جامعة الدكتور الطاهر مولاي سعيدة

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

الموضوع

السيادة الرقمية للدول دراسة حالة الجزائر

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في العلوم السياسية

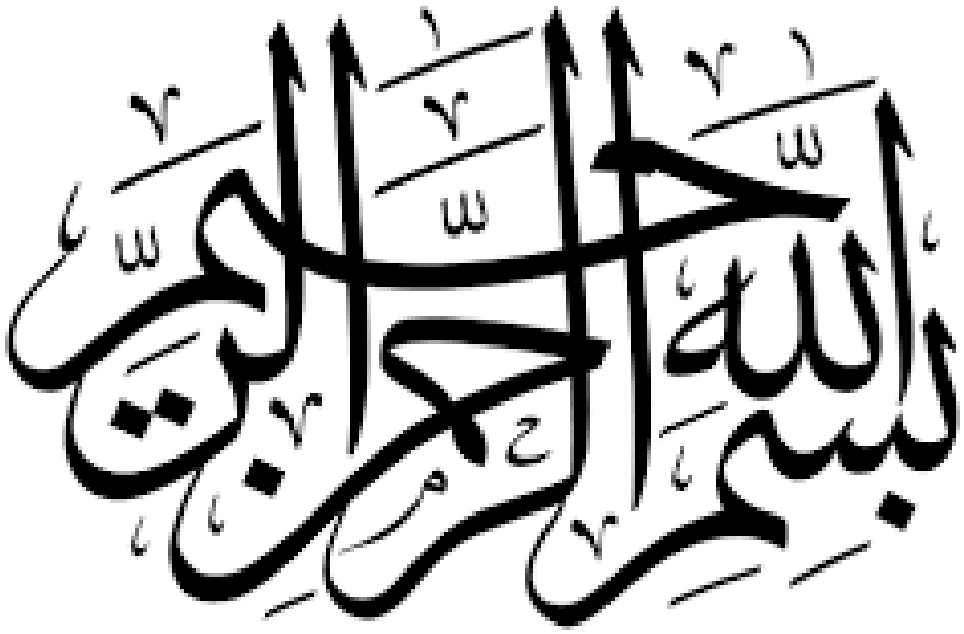
التخصص : العلاقات الدولية

من إعداد: تحت إشراف الأستاذ:

- خلف ايمان أ. د- خاطر خيرة

- لجنة المناقشة -	
خاطر خيرة	مشرفا
خروبي شوقي	رئيسا
حلوي خيرة	مناقشا

السنة الجامعية 2026/2025


بسم الله الرحمن الرحيم

شكر وتقدير

الحمد الله والصلاة والسلام على سيدنا محمد المصطفى الأمين و الحمد الله

حمدا جزيلا الذي وفقني في مشوار دراستي .

أتقدم بالشكر الجزيل الملئي بالاحترام والتقدير

الى كل أساتذة كلية الحقوق والعلوم السياسية وأخص بالذكر

الأستاذة المشرفة خاطر خيرة والذين أفادوني ولو

بكلمة في اعداد هذه المذكرة وكل من كان لهم

الفضل في مساري الدراسي

وختاما ندعوا الله أن يقبل هذا العمل خالصا لوجه الله الكريم لقوله تعالى :

"لئن شكرتم لازدنكم

الإهداء

ابتدأت بطموح، ثم فشلت ، ثم انهيت بنجاح ،خطوات الألف

ميل

الويم عديتها .....

أهدي هذا البحث الى من قال الحق تعالي فيهما "وقل ربي

ارحمهما كما ربياني صغيرا"

الى والدي العظيم حفظه الله ورعاه برعايته

الى والدتي تغمدها الله برحمته وأدخلها فسيح جناته

الى من هم عزوتي وسندي في الحياة .....أسرتي

الى من منني بكل ما يملك ولم يأخذ بهذا في تقديم الدعم لي

ماديا وعنويا وكان سببا في نجاحي

الى كل روح شاركتني بدعائها

الى كل من ساهم في انجاز هذا العمل المتواضع

لمين يمين

الإهداء

إلى قدوتي في الحياة ورمز الاحترام والتقدير أبي الغالي الذي تعب من أجلي

إلى هدية الرحمان منال الحب والحنان إلى التي علمتني الأصول والإحترام إلى أمي الغالية.

إلى كل أفراد العائلة كبيرا وصغيرا وأسأل الله أن يحفظهم

إلى كل أخوتي وأخواتي

إلى كل الزملاء والزميلات

إلى كل الذين يسعهم قلبي ولم تسعهم صفحتي.

خلف ايمان

ملخص :

تناولت هذه الدراسة موضوع **السيادة الرقمية للدول** باعتباره من القضايا الحديثة التي فرضها التطور التكنولوجي والثورة الرقمية، حيث أصبح الفضاء الرقمي مجالًا تمارس فيه الدول سيادتها وتسعى من خلاله إلى حماية أمنها القومي ومصالحها الاستراتيجية. وهدفت الدراسة إلى توضيح مفهوم السيادة الرقمية وأبعادها القانونية والسياسية والاقتصادية، مع بيان أهم التحديات التي تواجهها الدول في العصر الرقمي.

كما تناولت الدراسة دور الأمن السيبراني والبنية التحتية الرقمية والتشريعات القانونية في حماية الفضاء الرقمي، إضافة إلى إبراز مظاهر الصراعات الرقمية بين الدول، مثل الهجمات السيبرانية والتجسس الرقمي والنزاعات المتعلقة بالبيانات والخدمات الرقمية العابرة للحدود.

وتوصلت الدراسة إلى أن تحقيق السيادة الرقمية يتطلب تطوير البنية التحتية الرقمية، وتعزيز الأمن السيبراني، ودعم الصناعات التكنولوجية الوطنية، إلى جانب تحديث التشريعات القانونية وتعزيز التعاون الدولي في المجال الرقمي.

الكلمات المفتاحية:

السيادة الرقمية – الأمن السيبراني – الفضاء الرقمي – البيانات الرقمية – الهجمات السيبرانية – الذكاء الاصطناعي – العلاقات الدولية.

Study Abstract

This study examined the topic of **Digital Sovereignty of States** as one of the modern issues resulting from technological development and the digital revolution. The digital space has become a domain in which states exercise their sovereignty and seek to protect their national security and strategic interests. The study aimed to explain the concept of digital sovereignty and its legal, political, and economic dimensions, while highlighting the main challenges faced by states in the digital era.

The study also addressed the role of cybersecurity, digital infrastructure, and legal regulations in protecting the digital space, in addition to presenting the forms of digital conflicts between states, such as cyberattacks, digital espionage, and disputes over cross-border data and digital services.

The study concluded that achieving digital sovereignty requires developing digital infrastructure, strengthening cybersecurity, supporting national technological industries, modernizing legal frameworks, and enhancing international cooperation in the digital field.

Keywords

Digital Sovereignty – Cybersecurity – Digital Space – Digital Data – Cyberattacks – Artificial Intelligence – International Relations.

مقدمة

لقد شهد العالم خلال العقود الأخيرة تحولات نوعية وجذرية على كافة المستويات، بفعل الثورة الرقمية التي غيّرت طبيعة العلاقات بين الدول، وأعادت تعريف مفاهيم القوة والسيادة والسيطرة على المعلومات. فقد أصبح الفضاء الرقمي اليوم يشكل ساحة أساسية للنشاط البشري، يغطي مجالات متعددة تشمل الاقتصاد والسياسة والثقافة والأمن، ويؤثر بشكل مباشر في حياة الأفراد والمؤسسات والدول على حد سواء. وفي هذا السياق، برزت الحاجة إلى إعادة النظر في مفهوم السيادة التقليدية، وتوسيع نطاقه ليشمل ما يُعرف بالسيادة الرقمية، التي باتت تشكل عنصرًا حاسمًا في صيانة الاستقلال الوطني، وضمان الأمن المعلوماتي، وحماية المصالح الاقتصادية والاجتماعية والسياسية للدولة.

تتمثل السيادة الرقمية في قدرة الدولة على التحكم وإدارة الموارد الرقمية داخل حدودها، بما يشمل البيانات والمعلومات والمحتوى الرقمي، إضافة إلى السيطرة على البنية التحتية الرقمية التي تشكل العمود الفقري للاقتصاد الرقمي والخدمات الإلكترونية الحيوية. وباتت القدرة على حماية الفضاء الرقمي الوطني من التهديدات السيبرانية، ومن التدخلات الأجنبية، ومن الاختراقات التقنية، إحدى أبرز المؤشرات على قوة الدولة وفاعليتها في العصر الرقمي. كما أنها تمثل وسيلة لتعزيز الاستقلالية الاقتصادية، من خلال السيطرة على الصناعات الرقمية الوطنية، وإدارة البيانات التجارية والمالية بشكل يضمن الحد من الاعتماد على الأطراف الأجنبية، ويعزز القدرة التنافسية للدولة على المستوى الدولي.

إن مفهوم السيادة الرقمية يتجاوز حدود التعريف التقليدي للسيادة، الذي كان يرتبط بالتحكم في الأراضي والموارد الطبيعية والمقدرات العسكرية، ليصبح مرتبطًا اليوم بالقدرة على إدارة البيانات الرقمية وتأمين الشبكات الوطنية وحماية الحقوق الرقمية للمواطنين. فالدولة القادرة على فرض سيطرتها الرقمية تستطيع أن توازن بين حرية الإنترنت وحماية المصالح الوطنية، وأن تحد من المخاطر التي تنجم عن الهجمات السيبرانية، أو التجسس الرقمي، أو التدخلات الخارجية في الشؤون الوطنية، كما يمكنها أن تحدد إطارًا قانونيًا وتنظيميًا يضمن استقرار الفضاء الرقمي.

ومن الناحية السياسية، تمثل السيادة الرقمية أداة استراتيجية تؤثر في العلاقات الدولية، إذ أصبحت البيانات الرقمية والمعلومات الحيوية مصدرًا للقوة الناعمة والخشنة، حيث يمكن أن تؤثر النزاعات الرقمية بين الدول في موازين القوى التقليدية، وتؤدي إلى توترات دبلوماسية أو

اقتصادية، في حين يشكل التعاون الدولي في المجال الرقمي ركيزة أساسية للتعامل مع التحديات العابرة للحدود، مثل الأمن السيبراني، وحماية الخصوصية، وتنظيم التجارة الرقمية.

وفي هذا الإطار، يمكن القول إن السيادة الرقمية لم تعد مجرد مفهوم نظري أو مصطلح قانوني، بل أصبحت عنصرًا عمليًا واستراتيجيًا يحدد قدرة الدولة على حماية نفسها، وضمان استقرارها، وممارسة نفوذها في عالم متشابك رقميًا .فهي تُمثل امتدادًا حيويًا للسيادة التقليدية، لكنها تتميز بالمرونة والتعقيد والتشابك مع الأبعاد التقنية والاقتصادية والسياسية الحديثة، ما يجعل من فهمها وتحليلها أمرًا ضروريًا لفهم طبيعة الدولة الحديثة، وعلاقاتها الدولية، وآليات قدرتها على حماية مصالحها في بيئة رقمية متسارعة ومتغيرة باستمرار، وبناءا على ما سبق نطرح الاشكالية الرئيسية للدراسة :

الي أي مدى امتدت سيادة الدول في المجال الرقمي ؟

-التساؤلات الفرعية :

ومن خلال التساؤل الرئيسية للدراسة نطرح التساؤلات الفرعية التالية :

- ما الفرق بين السيادة التقليدية والسيادة الرقمية؟
- ما الدور الذي تلعبه التشريعات الوطنية والدولية في حماية السيادة الرقمية؟
- كيف تؤثر التكنولوجيا والابتكار الرقمي على قدرة الدولة على ممارسة سيادتها؟

فرضيات الدراسة:

تساهم التشريعات الوطنية والدولية في تعزيز وحماية السيادة الرقمية للدولة من خلال تنظيم الفضاء الرقمي وضمان أمن البيانات والمعلومات .

يؤثر التطور التكنولوجي والابتكار الرقمي بشكل مباشر على قدرة الدولة في ممارسة سيادتها، حيث يمكن أن يعزز هذه القدرة أو يحد منها تبعاً لمستوى التحكم في التقنيات والبنية التحتية الرقمية .

ترتبط فعالية السيادة الرقمية بمدى امتلاك الدولة للقدرات التقنية والقانونية والمؤسساتية اللازمة لإدارة الفضاء الرقمي وحمايته.

-أهمية الدراسة:

تكتسب هذه الدراسة أهمية بالغة في الوقت الراهن نظرًا للتحولات العميقة التي يشهدها الفضاء الرقمي على المستوى العالمي، حيث أصبح التحكم في المعلومات والبيانات الرقمية جزءًا أساسيًا من القوة الوطنية واستراتيجيات الأمن والسياسة الدولية. ففهم السيادة الرقمية

وتمكين الدول من إدارتها يحمي مصالحها الاقتصادية والسياسية، ويعزز قدرتها على مواجهة التهديدات السيبرانية والتدخلات الأجنبية، إضافةً إلى ضمان حماية المواطنين ومؤسسات الدولة. كما أن دراسة السيادة الرقمية تساعد على توضيح الفروق بين السيادة التقليدية والرقمية.

وتبرز دور التشريعات الوطنية والدولية في تنظيم الفضاء الرقمي، مما يسهم في تطوير استراتيجيات وطنية متكاملة لتعزيز الاستقلال الرقمي للأمم. علاوة على ذلك، فإن البحث في هذا الموضوع يسلط الضوء على انعكاسات التحولات التكنولوجية الحديثة، مثل الذكاء الاصطناعي والاقتصاد الرقمي، على قدرة الدولة على الحفاظ على سيادتها، ويتيح فهمًا أفضل لتحديات العصر الرقمي وفرص التعاون الدولي في حماية الأمن الرقمي واستقرار العلاقات بين الدول.

-أهداف الدراسة :

- توضيح مفهوم السيادة الرقمية وبيان الفروق بينها وبين السيادة التقليدية.
-تحليل الأبعاد السياسية والقانونية والاقتصادية للسيادة الرقمية وتأثيرها على الدولة.
-دراسة دور التشريعات الوطنية والدولية في حماية السيادة الرقمية وتعزيز الاستقلال الرقمي.
- التعرف على التحديات والتهديدات التي تواجه الدول في الحفاظ على سيادتها الرقمية، مثل الهجمات السيبرانية والتدخلات الأجنبية.
- استعراض انعكاسات التحولات التكنولوجية الحديثة، كالذكاء الاصطناعي والاقتصاد الرقمي، على القدرة الوطنية على ممارسة السيادة الرقمية.

-أسباب اختيار الدراسة :

أولاً: الأسباب الذاتية:

- اهتمام الباحث بالقضايا الرقمية وتأثيرها على السيادة الوطنية للدول.
- رغبة الباحث في فهم التحولات الرقمية الحديثة وآثارها على الأمن والسياسة والاقتصاد الوطني.
- حرص الباحث على المساهمة في إثراء المعرفة الأكاديمية حول موضوع حديث ومتجدد مثل السيادة الرقمية.

ثانياً: الأسباب الموضوعية:

– التحولات التكنولوجية المتسارعة واعتماد الدول بشكل متزايد على الفضاء الرقمي في مختلف المجالات.

– ظهور تهديدات سيبرانية ونزاعات رقمية بين الدول، مما يفرض دراسة السيادة الرقمية كأداة حماية واستراتيجية.

– الحاجة الماسة لفهم الأبعاد القانونية والسياسية والاقتصادية للسيادة الرقمية وتأثيرها على العلاقات الدولية.

– محدودية الدراسات المحلية والعربية المتخصصة في السيادة الرقمية، ما يجعل البحث في هذا المجال ذا قيمة علمية ومعرفية عالية.

–منهج الدراسة :

تعتمد هذه الدراسة على المنهج الوصفي التحليلي لتقديم عرض دقيق وشامل لمفهوم السيادة الرقمية وأبعادها القانونية والسياسية والاقتصادية، مع تحليل العلاقات بين البيانات الرقمية والاستراتيجيات الوطنية لحماية السيادة. كما يتم استخدام المنهج المقارن لمقارنة السيادة الرقمية بالسيادة التقليدية، ولتبيان الفروقات والانعكاسات العملية لهذه السيادة على سياسات الدول وعلاقاتها الدولية، بما يتيح فهمًا أعمق للتحديات والفرص المرتبطة بالتحولات الرقمية الحديثة.

–صعوبات الدراسة :

–سرعة التغيرات الرقمية وتقنيات المعلومات تجعل من الصعب متابعة كل المستجدات المتعلقة بالسيادة الرقمية.

– تعقيد الإطار القانوني للفضاء الرقمي بسبب التداخل بين القوانين المحلية والاتفاقيات والمعاهدات الدولية.

– صعوبة الوصول إلى بعض البيانات والمعلومات المتعلقة بالسياسة الرقمية والأمن السيبراني بسبب طبيعتها السرية.

–الدراسات السابقة :

1–**بن بية عادل وبلقرشي إيمان – "السياسة الرقمية في الجزائر بين التحول المنشود وتحديات السيادة الرقمية** "**التخصص** :العلوم السياسية والسياسات الرقمية – **الجهة الناشرة** :مجلة *الناقد للدراسات السياسية* –**السنة** .2025 :استعرضت هذه الدراسة **السياسة**

الرقمية في الجزائر عبر تحليل نماذج التحول الرقمي قبل وبعد جائحة كورونا، وتطرقت إلى البرامج الحكومية والتشريعات التي تم تبنيها لضمان السيادة الرقمية. كما تطرقت إلى تأثير العوامل الخارجية على العملية الرقمية، وخلصت إلى أن الجزائر أحرزت تقدمًا في التحول الرقمي، لكنها لا تزال تواجه تحديات في مجال الأمن السيبراني، مشددة على ضرورة تعزيز التعاون الدولي وتحسين الأداء الوطني في هذا المجال لضمان احترام السيادة الرقمية وحماية الأمن القومي خلال التحول الرقمي .

2- **صلاح قشير – "السيادة الرقمية والأمن السيبراني: الأبعاد القانونية والاستراتيجية في الجزائر"التخصص** :القانون والأمن الرقمي – **الجهة الناشرة** :مجلة *هيرودوت للعلوم الإنسانية والاجتماعية* –**السنة** .2025 :هدفت هذه الدراسة إلى **تحليل الترابط بين السيادة الرقمية والأمن السيبراني** في السياق الجزائري، معتبرة أن حماية البنية التحتية الرقمية والأمن السيبراني يشكلان ركيزتين أساسيتين للأمن القومي في العصر الرقمي. درست الدراسة الأطر القانونية والمبادرات الإستراتيجية التي تتبعها الجزائر لتعزيز بنيتها الرقمية وحماية بياناتها الوطنية، مع إبراز دور السياسات التقنية في التقليل من المخاطر الرقمية، وخلصت إلى أن السيادة الرقمية في الجزائر تتطلب تطويرًا متكاملًا للقوانين والتقنيات والتعاون بين المؤسسات لتحقيق حماية فعّالة ومستدامة.

3 -**بوعزة محمد وأيت حمودة سمية – "السيادة الرقمية في ظل التحولات التكنولوجية العالمية: التحديات والرهانات"**

التخصص: العلوم السياسية والعلاقات الدولية – الجهة الناشرة: مجلة الدراسات الاستراتيجية والسياسية – السنة: 2024. هدفت هذه الدراسة إلى تحليل مفهوم السيادة الرقمية باعتباره أحد الأبعاد الحديثة للسيادة الوطنية في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصال. كما تناولت التحديات التي تواجه الدول في التحكم في بياناتها وبنيتها التحتية الرقمية أمام هيمنة الشركات التكنولوجية العالمية. وتوصلت الدراسة إلى أن تحقيق السيادة الرقمية يتطلب بناء قدرات وطنية في مجال التكنولوجيا وتعزيز الأطر القانونية والتنظيمية الكفيلة بحماية الفضاء الرقمي الوطني.

-4دربال عبد القادر – "السيادة الرقمية وأمن البيانات الوطنية في عصر الاقتصاد الرقمي" التخصص: القانون العام والاقتصاد الرقمي – الجهة الناشرة: مجلة الباحث للدراسات القانونية والسياسية – السنة: 2023. تناولت هذه الدراسة العلاقة بين السيادة الرقمية وحماية البيانات الوطنية في ظل التوسع الكبير للاقتصاد الرقمي. وركزت على المخاطر الناجمة عن تخزين البيانات خارج الحدود الوطنية، وأهمية سن تشريعات وطنية تضمن التحكم في البيانات الاستراتيجية. وخلصت الدراسة إلى أن أمن البيانات أصبح أحد المؤشرات الأساسية لقياس مستوى السيادة الرقمية للدول وقدرتها على حماية مصالحها الوطنية.

-5حمادي ياسين وبن الشيخ راضية – "التحول الرقمي والسيادة الرقمية: دراسة في متطلبات بناء الدولة الرقمية"

التخصص: الإدارة العامة والسياسات الرقمية – الجهة الناشرة: مجلة العلوم الإدارية والاقتصادية – السنة: 2024. هدفت الدراسة إلى إبراز العلاقة بين التحول الرقمي والسيادة الرقمية، من خلال تحليل متطلبات بناء دولة رقمية قادرة على إدارة مواردها المعلوماتية بكفاءة. كما ناقشت دور البنية التحتية الرقمية والحوكمة الإلكترونية في تعزيز الاستقلالية الرقمية للدول. وأظهرت النتائج أن نجاح مشاريع التحول الرقمي مرتبط بمدى قدرة الدولة على التحكم في مواردها الرقمية وحماية بياناتها الاستراتيجية.

