

السيادة الرقمية وأهميتها في حماية الدولة

Digital sovereignty and its Importance in Protecting the State

د. عمر الحسين*

كلية الحقوق والعلوم السياسية، جامعة احمد

بوقرة - بومرداس

o.elhocine@univ-boumerdes.dz

تاريخ إرسال المقال: 2026-05-08 تاريخ قبول المقال: 2026-08-16 تاريخ نشر المقال: 2026-09-22

الملخص:

يُبرز هذا البحث أهمية السيادة الرقمية باعتبارها أحد المرتكزات الأساسية لممارسة الدولة لصلاحياتها داخل الفضاء السيبراني، ووسيلة فعّالة لتحقيق الاستقلال التكنولوجي وتقليص التبعية للقوى الأجنبية. وقد أظهر التحليل أن التحكم في التكنولوجيا وإنتاجها واستغلالها يُعدّ عاملاً حاسماً في تعزيز المكانة الأمنية والجيوسياسية للدولة. كما بيّن البحث أن الإطار التشريعي الجزائري، من خلال قانون العقوبات والقانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقانون الإجراءات الجزائية رقم 66-155، إضافة إلى المرسوم الرئاسي رقم 23-314 المتعلق بمحافضة سامية للرقمنة، يُوفّر أساساً قانونياً مهماً لتنظيم الفضاء الرقمي ومكافحة الجرائم السيبرانية، وإن كان لا يزال بحاجة إلى مزيد من التطوير لمواكبة التحولات المتسارعة.

وقد خلص البحث إلى أن تحقيق السيادة الرقمية يقتضي تبني رؤية استراتيجية شاملة تقوم على تعزيز الأمن السيبراني، وتطوير البنى التحتية الرقمية، وضمان مرونة نظم المعلومات داخل المؤسسات العامة. كما أبرزت النتائج ضرورة دعم الإطار القانوني بنصوص أكثر تخصصاً، وتعزيز التنسيق بين الهيئات المعنية، إلى جانب الاستثمار في القدرات التقنية والبشرية، بما يضمن حماية فعّالة للفضاء الرقمي ويُعزز الاستقلال التكنولوجي للدولة.

الكلمات المفتاحية: السيادة الرقمية، الاستقلال التكنولوجي للدولة، الفضاء الرقمي، الجرائم السيبرانية.

Abstract:

This research highlights the importance of digital sovereignty as a fundamental pillar for the exercise of state authority within cyberspace and as a key mechanism for achieving technological independence and reducing reliance on foreign powers. The analysis shows that controlling, producing, and effectively utilizing technology is a decisive factor in strengthening the state's security and geopolitical position. It also demonstrates that the Algerian legal framework—through the Penal Code, Law No. 09-04 on the prevention and fight against ICT-related crimes, Code of Criminal Procedure No. 66-155, and Presidential Decree No. 23-314 establishing the High Commission for Digitalization—provides a significant legal basis for regulating cyberspace and combating cybercrime, although it still requires further development to keep pace with rapid technological changes.

The research concludes that achieving digital sovereignty requires adopting a comprehensive strategic approach based on strengthening cybersecurity, developing digital infrastructure, and ensuring the resilience of information systems across public institutions. It also emphasizes the need to enhance the legal framework with more specialized provisions, improve coordination among relevant authorities, and invest in technical and human capacities, in order to ensure effective protection of cyberspace and reinforce the state's technological independence.

Keywords: Digital sovereignty, technological independence of the state, cyberspace, cybercrime.

المقدمة:

تُعدّ التحولات التكنولوجية المتسارعة من أبرز ملامح العصر الحديث، حيث أحدثت الرقمنة طفرة نوعية في مختلف مجالات الحياة، وأسهمت في تقليص المسافات وتحويل العالم إلى فضاء مترابط تنتقل فيه المعلومات بسرعة غير مسبوقة. وقد أفرز هذا الواقع مفاهيم جديدة تعكس طبيعة المرحلة، من أهمها مفهوم السيادة الرقمية، الذي أصبح يعبر عن قدرة الدولة على التحكم في بنيتها التكنولوجية وتأمين فضاءها الرقمي. ولم تعد السيادة بمفهومها التقليدي مقتصرة على الإقليم المادي، بل امتدت لتشمل الفضاء الافتراضي الذي أضحي جزءاً لا يتجزأ من كيان الدولة، في ظل ما يشهده من مخاطر متزايدة كالهجمات السيبرانية، والتجسس الإلكتروني، والتحكم الخارجي في البيانات والبنى التحتية، بما قد يهدد الاستقرار ويمس بالأمن القومي¹.

وفي هذا السياق، تبرز السيادة الرقمية كركيزة أساسية لحماية الدولة في العصر الرقمي، لما تعكسه من قدرة على امتلاك التكنولوجيا وتطويرها، والتحكم في تدفق المعلومات، وضمان أمن البيانات الاستراتيجية.

