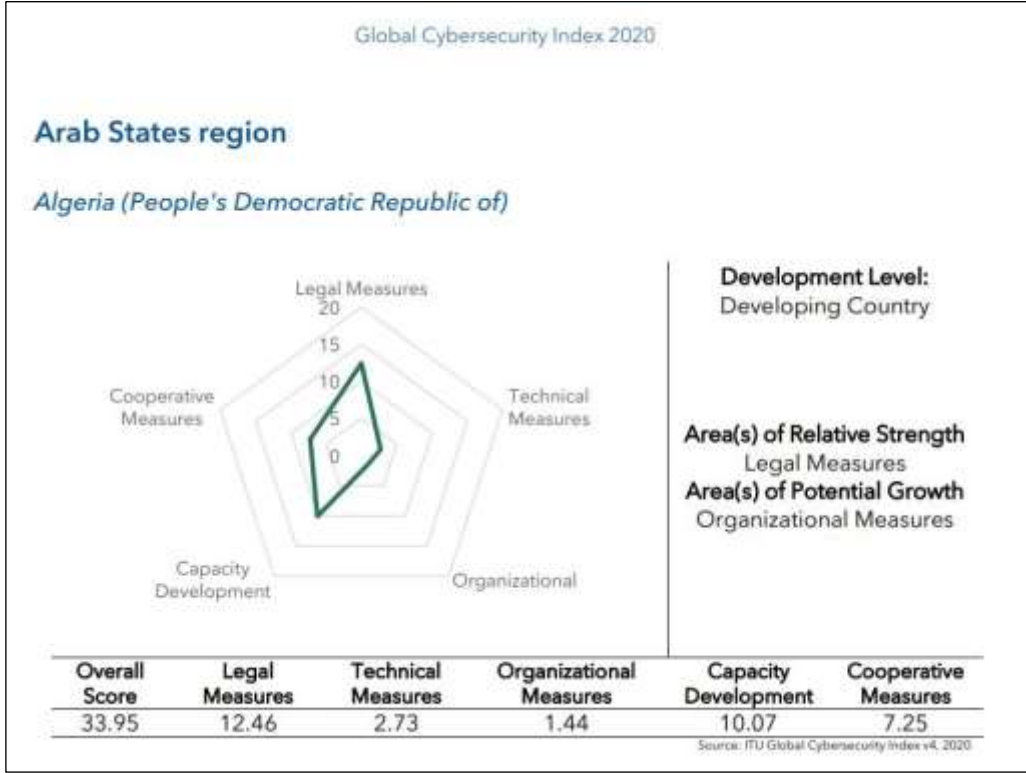
- موريتانيا : مؤشر رقم 100/18.94 | الثاني والثلاثين على منطقة المينا ¹².

يظهر المؤشر تقاربا كبير في مستوى الأمن السيبراني بين الجزائر وليبيا التي تعيش عدم استقرار سياسي منذ أكثر من عقد ، فيما يظهر نفس المؤشر الاختلاف الشاسع بين الجزائر - والدول الإفريقية وبين جارتها تونس والمغرب اللتين كانتا في صدارة الترتيب عربيا، هذه المرتبة المتدنية مقارنة بحجم الامكانيات البشرية والمادية التي تمتلكها الجزائر تطرح العديد من التساؤلات عن أسباب ذلك.

وحسب نفس التقرير فإن مؤشر الأمن السيبراني للجزائر تحصل على 33.95 نقطة من مجموع 100 نقطة، حسب المجالات التالية: الإجراءات القانونية 12.46 نقطة من 20 نقطة ويمكن اعتبارها نتيجة مرضية، الإجراءات التقنية 2.73 نقطة ومن هنا تظهر هشاشة الأمن السيبراني في هذا المجال، الإجراءات التنظيمية 1.44 نقطة وهو أضعف تنقيط، رغم المحاولات والمجهودات المبذولة في ميدان وضع هياكل إدارية وتنظيمية الإدارة الأمن السيبراني ، أما مجال تنمية القدرات فتحصل على 10.07 ويمكن

قراءتها على أنها تنقيط متوسط إلى إيجابية وأخيرا مجال إجراءات التعاون فكان تنقيطه 27.5 وهو تنقيط دون المتوسط¹³.