-6بن ساعد ليلى – "الأبعاد القانونية للسيادة الرقمية في مواجهة التهديدات السيبرانية" التخصص: القانون الدولي والأمن السيبراني – الجهة الناشرة: مجلة الحقوق والعلوم السياسية – السنة: 2024. سعت هذه الدراسة إلى توضيح الأبعاد القانونية المرتبطة بمفهوم السيادة الرقمية في ظل تزايد الهجمات السيبرانية العابرة للحدود. كما تناولت مختلف الآليات القانونية الوطنية والدولية التي تلجأ إليها الدول لحماية فضائها الرقمي. وخلصت الدراسة إلى أن تعزيز السيادة الرقمية يقتضي تطوير منظومة تشريعية مرنة ومتجددة قادرة على مواكبة التغيرات التكنولوجية المتسارعة.

-7بوشارب أمين – "السيادة الرقمية بين متطلبات الأمن القومي وإكراهات العولمة الرقمية" التخصص: العلوم السياسية والأمن الدولي – الجهة الناشرة: مجلة الحكمة للدراسات السياسية – السنة: 2023. ركزت هذه الدراسة على تأثير العولمة الرقمية في قدرة الدول على ممارسة

سيادتها داخل الفضاء الإلكتروني، مع تحليل العلاقة بين الأمن القومي والسيادة الرقمية. كما ناقشت دور المنصات الرقمية العالمية في إعادة تشكيل مفهوم السيادة التقليدية. وخلصت الدراسة إلى أن تحقيق السيادة الرقمية يتطلب تحقيق توازن بين الانفتاح على الاقتصاد الرقمي العالمي والحفاظ على المصالح الوطنية والأمن المعلوماتي للدولة.

-8كريمي فاطمة الزهراء – "حوكمة الإنترنت والسيادة الرقمية للدول: قراءة في التحديات المعاصرة"

التخصص: العلاقات الدولية والسياسات العامة – الجهة الناشرة: مجلة الدراسات الإفريقية والمتوسطية – السنة: 2022. تناولت الدراسة إشكالية حوكمة الإنترنت وعلاقتها بالسيادة الرقمية للدول، من خلال تحليل أدوار الفاعلين الدوليين والشركات التكنولوجية الكبرى في إدارة الفضاء الرقمي العالمي. وتوصلت إلى أن السيادة الرقمية أصبحت رهينة بقدرة الدول على المشاركة الفعالة في وضع قواعد الحوكمة الرقمية الدولية، مع تعزيز إمكاناتها التقنية والقانونية على المستوى الوطني.

تقسيمات الدراسة:

اقتضت طبيعة الدراسة والإجابة عن الإشكالية المطروحة تقسيم البحث إلى فصلين رئيسيين. تناول الفصل الأول الموسوم بـ "**الإطار المفاهيمي والسياسي للسيادة الرقمية** "الجوانب النظرية للموضوع، حيث خُصص المبحث الأول لدراسة مفهوم السيادة الرقمية وأبعادها المختلفة، بينما تناول المبحث الثاني الأسس القانونية والسياسية للسيادة الرقمية وما يرتبط بها من قواعد ومبادئ تنظم ممارسة الدولة لسيادتها في الفضاء الرقمي.

أما الفصل الثاني المعنون بـ "**تطبيقات السيادة الرقمية في العلاقات الدولية** "فقد تطرق إلى الجوانب التطبيقية والعملية للسيادة الرقمية، حيث خُصص المبحث الأول لدراسة الاستراتيجيات الوطنية لتحقيق السيادة الرقمية، في حين تناول المبحث الثاني السيادة الرقمية في العلاقات الدولية من خلال إبراز مظاهر التنافس والتعاون بين الدول في المجال الرقمي والتحديات المستقبلية المرتبطة بها، وصولاً إلى خاتمة تضمنت أهم النتائج المتوصل إليها والتوصيات المقترحة.

الفصل الأول

الاطار المفاهيمي والسياسي للسيادة الرقمية

برز مفهوم السيادة الرقمية باعتباره امتدادًا حديثًا لفكرة السيادة التقليدية، لكنه يختلف عنها من حيث المجال والوسائل والتحديات. فإذا كانت السيادة التقليدية تقوم على سلطة الدولة داخل إقليمها، فإن السيادة الرقمية ترتبط بقدرة الدولة على تنظيم فضائها الرقمي، وحماية بياناتها الوطنية، وتأمين بنيتها التحتية المعلوماتية، والحد من التبعية التكنولوجية للخارج.

وتزداد أهمية هذا الموضوع في ظل تنامي التهديدات السيبرانية، وتدخل الفاعلين الدوليين وغير الدوليين في المجال الرقمي، إضافة إلى سيطرة الشركات التكنولوجية الكبرى على كميات هائلة من البيانات. كما يطرح هذا الواقع إشكالية التوفيق بين حماية السيادة الوطنية من جهة، وضمان حرية الإنترنت والحقوق الرقمية للأفراد من جهة أخرى.

المبحث الأول: مفهوم السيادة الرقمية وأبعادها

لم يعد الفضاء الرقمي مجرد وسيلة للتواصل أو تبادل المعلومات، بل أصبح مجالًا استراتيجيًا تتقاطع فيه المصالح السياسية والأمنية والاقتصادية للدول. فقد أصبحت البيانات والمعلومات والبنية التحتية الرقمية عناصر مؤثرة في قوة الدولة وقدرتها على حماية مصالحها الحيوية، الأمر الذي أدى إلى بروز مفهوم السيادة الرقمية كأحد المفاهيم الحديثة المرتبطة باستقلال الدولة وأمنها في البيئة الرقمية.[1]

تختلف السيادة الرقمية عن السيادة التقليدية من حيث المجال والوسائل؛ فإذا كانت السيادة التقليدية تقوم على سلطة الدولة داخل حدودها الإقليمية، فإن السيادة الرقمية تتعلق بقدرة الدولة على التحكم في بياناتها الوطنية، وتأمين شبكاتها وأنظمتها المعلوماتية، وتنظيم تدفق المعلومات داخل فضائها الرقمي. ويزداد هذا الاختلاف وضوحًا بالنظر إلى أن الفضاء الرقمي فضاء عابر للحدود، تتحكم فيه أحيانًا شركات تكنولوجية ومنصات عالمية تملك قدرة كبيرة على التأثير في الأفراد والمؤسسات والرأي العام.[2]

ومن هنا، فإن الحديث عن السيادة الرقمية لا ينحصر في الجانب التقني فقط، بل يمتد إلى أبعاد سياسية وقانونية واقتصادية. فهي ترتبط بحماية القرار الوطني من التدخلات الخارجية، وبحماية المعطيات الشخصية والبيانات الحساسة، وبضمان أمن البنية التحتية الرقمية، فضلًا عن تقليل التبعية التكنولوجية للخارج. لذلك أصبحت السيادة الرقمية شرطًا أساسيًا لتعزيز استقلال الدولة في عصر التحول الرقمي.[3]

---

[1]– أحمد شحيرط، مراد قريبيز، "تحديات الإنترنت لسيادة الدول: السيادة الرقمية"، **مجلة البحوث القانونية والاقتصادية**، الجزائر، المجلد 5، العدد 1، 2022، ص 302.

[2]– محمد المجذوب، **القانون الدولي العام**، الطبعة السادسة، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص 563.

[3]– مروة خلة، بشرى سلاوي، سارة خلة، عبد النور البلدي، "مستقبل السيادة الرقمية في ظل التكنولوجيات الحديثة: دراسة تحليلية استشرافية"، **مجلة بحوث ودراسات في الميديا الجديدة**، الجزائر، المجلد 4، العدد 1، 31 مارس 2023، ص 61.

المطلب الأول: ماهية السيادة الرقمية

فرضت البيئة الرقمية واقعًا جديدًا على الدولة الحديثة، إذ أصبحت مظاهر السيادة لا تقتصر على ممارسة السلطة داخل الإقليم، بل امتدت إلى القدرة على التحكم في البيانات والمعلومات والأنظمة الرقمية. ومن ثم، ظهرت السيادة الرقمية باعتبارها شكلًا جديدًا من أشكال السيادة، يعكس قدرة الدولة على حماية مصالحها داخل الفضاء الإلكتروني[1].

تتطلب دراسة ماهية السيادة الرقمية الوقوف عند المفهوم التقليدي للسيادة، من حيث أساسه وخصائصه، ثم بيان مدى تأثره بالتطور الرقمي. كما يقتضي ذلك تحديد المفهوم الحديث للسيادة الرقمية، وإبراز العوامل التي أدت إلى ظهوره، والخصائص التي تميزه عن السيادة التقليدية[2].

ومن هنا، سيتم تقسيم هذا المطلب إلى فرعين؛ الأول يتناول التعريف التقليدي للسيادة ومقارنته بالسيادة الرقمية، والثاني يوضح التعريف الحديث للسيادة الرقمية وخصائصها الأساسية.

الفرع الأول: التعريف التقليدي للسيادة ومقارنته بالسيادة الرقمية

تعتبر السيادة من أهم المفاهيم التي قام عليها بناء الدولة الحديثة، إذ لا يمكن الحديث عن دولة كاملة الأركان دون وجود سلطة عليا قادرة على فرض إرادتها داخل الإقليم، وتنظيم شؤون المجتمع، وتمثيل الدولة في علاقاتها الخارجية. وقد ظل هذا المفهوم، لمدة طويلة، مرتبطًا بالإقليم الجغرافي والحدود السياسية، بحيث كانت الدولة تمارس سيادتها على الأشخاص والأموال والوقائع التي تقع داخل نطاقها الترابي[3].

---

[1]– كوثر منسل، **تفعيل دور الإدارة الإلكترونية في الجزائر: نحو بروز قانون للإدارة الإلكترونية**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، الجزائر، 2023، ص 45.

[2]– بلحاج خالدية، فرعون محمد، "السيادة الرقمية"، مجلة البحوث في الحقوق والعلوم السياسية، جامعة ابن خلدون تيارت، الجزائر، المجلد 11، العدد 1، 2025، ص 461.

[3]– فرحات علاء الدين، عمروس عمارة، "الفضاء السيبراني وتآكل مفهوم السيادة الوطنية"، **المجلة الجزائرية للدراسات السياسية**، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، المجلد 8، العدد 2، 31 ديسمبر 2021، ص 162.

غير أن التطور الرقمي غيّر جانبًا مهمًا من هذا التصور التقليدي، لأن جزءًا كبيرًا من النشاط السياسي والاقتصادي والاجتماعي أصبح يتم داخل فضاء غير مادي، يقوم على البيانات والشبكات والمنصات والخدمات الرقمية. ومن ثم، ظهرت الحاجة إلى إعادة قراءة مفهوم السيادة في ضوء البيئة الرقمية، خاصة أن الدولة لم تعد تواجه فقط تهديدات عسكرية أو سياسية تقليدية، بل أصبحت تواجه تهديدات سيبرانية قد تصيب مؤسساتها، وبيانات مواطنيها، وبنيتها التحتية الحيوية.[1]

أولًا: مفهوم السيادة التقليدية وخصائصها

يقصد بالسيادة التقليدية السلطة العليا التي تتمتع بها الدولة داخل حدودها، واستقلالها في مواجهة غيرها من الدول في الخارج. فهي تعبر، من الناحية الداخلية، عن قدرة الدولة على سن القوانين، وتنظيم الإدارة، وفرض الأمن، وممارسة القضاء، وإدارة المرافق العامة. أما من الناحية الخارجية، فتظهر في استقلال الدولة في اتخاذ قراراتها، وإقامة علاقاتها الدولية، وعدم خضوعها لسلطة دولة أخرى.

، وبذلك، فإن السيادة وتقوم السيادة التقليدية على عنصرين متكاملين :السيادة الداخلية، وتعني علو سلطة الدولة داخل إقليمها، والسيادة الخارجية، وتعني استقلالها في علاقاتها مع غيرها من الدول ليست مجرد فكرة سياسية، بل هي وصف قانوني يعبر عن مركز الدولة في النظام الدولي، وعن قدرتها على ممارسة الاختصاص داخل حدودها[2].

ومن أهم خصائص السيادة التقليدية أنها سلطة عليا، لأنها تعلو على جميع السلطات داخل الدولة؛ وسلطة أصلية، لأنها لا تستمد وجودها من سلطة أخرى؛ وسلطة مستقلة، لأنها تفترض عدم خضوع الدولة لإرادة خارجية؛ كما أنها مرتبطة بالإقليم، لأن الدولة تمارس اختصاصها عادة داخل حدود جغرافية محددة. ولهذا السبب ارتبطت السيادة التقليدية بفكرة الحدود، والرقابة على الإقليم، والتحكم في الموارد المادية، وتنظيم الأشخاص المقيمين داخل الدولة.

---

[1]– عبد الواحد محمد الفار، **القانون الدولي العام**، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2005، ص 215.

[2]– فاطمة بيرم، "السيادة الوطنية السيبرانية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجًا"، **المجلة الجزائرية للأمن الإنساني**، جامعة باتنة 1، الجزائر، المجلد 5، العدد 1، 2020، ص ص 789.

غير أن هذا التصور التقليدي كان مناسبًا لعالم تتحرك فيه الوقائع والأشخاص والأموال داخل نطاق مادي يمكن ضبطه نسبيًا، أما في العصر الرقمي فإن كثيرًا من الوقائع لم تعد تقع داخل مكان واضح. فقد تُنشأ المعلومة في دولة، وتُخزن في دولة ثانية، وتُعالج في دولة ثالثة، وتُستعمل للتأثير في مواطني دولة رابعة. وهنا تبدأ حدود السيادة التقليدية في الظهور[1].

ثانيًا: حدود السيادة التقليدية في ظل التطور الرقمي

أبرز ما كشفه التطور الرقمي هو أن الإقليم لم يعد وحده المجال الذي تمارس فيه الدولة سلطتها. فالفضاء الرقمي يتجاوز الحدود، ولا يخضع دائمًا لمنطق الرقابة الإقليمية التقليدية. فالدولة تستطيع مراقبة حدودها البرية أو البحرية أو الجوية، لكنها تجد صعوبة أكبر في مراقبة تدفق البيانات، أو تحديد مصدر الهجمات السيبرانية، أو فرض قوانينها على شركات رقمية كبرى توجد خوادمها ومراكز قرارها خارج إقليمها[2].

تظهر هذه الحدود في عدة مظاهر. أولها حركة البيانات عبر الحدود، حيث تنتقل بيانات المواطنين والمؤسسات بين دول متعددة في وقت قصير، وقد يتم تخزينها في مراكز بيانات أجنبية، مما يثير إشكالات حول من يملك سلطة التحكم فيها ومن يملك حق الوصول إليها. وثانيها صعود الشركات التكنولوجية الكبرى، التي أصبحت تتحكم في منصات التواصل، ومحركات البحث، والخدمات السحابية، وأنظمة التشغيل، وهي مجالات تؤثر مباشرة في الحياة السياسية والاقتصادية والاجتماعية للدول.[3]

أما المظهر الثالث، فيتمثل في صعوبة تحديد الاختصاص القضائي في البيئة الرقمية. فالجرائم السيبرانية والهجمات الإلكترونية غالبًا ما تتسم بالتعقيد، لأنها قد تُرتكب من خارج الإقليم، وبوسائل تقنية تخفي هوية الفاعل الحقيقي. وقد ينتج عن ذلك عجز القانون الوطني وحده عن مواجهة هذه الأفعال دون تعاون دولي أو آليات تقنية متطورة.

---

[1]– ليلى بعوني، "التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الإلكترونية نموذجًا"، **مجلة ستراتيجيا**، الجزائر، المجلد 8، العدد 16، 2021، ص 22.

[2]– ليلى بعوني، المرجع السابق ، ص23.

[3]– فادية سامي علي الخصاونة، **تأثير التكنولوجيا على السيادة القومية**، رسالة ماجستير، كلية الآداب، جامعة اليرموك، إربد، الأردن، 2003، ص47.

كما تظهر حدود السيادة التقليدية في مجال التأثير على الرأي العام .فقد أصبحت الحملات الرقمية، والأخبار المضللة، والتلاعب بالخوارزميات، والتوجيه السياسي عبر المنصات، وسائل جديدة للتأثير في المجتمعات دون تدخل عسكري أو سياسي مباشر. وهذا النوع من التأثير لا يستهدف الإقليم المادي، بل يستهدف الوعي الجماعي، والانتخابات، والثقة في المؤسسات، وهو ما يجعل حماية السيادة في العصر الرقمي أكثر تعقيدًا.[1]

وبناءً على ذلك، لم تعد السيادة التقليدية كافية وحدها لفهم واقع السلطة في العصر الرقمي، لأن الدولة أصبحت مطالبة بحماية مجال جديد لا تحده الجغرافيا بشكل واضح، وهو المجال الرقمي.

ثالثًا: أوجه المقارنة بين السيادة التقليدية والسيادة الرقمية

تختلف السيادة التقليدية عن السيادة الرقمية من عدة جوانب. فمن حيث **المجال**، تقوم السيادة التقليدية على الإقليم المادي، أي الأرض والحدود والمؤسسات، بينما تقوم السيادة الرقمية على الفضاء الإلكتروني، أي البيانات والشبكات والمنصات والأنظمة المعلوماتية، وهذا يعني أن السيادة الرقمية لا تنفصل عن السيادة التقليدية، لكنها تضيف إليها مجالًا جديدًا لم يكن مطروحًا بالشكل نفسه في السابق[2].

ومن حيث موضوع الحماية، تهدف السيادة التقليدية إلى حماية الحدود، والنظام العام، والاستقلال السياسي، والموارد الطبيعية، بينما تهدف السيادة الرقمية إلى حماية البيانات الوطنية، والبنية التحتية الرقمية، والاتصالات، والأنظمة الحساسة، والهوية الرقمية للمواطنين. فالدولة في المجال الرقمي لا تحمي الأرض فقط، بل تحمي المعلومة، والخوارزمية، والشبكة، والنظام المعلوماتي[3].

---

[1]– سامر محي عبد الحمزة، "موقف جامعة الدول العربية من السيادة على الفضاء السيبراني: دراسة في ضوء أحكام القانون الدولي العام"، **مجلة القانون الدولي للدراسات البحثية**، المركز الديمقراطي العربي، ألمانيا، العدد 4، مارس 2023، ص –24.

[2]– سامر محي عبد الحمزة، المرجع السابق ، ص26.

[3]– شرايطية سميرة، "السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي"، **المجلة الجزائرية للأمن والتنمية**، جامعة باتنة 1، الجزائر، المجلد 9، العدد 1، جانفي 2020، ص 396.

أما من حيث **وسائل الممارسة**، فإن السيادة التقليدية تمارس من خلال التشريع، والقضاء، والإدارة، والشرطة، والجيش، والرقابة على الحدود. في المقابل، تمارس السيادة الرقمية من خلال الأمن السيبراني، وتشريعات حماية البيانات، ومراكز البيانات الوطنية، وتوطين الخدمات الرقمية الحساسة، وتنظيم المنصات، وحماية البنية التحتية الحيوية، وتطوير قدرات وطنية في مجال التكنولوجيا.

فإن السيادة التقليدية تواجه عادة الاحتلال، والتدخل العسكري، والضغط السياسي، والاعتداء على الحدود. أما السيادة الرقمية فتواجه القرصنة، والتجسس الإلكتروني، وسرقة البيانات، وتعطيل الخدمات، والتلاعب بالمعلومات، والهيمنة التكنولوجية، والتبعية للبرمجيات أو المنصات الأجنبية. ولذلك فإن السيادة الرقمية لا تلغي السيادة التقليدية، بل تمثل امتدادًا لها في بيئة جديدة فرضتها الثورة الرقمية.

يمكن القول إن العلاقة بين السيادتين هي علاقة تكامل لا تعارض. فالدولة التي تفقد السيطرة على بياناتها ومؤسساتها الرقمية قد تتأثر سيادتها السياسية والاقتصادية، حتى لو ظلت حدودها المادية قائمة. ومن هنا تظهر أهمية الانتقال من الفهم التقليدي للسيادة إلى فهم أكثر اتساعًا يستوعب التحولات الرقمية[1].

الفرع الثاني: التعريف الحديث للسيادة الرقمية وخصائصها الأساسية

ارتبط ظهور السيادة الرقمية بتحول البيانات إلى مورد استراتيجي، وبانتقال جزء واسع من نشاط الدولة والمجتمع إلى الفضاء الإلكتروني. فالإدارة، والاقتصاد، والتعليم، والصحة، والأمن، والاتصال، والإعلام، والخدمات العمومية، كلها أصبحت تعتمد على أنظمة رقمية وشبكات معلوماتية. لذلك، أصبح ضعف الدولة في المجال الرقمي مصدرًا لتهديد استقلالها، تمامًا كما كان ضعفها العسكري أو الاقتصادي يمثل تهديدًا لسيادتها التقليدية[2].

---

[1]– بن قطاط خديجة، "تداعيات الحروب السيبرانية على السيادة الرقمية"، **مجلة القانون العام الجزائري والمقارن**، الجزائر، المجلد 10، العدد 2، 2024، ص 280.

[2]– كوثر منسل، **تفعيل دور الإدارة الإلكترونية في الجزائر: نحو بروز قانون للإدارة الإلكترونية**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، الجزائر، 2023، ص 47.

أولًا: مفهوم السيادة الرقمية

يمكن تعريف السيادة الرقمية بأنها قدرة الدولة على ممارسة سلطتها واستقلالها داخل الفضاء الرقمي، من خلال التحكم في البيانات الوطنية، وحماية الأنظمة المعلوماتية، وتنظيم تدفق المعلومات، وتأمين البنية التحتية الرقمية، وضمان عدم خضوع القرار الوطني للهيمنة أو التبعية التكنولوجية.

السيادة الرقمية تعني الانغلاق على الذات أو قطع الاتصال بالإنترنت العالمي، لأن ذلك يتعارض مع طبيعة البيئة الرقمية القائمة على التبادل والتواصل. وإنما تعني امتلاك الدولة القدرة القانونية والتقنية والسياسية التي تمكنها من حماية مصالحها داخل هذا الفضاء. فالدولة ذات السيادة الرقمية هي التي تستطيع أن تعرف أين توجد بياناتها، ومن يعالجها، وكيف تُستعمل، وما الضمانات القانونية والتقنية لحمايتها[1].