¹ - مازيا عيساوي، تحولات الرقمنة وعصر البحث المفتوح بين الأيديولوجيا والتطبيق، مجلة التغيير الاجتماعي، المجلد 10،

السيادة الرقمية وأهميتها في حماية الدولة

كما ترتبط بمدى استقلالية القرار الرقمي بعيدًا عن الهيمنة الأجنبية، وهو ما دفع الدول إلى تبني استراتيجيات متكاملة لتعزيزها، من خلال تطوير البنى التحتية الرقمية، وسنّ تشريعات لحماية البيانات، وتعزيز الأمن السيبراني، وتشجيع الابتكار المحلي، إلى جانب الانخراط في التعاون الدولي لمواجهة التهديدات العابرة للحدود. وفي هذا الإطار، يطرح البحث إشكالية مدى إسهام السيادة الرقمية في حماية الدولة وتعزيز أمنها القومي، والآليات القانونية الكفيلة بذلك. وقد أظهر التحليل أن الإطار التشريعي الجزائري، من خلال قانون العقوبات والقانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال² وقانون الإجراءات الجزائية رقم 66-155³، إضافة إلى المرسوم الرئاسي رقم 23-314 المتعلق بمحافظة سامية للرقمنة⁴، يوفر أساسًا مهمًا لتنظيم الفضاء الرقمي، غير أنه يظل بحاجة إلى تطوير لمواكبة التحولات المتسارعة. كما خلص البحث إلى أن تحقيق السيادة الرقمية يقتضي اعتماد رؤية استراتيجية شاملة تقوم على تعزيز الأمن السيبراني، وتطوير البنى التحتية، وضمان مرونة نظم المعلومات، إلى جانب دعم الإطار القانوني وتعزيز التنسيق المؤسسي والاستثمار في القدرات التقنية والبشرية، بما يكفل حماية فعّالة للفضاء الرقمي ويعزز الاستقلال التكنولوجي للدولة.

ومن هذا المنطلق تبرز إشكالية: إلى أي مدى تُسهم السيادة الرقمية في حماية الدولة وتعزيز أمنها القومي، وما هي الآليات القانونية والمؤسسية الكفيلة بمواجهة التهديدات الرقمية المعاصرة؟
للإجابة على الإشكالية المطروحة، تم تقسيم هذا البحث إلى مبحثين رئيسيين؛ يتناول المبحث الأول مفهوم السيادة الرقمية من خلال تحديد تعريفها وخصائصها وأبعادها القانونية، بما يسمح بفهم طبيعتها وحدودها في البيئة الرقمية. أما المبحث الثاني فيُخصّص لدراسة دور السيادة الرقمية في حماية الدولة، وذلك من خلال تحليل مساهمتها في تعزيز الأمن السيبراني، وصون البيانات، وضمان الاستقلال التكنولوجي في مواجهة التهديدات الرقمية المعاصرة.

² - قانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 200. يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج وعدد 47 بتاريخ 2009.02/08/16.

³ - قانون الإجراءات الجزائية أمر رقم 66-155 مؤرخ في 18 صفر 1386 الموافق 8، المعدل والمتمم بالقانون رقم 23-13 المؤرخ في 5 غشت سنة 2023 الجريدة الرسمية عدد 52.

⁴ - المرسوم الرئاسي رقم 23-314 الصادر في 20 صفر 1445هـ الموافق 6 سبتمبر 2023 يتعلق بإحداث محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسير عملها. ج وعدد 59 الصادرة بتاريخ 24 صفر 1445هـ الموافق لـ 2023/09/10.

السيادة الرقمية وأهميتها في حماية الدولة

ولمعالجة هذه الإشكالية، تم الاعتماد على المنهج التحليلي لدراسة النصوص القانونية ذات الصلة، إلى جانب المنهج الوصفي لعرض مفاهيم السيادة الرقمية وتطبيقاتها.