الشكل 03: مؤشر الأمن السيبراني الجزائري.



Source: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF

2. استراتيجية الجزائر لتعزيز الأمن السيبراني وتأمين السيادة الرقمية

بناءً على ما سبق، لا تزال جهود الجزائر لتحسين الأمن السيبراني وتحقيق السيادة الرقمية محدودة، مما يوحي بوجود الكثير من العمل الذي يتعين القيام به، لا سيما في الجوانب التقنية والتنظيمية للأمن السيبراني ونتيجةً لذلك، ركزت هذه الجهود في الغالب على مجال الإجراءات القانونية، دون غيرها من التدابير ويتجلى ذلك في صدور القانون رقم 04-09 المؤرخ 5 أوت 2009، الذي يتضمن قواعد خاصة للوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات و الاتصالات ومكافحتها، ويحدد الحالات التي تُجيز استخدام مراقبة الاتصالات الإلكترونية، وذلك استناداً إلى المادة 4 التي تنص على ما يلي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

-في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

-لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

نصّت المادة 2 أيضاً على إنشاء هيئة وطنية لكشف ومكافحة الجرائم المتعلقة بتكنولوجيا المعلومات و الاتصالات وقد تحقق ذلك بصدور المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، الذي حدد هيكل وتشكيل وأساليب عمل الهيئة الوطنية المكلفة بمنع ومكافحة الجرائم المتعلقة بتكنولوجيا المعلومات و الاتصالات كما أنشأت الجزائر هيئات إضافية ذات أهمية حاسمة في مكافحة مختلف أنواع الجرائم الإلكترونية، مثل:

-مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني.

-المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.

-المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني¹⁴.

وفي إطار إعداد الاستراتيجية الوطنية لأمن أنظمة المعلومات في الجزائر، تم إنشاء المجلس الوطني لأمن أنظمة المعلومات في الجزائر في مرسوم رئاسي رقم 05-20 بتاريخ 24 جمادى الأولى 1441 الموافق ل 20 جانفي 2020 يحمل عنوان "جهاز وطني لأمن أنظمة المعلومات"¹⁵.

وبأتي إهتمام الجزائر بإنشاء مثل هذه المؤسسات إلى تزايد معدلات الجرائم الإلكترونية التي أصبحت تشكل تهديدا كبيرا على الأمن الوطني، فقد ارتفع معدل الجرائم الإلكترونية في الجزائر بشكل كبير خلال السنوات الأخيرة حسب بعض التقارير الأمنية، يتعلق أبرزها بانتهاك الحريات الشخصية، والتهديد عبر الأنترنت، ونشر صور فاضحة، الابتزاز، والقرصنة الإلكترونية وغيرها .

كما وقع رئيس الجمهورية السيد عبد المجيد تبون 2020 على مرسوم تنفيذي يقضي بإرساء استراتيجية للأمن السيبراني وإنشاء مجلس ووكالة للأمن السيبراني واعتماد نظام يقظة شامل يهدف إلى التصدي للتهديدات الجديدة، وفي 2021 تم استحداث قطب جزائي جديد مكلف بمتابعة الجرائم السيبرانية ومكافحتها على مستوى الجيش الوطني الشعبي استخدمت مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة.

كما اهتمت مؤسسة الجيش بالذكاء الاصطناعي AI وحروب الجيل الخامس في مجال الدفاع السيبراني والتنبؤ بالهجمات حجمها ونوعها.

تركز الدولة في تطبيق استراتيجيات السيادة الرقمية بإشراك جميع الفئات وأجهزة الدولة وهي استراتيجية شاملة للأمن السيبراني تبدأ من المواطن ووعيه بمدى خطورة الفضاء السيبراني ثم المختصين في مجال الأمن السيبراني ثم المسؤولين على كافة المؤسسات الفاعلة في الدولة¹⁶.