وتتضمن السيادة الرقمية عدة عناصر، أهمها :**السيادة على البيانات،** أي قدرة الدولة على حماية البيانات الوطنية والشخصية والحساسة؛ و**السيادة على البنية التحتية،** أي التحكم في الشبكات ومراكز البيانات والمنصات الحيوية؛ و**السيادة التقنية،** أي امتلاك الحد الأدنى من القدرة على إنتاج أو إدارة التكنولوجيا الحساسة؛ و**السيادة القانونية،** أي قدرة الدولة على وضع قواعد تنظم الفضاء الرقمي وتفرض احترامها[2].

كما تتصل السيادة الرقمية بحماية المواطنين، لأن البيانات الشخصية أصبحت جزءًا من الحياة الخاصة للفرد. فإذا كانت الدولة عاجزة عن حماية بيانات مواطنيها من الاستغلال غير المشروع أو التخزين الخارجي غير الآمن، فإن ذلك يضعف ثقة الأفراد في المؤسسات، ويفتح المجال للمراقبة التجارية أو السياسية أو الأمنية من جهات أجنبية.

---

[1]– إيهاب خليفة، **القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت؟ الولايات المتحدة نموذجًا**، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، مصر، 2017، ص 81.

[2]– راضي زينب عباس، "فاعلية الأمن السيبراني في السياسة العالمية: المفهوم والتدابير الأمنية للدول"، **مجلة آشور للعلوم القانونية والسياسية**، العراق، المجلد 2، العدد 1، 2025، ص 548.

ثانيًا: أسباب ظهور السيادة الرقمية

يرجع ظهور مفهوم السيادة الرقمية إلى مجموعة من الأسباب التالية :

1- تزايد قيمة البيانات:

أول هذه الأسباب هو **تزايد قيمة البيانات،** إذ أصبحت البيانات تستخدم في التخطيط الاقتصادي، وصناعة القرار، وتوجيه الخدمات العمومية، وتطوير الذكاء الاصطناعي، وتحليل سلوك الأفراد والجماعات. ولذلك أصبحت البيانات تشبه الموارد الاستراتيجية، لأن من يتحكم فيها يستطيع التأثير في الاقتصاد والسياسة والإدارة والمجتمع[1].

2- تصاعد التهديدات السيبرانية:

لم تعد الهجمات الرقمية تستهدف الأفراد فقط، بل أصبحت تستهدف مؤسسات الدولة، والمصارف، وشبكات الطاقة، والاتصالات، والمستشفيات، والأنظمة الانتخابية، والمرافق الحيوية. وقد تؤدي هجمة سيبرانية واحدة إلى شلل إداري أو اقتصادي، دون استعمال أي قوة عسكرية تقليدية. وهذا ما جعل الأمن السيبراني عنصرًا مركزيًا في مفهوم السيادة الرقمية.[2]

3- الشركات التكنولوجية الكبرى:

أما السبب الثالث فهو **هيمنة الشركات التكنولوجية الكبرى** .فقد أصبحت بعض الشركات تتحكم في خدمات رقمية أساسية، مثل محركات البحث، والبريد الإلكتروني، والتخزين السحابي، ومنصات التواصل الاجتماعي، وأنظمة التشغيل، والإعلانات الرقمية. وهذا الوضع يجعل الدول، خاصة النامية منها، في حالة اعتماد واسع على خدمات أجنبية قد لا تخضع لقوانينها الوطنية بشكل كامل.

---

[1]- إيهاب خليفة، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي**، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، مصر، 2019، ص 123.

[2]- إيهاب خليفة، مرجع سابق،ص135.

4- التبعية التكنولوجية

اعتماد الدولة على برمجيات أو تجهيزات أو خدمات سحابية أجنبية في إدارة قطاعات حساسة قد يجعلها عرضة للضغط أو التجسس أو التعطيل. لذلك أصبح بناء قدرات وطنية في التكنولوجيا، وتطوير الكفاءات المحلية، ودعم الصناعات الرقمية الوطنية، من متطلبات السيادة الرقمية.

5- تحول الإعلام والرأي العام إلى المجال الرقمي.

أصبحت النقاش السياسي، وتشكيل الرأي العام، والحملات الانتخابية، والتعبئة الاجتماعية، تجري إلى حد كبير عبر المنصات الرقمية. وهذا جعل الدول تخشى من التدخل الخارجي عبر الأخبار المضللة، والحسابات الوهمية، والتلاعب بالمحتوى، والتأثير الخوارزمي على المستخدمين.[1]

ثالثًا: الخصائص الأساسية للسيادة الرقمية

1- الطابع اللامادي:

تتميز السيادة الرقمية بعدة خصائص تميزها عن السيادة التقليدية. أول هذه الخصائص هو **الطابع اللامادي**، لأن محل السيادة هنا ليس الأرض فقط، بل البيانات والمعلومات والشبكات والخوادم والبرمجيات. وهذا يجعل ممارسة السيادة أكثر تعقيدًا، لأن الدولة تتعامل مع أشياء غير ملموسة لكنها ذات أثر واقعي كبير[2].

2-الطابع العابر للحدود

وتتميز كذلك بـ **الطابع العابر للحدود**، لأن الفضاء الرقمي لا يتوقف عند حدود الدولة. فقد تكون البيانات الخاصة بمواطنين داخل دولة معينة مخزنة خارجها، وقد تقدم الخدمات الرقمية من شركات لا توجد داخل إقليمها، وقد تنطلق الهجمات السيبرانية من دول بعيدة. لذلك لا يمكن ممارسة السيادة الرقمية بمنطق الانفراد الوطني فقط، بل تحتاج إلى تعاون دولي وإقليمي.

---

[1]- محمد قسوم، المرجع السابق ، ص83.

[2]- ابن زرارة أمينة، أعراب فطيمة، "الحلول الرقمية الابتكارية في مجال حماية الهوية والخصوصية والأمن السيبراني خلال جائحة كوفيد-19"، **مجلة رقمنة للدراسات الإعلامية والاتصالية**، الجزائر، المجلد 3، العدد 1، عدد خاص، مارس 2023، ص 58.

3- الارتباط الوثيق بالأمن الوطني:

ومن خصائصها أيضًا **الارتباط الوثيق بالأمن الوطني** .فالسيادة الرقمية ليست مجرد مسألة تقنية تخص خبراء الإعلام الآلي، بل هي جزء من الأمن القومي. فاختراق أنظمة الدولة، أو تعطيل خدماتها، أو تسريب بياناتها، أو التأثير في رأيها العام، كلها أفعال يمكن أن تمس استقرار الدولة واستقلال قرارها.

4- البعد الاقتصادي:

كما تتميز السيادة الرقمية بـ **البعد الاقتصادي**، لأن الاقتصاد الحديث أصبح يعتمد على التجارة الإلكترونية، والدفع الإلكتروني، والخدمات السحابية، والذكاء الاصطناعي، والبيانات الضخمة. لذلك، فإن الدولة التي لا تملك اقتصادًا رقميًا قويًا تبقى أكثر عرضة للتبعية، لأن حاجتها إلى التكنولوجيا والخدمات الأجنبية تصبح مستمرة.

المطلب الثاني: أبعاد السيادة الرقمية وتمييزها عن السيادة التقليدية

لا تقتصر السيادة الرقمية على مجرد امتلاك الدولة لتقنيات حديثة أو استعمالها للإدارة الإلكترونية، بل تمتد إلى مجموعة من الأبعاد السياسية والتقنية والاقتصادية التي تعبّر عن قدرة الدولة على حماية استقلالها في البيئة الرقمية. فالسيادة في صورتها الرقمية تقوم على التحكم في البيانات، وتأمين البنية التحتية المعلوماتية، وحماية الأمن السيبراني، وتقليل التبعية للتكنولوجيا والخدمات الأجنبية[1].

وتختلف السيادة الرقمية عن السيادة التقليدية من حيث المجال والأدوات؛ فإذا كانت السيادة التقليدية تمارس أساسًا داخل الإقليم المادي، فإن السيادة الرقمية تمارس في فضاء مفتوح وعابر للحدود، تتحرك فيه البيانات بسرعة، وتؤثر فيه الشركات والمنصات العالمية إلى جانب الدول. ولهذا، فإن فهم أبعاد السيادة الرقمية يسمح بإبراز طبيعتها المركبة، فهي ليست مسألة قانونية فقط، ولا تقنية فقط، بل هي مسألة سياسية وأمنية واقتصادية في الوقت نفسه.

[1]- بورياح سلمة، "السياسات العامة الجزائرية في مجال السيبرانية: الواقع والتحديات"، **دفاتر السياسة والقانون**، جامعة قاصدي مرباح ورقلة، الجزائر، المجلد 15، العدد 1، جانفي 2023، ص 273.

وعليه، سيتم تناول هذا المطلب من خلال فرعين؛ يخصص الأول للبعد السياسي للسيادة الرقمية من حيث التحكم في البيانات والمعلومات الوطنية، بينما يخصص الثاني للبعد التقني والاقتصادي وأثره على استقلال الدولة الرقمي.

الفرع الأول: البعد السياسي للسيادة الرقمية: التحكم في البيانات والمعلومات الوطنية

يمثل البعد السياسي أحد أهم أبعاد السيادة الرقمية، لأن البيانات والمعلومات أصبحت من أدوات القوة والتأثير في الدولة الحديثة. فلم تعد السلطة السياسية تعتمد فقط على السيطرة على الإقليم والمؤسسات، بل أصبحت تحتاج كذلك إلى التحكم في تدفق البيانات، وحماية المعلومات الحساسة، وضمان عدم استعمال الفضاء الرقمي للتأثير في القرار الوطني أو توجيه الرأي العام من الخارج[1].

ومن هنا، فإن التحكم في البيانات الوطنية لا يعد مسألة تقنية محضة، بل هو جزء من حماية السيادة السياسية للدولة، خاصة في ظل تزايد استعمال المنصات الرقمية في الإعلام، والانتخابات، وصناعة الرأي العام، وإدارة الخدمات العمومية، وصنع القرار السياسي[2].

أولًا: البيانات كأداة من أدوات السيادة السياسية

أصبحت البيانات في العصر الرقمي موردًا استراتيجيًا شبيهًا بالموارد التقليدية، لأنها تكشف عن سلوك الأفراد، واتجاهات المجتمع، وحركة الاقتصاد، واحتياجات الإدارة، ونقاط القوة والضعف في المؤسسات. ومن ثم، فإن الدولة التي تملك القدرة على جمع بياناتها وتنظيمها وتحليلها وحمايتها تكون أقدر على رسم السياسات العامة واتخاذ القرارات المناسبة[3].

---

[1]– بن جدو أسماء، **سياسات الأمن السيبراني في الجزائر في ظل التهديدات الدولية 2008–2025**، أطروحة دكتوراه في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة أمحمد بوقرة بومرداس، الجزائر، 2026، ص 69 .

[2]– بن دعاس سهام، بن عثمان فوزية، "ضمانات حماية المعطيات الشخصية في البيئة الرقمية في التشريع الجزائري"، **مجلة الحقوق والعلوم الإنسانية**، جامعة محمد لمين دباغين، سطيف 2، الجزائر، المجلد 15، العدد 1، 2022، ص146.

[3]– بن دعاس سهام، المرجع نفسه ، ص148.

فالبيانات لم تعد مجرد معلومات مخزنة في قواعد إلكترونية، بل أصبحت أداة لصناعة القرار السياسي والإداري. إذ يمكن للدولة من خلال تحليل البيانات أن تضع سياسات أكثر دقة في مجالات الصحة، والتعليم، والضرائب، والنقل، والأمن، والخدمات العمومية. وفي المقابل، فإن فقدان السيطرة على هذه البيانات أو تخزينها لدى جهات أجنبية قد يؤدي إلى إضعاف قدرة الدولة على التحكم في معلوماتها السيادية.

وتزداد خطورة المسألة عندما يتعلق الأمر بالبيانات الحساسة، مثل بيانات المواطنين، والسجلات الصحية، والمعلومات المالية، وبيانات المؤسسات العمومية، والمعطيات الأمنية. فهذه البيانات إذا خضعت لسيطرة أطراف أجنبية أو شركات عالمية، فإن ذلك قد يسمح بالتأثير في اختيارات الدولة أو ابتزازها أو استغلال مواطنيها اقتصاديًا وسياسيًا[1].

ثانيًا: تحكم الدولة في المعلومات الوطنية وحمايتها

لا يتحقق البعد السياسي للسيادة الرقمية إلا بقدرة الدولة على حماية معلوماتها الوطنية من الاختراق أو التسريب أو التلاعب. ويشمل ذلك حماية قواعد البيانات الحكومية، ومراسلات المؤسسات الرسمية، والأنظمة المعلوماتية المرتبطة بالإدارة، والوثائق الرقمية ذات الطابع السيادي[2].

ويظهر هذا التحكم من خلال وضع تشريعات وطنية لحماية المعطيات الشخصية، وتجريم الاعتداء على الأنظمة المعلوماتية، وتنظيم معالجة البيانات، وإلزام الهيئات العمومية والخاصة باتخاذ تدابير أمنية لحماية المعلومات. كما يتطلب الأمر إنشاء مؤسسات رقابية وتقنية مختصة، قادرة على متابعة مدى احترام قواعد حماية البيانات والتدخل عند وقوع الخطر[3].

---

[1]– بارة سمير، "الأمن السيبراني في الجزائر: السياسات والمؤسسات"، **المجلة الجزائرية للأمن الإنساني**، جامعة باتنة 1، الجزائر، العدد 4، جويلية 2017، ص 255.

[2]– نعاس صلاح الدين، فاتح بلقاسم أولاد الهدار، "الرقمنة في الجزائر بين تحديات الذكاء الاصطناعي وتعزيز الأمن السيبراني"، ضمن أعمال ملتقى وطني حول الرقمنة في الجزائر، جامعة غرداية، الجزائر، 2025، ص 15.

[3]– نعاس صلاح الدين، المرجع نفسه ، ص16.

غير أن حماية المعلومات الوطنية لا تتحقق بالنصوص القانونية وحدها، بل تحتاج إلى بنية تقنية آمنة، وكفاءات بشرية متخصصة، وثقافة رقمية لدى الموظفين والمواطنين. فكثير من الاختراقات لا تتم فقط بسبب ضعف الأنظمة، بل بسبب ضعف الوعي الرقمي، وسوء استعمال كلمات المرور، وغياب التكوين، وعدم احترام قواعد السلامة المعلوماتية.

ومن ثم، فإن تحكم الدولة في المعلومات الوطنية يقوم على ثلاث ركائز متكاملة: ركيزة قانونية تحدد الحقوق والواجبات، وركيزة تقنية تؤمن الأنظمة والشبكات، وركيزة بشرية تقوم على التكوين والوعي والمسؤولية الرقمية[1].

ثالثًا: أثر السيادة الرقمية على الأمن الوطني والرأي العام

ترتبط السيادة الرقمية بالأمن الوطني ارتباطًا مباشرًا، لأن التهديدات المعاصرة لم تعد تقتصر على الحدود العسكرية أو الجغرافية. فقد أصبحت الهجمات السيبرانية قادرة على تعطيل خدمات حيوية، أو اختراق مؤسسات حساسة، أو تسريب بيانات المواطنين، أو التأثير في النظام المالي والإداري للدولة[2].

كما أن السيادة الرقمية ترتبط بحماية الرأي العام، لأن المنصات الرقمية أصبحت مجالًا رئيسيًا للتأثير السياسي والاجتماعي. فالأخبار المضللة، والحسابات الوهمية، والحملات الرقمية المنظمة، والتلاعب بالخوارزميات، كلها وسائل يمكن أن تستعمل للتأثير في اتجاهات المواطنين، وإضعاف الثقة في المؤسسات، والتدخل غير المباشر في الشؤون الداخلية للدولة.

ومن هنا، فإن الدولة تحتاج إلى تنظيم الفضاء الرقمي بما يحمي الأمن الوطني دون أن يتحول ذلك إلى تقييد غير مبرر للحريات. فالمطلوب ليس فرض رقابة شاملة على الإنترنت، بل بناء توازن بين حماية الدولة من التدخلات الرقمية الأجنبية، وضمان حرية التعبير، وحق المواطن في الوصول إلى المعلومات.

---

[1]– نعاس صلاح الدين، المرجع السابق، ص17.

[2]– طوايبية أحمد، **تطبيقات الاقتصاد الرقمي وأثرها على النمو الاقتصادي**، أطروحة دكتوراه علوم في العلوم الاقتصادية، تخصص التخطيط والتنمية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر، السنة الجامعية 2008–2009، 306 ص، ص 103.

الفرع الثاني: البعد التقني والاقتصادي وأثره على استقلال الدولة الرقمي

تتوقف فعالية السيادة الرقمية على مدى امتلاك الدولة لقدرات تقنية واقتصادية تمكنها من إدارة فضائها الرقمي بصورة مستقلة. فالسيادة الرقمية لا تتحقق بمجرد إعلان الدولة رغبتها في حماية بياناتها، بل تحتاج إلى شبكات آمنة، ومراكز بيانات وطنية، وكفاءات تقنية، وتشريعات فعالة، واقتصاد رقمي قادر على دعم هذا التوجه[1].

وتظهر أهمية هذا البعد في أن التبعية للتكنولوجيا الأجنبية قد تتحول إلى تبعية سياسية واقتصادية، خاصة عندما تكون الخدمات الرقمية الحيوية مرتبطة بمنصات أو شركات خارجية. لذلك فإن بناء بنية تحتية رقمية وطنية، وتعزيز الأمن السيبراني، ودعم الصناعات الرقمية المحلية، تعد من أهم شروط تحقيق الاستقلال الرقمي[2].

أولًا: البنية التحتية الرقمية كركيزة للسيادة الرقمية

تشكل البنية التحتية الرقمية الأساس المادي والتقني للسيادة الرقمية، لأنها تضم شبكات الاتصالات، ومراكز البيانات، والخوادم، والأنظمة الحكومية، ومنصات الخدمات العمومية، وشبكات الدفع الإلكتروني، والأنظمة المرتبطة بالقطاعات الحيوية مثل الطاقة، والنقل، والصحة، والبنوك.

فكلما كانت هذه البنية قوية وآمنة وموجودة تحت رقابة وطنية فعالة، كانت الدولة أقدر على حماية بياناتها وخدماتها الرقمية. أما إذا كانت هذه البنية ضعيفة أو تابعة كليًا لموردين أجانب، فإن الدولة تصبح عرضة للتعطيل أو التجسس أو التحكم الخارجي.

وتظهر أهمية البنية التحتية الرقمية أيضًا في مجال الإدارة الإلكترونية، لأن رقمنة الخدمات العمومية لا يمكن أن تنجح دون شبكات آمنة، ومنصات موثوقة، ومراكز بيانات قادرة على تخزين المعلومات وحمايتها. كما أن التحول الرقمي في الإدارة والاقتصاد يحتاج إلى ربط مؤسسات الدولة بعضها ببعض، وتوحيد قواعد البيانات، وتأمين تبادل المعلومات بينها.

---

[1]– بوازدية جمال، "الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية"، **مجلة العلوم القانونية والسياسية**، جامعة الشهيد حمه لخضر الوادي، الجزائر، المجلد 10، العدد 1، أفريل 2019، ص265.

[2]– هشام محمد بدر، **الحماية الجنائية للتعاملات الإلكترونية**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2012، ص 133.

فإن البنية التحتية الرقمية ليست مجرد وسيلة تقنية، بل هي ركيزة من ركائز السيادة، لأن من يتحكم في الشبكات ومراكز البيانات والخدمات الرقمية الحيوية يتحكم في جزء مهم من قدرة الدولة على العمل والاستمرار[1].

ثانيًا: الأمن السيبراني ودوره في حماية الاستقلال الرقمي

يمثل الأمن السيبراني الأداة العملية لحماية السيادة الرقمية، لأنه يهدف إلى حماية الأنظمة والشبكات والبيانات من الاختراق والتخريب والتجسس والسرقة. وإذا كانت السيادة التقليدية تحتاج إلى حدود وجيش ومؤسسات أمنية، فإن السيادة الرقمية تحتاج إلى أنظمة دفاع سيبراني، ومراكز للرصد والاستجابة، وخطط لحماية البنية التحتية الحيوية[2].

كما يتجلى دور الأمن السيبراني في عدة مستويات. فهو يحمي مؤسسات الدولة من الهجمات الرقمية، ويحمي بيانات المواطنين من الاستغلال غير المشروع، ويحمي الاقتصاد من الجرائم المالية الإلكترونية، ويحمي الخدمات الحيوية من التعطيل. كما يسمح للدولة بالرد السريع على الحوادث الرقمية، وتقليل آثارها، واستعادة الخدمات في أقصر وقت ممكن[3].

غير أن الأمن السيبراني لا يتحقق فقط عبر شراء برامج حماية أو أجهزة تقنية، بل يتطلب سياسة وطنية شاملة تشمل التشريع، والتكوين، والتنسيق بين المؤسسات، وتطوير الكفاءات، وتعزيز التعاون بين القطاع العام والخاص. فالقطاع الخاص يدير جزءًا كبيرًا من البنية الرقمية، ومن ثم فإن حماية السيادة الرقمية تحتاج إلى تعاون فعلي بين الدولة والمؤسسات الاقتصادية والتقنية.

يعد الأمن السيبراني شرطًا أساسيًا للاستقلال الرقمي، لأن الدولة التي لا تستطيع حماية فضائها الرقمي لا تستطيع ضمان استقلال قرارها ولا حماية بياناتها ولا تأمين خدماتها الحيوية.

---

[1]– حنان بوعكاز، **التنظيم القانوني للجرائم الإلكترونية في التشريع الجزائري**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة منتوري قسنطينة 1، الجزائر، 2020، ص 88.

[2]– ياسر عبد العزيز، **عصر ما بعد العولمة: السيادة الرقمية وصراع التحكم في البيانات**، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، مصر، 2022، ص 17.

[3]– ياسر عبد العزيز، المرجع نفسه ، ص18.