المبحث الأول: مفهوم السيادة الرقمية

تتعدد المفاهيم التي حاولت ضبط هذا المصطلح؛ إذ تُعرّف السيادة الرقمية، وفق اتجاه أول، بأنها قدرة الفاعلين—سواء كانوا دولاً أو أفراداً—على إتقان التكنولوجيا والتحكم في مساراتها الاقتصادية والاجتماعية والسياسية، بما يسمح بتحديد الخيارات التكنولوجية بشكل مستقل. ويُوسّع اتجاه آخر هذا المفهوم، كما ورد في تقارير رسمية، ليشمل قدرة الدولة على التصرف بحرية داخل الفضاء الإلكتروني، واتخاذ قرارات مستقلة، وممارسة سلطتها بما ينسجم مع قيمها ومصالحها الاستراتيجية. كما يربط اتجاه ثالث السيادة الرقمية بعلاقات القوة داخل السوق الرقمية، حيث تُفهم على أنها قدرة بعض الفاعلين المهيمنين—سواء كانوا دولاً أو شركات—على فرض قواعدهم ومعاييرهم التقنية والقانونية، وإلزام الآخرين بالامتثال لها، مستندين في ذلك إلى موقعهم المسيطر على البنى التحتية الرقمية وتدفقات البيانات تتعدد المفاهيم التي حاولت ضبط هذا المصطلح؛ إذ تُعرّف السيادة الرقمية، وفق اتجاه أول، بأنها قدرة الفاعلين—سواء كانوا دولاً أو أفراداً—على إتقان التكنولوجيا والتحكم في مساراتها الاقتصادية والاجتماعية والسياسية، بما يسمح بتحديد الخيارات التكنولوجية بشكل مستقل. ويُوسّع اتجاه آخر هذا المفهوم، كما ورد في تقارير رسمية، ليشمل قدرة الدولة على التصرف بحرية داخل الفضاء الإلكتروني، واتخاذ قرارات مستقلة، وممارسة سلطتها بما ينسجم مع قيمها ومصالحها الاستراتيجية. كما يربط اتجاه ثالث السيادة الرقمية بعلاقات القوة داخل السوق الرقمية، حيث تُفهم على أنها قدرة بعض الفاعلين المهيمنين—سواء كانوا دولاً أو

السيادة الرقمية وأهميتها في حماية الدولة

شركات—على فرض قواعدهم ومعاييرهم التقنية والقانونية، وإلزام الآخرين بالامتثال لها، مستندين في ذلك إلى موقعهم المسيطر على البنى التحتية الرقمية وتدفقات البيانات⁵.

المطلب الأول: تعريف السيادة الرقمية

تتمثل السيادة الرقمية في قدرة الدولة على بسط سيطرتها على المجال الرقمي، وقد تعددت التعريفات الفقهية لهذا المفهوم تبعاً لتطور البيئة التكنولوجية الحديثة. فُعرفت بأنها قدرة الدول على التحكم في بنيتها التحتية الرقمية وحماية بيانات مواطنيها، خاصة بعد أن أصبحت التكنولوجيا الرقمية مجالاً للتنافس والصراع الدولي. كما يُنظر إليها باعتبارها امتداداً للاستقلالية الاستراتيجية، من خلال تمكين الدولة من اتخاذ قراراتها الرقمية بصورة مستقلة في مختلف القطاعات المرتبطة بالتكنولوجيا والاتصال. كذلك تُجسد السيادة الرقمية قدرة الدولة على التحكم في مصيرها الرقمي عبر السيطرة على البيانات والأجهزة والبرمجيات التي تعتمد عليها في إدارة شؤونها المختلفة.

ويميز جانب من الفقه بين السيادة الرقمية للشعوب والسيادة الرقمية الشخصية؛ إذ تشير الأولى إلى تحكم الشعوب والمجتمعات في بياناتها ومصيرها الرقمي بما يعزز استقلالها وهويتها، بينما تعبر الثانية عن قدرة الأفراد على التحكم في تقنياتهم وبياناتهم باستخدام البرامج المفتوحة المصدر ووسائل الاتصال المشفرة. ومن جهة أخرى، ارتبط مفهوم السيادة الرقمية بقدرة الدول على فرض سلطتها على الشركات التكنولوجية العملاقة ومنصات التواصل الاجتماعي، خاصة عقب بعض الوقائع التي أثارت جدلاً سياسياً واسعاً نتيجة حذف أو تعليق حسابات رؤساء دول بدعوى مخالفة سياسات تلك المنصات. وبناءً على ذلك، أصبحت السيادة الرقمية تعبر عن سلطة قانونية وواقعية تخول للدولة تنظيم الفضاء الرقمي الذي يتفاعل داخله مواطنوها، في ظل اعتماد الشركات الرقمية الكبرى على البيانات الشخصية باعتبارها مورداً أساسياً لنشاطها الاقتصادي والتكنولوجي.

ويشير مفهوم السيادة الرقمية إلى امتداد مفهوم السيادة التقليدية إلى المجال الإلكتروني، حيث لم يعد نفوذ الدولة يقتصر على الحدود الجغرافية فقط، بل أصبح يشمل الفضاء السيبراني وما يرتبط به من تقنيات واتصالات وخدمات رقمية تؤثر في الأمن والاقتصاد والثقافة والسياسة.