يُمثل غياب جهة مستقلة تُعنى بالأمن السيبراني نقطة ضعف في خطة الحكومة الجزائرية للأمن السيبراني. فالأجهزة الأمنية التابعة لمؤسسات الدفاع الوطني، مثل الدرك الوطني والجيش الوطني الشعبي، مسؤولة عن معظم هذه الأنشطة وقد يُصعب حصرها في هذه المؤسسات وضع سياسات شاملة ومتوازنة بين مؤسسات الدفاع والمراكز الوطنية المستقلة لمواجهة التهديدات السيبرانية وجهود مكافحة مختلف الجرائم السيبرانية، مع أن هذا يُعدّ إضافة قيّمة تُضفي بُعدًا جديدًا على سياسة الدفاع الوطني الجزائرية كما أنه يُقلّل من المزايا المحتملة لفرص وقدرات الفضاء السيبراني، التي لا تزال حكرًا على الأجهزة العسكرية والأمنية.

ثالثا: العوامل الخارجية المهددة للسيادة الرقمية للدولة

يعد عصر الإنترنت سلاح ذو حدين ولعل الحد السلبي منها هو تعريض السيادة الرقمية لتحديات وضغوط غير محمودة العواقب خاصة على الدول الهشة رقميا، حيث تشكل السبل الجديدة للهجمات السيبرانية التطفل على الإمتيازات السيادية للدول، وفي هذا الصدد عجز القانون على مواكبة التكنولوجيا العصرية بمفهومها الأمني، وحسب القانون الدولي فإن مسؤوليات الدول عن معالجة الهجمات السيبرانية غير كاف وتتطلب التهديدات الخارجية التي تحدّد تشكيل السيادة الرقمية للدولة الحديثة إعادة الإعتبار لأهم التحديات والتهديدات التكنولوجية والإقتصادية والسياسية والإجتماعية.

1. التهديدات الخارجية الناشئة:

كانت للهجمات التي شنّها مجرمو الإنترنت على البنية التحتية الحيوية وموارد المعلومات على مدى العقود القليلة الماضية نتائج كارثية، تسببت الجرائم الإلكترونية في خسائر تقدر بأكثر من 6000 مليار

دولار على مستوى العالم في عام 2021، وهذا هو السبب الرئيسي في تطوير أساليب دولية وحكومية لمنع الهجمات الإلكترونية، وقد بدأت بعض البلدان بذلك فعلا، وبادرت في إنشاء كوادر مؤسسية على سبيل المثال، في عام 2013، أقر الاتحاد الروسي القانون الفيدرالي رقم FZ187، الذي "ينص على تعديل بعض القوانين التشريعية للاتحاد الروسي بشأن حماية الحقوق الفكرية على شبكات المعلومات والاتصالات"، أيضا قدمت الولايات المتحدة تدبيرين في عامي 2011 و2012 قانون منع التهديدات الحقيقية عبر الإنترنت للإبداع الاقتصادي وسرقة الملكية الفكرية وقانون وقف القرصنة على الإنترنت لكن بسبب العقوبات الصارمة، لم تغطي مشاريع القوانين هذه بالدعم بشأن الجرائم، يجب أيضا حماية الأسرار التجارية وأسرار الإنتاج في الفضاء الإلكتروني، بالإضافة إلى حقوق النشر وبراءات الاختراع من أجل توحيد القوانين في جميع الدول الأعضاء، قدم البرلمان الأوروبي التوجيه بشأن حماية الأسرار التجارية والمعرفة في الاتحاد الأوروبي في عام 2013، تعمل القوانين ضد المنافسة غير العادلة على حماية المعرفة هذه هي لوائح القانون العام في الولايات المتحدة والمملكة المتحدة يحكم القانون الاتحادي رقم FZ98- "بشأن الأسرار التجارية" والفصل 75 من القانون المدني¹⁷.

2. الأجندة السياسية الدولية:

لقد أدى التحول في النظام السياسي العالمي من عالم ثنائي القطب إلى عالم أحادي القطب بعد إختيار الاتحاد السوفيتي، وتشكل عدة أقطاب للقوة ما يبنى بإعادة تشكيل خارطة العلاقات بمبادئ جديدة في المستقبل القريب¹⁸ من الطبيعي والمتوقع أن يشكل رفض العولة السابقة حدثا هاما، لكنه يمثل تهديدا كبيرا للمجتمع العالمي والمنافسة على مناطق النفوذ، وتصعيد الصراعات العسكرية الإقليمية، من ناحية أخرى، أدت المنافسة بين الدول والشركات الناجمة عن المناخ الجيوسياسي الحالي إلى تسريع تطوير التكنولوجيا الرقمية بشكل كبير ومع ذلك، فإنها تجعل بعض الدول والمنظمات أكثر تقدما من الناحية التكنولوجية من غيرها في المنافسة على الموارد، وفي نهاية المطاف، على الزعامة السياسية العالمية، على الأمم المتحدة أن تأخذ زمام المبادرة في إنشاء إطار لتحقيق المساواة الرقمية العالمية والدعوة إلى استخدام الرقمنة لتسريع تحقيق أهداف التنمية المستدامة للكوكب¹⁹ وينبغي استخدام البيانات والتكنولوجيا الرقمية لإنشاء استراتيجيات سياسية أكثر مرونة، سيساعد التعاون بين الدول في الفضاء الرقمي على تقليل التوترات

الجيوسياسية وإنشاء معايير علمية عادلة في مجال الأمن واحترام حقوق الإنسان وترد هذه في تقارير الفريق الرفيع المستوى المعني بالتعاون الرقمي واستراتيجية الأمم المتحدة بشأن التكنولوجيا الجديدة²⁰.

3. الصراع من أجل الريادة التكنولوجية العالمية

لقد شهدت السنوات العشر الماضية تحولاً في دور الزعامة التقنية العالمية في السياسة الاقتصادية، الأمر الذي أثر على تفضيلات الإستيراد والتصدير لدى اتحادات الدول والأمم، إن إحدى الطرق التي يمكن للدول من خلالها تعزيز استقلالها التقني هي التنافس على التفوق التكنولوجي، لقد اتخذ مفهوم تحقيق الإستقلال التقني دور نموذج العملة الذي اعتمد على التعاون في مجال العلوم والتكنولوجيا، إن التهديدات التي تشكلها التكنولوجيا المتقدمة تتسبب في تدهور السيادة الرقمية للدول الفقيرة، مما يجعلها هدفاً وأداة تأثير لشركات التكنولوجيا العملاقة العالمية وقد يؤدي هذا إلى الاستعمار الرقمي للدول الفقيرة لذلك، فإن استخدام التكنولوجيا المتقدمة في العديد من المجالات، وخاصة تلك ذات الأهمية الوطنية، يضمن القدرة التنافسية للدول الفقيرة، وفقاً لمؤشر الابتكار العالمي، يجري الآن سباق بين الدول الرائدة لتطوير التقنيات في مجال الذكاء الاصطناعي²¹.

وفي عام 2017 قدمت الصين خطة لتطوير الذكاء الاصطناعي بحلول عام 2030 بتمويل إجمالي

قدره 150 مليار دولار.

4. بنية تحتية رقمية عالمية موحدة

توفر العناصر الحالية للبنية التحتية الرقمية، في شكل خطوط اتصالات الألياف الضوئية وأبراج الهاتف المحمول (G3، G4 ، G5) الوصول إلى الإنترنت العالمي لجزء فقط من سكان العالم إنشاء وصيانة البنية التحتية في المناطق النائية والريفية (وخاصة مناطق القطب الشمالي) مهمة صعبة تتطلب استثمارات مالية جادة وفي العقد الماضي، ظهرت طريقة بديلة، وهي الإنترنت عبر الأقمار الصناعية عالية الجودة والسرعة من مدار أرضي منخفض، مما سيسمح لمطوري تقنيات الفضاء والأقمار الصناعية بتغطية العالم كله ومع ذلك، لا تمتلك جميع الدول القدرات والموارد اللازمة لتطوير صناعاتها الفضائية ولا تزال الولايات المتحدة وروسيا والصين واليابان والهند وفرنسا والمملكة المتحدة هي الرائدة في عدد المركبات الفضائية وعمليات إطلاقها²² وتحاول دول أخرى أيضاً الدخول في سباق الفضاء الجديد، لكن الإفتقار إلى

البنية التحتية اللازمة لإطلاق الأقمار الصناعية، والتطورات العلمية والتكنولوجية الخاصة بها في صناعة الفضاء، والموارد الأخرى، تحد من قدراتها.