ثالثًا: الاقتصاد الرقمي وتقليل التبعية التكنولوجية للخارج

يمثل الاقتصاد الرقمي بعدًا مهمًا من أبعاد السيادة الرقمية، لأنه يرتبط بقدرة الدولة على إنتاج القيمة داخل البيئة الرقمية بدل الاكتفاء باستهلاك خدمات ومنتجات أجنبية. فالاقتصاد الرقمي يشمل التجارة الإلكترونية، والخدمات المالية الرقمية، والمنصات الوطنية، والبرمجيات، والذكاء الاصطناعي، والابتكار، والشركات الناشئة، وصناعة المحتوى، والخدمات السحابية[1].

وتكمن أهمية هذا البعد في أن التبعية التكنولوجية قد تتحول إلى تبعية سياسية واقتصادية. فإذا كانت الدولة تعتمد على منصات أجنبية في تخزين بياناتها، وعلى برمجيات أجنبية في إدارة مؤسساتها، وعلى شركات خارجية في تشغيل خدماتها الرقمية، فإن قدرتها على اتخاذ قرارات مستقلة تصبح محدودة، خاصة إذا تعرضت هذه الخدمات للتوقف أو الضغط أو الحظر[2].

ولهذا، فإن تقليل التبعية الرقمية لا يعني الانغلاق أو رفض التعاون الدولي، بل يعني بناء قدرات وطنية في المجالات الحيوية، وتشجيع الصناعات الرقمية المحلية، ودعم الشركات الناشئة، وتكوين الخبرات، وتطوير حلول وطنية في القطاعات الحساسة. فالدولة لا تستطيع تحقيق سيادة رقمية كاملة إذا كانت تعتمد كليًا على الخارج في التكنولوجيا والبرمجيات والخدمات السحابية[3].

كما أن الاقتصاد الرقمي يساعد على تعزيز القوة الاقتصادية للدولة، من خلال خلق فرص عمل جديدة، وتطوير الخدمات، وتحسين الإنتاجية، وجذب الاستثمار، ودعم الابتكار. ومن ثم، فإن السيادة الرقمية لا تنفصل عن التنمية الاقتصادية، بل تشكل أحد شروطها في العصر الحديث.

---

[1]– حنان بوعكاز، **التنظيم القانوني للجرائم الإلكترونية في التشريع الجزائري**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة منتوري قسنطينة 1، الجزائر، 2020، ص 88.

[2]– عبد الرحمان خلفي، **القانون الإداري الرقمي والتحول الإلكتروني للإدارة**، الطبعة الأولى، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2021، ص 77.

[3]– عبد الرحمان خلفي، المرجع نفسه ، ص81.

المبحث الثاني: الأسس القانونية والسياسية للسيادة الرقمية

أدى الطابع العابر للحدود للفضاء الرقمي إلى ظهور تحديات جديدة أمام الدولة، خاصة فيما يتعلق بتحديد الاختصاص القانوني، وحماية المعطيات الشخصية، ومكافحة الجرائم الإلكترونية، وتنظيم عمل المنصات الرقمية العالمية. ولهذا، لم يعد تحقيق السيادة الرقمية مرتبطًا فقط بقدرة الدولة على سن القوانين الوطنية، بل أصبح يتطلب كذلك تعاونًا دوليًا وإقليميًا من أجل وضع قواعد مشتركة لتنظيم الفضاء السيبراني وحماية الأمن الرقمي الجماعي.[1]

يثير موضوع السيادة الرقمية إشكالية دقيقة تتعلق بحدود تدخل الدولة في الفضاء الرقمي، إذ تسعى الدول إلى حماية أمنها الوطني وبياناتها الاستراتيجية، وفي الوقت نفسه تظل مطالبة باحترام الحقوق والحريات الرقمية، وعلى رأسها حرية التعبير، والحق في الوصول إلى المعلومات، وحماية الخصوصية. ومن هنا، فإن الأسس القانونية والسياسية للسيادة الرقمية تقوم على تحقيق التوازن بين مقتضيات الأمن والسيادة من جهة، ومتطلبات الحريات الرقمية من جهة أخرى.[2]

كما أن التطور السريع للتكنولوجيا، وظهور الذكاء الاصطناعي، والخدمات السحابية، والاقتصاد الرقمي، جعل استقلال الدولة الرقمي مرتبطًا بمدى قدرتها على امتلاك تشريعات فعالة، وبنية تحتية مؤمنة، واستراتيجية وطنية للأمن السيبراني، إضافة إلى تقليل التبعية للمنصات والتقنيات الأجنبية. لذلك أصبحت السيادة الرقمية جزءًا من السياسات العامة للدول الحديثة، ووسيلة لحماية القرار الوطني وتعزيز الاستقلال السياسي والاقتصادي.[3]

---

[1]– جمال الدين شيخي، **القانون الدولي للاتصالات وتحديات الفضاء السيبراني**، الطبعة الأولى، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2019، ص 62.

[2]– عبد الرحمان خلفي، **القانون الإداري الرقمي والتحول الإلكتروني للإدارة**، الطبعة الأولى، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2021، ص 88.

[3]– رحيم محمد، ابن يحي نبيلة، "الأمن السيبراني في المنشآت الحكومية"، **المجلة الجزائرية للدراسات السياسية**، الجزائر، المجلد 10، العدد 1، 2023، ص 179.

وعليه، سيتم تناول هذا المبحث من خلال مطلبين؛ يخصص الأول للإطار القانوني المنظم للسيادة الرقمية، من خلال دراسة التشريع الوطني والاتفاقيات الدولية ذات الصلة بالفضاء الرقمي، بينما يتناول الثاني مبدأ استقلال الدولة الرقمي والتحديات المرتبطة بالتوازن بين حماية السيادة وضمان حرية الإنترنت.

المطلب الأول: الإطار القانوني المنظم للسيادة الرقمية

تحتاج السيادة الرقمية إلى إطار قانوني واضح ينظم علاقة الدولة بفضائها الرقمي، ويحدد القواعد التي تحكم استعمال البيانات، وحماية الأنظمة المعلوماتية، ومكافحة الجرائم الإلكترونية، وضبط المعاملات الرقمية. فالدولة لا تستطيع ممارسة سيادتها الرقمية بمجرد امتلاك بنية تقنية أو إعلان سياسة عامة في المجال الرقمي، بل تحتاج إلى منظومة قانونية تمنحها أدوات التدخل والتنظيم والحماية[1].

ويكتسب الإطار القانوني أهمية خاصة لأن الفضاء الرقمي يتميز بطابع عابر للحدود، حيث قد تقع الجريمة الإلكترونية داخل دولة، وتُدار أدواتها من دولة ثانية، وتخزن أدلتها في خوادم موجودة في دولة ثالثة. لذلك، فإن التشريع الوطني وحده لا يكفي دائمًا لمواجهة المخاطر الرقمية، بل يجب أن يتكامل مع الاتفاقيات الدولية والإقليمية وآليات التعاون القضائي والأمني[2].

وفي الحالة الجزائرية، يظهر هذا الإطار من خلال عدة نصوص قانونية، منها قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وقانون التجارة الإلكترونية، وقانون التوقيع والتصديق الإلكترونيين. كما يتعزز هذا الإطار من خلال الاتفاقيات الدولية والإقليمية ذات الصلة بمكافحة الجريمة الإلكترونية وحماية البيانات.

---

[1]– محمد أمين بوخاري، **الاختصاص القضائي في الجرائم الإلكترونية**، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2016، ص 82.

[2]– عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي: دراسة متعمقة في القانون المعلوماتي**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 18.

الفرع الأول: القوانين الوطنية المنظمة للفضاء الرقمي: التشريع الجزائري نموذجًا

يمثل التشريع الوطني الأداة الأولى التي تعتمد عليها الدولة في تنظيم فضائها الرقمي، لأنه يحدد القواعد القانونية التي تضبط استعمال التكنولوجيا، وتحمي البيانات الشخصية، وتجرم الاعتداء على الأنظمة المعلوماتية، وتنظم المعاملات الإلكترونية. ومن خلال هذه القواعد تستطيع الدولة فرض سلطتها القانونية داخل البيئة الرقمية، بما يعزز سيادتها ويحمي أمنها الرقمي.

وقد اتجه المشرع الجزائري إلى وضع عدة نصوص قانونية لمواكبة التحول الرقمي، خاصة في مجال مكافحة الجرائم الإلكترونية، وحماية المعطيات الشخصية، وتنظيم التجارة الإلكترونية، والتوقيع والتصديق الإلكترونيين. وهذه النصوص تشكل مجتمعة أساسًا قانونيًا مهمًا للسيادة الرقمية، لأنها تسمح للدولة بحماية بياناتها، وضبط المعاملات الرقمية، وملاحقة الأفعال التي تهدد أمن الأنظمة المعلوماتية[1].

أولًا: دور التشريع الوطني في تنظيم الفضاء الرقمي

يقوم التشريع الوطني بدور أساسي في تنظيم الفضاء الرقمي، لأنه يحدد ما هو مشروع وما هو غير مشروع في استخدام تكنولوجيا الإعلام والاتصال. فالدولة، من خلال القانون، تستطيع وضع قواعد خاصة بالدخول إلى الأنظمة المعلوماتية، وحماية المعطيات، وتنظيم الخدمات الرقمية، وضبط التجارة الإلكترونية، وتحديد مسؤولية مقدمي الخدمات الرقمية[2].

يعد القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها من أوائل النصوص الخاصة التي حاولت وضع إطار قانوني للتعامل مع الجرائم الرقمية. فقد جاء هذا القانون ليضع قواعد للوقاية من الجرائم

[1]– فارس محمد العمارات، إبراهيم محمد الحمامصة، **الأمن السيبراني: المفهوم وتحديات العصر**، الطبعة الأولى، دار الخليج للنشر والتوزيع، عمان، الأردن، 2022، ص 43.

[2]– فارس محمد العمارات،المرجع السابق ،ى ص45.

المعلوماتية، ويحدد آليات مكافحتها، خاصة عندما يتعلق الأمر بالمساس بالأنظمة المعلوماتية أو استعمال الوسائل الإلكترونية في ارتكاب الجرائم.[1]

كما يمثل القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين خطوة مهمة في بناء الثقة في المعاملات الرقمية، لأنه نظم القواعد العامة للتوقيع الإلكتروني والتصديق الإلكتروني، بما يسمح بإضفاء الحجية القانونية على بعض المعاملات الإلكترونية. وتكمن أهمية هذا القانون في أنه يربط السيادة الرقمية بفكرة الثقة الرقمية، لأن الدولة لا تستطيع تطوير إدارة إلكترونية أو اقتصاد رقمي دون آليات قانونية للتحقق من الهوية الرقمية وصحة التعاملات الإلكترونية.[2]

أما القانون رقم 18-05 المتعلق بالتجارة الإلكترونية، فيظهر أهميته من حيث تنظيم النشاط التجاري عبر الوسائط الإلكترونية، وضبط العلاقة بين المورد الإلكتروني والمستهلك، وتحديد شروط ممارسة التجارة الإلكترونية. وهذا النص يرتبط بالسيادة الرقمية من زاوية اقتصادية، لأنه يسمح للدولة بتنظيم جزء من النشاط الاقتصادي الذي انتقل إلى الفضاء الرقمي.[3]

ثانيًا: حماية المعطيات الشخصية ومكافحة الجرائم الإلكترونية

تُعد حماية المعطيات الشخصية من أهم مظاهر السيادة الرقمية، لأن البيانات الشخصية أصبحت من أكثر الموارد الرقمية حساسية. فإذا لم تستطع الدولة حماية بيانات مواطنيها، فإن جزءًا من سيادتها الرقمية يصبح مهددًا، خاصة في ظل قدرة الشركات والمنصات الرقمية على جمع البيانات وتحليلها وتوظيفها لأغراض اقتصادية أو سياسية أو أمنية.

---

[1]- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية**، العدد 47، 16 أوت 2009، المواد 1-6 .

[2]- القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق 1 فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، **الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية**، العدد 6، 10 فبراير 2015، المواد 1-7 و27 وما بعدها .

[3]- القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018، يتعلق بالتجارة الإلكترونية، **الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية**، العدد 28، 16 ماي 2018، المواد 1-10 .

وقد خصص المشرع الجزائري القانون رقم 18-07 لحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. ويهدف هذا القانون إلى تحديد قواعد حماية الأشخاص عند معالجة بياناتهم، سواء تمت المعالجة بطريقة آلية كلية أو جزئية، أو تمت بطريقة غير آلية متى كانت البيانات واردة في ملفات يدوية. كما نص القانون على إنشاء سلطة وطنية مكلفة بحماية المعطيات ذات الطابع الشخصي، وهو ما يعكس توجهًا نحو بناء رقابة مؤسساتية على استعمال البيانات.[1]

كما تظهر أهمية هذا القانون أنه يمنح الأفراد حماية قانونية في مواجهة المعالجة غير المشروعة للبيانات، كما يفرض التزامات على الجهات التي تجمع البيانات أو تعالجها. ومن ثم، فهو لا يحمي الخصوصية الفردية فقط، بل يعزز أيضًا قدرة الدولة على التحكم في تداول البيانات داخل فضائها الرقمي.

أما في مجال مكافحة الجرائم الإلكترونية، فإن القانون رقم 09-04 يشكل إطارًا مهمًا لمواجهة الأفعال التي تهدد الأنظمة المعلوماتية، خاصة الجرائم التي تمس بسرية البيانات أو سلامة الأنظمة أو توفر الخدمات الرقمية. كما أن قانون العقوبات الجزائري يتضمن بدوره أحكامًا مرتبطة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهو ما يسمح بتوفير حماية جنائية للفضاء المعلوماتي[2].

غير أن مكافحة الجرائم الإلكترونية لا تعتمد فقط على التجريم والعقاب، بل تتطلب كذلك إجراءات بحث وتحري وجمع أدلة رقمية. فالجريمة الرقمية تتميز بسرعة ارتكابها وصعوبة تحديد مرتكبيها وسهولة إخفاء آثارها، لذلك فإن المشرع يحتاج دائمًا إلى تطوير آليات التحقيق الرقمي بما يتماشى مع طبيعة هذه الجرائم.

ثالثًا: حدود التشريع الوطني أمام الطابع العابر للحدود للفضاء الرقمي

رغم أهمية التشريع الوطني، إلا أنه يواجه عدة حدود في تنظيم الفضاء الرقمي. فالإنترنت لا يعترف بالحدود الجغرافية، والبيانات قد تنتقل بين دول متعددة في وقت

---

[1]- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 جوان سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، **الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية**، العدد 34، 10 جوان 2018، المواد 1-4 و22 وما بعدها .

[2]-- القانون رقم 09-04 ، المرجع السابق،

قصير، كما أن مرتكبي الجرائم الإلكترونية قد يستخدمون خوادم أو شبكات أو هويات رقمية خارج إقليم الدولة[1].

وتظهر صعوبة التشريع الوطني في مسألة الاختصاص القضائي، إذ قد يكون الفاعل في دولة، والضحية في دولة أخرى، والخادم المستعمل في دولة ثالثة. وفي هذه الحالة، يصبح تطبيق القانون الوطني وحده غير كافٍ، لأن الوصول إلى الأدلة الرقمية أو توقيف الجناة أو ملاحقتهم يحتاج إلى تعاون دولي.

كما تواجه الدولة تحديًا آخر يتعلق بالشركات الرقمية العالمية، التي قد تقدم خدماتها داخل الدولة دون أن تكون مراكزها القانونية أو التقنية موجودة داخل الإقليم الوطني. وهذا يضعف قدرة الدولة على فرض قوانينها عليها، خاصة في مسائل حماية البيانات، وإزالة المحتوى غير المشروع، وتسليم المعلومات، أو الامتثال لأوامر القضاء الوطني.

الفرع الثاني: الاتفاقيات والمعاهدات الدولية ذات الصلة بالفضاء الرقمي

يتميز الفضاء الرقمي بطبيعته العالمية، ولذلك لا تستطيع الدولة أن تحمي سيادتها الرقمية اعتمادًا على قوانينها الداخلية فقط. فالجرائم الإلكترونية والاعتداءات السيبرانية ونقل البيانات عبر الحدود كلها مسائل تتطلب تعاونًا دوليًا وإقليميًا، سواء من خلال الاتفاقيات أو تبادل المعلومات أو المساعدة القضائية أو توحيد بعض قواعد التجريم والإجراءات[2].

من هنا تبرز أهمية الاتفاقيات والمعاهدات الدولية المتعلقة بالجريمة الإلكترونية وحماية البيانات والأمن السيبراني، لأنها تسعى إلى تقريب التشريعات الوطنية، وتسهيل التعاون بين الدول، وتوفير قواعد مشتركة للتعامل مع الجرائم والتهديدات الرقمية[3].

---

[1]–زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دون طبعة مذكورة، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011، ص 35.

[2]–قلات سومية، **الأحكام الإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2024، ص74.

[3]– خيدل وردة، "إجراءات جمع الأدلة الرقمية طبقًا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات"، **مجلة الدراسات القانونية المقارنة**، جامعة حسيبة بن بوعلي، الشلف، الجزائر، المجلد 8، العدد 1، 2022، ص36.

أولًا: أهمية التعاون الدولي في المجال الرقمي

يعد التعاون الدولي شرطًا أساسيًا لحماية السيادة الرقمية، لأن التهديدات الرقمية غالبًا ما تكون عابرة للحدود. فالهجمة السيبرانية قد تنطلق من إقليم لا علاقة له بالضحية، وقد تستعمل شبكات وسيطة لإخفاء المصدر الحقيقي، كما أن الأدلة الرقمية قد تكون مخزنة لدى مزود خدمة أجنبي.

لهذا، تحتاج الدول إلى آليات تعاون تسمح بتبادل المعلومات، وتسليم المجرمين، وتجميد الأدلة الرقمية، وتقديم المساعدة القضائية، وتنسيق الاستجابة للحوادث السيبرانية. كما تحتاج إلى قواعد مشتركة تحدد صور الجرائم الإلكترونية وتوحّد الحد الأدنى من إجراءات مكافحتها. [1]

تظهر أهمية التعاون الدولي أيضًا في حماية البيانات الشخصية، لأن البيانات قد تعالج أو تخزن خارج الدولة. فإذا لم توجد قواعد تنظم نقل البيانات عبر الحدود، فقد تصبح حماية المعطيات الشخصية ضعيفة أو شكلية، خاصة عندما تنتقل البيانات إلى دول لا توفر مستوى حماية مناسب.

ثانيًا: الاتفاقيات الدولية المتعلقة بمكافحة الجريمة الإلكترونية وحماية البيانات

تعد اتفاقية بودابست لسنة 2001 بشأن الجريمة المعلوماتية من أهم الاتفاقيات الدولية في هذا المجال، لأنها وضعت إطارًا لتجريم بعض الأفعال المعلوماتية، وتنظيم إجراءات التحقيق، وتعزيز التعاون الدولي في مكافحة الجريمة الإلكترونية. ورغم أنها اتفاقية أوروبية من حيث النشأة، إلا أنها اكتسبت بعدًا دوليًا بسبب انضمام دول من خارج أوروبا إليها أو استعمالها كنموذج تشريعي.[2]

وعلى المستوى العربي، تعد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 إطارًا إقليميًا يهدف إلى تعزيز التعاون بين الدول العربية في مكافحة جرائم تقنية

---

[1]–قونان كهينة، حمليل نوارة، "السلطة الوطنية كهيئة مكلفة برقابة احترام تطبيق قانون حماية المعطيات الشخصية رقم 18-07"، **مجلة الدراسات القانونية**، الجزائر، المجلد 7، العدد 2، جوان 2021، ص 267.

[2]– اتفاقية مجلس أوروبا بشأن الجريمة المعلوماتية، بودابست، 23 نوفمبر 2001، المواد 2-11 المتعلقة بتجريم الأفعال المعلوماتية، والمواد 23 وما بعدها المتعلقة بالتعاون الدولي .

المعلومات، حمايةً لأمن الدول ومصالحها وسلامة مجتمعاتها وأفرادها[1]. وقد صادقت الجزائر على هذه الاتفاقية بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014، وهو ما يعكس توجهًا نحو التعاون الإقليمي في مواجهة الجرائم الرقمية.[2]

أما المستوى الإفريقي، تبرز اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، المعروفة باتفاقية مالابو لسنة 2014، باعتبارها إطارًا قاريًا يجمع بين الأمن السيبراني، والمعاملات الإلكترونية، وحماية البيانات الشخصية. وتكمن أهميتها في أنها تحاول وضع قواعد إفريقية مشتركة لمواجهة التهديدات الرقمية وبناء الثقة في الفضاء الإلكتروني.[3]

كما اعتمدت الجمعية العامة للأمم المتحدة في ديسمبر 2024 اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، وهي أول اتفاقية عالمية شاملة في هذا المجال، وتهدف إلى تعزيز التعاون الدولي في مكافحة الجرائم المرتكبة بواسطة أنظمة تكنولوجيا المعلومات والاتصال، وتبادل الأدلة الإلكترونية في الجرائم الخطيرة. وهذه الاتفاقية تعكس اتجاه المجتمع الدولي نحو بناء إطار عالمي أكثر اتساعًا للتعاون في المجال السيبراني[4].

ثالثًا: دور المنظمات الدولية في تنظيم الفضاء الرقمي

تلعب المنظمات الدولية دورًا مهمًا في تنظيم الفضاء الرقمي، سواء من خلال إعداد الاتفاقيات، أو إصدار التوصيات، أو مساعدة الدول على بناء استراتيجيات الأمن

---

[1]- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة، 21 ديسمبر 2010، المادة 1 المتعلقة بهدف الاتفاقية، والمادة 2 المتعلقة بالمصطلحات، والمواد المتعلقة بالتعاون القضائي .

[2]- المرسوم الرئاسي رقم 14-252 المؤرخ في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، **الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية**، العدد 57، 28 سبتمبر 2014 .