⁵ - خالدية بلحاج، محمد فرعون، السيادة الرقمية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 11، العدد 1، 2025، ص

السيادة الرقمية وأهميتها في حماية الدولة

المطلب الثاني: أبعاد السيادة الرقمية

تبرز أهمية دراسة أبعاد السيادة الرقمية باعتبارها مفهوماً متعدد الجوانب يشمل البعد السياسي، والأمني، والاقتصادي، والتقني، والثقافي، حيث تتداخل هذه الأبعاد لتشكل إطاراً جديداً لممارسة الدولة لسلطتها في البيئة الرقمية، بما يضمن حماية مصالحها الوطنية وتحقيق استقلالها في مواجهة التحديات الرقمية المعاصرة.

أولاً: السيادة الرقمية في بعدها القانوني

يُعبّر البعد القانوني للسيادة الرقمية عن امتداد مفهوم السيادة التقليدية ليشمل الفضاء الرقمي، حيث تسعى الدول إلى بسط سلطتها التنظيمية على الشبكات والمنصات الإلكترونية. ويظهر هذا التوجه في سعي الدول إلى سنّ تشريعات تُنظّم تدفق البيانات وتحمي أمنها الرقمي، خاصة في ظل هيمنة قوى تكنولوجية عالمية. غير أن هذا المفهوم يختلف من دولة لأخرى، فبينما تتبنى بعض الدول نهجاً صارماً يقوم على فرض السيطرة الكاملة على الفضاء الرقمي، تتجه دول أخرى، لاسيما الأوروبية، إلى تحقيق توازن بين السيادة وحماية الحقوق والحريات الأساسية للمستخدمين.

ثانياً: السيادة الرقمية في بعدها السياسي والاقتصادي

يتجلى هذا البعد في بروز فاعلين اقتصاديين كبار، مثل الشركات التكنولوجية العالمية، الذين أصبحوا يمارسون نفوذاً واسعاً داخل الفضاء الرقمي. فبفضل سيطرتهم على البنى التحتية والخدمات الرقمية، باتوا قادرين على فرض قواعدهم الخاصة، وإدارة المحتوى، والتحكم في البيانات الشخصية للمستخدمين. ويؤدي هذا الواقع إلى إعادة تشكيل مفهوم السيادة، حيث لم تعد الدولة الفاعل الوحيد، بل أصبحت السيادة موزعة بين الدولة وهذه الكيانات الاقتصادية التي تملك قدرات تقنية وتنظيمية متقدمة⁶.

ثالثاً: السيادة الرقمية في بعدها الليبرالي (سيادة المستخدم)

يركّز هذا الاتجاه على تمكين الفرد داخل البيئة الرقمية، من خلال منحه القدرة على التحكم في بياناته واختيار الخدمات التي يستخدمها بحرية. فالمستخدم، في هذا الإطار، يُعدّ محور السيادة الرقمية، حيث

⁶ - لزرق نبيلة، بن زيدان حاج، الاقتصاد الرقمي والفجوة الرقمية: حالة الجزائر، مجلة الدراسات الاقتصادية المعمقة، المجلد 2، العدد 1، 2017، ص ص 158-183.

السيادة الرقمية وأهميتها في حماية الدولة

تهدف هذه المقاربة إلى حماية خصوصيته وضمان عدم استغلال بياناته من قبل الشركات أو الجهات الأخرى. ويعكس هذا التوجه تطوراً في فهم السيادة، إذ لم تعد مقتصرة على الدولة، بل أصبحت تشمل أيضاً حقوق الأفراد في الفضاء الرقمي⁷.

رابعاً: السيادة الرقمية كمدخل لتحقيق الاستقلال التكنولوجي

يرتبط تحقيق السيادة الرقمية بضرورة بناء بنية تحتية رقمية قوية ومتطورة، تُشكّل الأساس لأي تحول رقمي ناجح. وفي هذا السياق، تعمل الدول، ومنها الجزائر، على تطوير مشاريع رقمية وطنية، مثل رقمنة الخدمات العمومية وتوطين البيانات، إلى جانب سنّ تشريعات حديثة تُنظّم هذا المجال. كما يتطلب هذا المسار الاستثمار في الكفاءات التقنية وتعزيز الابتكار المحلي، بما يُمكن الدولة من تقليل تبعيتها التكنولوجية وتحقيق استقلالها الرقمي في مواجهة التحديات الدولية المتزايدة.

المبحث الثاني: دور السيادة الرقمية في حماية الدولة

تُبرز التطورات الدولية منذ سنة 2013 حجم التهديدات السيبرانية المرتبطة بهيمنة القوى التكنولوجية الكبرى، حيث كشفت تسريبات إدوارد سنودن عن وجود برامج مراقبة واسعة للإنترنت تديرها جهات أمريكية، الأمر الذي أدى إلى تراجع الثقة العالمية في التقنيات الرقمية الأجنبية، خاصة الأمريكية منها، وأثار موجة من الغضب الدولي. كما ساهم اكتشاف برامج تجسس متطورة، مثل بيغاسوس، في تعزيز المخاوف المتعلقة بانتهاك السيادة الرقمية للدول، لاسيما عندما استُخدمت هذه التقنيات في استهداف مؤسسات وأفراد، وهو ما اعتبرته العديد من الدول تهديداً مباشراً لأمنها القومي واستقرارها⁸.