5. الحماية الرقمية

لقد أجبرت رقمنة الإقتصاد العالمي العديد من البلدان على تنفيذ سياسات الحماية الرقمية بسبب ضبابية وغياب الوضوح في الحدود الوطنية للأسواق الرقمية، وطرق الإتصال ونقل البيانات عبر الحدود وضعف البنية التحتية الرقمية وحمايتها من المخاطر، إلى جانب القيود الإصطناعية على استيراد التقنيات والسلع والبيانات والخدمات الرقمية، هذه السياسات لها آثار إيجابية وسلبية على السيادة الرقمية للدولة، إحدى الطرق التي قد تساعد بها سياسة استبدال الواردات العدوانية الأمة في بناء تقنياتها الرقمية الخاصة هي من خلال الترويج لاستخدامها ومع ذلك، فإن غياب المنافسة من السلع المستوردة يمكن أن يشجع أيضاً الابتكار ويخفض جودة السلع المحلية، مما يقوض السيادة الرقمية²³ وفي هذا الصدد، تحاول الدول الفردية (المجموعات أو النقابات) ضمان أمن الفضاء الرقمي الوطني الخاص بها²⁴ عندما وضعت العديد من الدول متطلبات إلزامية للشركات الرقمية العالمية (على سبيل المثال، جوجل) لتحديد قواعد البيانات الخاصة بمواطنيها في أراضيها لقد تطورت الحاجة إلى تحديد وحماية البيانات الشخصية للمواطنين تدريجياً إلى الحماية الرقمية في قطاع التجارة ومع إطلاق الأسواق العالمية الكبيرة، أصبح من الممكن شراء البضائع من وفي أي مكان في العالم.

6. الشركات العابرة للحدود

إن التوسع الجغرافي للشركات عبر الوطنية لها تأثير إيجابي على النظم الإجتماعية والإقتصادية للبلدان التي تعمل فيها حيث ترتبط التغييرات الإيجابية بنقل المعرفة وإدخال تقنيات وأساليب إدارية جديدة تعمل الشركات عبر الوطنية كمصدر للاستثمارات الأجنبية المباشرة في المناطق والصناعات تنتقل العديد من الشركات عبر الوطنية إلى تصميم الأعمال الرقمية تزايد حصة الشركات الرقمية التي تقدم الخدمات من خلال منصاتها الخاصة (Google، Amazon، Apple، وMicrosoft، وeBay،

و Airbnb) وتدخل بلداناً جديدة ليس فقط من خلال التنوع الجغرافي ولكن أيضاً من خلال التوسع الرقمي (جمع البيانات وتخزينها ومعالجتها) يتزايد عدد المستخدمين تدريجياً وتتوسع تغطية بيانات المستخدم تصبح هذه البيانات مورداً جديداً في السوق الرقمية والتكنولوجيا الفائقة بامتلاكها مجموعة فريدة من البيانات، بما في ذلك البيانات الشخصية، يمكن للشركات التأثير على العمليات الاجتماعية والاقتصادية والسياسية في المناطق التي تعمل فيها وبالتالي، فإن التهديد الرئيسي هو انتقال بعض وظائف الدولة إلى منطقة نفوذ الشركات عبر الوطنية.

قد تنشأ اتجاهات سلبية أخرى أثناء التوسع الاستثماري والتكامل الرأسي من خلال اندماج الشركات المحلية الصغيرة والمتوسطة الحجم التي إما تتنافس مع الشركات في محاولات تطوير وتنفيذ تقنيات مبتكرة أو تقديم خدمات أخرى لنفس المستهلكين²⁵.

خاتمة

من خلال النتائج نقر بأن هناك انخفاض في مؤشرات نضج الحكومة الإلكترونية رغم الجهود الإصلاحية للحكومة الجزائرية المقتربة بالتحول الرقمي، حيث يبقى هذا التحول غير كافٍ لرفع قيمة مؤشر تنمية الحكومة الإلكترونية، كما أن مؤشر الأمن السيبراني للجزائر تحصل على نقاط متدنية لتظهر بذلك هشاشة الأمن السيبراني، رغم المحاولات والمجهودات المبذولة في وضع هياكل إدارية وتنظيمية لإدارة الأمن السيبراني، رغم ذلك فإن إحصائيات آخر السنوات مطمئنة بسبب بعض التقدم في عدد مستخدمي الإنترنت في الجزائر بزيادة 0.1% بين عامي 2022-2023 كما أنه من المتوقع حسب Statista أن ترتفع حصة السكان الذين لديهم إمكانية الوصول إلى الإنترنت في الجزائر بشكل مستمر بين عامي 2024 و 2028 بإجمالي 15.3 نقطة مئوية.