[3]- اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، مالابو، 27 جوان 2014، المواد المتعلقة بالأمن السيبراني وحماية البيانات الشخصية والمعاملات الإلكترونية .

[4]- اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المعتمدة بموجب قرار الجمعية العامة للأمم المتحدة رقم 243/79، نيويورك، 24 ديسمبر 2024، المواد 2 وما بعدها المتعلقة بالمصطلحات، والمواد المتعلقة بالتعاون الدولي والأدلة الإلكترونية .

السيبراني. فالأمم المتحدة أصبحت فضاءً مهمًا لمناقشة قواعد السلوك المسؤول للدول في الفضاء السيبراني، ومكافحة الجريمة الإلكترونية، وحماية الحقوق الرقمية[1].

كما يؤدي الاتحاد الدولي للاتصالات دورًا تقنيًا وتنظيميًا مهمًا، خاصة من خلال مساعدة الدول على وضع استراتيجيات وطنية للأمن السيبراني، وقياس جاهزية الدول، وتطوير القدرات الرقمية. ويظهر ذلك من خلال الأدلة التي يصدرها الاتحاد حول إعداد الاستراتيجيات الوطنية للأمن السيبراني[2] .

أما على المستوى الإقليمي، فتساهم جامعة الدول العربية والاتحاد الإفريقي في وضع أطر قانونية وسياسية مشتركة، مثل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، واتفاقية مالابو الإفريقية. وتساعد هذه الأطر على تقريب التشريعات، وتسهيل التعاون، وحماية الأمن الرقمي الإقليمي[3].

غير أن دور المنظمات الدولية لا يخلو من صعوبات، لأن تنظيم الفضاء الرقمي يثير خلافات بين الدول حول حدود السيادة، وحرية الإنترنت، وحماية الخصوصية، ومكافحة الإرهاب والجريمة، ومسؤولية الشركات الرقمية الكبرى. لذلك، فإن بناء قواعد دولية فعالة في هذا المجال يتطلب توازنًا بين حماية الأمن والسيادة من جهة، وضمان الحقوق والحريات الرقمية من جهة أخرى.

المطلب الثاني: مبدأ استقلال الدولة الرقمي وتحدياته

أصبح استقلال الدولة في العصر الرقمي لا يقاس فقط بقدرتها على حماية حدودها المادية أو إدارة مؤسساتها التقليدية، بل أصبح يرتبط كذلك بمدى قدرتها على التحكم في فضائها الرقمي، وتنظيم تدفق البيانات داخله، وحماية بنيتها التحتية المعلوماتية من التبعية والاختراق. فالفضاء الرقمي لم يعد مجالًا تقنيًا محايدًا، بل تحول

---

[1]–قطاف سليمان، بوقرين عبد الحليم، "الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، **المجلة الأكاديمية للبحوث القانونية والسياسية**، جامعة عمار ثليجي، الأغواط، الجزائر، المجلد 6، العدد 1، 2022،ص 154.

[2]– محمد العيداني، "حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18–07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"، **مجلة الاجتهاد القضائي**، جامعة محمد خيضر بسكرة، الجزائر، المجلد 10، العدد 2، 2018، ص ص 115–127 .

[3]– قطاف سليمان، المرجع السابق ، ص157.

إلى ساحة تمارس فيها الدول والشركات الكبرى والفاعلون غير الحكوميين أشكالًا متعددة من التأثير والضغط والسيطرة.

ومن هذا المنطلق، يبرز مبدأ استقلال الدولة الرقمي بوصفه امتدادًا حديثًا لفكرة السيادة، حيث تسعى الدولة من خلاله إلى ضمان قدرتها على اتخاذ قراراتها الرقمية بحرية، وتنظيم الإنترنت والخدمات الرقمية وفق قوانينها الوطنية، وحماية بيانات مواطنيها ومؤسساتها من الاستغلال الخارجي. غير أن هذا الاستقلال يواجه عدة تحديات، أهمها صعوبة ضبط الاختصاص القانوني في الفضاء الإلكتروني، وتزايد الجرائم الرقمية، والتدخلات السيبرانية الأجنبية، إضافة إلى الإشكال المتعلق بالتوفيق بين حماية السيادة الرقمية وضمان حرية الإنترنت[1].

وعليه، سيتم تناول هذا المطلب من خلال فرعين؛ يخصص الأول لحق الدولة في تنظيم وإدارة فضائها الرقمي، بينما يعالج الثاني التحديات القانونية والسياسية الناتجة عن محاولة تحقيق التوازن بين حماية السيادة الرقمية واحترام حرية الإنترنت.

الفرع الأول: حق الدولة في تنظيم وإدارة فضائها الرقمي

يقوم حق الدولة في تنظيم فضائها الرقمي على فكرة أساسية مفادها أن الدولة تملك، في حدود القانون، سلطة وضع القواعد التي تنظم الأنشطة الرقمية الواقعة داخل نطاقها، سواء تعلقت هذه الأنشطة بالاتصالات، أو البيانات، أو التجارة الإلكترونية، أو الإعلام الرقمي، أو حماية الأنظمة المعلوماتية.[2] غير أن ممارسة هذا الحق في البيئة الرقمية تختلف عن ممارسته في المجال التقليدي، لأن الفضاء الرقمي يتجاوز الحدود الإقليمية، وتشارك فيه جهات متعددة، منها الدول، والشركات التكنولوجية، والمنصات العالمية، ومزودو الخدمات الرقمية.

[1]– داون نونسياتو، **الحرية الافتراضية: حيادية الشبكة وحرية التعبير في عصر الإنترنت**، ترجمة أنور الشامي، الطبعة الأولى، وزارة الثقافة والفنون والتراث، قطر، 2011، ص 25.

[2]– داود كمال، "حقوق الإنسان في الفضاء الرقمي: التعزيز والحماية"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، جامعة محمد بوضياف المسيلة، الجزائر، المجلد 10، العدد 1، 2025، ص 463

لذلك فإن تنظيم الدولة لفضائها الرقمي لا يعني الانغلاق أو فرض الرقابة المطلقة، وإنما يعني بناء قدرة قانونية وتقنية ومؤسساتية تسمح للدولة بحماية مصالحها الوطنية، وضمان أمنها الرقمي، وتنظيم استخدام التكنولوجيا بما لا يمس الحقوق الأساسية للأفراد.

أولًا: مضمون استقلال الدولة الرقمي

يقصد باستقلال الدولة الرقمي قدرة الدولة على إدارة مواردها الرقمية بصورة مستقلة، وحماية بياناتها ومعلوماتها الاستراتيجية، وضمان عدم خضوع بنيتها الرقمية الحيوية لسيطرة خارجية مباشرة أو غير مباشرة. ويشمل هذا الاستقلال عدة عناصر، أهمها استقلال القرار الرقمي، وحماية البيانات الوطنية، وامتلاك بنية تحتية رقمية مؤمنة، وتطوير تشريعات قادرة على تنظيم البيئة الرقمية[1].

ولا يتحقق الاستقلال الرقمي بمجرد إعلان الدولة رغبتها في حماية فضائها الإلكتروني، بل يحتاج إلى سياسة عامة واضحة تقوم على تحديد الأولويات الرقمية للدولة، وتطوير الكفاءات الوطنية، وضمان حماية الأنظمة المعلوماتية، وتقليل الاعتماد الكلي على البرمجيات والمنصات والخدمات الأجنبية. فالتبعية الرقمية قد تؤدي إلى إضعاف الدولة حتى لو كانت تتمتع بسيادة تقليدية كاملة؛ لأن من يتحكم في البيانات والمنصات والبنية التحتية يستطيع التأثير في الإدارة والاقتصاد والرأي العام[2].

ثانيًا: سلطة الدولة في تنظيم الإنترنت والبنية التحتية الرقمية

تمارس الدولة سلطتها في تنظيم الإنترنت من خلال وضع قواعد قانونية تضبط عمل مزودي خدمات الإنترنت، وتنظيم المنصات الرقمية، وتحديد شروط حماية البيانات، ومكافحة الجرائم الإلكترونية، وضمان أمن الشبكات الوطنية. ويُعد هذا التنظيم ضروريًا لأن الإنترنت أصبح مرتبطًا بالمرافق الحيوية، والخدمات العمومية، والتجارة، والتعليم، والصحة، والإعلام، والاتصال.

---

[1]– لسود موسى، "معايير الاختصاص القضائي في جرائم قانون التجارة الإلكترونية الجزائري 18-05"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، جامعة محمد بوضياف المسيلة، الجزائر، المجلد 4، العدد 2، 2020، ص 366.

[2]– بوعزة حكيمة، "معايير تحديد الاختصاص القضائي للجريمة المعلوماتية"، **مجلة القانون والعلوم السياسية**، الجزائر، المجلد 11، العدد 2، 2025، ص 289.

غير أن سلطة الدولة في تنظيم الإنترنت لا ينبغي أن تفهم باعتبارها سلطة مطلقة، لأن الإنترنت فضاء يرتبط كذلك بحرية التعبير، والحق في الوصول إلى المعلومات، والحق في الخصوصية. لذلك، فإن التنظيم المشروع هو الذي يهدف إلى حماية الأمن الوطني والنظام العام والحقوق الرقمية، دون أن يتحول إلى وسيلة لتعطيل الحريات أو فرض رقابة غير مبررة[1].

أما البنية التحتية الرقمية، فهي تمثل الأساس المادي والتقني للاستقلال الرقمي. وتشمل شبكات الاتصال، ومراكز البيانات، والخوادم، والمنصات الحكومية، وأنظمة الدفع الإلكتروني، وشبكات المؤسسات الحيوية. وكلما كانت هذه البنية خاضعة لحماية وطنية فعالة، زادت قدرة الدولة على التحكم في خدماتها وبياناتها. أما إذا كانت الدولة تعتمد كليًا على بنية أجنبية أو خدمات سحابية لا تخضع لقوانينها، فإن استقلالها الرقمي يصبح محدودًا[2].

ثالثًا: حماية القرار الوطني من التبعية والتأثير الرقمي الخارجي

يعد القرار الوطني من أهم المجالات التي تتأثر بالسيادة الرقمية. ففي العصر الرقمي، لم يعد التأثير الخارجي يتم فقط عن طريق الضغط الدبلوماسي أو الاقتصادي، بل قد يتم عبر التحكم في المعلومات، أو توجيه الرأي العام، أو نشر الأخبار المضللة، أو اختراق المؤسسات، أو تعطيل الخدمات الحيوية. لذلك، فإن حماية القرار الوطني أصبحت مرتبطة بقدرة الدولة على حماية فضائها الإعلامي والمعلوماتي والسيبراني[3].

وتظهر التبعية الرقمية عندما تعتمد الدولة بشكل واسع على تقنيات لا تملك التحكم فيها، أو على منصات خارجية تتحكم في تدفق المعلومات، أو على خدمات سحابية أجنبية تخزن بيانات حساسة. ففي هذه الحالة، تصبح الدولة معرضة لمخاطر متعددة،

[1]– محمد سامي الشوا، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 1994، ص60.

[2]– نصيرة بوحزمة، **التحقيق الجنائي في الجرائم الإلكترونية: دراسة مقارنة**، أطروحة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس، الجزائر، 2022، ص 109.

[3]– نصيرة بوحزمة، المرجع نفسه ، ص110.

منها فقدان السيطرة على البيانات، وصعوبة فرض القانون الوطني، واحتمال تعرض الخدمات الرقمية للتوقف أو الحظر أو الاستغلال[1].

كما أن التأثير الرقمي الخارجي قد يمس الرأي العام من خلال الحملات الإلكترونية المنظمة، والحسابات الوهمية، والتلاعب بالخوارزميات، ونشر المحتوى المضلل، وهذا النوع من التأثير لا يستهدف مؤسسات الدولة فقط، بل يستهدف الثقة الاجتماعية والسياسية، وقد يؤثر في الانتخابات والنقاش العام والأمن الداخلي.

الفرع الثاني: التحديات القانونية والسياسية بين حماية السيادة وحرية الإنترنت

تواجه السيادة الرقمية تحديًا مزدوجًا؛ فمن جهة تحتاج الدولة إلى حماية أمنها الوطني وبياناتها وبنيتها الرقمية، ومن جهة أخرى يجب عليها احترام حرية الإنترنت والحقوق الرقمية للأفراد. وتظهر صعوبة هذا التوازن في أن التدخل المفرط باسم حماية السيادة قد يؤدي إلى تقييد حرية التعبير والوصول إلى المعلومات، بينما قد يؤدي الانفتاح غير المنظم إلى تعريض الدولة والمجتمع لمخاطر الجرائم الإلكترونية، والتدخلات الأجنبية، والتضليل الرقمي[2].

أولًا: التحديات القانونية المرتبطة بالاختصاص والجرائم الرقمية

تعد مسألة الاختصاص من أبرز التحديات القانونية في المجال الرقمي، لأن الجرائم الإلكترونية غالبًا ما تكون عابرة للحدود. فقد يرتكب الجاني فعله من دولة، ويستعمل خوادم في دولة أخرى، وتظهر آثار الجريمة في دولة ثالثة. وهذا الوضع يطرح سؤالًا مهمًا: أي قانون يطبق؟ وأي قضاء يختص؟ وكيف يمكن جمع الأدلة الرقمية إذا كانت موجودة خارج الإقليم الوطني؟

وتزداد هذه الصعوبة بسبب الطبيعة غير المادية للدليل الرقمي، إذ يمكن محوه أو تعديله أو نقله بسرعة. كما أن الوصول إلى البيانات قد يتطلب تعاونًا مع شركات أجنبية أو سلطات قضائية في دول أخرى. لذلك، فإن القواعد التقليدية للاختصاص لا تكون دائمًا

[1]– نصيرة بوحزمة، المرجع السابق ، ص112.

[2]– فارس محمد العمارات، إبراهيم محمد الحمامصة، **الأمن السيبراني: المفهوم وتحديات العصر**، الطبعة الأولى، دار الخليج للنشر والتوزيع، عمان، الأردن، 2022، ص83.

كافية لمواجهة الجرائم الرقمية، وهو ما يفرض تطوير قواعد إجرائية خاصة، وتعزيز التعاون القضائي الدولي[1].

ومن جهة أخرى، تواجه الدولة تحديًا في تجريم الأفعال الرقمية دون المساس بالحريات. فليس كل استعمال للإنترنت ينبغي أن يخضع للتجريم، بل يجب أن يكون القانون واضحًا ودقيقًا حتى لا يتحول إلى أداة لتقييد حرية التعبير أو النشاط المشروع. ومن هنا، يجب التمييز بين الأفعال التي تمس الأمن الرقمي فعلًا، مثل الاختراق والتجسس وسرقة البيانات، وبين الممارسات المرتبطة بالتعبير والنقاش العام[2].

ثانيًا: التحديات السياسية الناتجة عن التدخلات السيبرانية الأجنبية

لم تعد التدخلات الأجنبية في شؤون الدول تتم بالوسائل التقليدية فقط، بل أصبحت التدخلات السيبرانية من أخطر مظاهر التأثير الخارجي. فقد تستهدف هذه التدخلات مؤسسات الدولة، أو البنية التحتية، أو قواعد البيانات، أو الرأي العام، أو العمليات الانتخابية. وقد تكون هذه التدخلات صادرة عن دول، أو جماعات منظمة، أو شركات، أو فاعلين مجهولين يصعب تحديدهم[3].

وتكمن خطورة التدخلات السيبرانية في أنها قد تتم دون إعلان، ودون مواجهة مباشرة، وقد يصعب إثبات مصدرها بدقة. فالهجوم السيبراني يمكن أن يسبب أضرارًا اقتصادية وأمنية كبيرة دون استعمال السلاح التقليدي. كما يمكن أن يؤدي تسريب البيانات أو التلاعب بالمعلومات إلى إضعاف الثقة في مؤسسات الدولة.

ومن صور التدخل السياسي الرقمي نشر الأخبار المضللة، والتأثير في النقاش العام، وتوجيه الحملات الرقمية ضد مؤسسات الدولة، واستغلال المنصات الاجتماعية لإثارة الانقسام الداخلي. وهذه الممارسات تجعل حماية السيادة الرقمية مرتبطة ليس فقط

---

[1]– سومية قلات، **الأحكام الإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2024، ص 52

[2]– سامر محي عبد الحمزة، "موقف جامعة الدول العربية من السيادة على الفضاء السيبراني: دراسة في ضوء أحكام القانون الدولي العام"، **مجلة القانون الدولي للدراسات البحثية**، المركز الديمقراطي العربي، برلين، ألمانيا، المجلد 4، العدد 12، مارس 2023، ص –24 .

[3]– سامر محي عبد الحمزة، المرجع نفسه ، ص25

بحماية الشبكات والأنظمة، بل أيضًا بحماية المجال العام الرقمي من التلاعب والتأثير غير المشروع[1].

ثالثًا: التوازن بين حماية السيادة الرقمية وضمان حرية الإنترنت

تعد حرية الإنترنت من المسائل الأساسية في البيئة الرقمية، لأنها ترتبط بحرية التعبير، والحق في الوصول إلى المعلومات، والحق في الخصوصية، والمشاركة في النقاش العام. غير أن هذه الحرية لا تعني غياب التنظيم، كما أن حماية السيادة لا تعني إلغاء الحرية. ولذلك، فإن التحدي يكمن في بناء توازن يسمح للدولة بحماية أمنها الرقمي دون المساس غير المبرر بالحقوق الرقمية[2].

ويتحقق هذا التوازن من خلال عدة شروط. أولها أن تكون القيود المفروضة على الإنترنت منصوصًا عليها في القانون بشكل واضح، حتى لا تكون خاضعة للسلطة التقديرية المطلقة. وثانيها أن تكون القيود ضرورية لحماية مصلحة مشروعة، مثل الأمن الوطني أو النظام العام أو حماية حقوق الآخرين. وثالثها أن تكون القيود متناسبة، أي لا تتجاوز ما هو لازم لتحقيق الغرض المشروع[3].

كما يتطلب التوازن بين السيادة والحرية وجود رقابة قضائية ومؤسساتية على إجراءات الدولة في الفضاء الرقمي، خاصة في مسائل حجب المواقع، أو مراقبة الاتصالات، أو جمع البيانات، أو تتبع المستخدمين. فغياب الرقابة قد يؤدي إلى انتهاك الخصوصية والحريات، بينما وجودها يعزز شرعية تدخل الدولة ويحمي الثقة بين المواطن والمؤسسات.

ومن جهة أخرى، فإن حرية الإنترنت لا يمكن أن تكون فعالة إذا ترك المجال الرقمي خاضعًا بالكامل لسلطة الشركات الخاصة الكبرى. فهذه الشركات تملك قدرة كبيرة على تنظيم المحتوى، وترتيب الظهور، وتوجيه النقاش، وجمع البيانات. ولذلك، فإن حماية

---

[1]– إيهاب خليفة، **الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس**، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، مصر، 2021، ص 142.

[2]– إيهاب خليفة، المرجع نفسه ، ص143.

[3]– كوثر منسل، **تفعيل دور الإدارة الإلكترونية في الجزائر: نحو بروز قانون للإدارة الإلكترونية**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945، قالمة، الجزائر، 2023، ص 76.

حرية الإنترنت تقتضي أيضًا مساءلة المنصات الرقمية وضمان الشفافية في خوارزمياتها وسياساتها، حتى لا تتحول إلى سلطة خاصة تتحكم في التعبير والمعلومات دون رقابة كافية[1].

وبذلك، فإن السيادة الرقمية المتوازنة هي التي تجمع بين حماية الدولة من التهديدات الرقمية، وضمان حرية الإنترنت، وحماية الخصوصية، ومساءلة الفاعلين العموميين والخواص داخل الفضاء الرقمي.

[1]– كوثر منسل، المرجع السابق ، ص77.

يتضح من خلال هذا الفصل أن السيادة الرقمية أصبحت من المفاهيم الحديثة التي فرضها التحول الرقمي على الفكر القانوني والسياسي، حيث لم تعد السيادة تقتصر على السيطرة على الإقليم المادي، بل امتدت إلى التحكم في البيانات والمعلومات والبنية التحتية الرقمية. ومن ثم، فإن الدولة التي لا تملك القدرة على حماية فضائها الرقمي قد تجد سيادتها التقليدية نفسها مهددة بوسائل جديدة وغير مباشرة.

وقد تبين أن السيادة الرقمية تقوم على عدة أبعاد مترابطة، أهمها البعد السياسي المتعلق بتحكم الدولة في بياناتها ومعلوماتها الوطنية، والبعد التقني المرتبط بالبنية التحتية الرقمية والأمن السيبراني، فضلًا عن البعد الاقتصادي الذي يظهر من خلال دعم الاقتصاد الرقمي وتقليل الاعتماد على التكنولوجيا الأجنبية.

كما أظهر الفصل أن تحقيق السيادة الرقمية يتطلب وجود إطار قانوني واضح ينظم الفضاء الرقمي، ويحمي المعطيات الشخصية، ويكافح الجرائم الإلكترونية، مع ضرورة الاستفادة من التعاون الدولي في مواجهة التهديدات العابرة للحدود. غير أن هذا التنظيم يظل مرتبطًا بتحدٍّ أساسي يتمثل في تحقيق التوازن بين حماية السيادة والأمن الوطني من جهة، وضمان حرية الإنترنت والحقوق الرقمية من جهة أخرى.

الفصل الثانـي

تطبيقات السيادة الرقمية في العلاقات الدولية

مع تنامي الاعتماد على الوسائل الرقمية في مختلف المجالات السياسية والاقتصادية والأمنية، اتجهت الدول إلى وضع سياسات واستراتيجيات تهدف إلى تعزيز استقلالها الرقمي وتقليص تبعيتها التكنولوجية، وذلك من خلال تطوير التشريعات الوطنية، ودعم الأمن السيبراني، وتشجيع الاقتصاد الرقمي الوطني. كما أصبحت القضايا الرقمية جزءًا مهمًا من العلاقات الدولية، سواء من خلال التنافس والصراعات السيبرانية، أو عبر التعاون الدولي الرامي إلى تنظيم استخدام التكنولوجيا الحديثة وضمان الأمن الرقمي العالمي.