وانطلاقاً من هذه التحديات، سعت الجزائر إلى تبني مقاربة استباقية لتعزيز سيادتها الرقمية وأمنها السيبراني، من خلال تطوير آليات حامية وتقوية استقلالها التكنولوجي، أسوة بعدد من الدول التي سبقتها في هذا المجال. فقد اعتمدت دول مثل كندا والصين ومصر والسعودية استراتيجيات وطنية للأمن السيبراني، وهو

⁷ - مروة خلة، سارة خلة، بشرى سلاوي، عبد النور البلدي، مستقبل السيادة الرقمية في ظل التكنولوجيات الحديثة: دراسة تحليلية استشرافية، مجلة بحوث ودراسات في الميديا الجديدة، 2023، المجلد 4، العدد 1، 2023، ص ص 61-79.

⁸ - كلاع شريفة، الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 1، 2022، ص ص 292-314.

السيادة الرقمية وأهميتها في حماية الدولة

ما يعكس إدراكًا عالميًا متزايدًا بأهمية السيادة الرقمية كوسيلة أساسية لحماية الدول من التهديدات السيبرانية وضمان استقلالها في الفضاء الرقمي.

المطلب الأول: صور التعدي على السيادة الرقمية للدول

يُقصد بالتعدي على السيادة الرقمية تلك الانتهاكات التي تمس قدرة الدولة على التحكم في بياناتها الرقمية وحمايتها وإدارة فضاءها السيبراني بشكل مستقل. وتتخذ هذه التعديات صورًا متعددة تعكس تنوع التهديدات التي تواجهها الدول في العصر الرقمي، ومن أبرزها الهجمات الإلكترونية والتجسس السيبراني، لما لهما من تأثير مباشر على الأمن القومي والبنية التحتية الرقمية⁹.

أولاً: الهجوم الإلكتروني

يتمثل الهجوم الإلكتروني في استخدام وسائل وتقنيات رقمية أو كهرومغناطيسية لاستهداف الأنظمة المعلوماتية والبنى التحتية الحيوية للدولة، بهدف تعطيلها أو إضعاف كفاءتها. وتشمل هذه الهجمات عمليات التشويش والتضليل الإلكتروني، وقد تؤدي إلى خسائر مادية جسيمة دون أن تتسبب بالضرورة في خسائر بشرية كما هو الحال في الحروب التقليدية. ومن أمثلة ذلك تعطيل أنظمة الاتصالات والدعم اللوجستي، أو التحكم في شبكات الطاقة والكهرباء، مما ينعكس سلبًا على قدرات الدولة التشغيلية والأمنية¹⁰.

ثانياً: التجسس الإلكتروني

يُعدّ التجسس الإلكتروني من أخطر أشكال التعدي على السيادة الرقمية، حيث يقوم على اختراق الأنظمة والشبكات المعلوماتية بطريقة غير مشروعة بهدف الحصول على معلومات حساسة أو التلاعب بها. ويُنظر إليه كمرحلة تمهيدية في الحروب السيبرانية، لما له من دور في جمع المعلومات الاستراتيجية. كما يشمل محاولات اختراق أجهزة الحاسوب والمواقع الرسمية التابعة للدول، بهدف سرقة البيانات السرية أو استخدامها لتحقيق أهداف سياسية أو اقتصادية، مما يشكل تهديدًا مباشرًا للأمن القومي ومصالح الدول.

ثالثاً: التجسس الإلكتروني في أبعاده الحديثة

⁹ - ليلي بعوني، التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الإلكترونية نموذجاً، مجلة ستراتيجيا، المجلد8، العدد2، 2021، ص ص 6-22.

¹⁰ - محمد الصغير كاجه، الهجمات السيبرانية بين الواقع وسبل المواجهة، مجلة الرسالة للدراسات الإعلامية، المجلد6، العدد3، 2022، ص ص 108-117.

السيادة الرقمية وأهميتها في حماية الدولة

يشهد مفهوم التجسس في العصر الرقمي تحولاً جذرياً، حيث لم يعد مقتصرًا على المجال العسكري كما كان في السابق، بل امتد ليشمل مجالات متعددة مثل الاقتصاد، والتكنولوجيا، والسياسة، والصناعة. ورغم استمرار أهمية التجسس العسكري، فإن طبيعة المعلومات المستهدفة تغيرت؛ فبعد أن كانت تتركز حول حجم الجيوش وتسليحها، أصبحت اليوم متاحة جزئيًا عبر وسائل الإعلام، مما دفع إلى التركيز على معلومات أكثر دقة وحساسية، كالتكنولوجيا المتقدمة، والاستراتيجيات الاقتصادية، والبيانات العلمية والصناعية. ويعكس هذا التحول تطور مفهوم الأمن القومي، الذي أصبح يعتمد بشكل كبير على التحكم في المعرفة والمعلومات في البيئة الرقمية¹¹.