إن العوامل الخارجية المهددة للسيادة الرقمية شكلت عبئاً إضافياً على إرساء عملية التحول الرقمي في الجزائر خاصة في ظل انتشار الشركات العابرة للقارات، وبروز أجنداث عالمية رقمية جديدة إضافة إلى الصراع من أجل الريادة الإلكترونية كلها عوامل تستدعي بناء نظام متكامل لإجراءات الاستجابة في مجال سياسة التحول الرقمي وتحويل كل تلك التهديدات إلى فرص حقيقية.

توصي الدراسة بما يلي:

- تمتلك الجزائر مهارات بشرية هائلة من شأنها خلق فوارق رقمية في مجال الأمن الرقمي لو يتم استغلالها بالشكل المطلوب وتوفير الإمكانيات اللازمة لإبداعاتها في هذا المجال.
 - على الجزائر تقوية بيئتها الرقمية في مجال تكنولوجيا الاعلام والاتصال بما يواكب ويتناسب مع المتطلبات والتحديات العالمية الرقمية.
 - تطوير استراتيجيات أمنية الكترونية حقيقية، عبر انشاء مؤسسات مستقلة للتأمين الإلكتروني وعدم حصرها في الأجهزة الأمنية للدولة فقط.
 - ضرورة الإنفاق على تكنولوجيا المعلومات و الإقتناع بكونها مهمة أهمية الإنفاق العسكري كونها عنصر مضاعف لقوة الدولة.
 - ضبط وتعديل المنظومة القانونية والتشريعية وتكييفها مع القوانين الدولية لتفادي التهديدات السيبرانية.
 - المراقبة والتعامل الذكي مع التهديدات الخارجية للشركات العابرة للحدود في إطار قانون دولي يحمي المصالح الداخلية لأنه يمكن للشركات التي تمتلك التكنولوجيا الفائقة ومجموعة فريدة من البيانات التأثير على العمليات الاجتماعية والإقتصادية والسياسية في المناطق التي تعمل فيها وبالتالي، ينتقل التهديد من بعض وظائف الدولة إلى منطقة نفوذ الشركات عبر الوطنية.
 - كما تقترح الدراسة ضرورة إتباع نهج علمي متوازن لدراسة الإمكانيات الإيجابية وخصائص العوامل الخارجية في تشكيل السيادة الرقمية.
- التهميش:**

¹ - Shcherbakova L.N.*others"Advances in Economics, Business and Management Research", volume 148 ,2020, Department of Economic Theory and Public Administration Kemerovo State University Kemerovo, Russia.

²بسمه محرم الحداد، محمود مُجَدَّ إبراهيم، "منشآت الأعمال والتحول الرقمي"، مجلة الجمعية المصرية لنظم المعلومات وتكنولوجيا الحاسبات، المجلد 21 ، (2018)، ص25.

³ -Euro pean Digital Sovereignty. Institute of European Democrats. <https://www.iedonline.eu/download/2021/IED-Research-Paper-Innerarity.pdf> (date of access: 25/03/2025)

⁴ - دحان حازم، ناصر القريطي، الأمن السيبراني وحماية أمن المعلومات، الإسكندرية، دار الفكر الجامعي، الطبعة الأولى، 2021، ص7

⁵ - Pohle Julia Digital **sovereignty** Internet Policy Review 9(4) | 2020

⁶ - Christl, W. *Corporate Surveillance In Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions* [Report]. Cracked Labs 2017. <http://crackedlabs.org/en/corporate-surveillance>

⁷ - Staab, P. *Digitaler Kapitalismus: Markt und Herrschaft in der Ökonomie der Unknappheit*. Suhrkamp. 2019.