وانطلاقًا من ذلك، يسعى هذا الفصل إلى تسليط الضوء على أبرز تطبيقات السيادة الرقمية في العلاقات الدولية، من خلال دراسة أهم الاستراتيجيات الوطنية المعتمدة لتحقيقها، إضافة إلى تحليل مظاهر الصراع والتعاون في الفضاء الرقمي، مع التطرق إلى أهم التحديات المستقبلية التي تفرضها التقنيات الحديثة والتطورات المتسارعة في المجال الرقمي.

المبحث الأول: الاستراتيجيات الوطنية لتحقيق السيادة الرقمية

أصبحت السيادة الرقمية في الوقت الراهن من أهم القضايا التي تحظى باهتمام الدول، وذلك نتيجة التحولات العميقة التي فرضتها الثورة الرقمية والتطور التكنولوجي المتسارع على مختلف المجالات السياسية والاقتصادية والأمنية. فلم يعد مفهوم السيادة يقتصر على الحدود الجغرافية والسيطرة الإقليمية، بل امتد ليشمل القدرة على التحكم في الفضاء الرقمي الوطني، وحماية البيانات والمعلومات، وتأمين البنية التحتية التكنولوجية من مختلف التهديدات السيبرانية.[1]

وفي ظل تصاعد الاعتماد على التكنولوجيا الرقمية في إدارة مؤسسات الدولة وتسيير الأنشطة الاقتصادية والخدمات العامة، برزت الحاجة إلى تبني استراتيجيات وطنية متكاملة تهدف إلى تحقيق الاستقلال الرقمي وتقليص التبعية التكنولوجية للدول الكبرى والشركات العالمية المسيطرة على قطاع التكنولوجيا والبيانات. ولهذا أصبحت العديد من الدول تعمل على تطوير بنى تحتية رقمية وطنية، وسن تشريعات قانونية لحماية البيانات والمعلومات، إلى جانب تعزيز الأمن السيبراني باعتباره أحد أهم أدوات حماية السيادة الوطنية في العصر الرقمي.[2]

كما يرتبط تحقيق السيادة الرقمية بشكل وثيق بتطوير الاقتصاد الرقمي الوطني، من خلال دعم الصناعات التكنولوجية المحلية، وتشجيع الابتكار الرقمي، والتحكم في تدفق البيانات الاقتصادية والتجارية، بما يساهم في تعزيز القدرة التنافسية للدولة وضمان استقلال قرارها السياسي والاقتصادي.[3] وقد أدى ذلك إلى ظهور توجهات دولية جديدة تسعى إلى بناء

[1]– عبد الفتاح بيومي حجازي، الحكومة الإلكترونية وحماية الأمن المعلوماتي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2010، ص 35.

[2]– سامي عبد الحميد رضوان، الأمن السيبراني والسيادة الرقمية في العلاقات الدولية، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، مصر، 2022، ص 77 .

[3]– أحمد بن ناصر، "تحديات السيادة الرقمية في ظل العولمة التكنولوجية"، مجلة الباحث للدراسات الأكاديمية، العدد 14، جامعة باتنة 1، الجزائر، 2020، ص 91 .

نماذج وطنية مستقلة للحوكمة الرقمية، خاصة في ظل التنافس الدولي المتزايد حول السيطرة على البيانات والتكنولوجيا الحديثة.[1]

المطلب الأول: السياسات الوطنية للسيادة الرقمية

أدى التطور المتسارع في مجال تكنولوجيا المعلومات والاتصال إلى إحداث تحولات عميقة في طبيعة وظائف الدولة الحديثة، حيث أصبحت الرقمنة تمثل عنصرًا أساسيًا في إدارة المؤسسات، وتسيير الاقتصاد، وتقديم الخدمات العمومية، وحتى في حماية الأمن القومي. وفي ظل هذا التحول، برزت الحاجة إلى تبني سياسات وطنية قادرة على حماية الفضاء الرقمي للدولة وضمان التحكم في البيانات والمعلومات الوطنية، خاصة مع تنامي التهديدات السيبرانية والتبعية التكنولوجية للدول الكبرى والشركات الرقمية العالمية.[2]

ولم تعد السيادة الوطنية تقتصر على السيطرة على الحدود البرية أو البحرية والجوية فقط، بل امتدت لتشمل المجال الرقمي الذي أصبح فضاءً جديدًا للتنافس والصراع بين الدول. ولهذا اتجهت الحكومات إلى تطوير استراتيجيات رقمية ترتكز على إنشاء بنية تحتية معلوماتية قوية، وتأمين البيانات الوطنية، ووضع تشريعات قانونية تنظم استخدام التكنولوجيا وتحمي المواطنين من المخاطر المرتبطة بالفضاء الإلكتروني.[3]

كما تسعى الدول من خلال هذه السياسات إلى تحقيق نوع من الاستقلال الرقمي، عبر تقليل الاعتماد على التكنولوجيا الأجنبية وتعزيز قدراتها الوطنية في مجال الاتصالات والأمن السيبراني والصناعات الرقمية. ويعكس هذا التوجه إدراك الدول لأهمية التكنولوجيا باعتبارها أحد أهم مصادر القوة والنفوذ في العلاقات الدولية المعاصرة.[4]

---

[1]– أحمد بن ناصر، المرجع السابق ، ص92

[2]– عبد الفتاح بيومي حجازي، الحكومة الإلكترونية وحماية الأمن المعلوماتي، ط1، دار الفكر الجامعي، الإسكندرية، 2010، ص 46 .

[3]– سامي عبد الحميد رضوان، الأمن السيبراني والسيادة الرقمية في العلاقات الدولية، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، جمهورية مصر العربية، 2022، ص 97 .

[4]– عبد العزيز سعد، القانون الرقمي وحماية البيانات الشخصية، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2021، ص 77 .

وعليه، سيتم التطرق في هذا المطلب إلى أهم السياسات الوطنية التي تعتمدها الدول لتحقيق السيادة الرقمية، وذلك من خلال دراسة دور البنية التحتية الرقمية في حماية البيانات، ثم إبراز أهمية التشريعات الوطنية في حماية المعلومات والمواطنين.

الفرع الأول: إنشاء البنية التحتية الرقمية الوطنية وتأمين البيانات

تُعتبر البنية التحتية الرقمية من الركائز الأساسية التي تعتمد عليها الدول في تحقيق السيادة الرقمية، لأنها تمثل القاعدة التقنية التي تسمح بإدارة البيانات والمعلومات وضمان استمرارية الخدمات الرقمية. وقد أصبحت الدول في العصر الحديث مطالبة بتطوير شبكات الاتصال وأنظمة المعلومات ومراكز تخزين البيانات، نظرًا للدور المتزايد الذي تلعبه التكنولوجيا في مختلف القطاعات الحيوية.[1]

كما أن التحكم في البنية التحتية الرقمية لم يعد مسألة تقنية فقط، بل أصبح مرتبطًا بالأمن القومي والاستقرار السياسي والاقتصادي للدولة، خاصة في ظل تصاعد التهديدات الإلكترونية ومحاولات الاختراق والتجسس الرقمي.[2]

أولًا: مفهوم البنية التحتية الرقمية الوطنية

يقصد بالبنية التحتية الرقمية مجموع الوسائل والأنظمة التكنولوجية التي تعتمد عليها الدولة في إدارة الفضاء الرقمي وتبادل المعلومات وتقديم الخدمات الإلكترونية. وتشمل هذه البنية شبكات الإنترنت، وأنظمة الاتصالات، ومراكز البيانات، وشبكات الألياف البصرية، والحوسبة السحابية، والأقمار الصناعية، إضافة إلى مختلف الأنظمة المعلوماتية المستخدمة في المؤسسات الحكومية والاقتصادية.

[1]– يوسف بن عدة، السيادة الرقمية والأمن السيبراني في القانون الدولي المعاصر، أطروحة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1 يوسف بن خدة، الجزائر، السنة الجامعية 2021–2022، ص 84 .

[2]– جميلة قرفي، "الاقتصاد الرقمي كآلية لتعزيز السيادة الوطنية"، ضمن أعمال الملتقى الوطني حول التحول الرقمي والسيادة الإلكترونية، كلية العلوم السياسية والعلاقات الدولية، جامعة قسنطينة 3 صالح بوبنيدر، الجزائر، المنعقد بتاريخ 15 مارس 2023، ص 66 .

وتكتسي هذه البنية أهمية كبيرة باعتبارها الوسيلة التي تُمكن الدولة من التحكم في بياناتها الوطنية وضمان استقلالها الرقمي. فكلما كانت البنية التحتية أكثر تطورًا وحداثة، ازدادت قدرة الدولة على مواجهة التهديدات السيبرانية وتأمين المعلومات الحساسة المرتبطة بالأمن الوطني والمؤسسات الحيوية.[1]

كما أن امتلاك بنية تحتية رقمية وطنية يساهم في تقليل التبعية التكنولوجية للخارج، خاصة في ظل هيمنة بعض الشركات العالمية على خدمات التخزين السحابي ومنصات الاتصال الرقمية، الأمر الذي قد يعرض بيانات الدول ومؤسساتها لمخاطر الاختراق أو الاستغلال الخارجي.[2]

ثانيًا: أهمية تأمين البيانات الوطنية

تعتبر البيانات أهم الموارد الاستراتيجية التي تعتمد عليها الدول في إدارة شؤونها السياسية والاقتصادية والأمنية، ولذلك تسعى الحكومات إلى توفير حماية قانونية وتقنية للمعلومات الوطنية من مختلف المخاطر الإلكترونية.[3]

وتتمثل أهمية تأمين البيانات في حماية المعلومات الحساسة المتعلقة بالمؤسسات الحكومية والقطاعات الاقتصادية الحيوية، ومنع عمليات التجسس الرقمي والاختراقات الإلكترونية التي قد تؤثر على استقرار الدولة وأمنها القومي. كما يساهم تأمين البيانات في تعزيز ثقة المواطنين في الخدمات الإلكترونية وضمان سلامة المعاملات الرقمية.

وفي هذا السياق، اتجهت العديد من الدول إلى إنشاء مراكز وطنية للبيانات تهدف إلى تخزين المعلومات داخل حدودها الإقليمية، بما يسمح بخضوعها للقوانين الوطنية وعدم

[1]– جميلة قرفي،المرجع السابق ، ص67.

[2]– بن برغوث ليلى، "الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي: التهديدات، التقنيات، التحديات وآليات التصدي"، المجلة الدولية للاتصال الاجتماعي، المجلد 10، العدد 01، جامعة عبد الحميد بن باديس مستغانم، الجزائر، مارس 2023، ص 443.

[3]– سمير بارة، "الأمن السيبراني (Cyber Security) في الجزائر: السياسات والمؤسسات"، المجلة الجزائرية للأمن الإنساني، المجلد 02، العدد 02، جامعة قاصدي مرباح ورقلة، الجزائر، 2017، ص 87.

انتقالها إلى جهات أجنبية. ويُعرف هذا التوجه بسياسة "توطين البيانات"، التي أصبحت من أبرز مظاهر السيادة الرقمية الحديثة.

كما تعتمد الدول على أنظمة التشفير والحماية الإلكترونية، إضافة إلى تطوير برامج المراقبة السيبرانية واستخدام الذكاء الاصطناعي للكشف المبكر عن التهديدات والهجمات الرقمية، بهدف ضمان سلامة البنية التحتية المعلوماتية.[1]

ثالثًا: جهود الجزائر في تعزيز البنية التحتية الرقمية

شهدت الجزائر خلال السنوات الأخيرة اهتمامًا متزايدًا بتطوير البنية التحتية الرقمية، وذلك من خلال تحديث شبكات الاتصالات وتوسيع استخدام الألياف البصرية وتطوير خدمات الحكومة الإلكترونية. كما سعت الدولة إلى تحسين جودة خدمات الإنترنت وتعزيز استخدام الوسائل الرقمية في مختلف الإدارات والمؤسسات العمومية.

وفي إطار حماية الفضاء الرقمي الوطني، عملت الجزائر على إنشاء منظومة وطنية لأمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي رقم 20-05، بهدف تعزيز الأمن السيبراني وحماية الشبكات الوطنية من التهديدات الإلكترونية.[2]

كما تبنت الدولة عدة مشاريع مرتبطة بالتحول الرقمي والرقمنة الإدارية، بهدف تحسين الخدمات العمومية وتعزيز القدرة الوطنية على التحكم في البيانات والمعلومات الرقمية، بما يساهم في دعم السيادة الوطنية في المجال الرقمي.

[1]- أحمد بن ناصر، "تحديات السيادة الرقمية في ظل العولمة التكنولوجية"، مجلة الباحث للدراسات الأكاديمية، العدد 14، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، 2020، ص 91-

[2]- المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، الجريدة الرسمية للجمهورية الجزائرية، العدد 04، الصادرة بتاريخ 22 جانفي 2020 .

الفرع الثاني: تطوير التشريعات الوطنية لحماية المعلومات والمواطنين

إلى جانب تطوير البنية التحتية الرقمية، أصبح من الضروري وضع إطار قانوني ينظم استخدام الوسائل التكنولوجية ويحمي البيانات والمعلومات الوطنية من مختلف أشكال الاستغلال أو الاعتداء الإلكتروني. وقد أدى الانتشار الواسع لاستخدام الإنترنت والخدمات الرقمية إلى ظهور جرائم جديدة، مثل القرصنة الإلكترونية وسرقة البيانات والاحتيال الرقمي، الأمر الذي دفع الدول إلى تحديث تشريعاتها القانونية لمواكبة التطورات التكنولوجية الحديثة.[1]

كما أصبحت القوانين الرقمية أداة أساسية لحماية الأمن الوطني وضمان احترام حقوق الأفراد داخل البيئة الرقمية، خاصة في ظل تزايد المخاوف المرتبطة بانتهاك الخصوصية الرقمية واستغلال البيانات الشخصية من طرف الشركات والمنصات الإلكترونية العالمية.[17]

أولًا: مفهوم التشريعات الرقمية وأهدافها

يقصد بالتشريعات الرقمية مجموع القواعد القانونية التي تنظم استخدام تكنولوجيا المعلومات والاتصال، وتهدف إلى حماية البيانات الشخصية، وتنظيم المعاملات الإلكترونية، ومكافحة الجرائم السيبرانية، وضمان أمن الفضاء الرقمي. [2]

وتسعى هذه التشريعات إلى تحقيق عدة أهداف، من أهمها حماية الخصوصية الرقمية للأفراد، وضمان سرية المعلومات، ومواجهة الجرائم الإلكترونية، إضافة إلى تعزيز الثقة في الخدمات الإلكترونية والمعاملات الرقمية. كما تسمح للدولة بفرض رقابتها القانونية على الأنشطة الرقمية بما يحقق الأمن والاستقرار داخل المجتمع.

[1]– محمد بن يحي، "الاقتصاد الرقمي كمدخل لتحقيق السيادة الوطنية"، مجلة العلوم السياسية والقانون، العدد 09، جامعة الجزائر 3، الجزائر، 2022، ص 80.

[2]– يوسف بن عدة، السيادة الرقمية والأمن السيبراني في القانون الدولي المعاصر، أطروحة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1 يوسف بن خدة، الجزائر، السنة الجامعية 2021–2022، ص 54.

ثانيًا: حماية المعلومات والبيانات الشخصية

تُعد حماية البيانات الشخصية من أبرز القضايا التي اهتمت بها التشريعات الحديثة، نظرًا لتزايد استخدام المعلومات الشخصية في مختلف التطبيقات والمنصات الرقمية. ولذلك اتجهت الدول إلى سن قوانين تضمن حماية خصوصية المواطنين وتنظم طرق جمع البيانات ومعالجتها وتخزينها. [1]

وقد ساهمت هذه القوانين في الحد من الاستغلال غير المشروع للمعلومات الشخصية، خاصة من طرف الشركات الرقمية الكبرى التي تعتمد بشكل واسع على جمع البيانات وتحليلها لأغراض تجارية أو سياسية. كما تهدف إلى ضمان حق الأفراد في التحكم في بياناتهم الشخصية ومعرفة كيفية استخدامها.

ويُعتبر النظام الأوروبي لحماية البيانات الشخصية (GDPR) من أبرز التشريعات الحديثة في هذا المجال، حيث فرض قواعد صارمة على المؤسسات والشركات فيما يتعلق بحماية البيانات الرقمية واحترام خصوصية الأفراد.

ثالثًا: التشريعات الجزائرية المتعلقة بالأمن الرقمي

عمل المشرع الجزائري على تعزيز الحماية القانونية للفضاء الرقمي من خلال إصدار عدة قوانين وتنظيمات تهدف إلى حماية المعلومات ومكافحة الجرائم الإلكترونية. ومن أهم هذه النصوص القانونية القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والذي يهدف إلى حماية الحياة الخاصة للمواطنين أثناء معالجة بياناتهم الرقمية.[2]

[1]- يوسف بن عدة، المرجع السابق ، ص55

[2]- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق لـ 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 34، الصادرة بتاريخ 10 جوان 2018 .

كما صدر القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بهدف التصدي للجرائم الإلكترونية والاختراقات الرقمية التي قد تهدد أمن الدولة والأفراد.[1]

إضافة إلى ذلك، قامت الدولة بإصدار مراسيم تنظيمية تتعلق بأمن الأنظمة المعلوماتية وإنشاء هيئات مختصة بالأمن السيبراني، وهو ما يعكس اهتمام الجزائر بتطوير منظومة قانونية قادرة على مواكبة التحولات الرقمية الحديثة.[2]

المطلب الثاني: الأمن السيبراني والاقتصاد الرقمي كأداة للسيادة الرقمية

لا تتحقق السيادة الرقمية بمجرد امتلاك الدولة لتشريعات تنظم الفضاء الرقمي، بل تحتاج كذلك إلى أدوات عملية تضمن حماية هذا الفضاء واستثماره. ويأتي الأمن السيبراني في مقدمة هذه الأدوات، باعتباره الوسيلة التي تمكّن الدولة من حماية شبكاتها وأنظمتها وبياناتها من الاختراق والتجسس والتعطيل، خاصة في ظل تزايد الهجمات الرقمية التي تستهدف المؤسسات الحيوية والبنية التحتية المعلوماتية[3].

كما يشكل الاقتصاد الرقمي أداة أساسية لتعزيز السيادة الرقمية، لأنه يسمح للدولة بتطوير قدراتها التكنولوجية، ودعم الابتكار، وتشجيع المؤسسات الرقمية الوطنية، وتقليل الاعتماد على الحلول والمنصات الأجنبية. فكلما تمكنت الدولة من بناء اقتصاد رقمي قوي وآمن، زادت قدرتها على حماية استقلالها الرقمي، وتعزيز مكانتها في العلاقات الدولية المعاصرة.

---

[1]- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادرة بتاريخ 16 أوت 2009 .

[2]- المرسوم الرئاسي رقم 20-05 المؤرخ في 24 جمادى الأولى عام 1441 الموافق لـ 20 جانفي 2020، المتعلق بإنشاء منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 04، الصادرة بتاريخ 22 جانفي 2020 .

[3]- فارس محمد العمارات، إبراهيم محمد الحمامصة، **الأمن السيبراني: المفهوم وتحديات العصر**، الطبعة الأولى، دار الخليج للنشر والتوزيع، عمان، الأردن، 2022، ص 74

وعليه، سيتم تناول هذا المطلب من خلال بيان دور الأمن السيبراني في حماية السيادة الرقمية، ثم إبراز أهمية الاقتصاد الرقمي في دعم الاستقلال التكنولوجي وتقليل التبعية للخارج.

الفرع الاول :الأمن السيبراني والسيادة الرقمية

لم يعد مفهوم الأمن القومي مرتبطًا فقط بالقدرات العسكرية التقليدية، بل أصبح يشمل أيضًا القدرة على حماية الفضاء الرقمي الوطني من الهجمات السيبرانية والاختراقات الإلكترونية والتجسس الرقمي. ولهذا اتجهت العديد من الدول إلى تطوير استراتيجيات وطنية للأمن السيبراني، تقوم على إنشاء أجهزة متخصصة في الدفاع الرقمي، وتعزيز أنظمة المراقبة الإلكترونية، وتطوير آليات الاستجابة السريعة للتهديدات السيبرانية.[1]

كما أن تحقيق الأمن السيبراني لا يقتصر على جهود المؤسسات الحكومية فقط، بل يتطلب تعاونًا مستمرًا بين مختلف الفاعلين، بما في ذلك القطاع الخاص والمؤسسات الاقتصادية وشركات التكنولوجيا، نظرًا لارتباط الأمن الرقمي بحماية البنية التحتية الوطنية وضمان استقرار الدولة.

أولا: برامج الدفاع السيبراني ومراقبة الهجمات الرقمية

أدى تصاعد التهديدات الإلكترونية والهجمات السيبرانية إلى توجه الدول نحو إنشاء منظومات دفاعية رقمية تهدف إلى حماية أنظمتها المعلوماتية ومؤسساتها الحيوية من مختلف أشكال الاختراق والتجسس الإلكتروني. وقد أصبحت برامج الدفاع السيبراني جزءًا أساسيًا من استراتيجيات الأمن القومي، بالنظر إلى خطورة الهجمات الرقمية وتأثيرها المباشر على استقرار الدول ومصالحها الحيوية.[2]

[1]– عبد الرؤوف منصور، الأمن السيبراني وحروب الجيل الجديد، الطبعة الأولى، دار الأيام للنشر والتوزيع، عمان، الأردن، 2021، ص 55 .

[2]– محمد شتاتحة، "الأمن السيبراني وأثره على الأمن القومي للدول"، مجلة العلوم القانونية والسياسية، المجلد 11، العدد 02، جامعة الجلفة، الجزائر، 2020، ص 143 .