رابعاً: الاختراق الإلكتروني

يُعدّ الاختراق الإلكتروني من أبرز صور التعدي على السيادة الرقمية، حيث يتمثل في التسلل غير المشروع إلى الأنظمة المعلوماتية بهدف الحصول على معلومات استخباراتية أو إلحاق الضرر بالبنية الرقمية للدولة أو المؤسسة المستهدفة. ويتم ذلك عبر برامج أو أدوات مصممة لاختراق الأنظمة واستغلال الثغرات التقنية، بهدف السيطرة على البيانات أو تعطيل الأنظمة. وقد يتم هذا الاختراق على مستويات مختلفة، سواء من قبل أفراد أو جماعات منظمة أو حتى دول، ويهدف في النهاية إلى تحقيق التفوق في المجالات الأمنية أو العسكرية أو السياسية من خلال السيطرة على المعلومات الحيوية.

خامساً: الهجمات على البنية التحتية الحيوية

تُعدّ الهجمات التي تستهدف البنية التحتية الحيوية من أخطر التهديدات السيبرانية، نظراً لتأثيرها المباشر على حياة الأفراد واستقرار الدول، فبالرغم من أن بعض الهجمات، مثل هجمات الحرمان من الخدمة، قد تبدو محدودة التأثير تقنياً، إلا أن استهداف الأنظمة الصناعية أو الإدارية المرتبطة بالبنية التحتية قد يؤدي إلى نتائج كارثية، مثل تعطيل شبكات الطاقة أو إمدادات النفط والغاز أو أنظمة النقل. وقد شهد العالم حوادث فعلية تؤكد خطورة هذه التهديدات، مثل الهجمات التي استهدفت مؤسسات صحية وأدت إلى تعطيل خدماتها، أو تلك التي طالت شبكات الكهرباء وأدت إلى انقطاع التيار عن مئات الآلاف من

¹¹ - مريم نباش، سعاد بولقرون، التجسس وانتهاك حق الخصوصية في العصر الرقمي دراسة وصفية تحليلية لبرنامج بيغاسوس،

مجلة رقمنة للدراسات الإعلامية والاتصالية، المجلد 2، العدد 3، 2022، ص ص 63-78.

السيادة الرقمية وأهميتها في حماية الدولة

المستخدمين. وتبرز هذه الوقائع الحاجة الملحة إلى تعزيز أمن البنية التحتية الرقمية باعتبارها ركيزة أساسية للأمن الوطني¹².

المطلب الثاني: الآليات القانونية ودور السيادة الرقمية في حماية الدولة

يبرز دور السيادة الرقمية في حماية الدولة من خلال إرساء منظومة قانونية متكاملة تمكّنها من مواجهة مختلف التهديدات والانتهاكات التي تستهدف فضاءها الرقمي، وذلك عبر تجريم الأفعال الماسة بأنظمة المعلومات وتأمين الإطار القانوني اللازم لمعاقبة مرتكبيها. وفي هذا السياق، عملت الدول، سواء بشكل فردي أو ضمن تكتلات دولية، على سنّ تشريعات خاصة لمكافحة الجرائم العابرة للحدود، نظراً لطبيعتها التي تستدعي تعاوناً دولياً واستجابة سريعة ضمن إطار قانوني فعال.

وفي الجزائر، تجسّد هذا التوجه من خلال تطوير الترسانة القانونية بما يواكب التطور التكنولوجي، حيث تم تعديل قانون العقوبات بموجب القانون رقم 04-10 المؤرخ في 10 نوفمبر 2004، وإدراج أحكام خاصة تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، من خلال تجريم الولوج غير المشروع، والبقاء الاحتيالي، وتخريب أو تعديل البيانات أو الأنظمة. كما شدّد المشرّع العقوبات عند استهداف مؤسسات حساسة، كالدفاع الوطني، واعتبر الشروع في هذه الجرائم معاقباً عليه. ويُسّكمل هذا الإطار بقانون الإجراءات الجزائية الذي حدّد الاختصاص القضائي في الجرائم المعلوماتية، إلى جانب القانون رقم 09-04 المؤرخ في 05 أوت 2009، الذي وضع قواعد خاصة للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، بما يعكس الدور المحوري للسيادة الرقمية في تعزيز أمن الدولة وحماية مصالحها الاستراتيجية.