⁸ - van Dijck, J.. Governing digital societies: Private platforms, public values. *Computer Law & Security Review*, 36 2020. <https://doi.org/10.1016/j.clsr.2019.105377>

⁹ - SIMON KEMP, *DIGITAL 2023: ALGERIA*, 13 FEBRUARY 2023, <https://vu.fr/HgWQm>(date of access: 25/03/2025)

¹⁰ - Saifaddin Galal, *Percentage change in the number of internet users in Algeria from 2014 to 2023* Jun 29, 2023

¹¹ - Degenhard, Internet usage, 2023 <https://www.statista.com/forecasts/1137904/internet-penetration-forecast-in-algeria> (date of access: 23/03/2025)

¹² - *Cybersécurité : l'Algérie classée 23e en Afrique*, 8 Septembre 2021 <https://vinybusiness.com/algerie-23e-afrique-cybersecurite> (date of access: 23/03/2025)

¹³ - زمورة جمال، بن عيسى ليلي، "أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر"، مجلة البحوث، الإقتصادية المتقدمة، المجلد 07، العدد 02، 2022، ص 429-415.

¹⁴ - بن مرزوق عنتر، حرشاوي محي الدين، "الأمن السيبراني كبعد جديد في السياسة الجزائرية"، مجلة دفاتر السياسة والقانون، العدد 17، جامعة قاصدي مرباح، 2017، ص ص 65-80، ص ص 64-63

¹⁵ - *Indice Développement Cybersécurité par Pays [Cas de l'Algérie]* AfricaCyberMag, 27 avril 2022 <https://cybersecuritymag.africa/docs/Index-Cybers%C3%A9curit%C3%A9-Algerie.pdf>(date of access: 25/03/2025)f

-¹⁶ ليلي بن برغوث، "الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر"، المجلة الدولية للاتصال الاجتماعي، المجلد 10، العدد 01 (2023)، ص 453-454.

¹⁷ - The European Parliament and the Council of the European Union. (2016). Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Retrieved from <https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0402> (date of access: 07/09/2024).

¹⁸ -Dugin, A.G." Geopolitical future of Russia: Multipolarity and main strategic prospects in the 21st century". Moscow University Bulletin. Series 18. Sotsiologiyaipolitologiya, 2, (2011), 68-97.

¹⁹ - **United Nations**. "The impact of digital technologies". (2020). Retrieved from <https://www.un.org/ru/un75/impact-digital-technologies> (date of access 08/09/2024)

²⁰ - United Nations Secretary-General. Secretary-General's Strategy on new technologies. (2018). Retrieved from <https://www.un.org/en/newtechnologies/> (date of access: 07/09/2024)

²¹ - Yan, X.. China-US "competition in digital era. Global Times". (2021).Retrieved from <https://www.globaltimes.cn/content/1177615.shtml> (date of access: 05/09/2024).

²² - Acharya, A., Arnold, Z.. Chinese public AI R&D "spending: Provisional findings. Center for Security and Emerging Technology (CSET) Issue Brief". (2019). Retrieved from <https://cset.georgetown.edu/research/chinese-public-ai-rd-spending-provisional-findings/> (date of access: 05/09/2024).

²³ - Kamolov, S.G., Mirakova, D.A.. Kommertsializatsiya kosmicheskoi deyatel'nosti: Klyuchevye trendy sovremennosti [Commercialization of space activities: Key trends of our time]. Intellect. Innovatsii. Investitsii, 7, 52-63. (2019) Retrieved from <https://doi.org/10.25198/2077-7175-2019-7-52> date of access: 12/09/2024

²⁴ - Markova, O.A., Meleshkina, A.I.. "Digital protectionism: Myth or reality Dizhital protestionist: Mytn or realtyshch". Scientific research of the Faculty of Economics. Electronic journal, 13(2), (2021).26-40. Retrieved from <https://doi.org/10.38050/2078-3809-2021-13-2-26-40> date of access: 29/08/2024

²⁵ - Dhulipala, R., Mehrotra, N., Kanitkar, A.. "The vision of a digital public infrastructure for agriculture". T20 Policy Brief. (2023). Retrieved from https://t20ind.org/wpcontent/uploads/2023/06/T20_PolicyBrief_TF2_252_DPI4A-N.pdf date of access: 02/09/2024