كما ساهم التطور التكنولوجي في ظهور أدوات متقدمة للهجوم الإلكتروني، الأمر الذي دفع الحكومات إلى تطوير أنظمة المراقبة والاستجابة الرقمية وتعزيز قدراتها التقنية والبشرية في مجال الأمن السيبراني.[1]

1- مفهوم الدفاع السيبراني

يقصد بالدفاع السيبراني مجموعة التدابير والإجراءات التقنية والقانونية والأمنية التي تعتمدها الدولة لحماية شبكاتها وأنظمتها الرقمية من الهجمات الإلكترونية والاختراقات السيبرانية. ويهدف هذا النوع من الدفاع إلى ضمان سلامة المعلومات والبيانات الوطنية والحفاظ على استمرارية عمل المؤسسات الحيوية.

ويشمل الدفاع السيبراني عدة مجالات، مثل حماية الشبكات الحكومية، وتأمين البنية التحتية الرقمية، وتطوير برامج مكافحة الفيروسات والهجمات الإلكترونية، إضافة إلى إنشاء فرق مختصة بالاستجابة للحوادث السيبرانية.[2]

وقد أصبح هذا النوع من الدفاع يشكل امتدادًا لمفهوم الدفاع التقليدي، خاصة مع انتقال الصراعات الدولية إلى الفضاء الرقمي واستخدام الهجمات الإلكترونية كوسيلة للتأثير السياسي والاقتصادي والعسكري بين الدول.

2- برامج الدفاع السيبراني

تعتمد الدول على عدة برامج وآليات لتعزيز دفاعها السيبراني، ومن أهمها:

أ-إنشاء مراكز وطنية للأمن السيبراني

اتجهت العديد من الدول إلى إنشاء هيئات ومراكز وطنية مختصة بالأمن السيبراني، تتولى مراقبة التهديدات الإلكترونية والاستجابة للهجمات الرقمية. وتعمل هذه الهيئات على تنسيق الجهود الوطنية المتعلقة بحماية الأنظمة المعلوماتية والبنية التحتية الحساسة.[3]

---

[1]- علي محفوظ، "التهديدات الإلكترونية وانعكاساتها على الأمن الوطني"، مجلة الباحث الأكاديمي، العدد 15، جامعة بسكرة، الجزائر، 2021، ص 96 .

[2]- محمد عبد الحميد، الأمن المعلوماتي والأمن السيبراني، الطبعة الثانية، دار الجامعة الجديدة، الإسكندرية، مصر، 2020، ص 71 .

[3]- عبد الكريم سلامة، "السياسات الوطنية للأمن السيبراني"، ضمن أعمال الملتقى الدولي حول الأمن الرقمي والتحولات التكنولوجية، جامعة سطيف 2، الجزائر، 2023، ص 41 .

وفي الجزائر، تم إنشاء منظومة وطنية لأمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي رقم 20-05، بهدف تعزيز الأمن الرقمي الوطني وحماية الشبكات المعلوماتية للدولة.[1]

ب-تطوير أنظمة الحماية والمراقبة الرقمية

تستخدم الدول أنظمة متطورة لمراقبة الشبكات واكتشاف الاختراقات الإلكترونية، مثل أنظمة التشفير، والجدران النارية، وبرامج الكشف عن الهجمات السيبرانية. كما يتم الاعتماد على تقنيات الذكاء الاصطناعي لتحليل التهديدات الرقمية والتنبؤ بالهجمات المحتملة.

وتساعد هذه الأنظمة في حماية البيانات الوطنية وضمان استمرارية الخدمات الإلكترونية، خاصة في القطاعات الحساسة كالدفاع والطاقة والاتصالات والبنوك.

ج-تكوين الموارد البشرية المتخصصة

يُعتبر العنصر البشري من أهم مكونات الأمن السيبراني، لذلك تعمل الدول على تكوين خبراء ومختصين في مجال الحماية الرقمية والأمن المعلوماتي. كما يتم تنظيم دورات تدريبية وبرامج توعوية تهدف إلى رفع مستوى الوعي بالمخاطر الإلكترونية داخل المؤسسات الحكومية والخاصة.[2]

د-إعداد استراتيجيات وطنية للأمن السيبراني

تقوم الحكومات بوضع استراتيجيات وطنية تهدف إلى تحديد المخاطر السيبرانية ووضع خطط لمواجهتها، إضافة إلى تعزيز التنسيق بين مختلف المؤسسات الأمنية والتقنية.

[1]- المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، المتعلق بإنشاء منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 04، الصادرة بتاريخ 22 جانفي 2020 .

[2]- عبد القادر بوزيان، الأمن الرقمي والسياسات الحكومية الحديثة، الطبعة الأولى، دار هومة، الجزائر، 2022، ص 131 .

وتساعد هذه الاستراتيجيات على ضمان الجاهزية الرقمية للدولة وتحسين قدرتها على التعامل مع الأزمات السيبرانية.[1]

2- مراقبة الهجمات الرقمية

أصبحت مراقبة الهجمات الإلكترونية من أهم الأدوات التي تعتمد عليها الدول لحماية فضائها الرقمي، وذلك من خلال تتبع الأنشطة المشبوهة وتحليل مصادر التهديدات السيبرانية. وتعتمد الحكومات في ذلك على أنظمة رقمية متطورة قادرة على رصد محاولات الاختراق والكشف المبكر عن الهجمات الإلكترونية.

كما تقوم أجهزة الأمن السيبراني بجمع وتحليل المعلومات المتعلقة بالهجمات الرقمية، بهدف تحديد الجهات المسؤولة عنها واتخاذ الإجراءات اللازمة لمنع تكرارها. وقد ساهمت تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة في تطوير قدرات الدول على مراقبة الفضاء الإلكتروني بشكل أكثر فعالية.[2]

ثانيا: التعاون بين الأجهزة الحكومية والخاصة لضمان أمن الدولة

لا يمكن تحقيق الأمن السيبراني بشكل فعال دون وجود تعاون وتنسيق بين مختلف الفاعلين داخل الدولة، خاصة في ظل الترابط الكبير بين المؤسسات الحكومية والقطاع الخاص في إدارة البنية التحتية الرقمية. فالكثير من الشبكات والخدمات الرقمية الحيوية أصبحت تُدار من طرف شركات خاصة، الأمر الذي يجعل حماية الأمن الرقمي مسؤولية مشتركة بين الدولة والمؤسسات الاقتصادية والتكنولوجية.[3]

---

[1]- فاطمة الزهراء بوعلام، السيادة الرقمية في ظل التحولات التكنولوجية الحديثة، أطروحة دكتوراه لنيل شهادة الدكتوراه في العلوم السياسية والعلاقات الدولية، تخصص تنظيمات سياسية وإدارية، كلية الحقوق والعلوم السياسية، جامعة وهران 2 محمد بن أحمد، الجزائر، السنة الجامعية 2021-2022، ص 117،

[2]- فاطمة الزهراء بوعلام ، المرجع السابق ، ص118

[3]- نور الدين بوطبة، الأمن السيبراني في التشريع الجزائري، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة الجزائر 1 يوسف بن خدة، الجزائر، السنة الجامعية 2018-2019، ص 52، 66.

كما أن الطابع العابر للحدود للتهديدات السيبرانية يفرض ضرورة تعزيز التعاون الداخلي والخارجي من أجل مواجهة المخاطر الرقمية وضمان استقرار الفضاء الإلكتروني الوطني.

1- أهمية التعاون بين القطاعين العام والخاص

يُساهم التعاون بين الأجهزة الحكومية والقطاع الخاص في تعزيز فعالية أنظمة الأمن السيبراني، من خلال تبادل المعلومات والخبرات المتعلقة بالتهديدات الإلكترونية. كما يسمح هذا التعاون بتنسيق الجهود لحماية البنية التحتية الحيوية، مثل شبكات الاتصالات والطاقة والنظام المصرفي.

وتعتمد العديد من الدول على شركات التكنولوجيا الخاصة في تطوير الحلول الرقمية وأنظمة الحماية الإلكترونية، وهو ما يجعل القطاع الخاص شريكًا أساسيًا في حماية الأمن الرقمي الوطني.

2- مجالات التعاون في الأمن السيبراني

تشمل مجالات التعاون بين الأجهزة الحكومية والخاصة عدة جوانب، أهمها[1]:

أ-تبادل المعلومات المتعلقة بالتهديدات السيبرانية

تقوم المؤسسات الحكومية والشركات الخاصة بتبادل البيانات المتعلقة بالهجمات الإلكترونية وأساليب الاختراق الحديثة، بما يساعد على تعزيز سرعة الاستجابة للتهديدات الرقمية.

ب-تطوير أنظمة الحماية الإلكترونية

يساهم القطاع الخاص في تطوير البرمجيات وأنظمة الحماية الرقمية التي تستخدمها المؤسسات الحكومية لحماية بياناتها وشبكاتها.[1]

[1]- محمد شتاتحة، "الأمن السيبراني وأثره على الأمن القومي للدول"، مجلة العلوم القانونية والسياسية، المجلد 11، العدد 02، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، الجزائر، 2020، ص 143 .

ج-التدريب والتكوين

يتم تنظيم برامج تدريبية مشتركة تهدف إلى تكوين مختصين في مجال الأمن السيبراني ورفع مستوى الوعي الرقمي داخل المؤسسات.

د-إدارة الأزمات السيبرانية

تعمل مختلف الأجهزة الحكومية والخاصة على التنسيق أثناء وقوع الهجمات الإلكترونية من أجل الحد من آثارها وضمان استمرارية الخدمات الحيوية.

2- التحديات التي تواجه التعاون السيبراني

رغم أهمية التعاون بين القطاعين العام والخاص، إلا أنه يواجه عدة صعوبات، من أبرزها:

- ✓ نقص الكفاءات المتخصصة في مجال الأمن السيبراني[2] .
- ✓ صعوبة تبادل المعلومات الحساسة بين المؤسسات .
- ✓ ارتفاع تكاليف أنظمة الحماية الرقمية .
- ✓ التطور المستمر لأساليب الهجمات الإلكترونية.

[1]- فوزية لعور، "الشراكة بين القطاعين العام والخاص في مجال الأمن السيبراني"، مجلة الدراسات الأمنية والاستراتيجية، العدد 06، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، الجزائر، 2022، ص 77 .

[2]- فوزية لعور، المرجع السابق ، ص77

الفرع الثاني: الاقتصاد الرقمي والسيادة

فرضت التحولات التكنولوجية الحديثة واقعًا اقتصاديًا جديدًا أصبحت فيه الرقمنة عنصرًا أساسيًا في مختلف الأنشطة الاقتصادية والتجارية. فمع التطور الكبير في تكنولوجيا المعلومات والاتصال، برز الاقتصاد الرقمي كأحد أهم الدعائم التي تعتمد عليها الدول لتحقيق التنمية وتعزيز قدرتها التنافسية في النظام الدولي المعاصر.[1]

وفي ظل هذا التحول، لم تعد السيادة الوطنية مرتبطة فقط بالسيطرة على الموارد التقليدية، بل امتدت لتشمل التحكم في البيانات الاقتصادية والتجارية وحماية المصالح الرقمية للدولة. كما أصبحت القدرة على تطوير التكنولوجيا الوطنية وتقليل التبعية للخارج من أهم المؤشرات التي تعكس قوة الدولة واستقلالها الاقتصادي.[2]

وانطلاقًا من ذلك، سيتم التطرق في هذا المطلب إلى أهمية التحكم في البيانات الاقتصادية والتجارية الوطنية، ثم دراسة دور الصناعات الرقمية الوطنية في دعم السيادة الرقمية وتقليل الاعتماد على التكنولوجيا الأجنبية.

أولا: التحكم في البيانات الاقتصادية والتجارية الوطنية

يشهد العالم اليوم تزايدًا كبيرًا في الاعتماد على البيانات الرقمية في إدارة الأنشطة الاقتصادية والتجارية، حيث أصبحت المعلومات تمثل موردًا استراتيجيًا تعتمد عليه الدول والمؤسسات في اتخاذ القرارات وتوجيه السياسات الاقتصادية. ولهذا اتجهت الحكومات إلى تعزيز الرقابة على البيانات الاقتصادية بهدف حماية الأمن الاقتصادي وضمان السيادة الوطنية في الفضاء الرقمي.[3]

[1]– مصطفى يوسف كافي، الاقتصاد الرقمي والتجارة الإلكترونية، الطبعة الأولى، دار رسلان للطباعة والنشر والتوزيع، دمشق، سوريا، 2017، ص 33 .

[2]– عبد المجيد قدي، "السيادة الرقمية والرهانات الاقتصادية المعاصرة"، مجلة الاقتصاد والتنمية، المجلد 09، العدد 01، جامعة حسيبة بن بوعلي الشلف، الجزائر، 2021، ص 144 .

[3]– ليلى بن سالم، الاقتصاد الرقمي وأثره على سيادة الدولة، أطروحة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجزائر 3 إبراهيم سلطان شيبوط، الجزائر، 2022، ص 97.

1- أهمية البيانات الاقتصادية في الاقتصاد الرقمي

تُعتبر البيانات الاقتصادية من أبرز مقومات الاقتصاد الرقمي، لأنها توفر المعلومات المتعلقة بالأسواق والاستثمارات والمعاملات المالية والتجارية. كما تساعد المؤسسات والدول على تحليل المؤشرات الاقتصادية وتوقع التغيرات التي قد تؤثر على النشاط الاقتصادي.[1]

ومن جهة أخرى، أصبحت البيانات تُشكل مصدرًا للقوة الاقتصادية، خاصة في ظل التوسع الكبير لاستخدام المنصات الرقمية والتجارة الإلكترونية. ولهذا تسعى الدول إلى حماية معلوماتها الاقتصادية من التسريب أو الاستغلال الخارجي، نظرًا لما قد يترتب عن ذلك من تهديد للمصالح الوطنية.

2- آليات التحكم في البيانات الاقتصادية

عملت العديد من الدول على تبني سياسات تهدف إلى التحكم في البيانات الاقتصادية والتجارية، وذلك من خلال إنشاء مراكز وطنية لحفظ البيانات، وفرض قوانين تنظم استخدام المعلومات الرقمية داخل المؤسسات الاقتصادية. كما تلجأ الحكومات إلى استخدام أنظمة حماية إلكترونية متطورة لمواجهة الهجمات السيبرانية التي تستهدف البنوك والشركات والأسواق المالية.[2]

وفي السياق نفسه، ساهمت التشريعات المتعلقة بالتجارة الإلكترونية والمعاملات الرقمية في تنظيم البيئة الاقتصادية الرقمية وضمان حماية المتعاملين داخل الفضاء الإلكتروني. ويُعد القانون الجزائري رقم 18-05 المتعلق بالتجارة الإلكترونية من بين النصوص القانونية التي هدفت إلى تنظيم النشاط التجاري الرقمي داخل الجزائر.[3]

---

[1]- ليلى بن سالم، المرجع السابق ، ص98

[2]- شيماء بوحفص، "البيانات الضخمة والسيادة الاقتصادية للدول"، مجلة العلوم السياسية والقانون، العدد 12، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، الجزائر، 2022، ص 117 .

[3]- القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق لـ 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 28، الصادرة بتاريخ 16 ماي 2018 .

3- تحديات حماية البيانات الاقتصادية

رغم الجهود المبذولة لحماية البيانات الاقتصادية، إلا أن الدول لا تزال تواجه عدة تحديات مرتبطة بالتحول الرقمي، من أبرزها تزايد الهجمات الإلكترونية، وهيمنة الشركات التكنولوجية العالمية على الأسواق الرقمية، إضافة إلى صعوبة التحكم في تدفق البيانات عبر الحدود.[1]

كما أن الاعتماد المتزايد على المنصات الأجنبية والخدمات السحابية العالمية قد يؤدي إلى تسرب البيانات الاقتصادية الحساسة، وهو ما يشكل تهديدًا مباشرًا للسيادة الاقتصادية للدول، خاصة النامية منها.

ثانيا: دعم الصناعات الرقمية الوطنية وتقليل الاعتماد على الخارج

الصناعات الرقمية في الوقت الراهن هي من أهم القطاعات التي تسعى الدول إلى تطويرها من أجل تعزيز استقلالها التكنولوجي وتحقيق التنمية الاقتصادية. فالتقدم في مجالات البرمجيات والاتصالات والذكاء الاصطناعي لم يعد مجرد وسيلة للتطور التقني، بل تحول إلى عامل أساسي في تعزيز النفوذ الاقتصادي والسياسي للدول.[2]

ولهذا تعمل الحكومات على دعم الصناعات الرقمية المحلية وتشجيع الابتكار التكنولوجي، بهدف بناء اقتصاد رقمي وطني قادر على المنافسة وتقليل التبعية للخارج.

---

[1]- كمال رزيق، "التحول الرقمي وتحديات الأمن الاقتصادي"، مجلة الدراسات الاقتصادية المعاصرة، العدد 08، كلية العلوم الاقتصادية، جامعة محمد بوضياف بالمسيلة، الجزائر، 2020، ص 88 .

[2] - Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think, First Edition, Houghton Mifflin Harcourt Publishing, New York, United States, 2013, p.73.

1- أهمية الصناعات الرقمية الوطنية

تساهم الصناعات الرقمية في تطوير الاقتصاد الوطني من خلال توفير التكنولوجيا والخدمات الإلكترونية التي تحتاجها المؤسسات والإدارات المختلفة. كما تساعد على خلق فرص العمل وتشجيع الاستثمار والابتكار في مجالات التكنولوجيا الحديثة.[1]

إضافة إلى ذلك، فإن امتلاك صناعات رقمية وطنية يسمح للدولة بالتحكم في وسائلها التكنولوجية وتقليل مخاطر الاعتماد على الشركات الأجنبية، خاصة في المجالات الحساسة المرتبطة بالأمن السيبراني والاتصالات.

2- وسائل دعم الصناعات الرقمية

حرصت الدول على تبني عدة آليات لدعم الصناعات الرقمية الوطنية، من بينها تشجيع الاستثمار في قطاع التكنولوجيا، وتمويل المؤسسات الناشئة، وتطوير برامج التكوين والبحث العلمي في المجالات الرقمية. كما تعمل الحكومات على دعم استخدام البرمجيات الوطنية داخل الإدارات والمؤسسات العمومية بهدف تعزيز الاستقلال الرقمي.

ومن ناحية أخرى، تلعب الجامعات ومراكز البحث دورًا مهمًا في تطوير الابتكار التكنولوجي وإعداد الكفاءات المتخصصة التي تحتاجها الصناعات الرقمية الحديثة.[2]

3- معوقات تحقيق الاستقلال الرقمي

على الرغم من أهمية الصناعات الرقمية، إلا أن العديد من الدول تواجه صعوبات في تحقيق استقلالها التكنولوجي، بسبب نقص التمويل وضعف البنية التحتية الرقمية وهيمنة

---

[1]- محمد بن عيسى، الصناعات الرقمية ودورها في التنمية الاقتصادية، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2020، ص 101 .

[2]- جميلة قرفي، "الاقتصاد الرقمي كآلية لتعزيز السيادة الوطنية"، ضمن أعمال الملتقى الوطني حول التحول الرقمي والسيادة الإلكترونية، كلية العلوم السياسية والعلاقات الدولية، جامعة قسنطينة 3 صالح بوبنيدر، الجزائر، 15 مارس 2023، ص 74 .

الشركات العالمية الكبرى على الأسواق التكنولوجية. كما تعاني بعض الدول من هجرة الكفاءات الرقمية نحو الخارج، وهو ما يحد من قدرتها على تطوير صناعات وطنية قوية.[1]

وفي ظل هذه التحديات، أصبح من الضروري اعتماد استراتيجيات طويلة المدى تهدف إلى تعزيز الاقتصاد الرقمي الوطني وتشجيع البحث العلمي والابتكار، بما يسمح بتحقيق السيادة الرقمية وتقوية القدرة التنافسية للدولة في الاقتصاد العالمي.

المبحث الثاني: السيادة الرقمية في العلاقات الدولية.

ساهمت الثورة الرقمية في إحداث تغيرات جذرية في طبيعة العلاقات الدولية، حيث أصبح الفضاء الإلكتروني مجالًا استراتيجيًا تتقاطع فيه المصالح السياسية والاقتصادية والأمنية للدول. ولم يعد النفوذ الدولي مرتبطًا فقط بالقوة العسكرية أو الاقتصادية، بل أصبح التحكم في التكنولوجيا والبيانات والمعلومات أحد أهم مصادر القوة في النظام الدولي المعاصر.[2]

وفي ظل هذا الواقع الجديد، برزت السيادة الرقمية كأحد المفاهيم الحديثة التي تعبر عن قدرة الدولة على حماية فضائها الإلكتروني والتحكم في مواردها الرقمية، خاصة مع تصاعد التهديدات السيبرانية وتزايد الاعتماد على الأنظمة الرقمية في مختلف المجالات.[3]

كما أدى الطابع العالمي للفضاء الرقمي إلى تعزيز الحاجة للتعاون بين الدول والمنظمات الدولية من أجل مواجهة التحديات المشتركة المرتبطة بالأمن السيبراني وحماية البيانات وتنظيم استخدام التكنولوجيا الحديثة.[4]

---

[1]– جميلة قرفي، المرجع نفسه ، ص75.

[2]– سليمان أعراج، "السيادة الرقمية والتحديات الجيوسياسية الجديدة"، مداخلة ضمن أعمال الملتقى الدولي حول السيادة الرقمية والأمن السيبراني، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، الجزائر، المنعقد بتاريخ 06 ديسمبر 2022، ص 17.

[3]– فهد بن محمد الحربي، "الأمن السيبراني كمدخل لحماية السيادة الوطنية"، ضمن أعمال الملتقى العربي للأمن الرقمي والتحول التكنولوجي، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2022، ص 52.

[4]– ياسين بن حمادي، التحديات القانونية للسيادة الرقمية في ظل العولمة الرقمية، أطروحة دكتوراه في القانون الدولي العام، كلية الحقوق، جامعة مولود معمري تيزي وزو، الجزائر، السنة الجامعية 2021–2022، ص 76 .