لا تكتمل الجهود القانونية في تعزيز دور السيادة الرقمية في حماية الدولة إلا بوجود أجهزة وهيئات متخصصة تسهر على التطبيق الفعلي للقواعد القانونية على أرض الواقع. وفي هذا الإطار، أنشأت الجزائر عدة هيكل أمنية وتقنية لمكافحة الجرائم ذات الطابع الرقمي، من أبرزها خلية مكافحة الجريمة الإلكترونية

¹² - وداد بوطلاعة، الهجمات السيبرانية على البنية التحتية الحرجة : دراسة في ضوء القانون الدولي، مجلة حقوق الانسان والحريات العامة، المجلد7، العدد2، 2022، ص ص 322-355.

السيادة الرقمية وأهميتها في حماية الدولة

على مستوى المديرية العامة للأمن الوطنى سنة 2011، والتي تم تعزيزها لاحقاً بإنشاء المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال سنة 2015، التابعة للشرطة القضائية. وتُعدّ هذه المصلحة جهازاً عملياً متخصصاً يضم محققين ذوي كفاءة عالية في مجال التحقيقات الرقمية، حيث سجلت مئات القضايا المرتبطة بالمراس بالمراس بأنظمة المعالجة الآلية للمعطيات خلال السنوات الأخيرة، ما يعكس تزايد التهديدات الرقمية وأهمية التصدي لها¹³.

كما تم بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08 نوفمبر 2015 إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهي هيئة إدارية مستقلة تتمتع بالشخصية المعنوية، تعمل تحت إشراف وزير العدل ورقابة السلطة القضائية. وتضطلع هذه الهيئة بمهام تنسيق عمليات الوقاية، وجمع المعلومات، وضمان مراقبة وتسجيل وحفظ المعطيات الرقمية، مع تقديم الدعم للجهات القضائية في مجال الإجراءات المرتبطة بالجرائم المعلوماتية¹⁴.

ولا تقتصر جهود الجزائر في تعزيز سيادتها الرقمية على هذه الهياكل فقط، بل تمتد إلى مشاريع استراتيجية مستقبلية، من بينها إنشاء المركز الوطنى الجزائري للخدمات الرقمية، الذي يُعد خطوة مهمة نحو تحقيق الاستقلال التكنولوجي وتعزيز البنية التحتية الرقمية، وذلك في إطار شراكات تقنية دولية، من بينها التعاون مع Huawei، بما يعكس توجه الدولة نحو بناء منظومة رقمية متكاملة ومستدامة.

الخاتمة:

يُظهر هذا البحث أن السيادة الرقمية أصبحت عنصراً جوهرياً في بنية الدولة الحديثة، ولم تعد مجرد مفهوم نظري، بل أضحت ضرورة استراتيجية تفرضها التحولات التكنولوجية المتسارعة. فقد أدى الانتقال إلى البيئة الرقمية إلى إعادة تشكيل مفهوم السيادة، بحيث امتد من المجال الجغرافي التقليدي إلى الفضاء السيبراني، بما يحمله من فرص ومخاطر في آن واحد. وفي هذا السياق، يتجلى الدور المحوري للسيادة

¹³ - توفيق تقيّة، رشيد بويكر، الأطر القانونية لتعزيز السيادة الرقمية للدولة في مواجهة التحديات المتعلقة بالاستخدامات السلبية المحتملة للذكاء الاصطناعي، المجلد 11، العدد 1، 2024، ص ص 130-148.

¹⁴ - رامي حليم، إجراءات استخلاص الدليل في الجرائم المعلوماتية، دفاثر البحوث العلمية، المجلد 09، العدد 01، 2021، ص

السيادة الرقمية وأهميتها في حماية الدولة

الرقمية في حماية الدولة من التهديدات السيبرانية، وضمان استقلال قرارها التكنولوجي، وتعزيز أمنها القومي في ظل تزايد التحديات المرتبطة بالاختراقات والتجسس والتحكم الخارجي في البيانات.

كما تبين أن المشرع الجزائري قد سعى إلى مواكبة هذه التحولات من خلال ترسانة قانونية تشمل قانون العقوبات والقانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقانون الإجراءات الجزائية رقم 66-155، إلى جانب المرسوم الرئاسي رقم 23-314 المتعلق بمحافظة سامية للرقمنة، غير أن هذه الجهود، رغم أهميتها، لا تزال بحاجة إلى تطوير مستمر لمواكبة الديناميكية الرقمية العالمية.

النتائج

- تبين أن السيادة الرقمية تمثل ركيزة أساسية لحماية الدولة وضمان أمنها القومي في العصر الرقمي .
- أظهر البحث أن التحكم في التكنولوجيا والبنى التحتية الرقمية يُعدّ عاملاً حاسماً في تعزيز الاستقلال التكنولوجي وتقليل التبعية الخارجية .
- وجود إطار قانوني جزائري مهم لتنظيم الفضاء الرقمي ومكافحة الجرائم السيبرانية، إلا أنه يتسم بالتشتت ويحتاج إلى مزيد من التخصص والتحديث .
- تزايد التهديدات السيبرانية، مثل الهجمات الإلكترونية والتجسس الرقمي، يفرض على الدول تطوير آليات وقائية واستباقية .
- وجود جهود مؤسساتية في الجزائر لتعزيز الأمن السيبراني، لكنها تحتاج إلى تنسيق أكبر وفعالية أعلى .

التوصيات

- ضرورة تحديث الإطار التشريعي الجزائري بشكل دوري لمواكبة التطورات التكنولوجية المتسارعة، مع سنّ قانون خاص بالسيادة الرقمية .
- تعزيز الأمن السيبراني من خلال تطوير البنى التحتية الرقمية وتحديث أنظمة الحماية المعلوماتية .
- دعم التنسيق بين مختلف الهيئات والمؤسسات المعنية بالأمن الرقمي لضمان فعالية الاستجابة للتهديدات .
- الاستثمار في تكوين الموارد البشرية المتخصصة في مجال الأمن السيبراني والتقنيات الرقمية .
- تشجيع الابتكار المحلي وتطوير الصناعات التكنولوجية الوطنية لتحقيق الاستقلال الرقمي .

السيادة الرقمية وأهميتها في حماية الدولة

- تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية وتبادل الخبرات والمعلومات.

قائمة المصادر والمراجع:

أولا: النصوص القانونية

- قانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 200. يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج وعدد 47 بتاريخ - 2009.02/08/16.
- قانون الإجراءات الجزائية أمر رقم 66-155 مؤرخ في 18 صفر 1386 الموافق 8، المعدل والمتمم بالقانون رقم 23-13 المؤرخ في 5 غشت سنة 2023 الجريدة الرسمية عدد 52.
- المرسوم الرئاسي رقم 23-314 الصادر في 20 صفر 1445 هـ الموافق 6 سبتمبر 2023 يتعلق بإحداث محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسير عملها. ج وعدد 59 الصادرة بتاريخ 24 صفر 1445 هـ الموافق لـ 2023/09/10.

ثانيا: المقالات

- مازيا عيساوي، تحولات الرقمنة وعصر البحث المفتوح بين الأيديولوجيا والتطبيق، مجلة التغيير الاجتماعي، المجلد 10، العدد 2، 2025، ص ص 79-94.
- خالدية بلحاج، محمد فرعون، السيادة الرقمية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 11، العدد 1، 2025، ص ص 461-477.
- لزرق نبيلة، بن زيدان حاج، الاقتصاد الرقمي والفجوة الرقمية: حالة الجزائر، مجلة الدراسات الاقتصادية المعمقة، المجلد 2، العدد 1، 2017، ص ص 158-183.
- مروة خلة، سارة خلة، بشرى سلاوي، عبد النور البلدي، مستقبل السيادة الرقمية في ظل التكنولوجيات الحديثة: دراسة تحليلية استشرافية، مجلة بحوث ودراسات في الميديا الجديدة، 2023، المجلد 4، العدد 1، 2023، ص ص 61-79.
- كلاع شريفة، الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 1، 2022، ص ص 292-314.
- ليلي بعوني، التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الالكترونية نموذجا، مجلة ستراتيجيا، المجلد 8، العدد 2، 2021، ص ص 6-22.

السيادة الرقمية وأهميتها في حماية الدولة

- محمد الصغير كاجه، الهجمات السيبرانية بين الواقع وسبل المواجهة، مجلة الرسالة للدراسات الإعلامية، المجلد 6، العدد 3، 2022، ص ص 108-117.
- مريم نباش، سعاد بولقرون، التجسس وانتهاك حق الخصوصية في العصر الرقمي دراسة وصفية تحليلية لبرنامج بيغاسوس، مجلة رقمنة للدراسات الإعلامية والاتصالية، المجلد 2، العدد 3، 2022، ص ص 63-78.
- وداد بوطلاعة، الهجمات السيبرانية على البنية التحتية الحرجة: دراسة في ضوء القانون الدولي، مجلة حقوق الانسان والحريات العامة، المجلد 7، العدد 2، 2022، ص ص 322-355.
- توفيق تقيّة، رشيد بوبكر، الأطر القانونية لتعزيز السيادة الرقمية للدولة في مواجهة التحديات المتعلقة بالاستخدامات السلبية المحتملة للذكاء الاصطناعي، المجلد 11، العدد 1، 2024، ص ص 130-148.
- حزام فتيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية: قراءة في أحكام المرسوم الرئاسي رقم 20-0، مجلة الحقوق والعلوم الإنسانية، العدد 03، أكتوبر 2020، ص ص 182-183.
- رامي حليم، إجراءات استخلاص الدليل في الجرائم المعلوماتية، دفاثر البحوث العلمية، المجلد 09، العدد 01، 2021، ص 228.