وعليه، سيتم التطرق في هذا المبحث إلى مختلف أبعاد السيادة الرقمية في العلاقات الدولية، سواء من خلال دراسة الصراعات السيبرانية بين الدول، أو إبراز جهود التعاون الدولي، بالإضافة إلى تحليل التحديات المستقبلية التي قد تؤثر على سيادة الدول الرقمية.

المطلب الأول: الصراعات الرقمية بين الدول

شهدت العلاقات الدولية خلال العقود الأخيرة تحولات عميقة نتيجة التطور السريع في مجال التكنولوجيا الرقمية، حيث أصبح الفضاء السيبراني مجالًا جديدًا للتنافس والصراع بين الدول. فلم تعد القوة الدولية ترتبط فقط بالإمكانات العسكرية والاقتصادية التقليدية، بل أضحت القدرة على التحكم في المعلومات والبيانات والأنظمة الرقمية من أبرز عناصر النفوذ في النظام الدولي الحديث.[1]

وفي ظل هذا الواقع، برزت الصراعات الرقمية كأحد أهم التحديات التي تواجه الدول، خاصة مع تزايد الاعتماد على التكنولوجيا في إدارة المؤسسات والقطاعات الحيوية. وقد أدى ذلك إلى ظهور أنماط جديدة من التهديدات، مثل الهجمات السيبرانية والتجسس الرقمي والنزاعات المرتبطة بالتحكم في البيانات والخدمات الرقمية العابرة للحدود.[2]

كما ساهمت الطبيعة المفتوحة للفضاء الرقمي في تعقيد العلاقات الدولية، نظرًا لصعوبة تحديد مصدر الهجمات الإلكترونية أو إخضاع الفضاء السيبراني لقواعد السيادة التقليدية. ولهذا أصبحت الدول تسعى إلى تعزيز قدراتها الرقمية لحماية أمنها القومي ومصالحها الاستراتيجية في مواجهة التحديات السيبرانية المتزايدة.[3]

وانطلاقًا من ذلك، سيتم التطرق في هذا المطلب إلى الهجمات السيبرانية والتجسس الرقمي بين الدول، ثم دراسة النزاعات المرتبطة بالبيانات والخدمات الرقمية العابرة للحدود.

---

[1]– نبيل صقر، الحروب السيبرانية وتحولات الصراع الدولي، الطبعة الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2022، ص 51 .

[2]– عبد الله الأشعل، القانون الدولي والسيادة الرقمية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2021، ص 88 .

[3]– ياسين بن حمادي، التحديات القانونية للسيادة الرقمية في ظل العولمة الرقمية، أطروحة دكتوراه في القانون الدولي العام، كلية الحقوق، جامعة مولود معمري تيزي وزو، الجزائر، السنة الجامعية 2021–2022، ص 76 .

الفرع الأول: الهجمات السيبرانية والتجسس الرقمي بين الدول

الفضاء السيبراني في العصر الحديث هو أحد أهم مجالات الصراع الدولي، بعدما تحولت التكنولوجيا الرقمية إلى وسيلة تستخدمها الدول لتحقيق أهداف سياسية وأمنية واقتصادية. فمع توسع الاعتماد على الأنظمة المعلوماتية، ازدادت مخاطر الاختراقات الإلكترونية والهجمات السيبرانية التي تستهدف المؤسسات الحيوية والبنية التحتية الرقمية للدول.[1]

كما ساهم التطور الكبير في وسائل الاتصال والتكنولوجيا الحديثة في تسهيل عمليات التجسس الرقمي وجمع المعلومات السرية، الأمر الذي جعل الأمن السيبراني جزءًا أساسيًا من استراتيجيات الأمن القومي للدول.

أولًا: الهجمات السيبرانية كوسيلة للصراع الدولي

تُعرف الهجمات السيبرانية بأنها عمليات إلكترونية تستهدف الأنظمة الرقمية والشبكات المعلوماتية بهدف تعطيلها أو اختراقها أو سرقة المعلومات المخزنة داخلها. وتتنوع هذه الهجمات بين اختراق المواقع الحكومية، وتعطيل الأنظمة البنكية، واستهداف شبكات الطاقة والاتصالات، إضافة إلى الهجمات التي تستهدف المؤسسات العسكرية والأمنية.[2]

وقد أصبحت بعض الدول تعتمد على الهجمات الإلكترونية كبديل عن المواجهات العسكرية التقليدية، نظرًا لما توفره من قدرة على إلحاق أضرار كبيرة بالخصم بأقل تكلفة ممكنة. كما تسمح هذه الهجمات بتنفيذ عمليات سرية يصعب أحيانًا تحديد الجهة المسؤولة عنها بشكل دقيق.

---

[1] – Herbert Lin & Amy Zegart, Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, First Edition, Brookings Institution Press, Washington DC, United States, 2018, p.91.

[2] – خولة رحموني، الأمن السيبراني والسيادة الرقمية في العلاقات الدولية المعاصرة، أطروحة دكتوراه في العلوم السياسية والعلاقات الدولية، كلية الحقوق والعلوم السياسية، جامعة الجزائر 3 إبراهيم سلطان شيبوط، الجزائر، السنة الجامعية 2022-2023، ص 104 .

ومن أبرز الأمثلة على ذلك الهجوم الإلكتروني الذي استهدف المنشآت النووية الإيرانية سنة 2010 بواسطة فيروس "ستاكسنت"، والذي يُعد من أخطر الهجمات السيبرانية التي استهدفت البنية التحتية الحيوية لدولة ما.[1]

ثانيًا: التجسس الرقمي بين الدول

إلى جانب الهجمات الإلكترونية، يُعد التجسس الرقمي من أبرز مظاهر الصراعات السيبرانية الحديثة، حيث تستخدم الدول الوسائل التكنولوجية لاختراق الأنظمة المعلوماتية والحصول على بيانات سرية تتعلق بالمجالات السياسية والعسكرية والاقتصادية.

وتعتمد عمليات التجسس الإلكتروني على تقنيات متطورة، مثل مراقبة الاتصالات الرقمية، واختراق الهواتف والأجهزة الإلكترونية، واستخدام البرمجيات الخبيثة لجمع المعلومات الحساسة. وقد أدى التطور في مجال الذكاء الاصطناعي وتحليل البيانات إلى زيادة فعالية هذه العمليات وتعقيدها.

كما أثارت برامج التجسس الحديثة، مثل برنامج "بيغاسوس"، جدلًا واسعًا على المستوى الدولي بسبب استخدامها في مراقبة شخصيات سياسية وصحفيين وناشطين في عدة دول، وهو ما اعتُبر تهديدًا مباشرًا للخصوصية والسيادة الرقمية للدول.[2]

ثالثًا: آثار الصراعات السيبرانية على العلاقات الدولية

ساهمت الصراعات الرقمية في تغيير طبيعة العلاقات الدولية، حيث أصبحت الهجمات الإلكترونية مصدرًا دائمًا للتوتر بين الدول. وقد تؤدي هذه الهجمات إلى خسائر اقتصادية كبيرة وتعطيل المرافق الحيوية، إضافة إلى التأثير على الاستقرار السياسي والأمني للدول المستهدفة.

---

[1]– محمد عبد الواحد، الأمن المعلوماتي والجرائم الإلكترونية، الطبعة الثانية، دار الجامعة الجديدة، الإسكندرية، مصر، 2020، ص 67 .

[2]– أسماء بوقرة، الفضاء السيبراني وتحول مفهوم السيادة الدولية، رسالة ماجستير في العلاقات الدولية، كلية العلوم السياسية، جامعة قسنطينة 3 صالح بوبنيدر، الجزائر، السنة الجامعية 2019–2020، ص 58 .

كما دفعت هذه التهديدات العديد من الدول إلى تطوير قدراتها الدفاعية الرقمية والدخول في سباق تسلح سيبراني، خاصة بين القوى الكبرى التي تسعى إلى تعزيز نفوذها في الفضاء الرقمي.[1]

ومن جهة أخرى، أدى غياب إطار قانوني دولي واضح ينظم استخدام الفضاء السيبراني إلى صعوبة تحديد المسؤولية القانونية عن الهجمات الإلكترونية، وهو ما يزيد من تعقيد إدارة النزاعات الرقمية على المستوى الدولي.

الفرع الثاني: النزاعات حول البيانات والخدمات الرقمية العابرة للحدود

ساهمت هيمنة الشركات التكنولوجية الكبرى على الأسواق الرقمية العالمية في زيادة المخاوف المتعلقة بفقدان الدول لجزء من سيادتها الرقمية، خاصة في ظل تحكم هذه الشركات في تدفق المعلومات والبيانات على المستوى العالمي.[2]

أولًا: النزاعات المرتبطة بالبيانات الرقمية

أصبحت البيانات الرقمية من أهم عناصر القوة الاقتصادية والسياسية، لذلك تسعى الدول إلى فرض سيطرتها على المعلومات المتعلقة بمواطنيها ومؤسساتها الاقتصادية. ولهذا ظهرت خلافات دولية مرتبطة بعمليات نقل البيانات عبر الحدود وطريقة تخزينها واستخدامها.

وفي هذا الإطار، تبنت العديد من الدول سياسات "توطين البيانات"، التي تقوم على إلزام الشركات الرقمية بحفظ البيانات داخل الإقليم الوطني بهدف ضمان خضوعها للقوانين الوطنية وحمايتها من الاستغلال الخارجي.[3]

---

[1]– حسام الدين قاسمي، "الهيمنة الرقمية وأثرها على سيادة الدول"، مجلة السياسة الدولية، العدد 234، مؤسسة الأهرام، القاهرة، مصر، 2023، ص 44–59 .

[2]– عبد الحكيم بوزيدي، الدبلوماسية الرقمية وأثرها على العلاقات الدولية، أطروحة دكتوراه في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة وهران 2 محمد بن أحمد، الجزائر، السنة الجامعية 2020–2021، ص 133 .

[3]– أمينة إيجر، "السيادة الرقمية في العالم المعولم: التحديات والرهانات"، مجلة الدراسات القانونية والسياسية، المجلد 10، العدد 02، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي بالأغواط، الجزائر، 2024، ص 71.

كما أثارت برامج المراقبة الإلكترونية التي تستخدمها بعض الدول جدلًا واسعًا، خاصة بعد الكشف عن عمليات تجسس استهدفت بيانات مستخدمي الإنترنت حول العالم، وهو ما اعتُبر انتهاكًا للخصوصية والسيادة الرقمية للدول.

ثانيًا: الصراع حول الخدمات الرقمية العالمية

تشكل الخدمات الرقمية العالمية، مثل محركات البحث ومنصات التواصل الاجتماعي والحوسبة السحابية، أحد أهم مجالات التنافس بين الدول، نظرًا لما تمتلكه من قدرة على التأثير في الاقتصاد والإعلام والرأي العام.

ولهذا تسعى العديد من الحكومات إلى فرض رقابة قانونية على نشاط الشركات الرقمية الأجنبية، سواء من خلال فرض الضرائب الرقمية أو إلزام هذه الشركات باحترام التشريعات الوطنية المتعلقة بحماية البيانات والمحتوى الإلكتروني.[1]

وفي المقابل، ترى بعض الدول والشركات أن هذه القيود قد تُستخدم لتقييد حرية الإنترنت والتأثير على التجارة الرقمية الدولية، وهو ما أدى إلى تصاعد الخلافات المرتبطة بتنظيم الفضاء الرقمي العالمي.[2]

ثالثًا: الجهود الدولية لمواجهة النزاعات الرقمية

دفعت التحديات المرتبطة بالصراعات الرقمية المجتمع الدولي إلى تعزيز التعاون في مجال الأمن السيبراني وتنظيم استخدام التكنولوجيا الحديثة. ولهذا ظهرت عدة اتفاقيات ومبادرات دولية تهدف إلى مكافحة الجرائم الإلكترونية وحماية البيانات الرقمية.

ومن بين أبرز هذه الجهود اتفاقية بودابست المتعلقة بالجرائم الإلكترونية، التي تُعد أول اتفاقية دولية تهدف إلى تنظيم التعاون بين الدول في مجال مكافحة الجرائم السيبرانية وتبادل المعلومات المتعلقة بالتهديدات الرقمية.

---

[1]– أمينة إيجر، المرجع السابق ، ص72.

[2]– شيماء بوحفص، "البيانات الضخمة والسيادة الاقتصادية للدول"، مجلة العلوم السياسية والقانون، العدد 12، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3 إبراهيم سلطان شيبوط، الجزائر، 2022، ص 117 .

المطلب الثاني: التعاون الدولي والتحديات المستقبلية للسيادة الرقمية

لم تعد السيادة الرقمية مسألة داخلية ترتبط بقدرة الدولة على تنظيم فضائها الرقمي الوطني فحسب، بل أصبحت قضية ذات بعد دولي واضح، نظرًا للطبيعة العابرة للحدود للفضاء الرقمي. فالبيانات تنتقل بين الدول في لحظات، والهجمات السيبرانية قد تنطلق من إقليم دولة وتستهدف مؤسسات دولة أخرى، كما أن الخدمات والمنصات الرقمية الكبرى تعمل في أكثر من نظام قانوني في الوقت نفسه. وهذا الواقع جعل التعاون الدولي ضرورة أساسية لتنظيم الفضاء الرقمي ومواجهة التهديدات المشتركة.[1]

ويبرز دور المنظمات الدولية والاتفاقيات الثنائية والإقليمية في وضع قواعد مشتركة تساعد الدول على مكافحة الجرائم الإلكترونية، وحماية البيانات، وتعزيز الأمن السيبراني، وتنظيم استخدام التكنولوجيا الحديثة. ومن أهم هذه الأطر الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، واتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لسنة 2014، إضافة إلى اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية التي اعتمدتها الجمعية العامة للأمم المتحدة سنة 2024.[2]

غير أن هذا التعاون يظل مرتبطًا بتحديات عديدة، خاصة اختلاف مصالح الدول، وتباين مستويات التطور الرقمي بينها، وصعوبة التوفيق بين حماية السيادة الوطنية وضمان حرية الإنترنت وتدفق المعلومات. كما أن مستقبل السيادة الرقمية يطرح إشكالات جديدة بفعل تطور الذكاء الاصطناعي، والحوسبة السحابية، والبيانات الضخمة، وإنترنت الأشياء، وهي تقنيات قد تزيد من اعتماد الدول على فاعلين خارجيين أو شركات تكنولوجية كبرى.[3]

---

[1]–محمد حسن قاسم، **الإنترنت والقانون الدولي**، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009، ص 66

[2]– الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة، 21 ديسمبر 2010، المادة 1؛ وقد صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14–252 المؤرخ في 8 سبتمبر 2014، **الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية**، العدد 57، 28 سبتمبر 2014 .

[3]– اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، مالابو، 27 جوان 2014، الديباجة والمواد المتعلقة بالأمن السيبراني وحماية البيانات الشخصية. وتشير صفحة الاتحاد الإفريقي الرسمية إلى اعتماد الاتفاقية بتاريخ 27 جوان 2014 .

الفرع الأول :دور المنظمات الدولية والاتفقيات التنائية والاقليمية في تنظيم الفضاء الرقمي

فرضت الطبيعة العالمية للفضاء الرقمي على الدول ضرورة تعزيز التعاون الدولي لمواجهة التحديات المرتبطة بالأمن السيبراني وحماية البيانات وتنظيم استخدام التكنولوجيا الحديثة. فمع تزايد الاعتماد على الأنظمة الرقمية في مختلف المجالات، أصبحت التهديدات الإلكترونية تتجاوز الحدود الجغرافية للدول، الأمر الذي جعل مواجهتها تتطلب تنسيقًا دوليًا وتعاونًا مستمرًا بين الحكومات والمنظمات الدولية والمؤسسات التقنية.[1]

كما أدى التطور السريع للتكنولوجيا إلى بروز العديد من الإشكالات القانونية والسياسية المتعلقة بحماية السيادة الرقمية، خاصة في ظل غياب قواعد دولية موحدة تنظم استخدام الفضاء السيبراني. ولهذا اتجهت الدول إلى إنشاء آليات تعاون دولي تهدف إلى مكافحة الجرائم الإلكترونية وتعزيز أمن المعلومات وضمان الاستخدام الآمن للتكنولوجيا الرقمية.[2]

أولا: المنظمات الدولية ودورها في تنظيم السيادة الرقمية

تؤدي المنظمات الدولية دورًا متزايد الأهمية في تنظيم الفضاء الرقمي العالمي، خاصة مع تزايد المخاطر المرتبطة بالهجمات الإلكترونية والجرائم السيبرانية. فالتطور المستمر للتكنولوجيا فرض الحاجة إلى وجود أطر دولية تُسهم في وضع قواعد مشتركة تنظم استخدام الفضاء السيبراني وتحمي الأمن الرقمي للدول.

كما تسعى هذه المنظمات إلى تعزيز التعاون بين الدول في مجالات الأمن السيبراني وحماية البيانات والاتصالات الرقمية، بما يساهم في تحقيق التوازن بين حرية استخدام التكنولوجيا ومتطلبات حماية السيادة الوطنية.

---

[1]– عبد الرزاق السنهوري، الأمن السيبراني والتعاون الدولي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2022، ص 63 .

[2]– سعيد بوشعير، القانون الدولي والتحولات الرقمية الحديثة، الطبعة الأولى، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2021، ص 118 .

1- دور الاتحاد الدولي للاتصالات في تنظيم الفضاء الرقمي

يُعد الاتحاد الدولي للاتصالات (ITU) من أبرز المنظمات الدولية المتخصصة في مجال تكنولوجيا المعلومات والاتصال، حيث يعمل على تطوير التعاون الدولي في قطاع الاتصالات ووضع المعايير التقنية المتعلقة بالبنية التحتية الرقمية.[1]

كما يساهم الاتحاد في دعم الدول من خلال إعداد تقارير ومؤشرات خاصة بالأمن السيبراني، من بينها "المؤشر العالمي للأمن السيبراني"، الذي يُستخدم لتقييم جاهزية الدول في مواجهة التهديدات الرقمية.[2]

إضافة إلى ذلك، يعمل الاتحاد على تشجيع تبادل الخبرات التقنية وتعزيز قدرات الدول النامية في مجال التحول الرقمي وحماية البنية التحتية المعلوماتية.[3]

2- دور الأمم المتحدة في الأمن السيبراني

اهتمت منظمة الأمم المتحدة بقضايا الأمن الرقمي والسيادة السيبرانية، نظرًا لما تمثله الهجمات الإلكترونية من تهديد للسلم والأمن الدوليين. ولهذا أنشأت الأمم المتحدة عدة فرق عمل ومجموعات خبراء لدراسة التحديات المرتبطة باستخدام الفضاء السيبراني ووضع مبادئ تنظم سلوك الدول في هذا المجال.

كما تدعو الأمم المتحدة إلى تعزيز التعاون الدولي في مكافحة الجرائم الإلكترونية وحماية حقوق الإنسان الرقمية، مع التأكيد على احترام سيادة الدول وعدم استخدام التكنولوجيا للإضرار بأمنها واستقرارها.

---

[1]- أحمد مومن، "التعاون الدولي في مجال الأمن السيبراني"، مجلة الحقوق والعلوم السياسية، المجلد 08، العدد 01، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، 2023، ص 144 .

[2]- نوال زروقي، السيادة الرقمية في ظل العولمة التكنولوجية، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 1 يوسف بن خدة، الجزائر، السنة الجامعية 2022-2023، ص 96 .

[3]- نوال زروقي، المرجع السابق ، ص97

3- دور المنظمات الإقليمية في تعزيز الأمن الرقمي

إلى جانب المنظمات الدولية، تساهم العديد من المنظمات الإقليمية في تطوير التعاون السيبراني بين الدول الأعضاء، مثل الاتحاد الأوروبي والاتحاد الإفريقي وجامعة الدول العربية.

فالاتحاد الأوروبي يُعتبر من أبرز الفاعلين في مجال حماية البيانات الرقمية، خاصة بعد إصدار اللائحة العامة لحماية البيانات(GDPR) ، التي فرضت معايير صارمة لحماية الخصوصية الرقمية.[1]

كما يعمل الاتحاد الإفريقي على تعزيز التعاون بين الدول الإفريقية في مجالات الأمن السيبراني وحماية البنية التحتية الرقمية، من خلال الاتفاقيات والمبادرات المتعلقة بالأمن الرقمي.[2]

ثانيا: الاتفاقيات الثنائية والإقليمية لتعزيز الأمن الرقمي

أدى تصاعد التهديدات السيبرانية إلى دفع الدول نحو إبرام اتفاقيات ثنائية وإقليمية تهدف إلى تعزيز التعاون في مجال الأمن الرقمي ومواجهة الجرائم الإلكترونية. وقد أصبحت هذه الاتفاقيات أداة مهمة لتبادل المعلومات والخبرات التقنية وتنسيق الجهود المتعلقة بحماية الفضاء السيبراني.[13]

كما تعكس هذه الاتفاقيات إدراك الدول للطابع العابر للحدود للتهديدات الرقمية، الأمر الذي يجعل مواجهتها تتطلب تعاونًا دوليًا يتجاوز الحدود الوطنية التقليدية.

---

[1] – International Telecommunication Union (ITU), Understanding Cybersecurity, First Edition, International Telecommunication Union Publishing, Geneva, Switzerland, 2021, p.22.

[2] – مصطفى بوعزيز، "دور المنظمات الدولية في تنظيم الفضاء السيبراني"، مجلة الدراسات القانونية المقارنة، العدد 11، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، 2022، ص 77 .

1- الاتفاقيات الدولية المتعلقة بالأمن السيبراني

تُعتبر اتفاقية بودابست حول الجرائم الإلكترونية من أهم الاتفاقيات الدولية في مجال مكافحة الجرائم السيبرانية، حيث تهدف إلى تعزيز التعاون بين الدول وتوحيد الإجراءات القانونية المتعلقة بمواجهة الجرائم الرقمية.[1]

كما تتضمن الاتفاقية أحكامًا تتعلق بتبادل المعلومات بين الدول وتسهيل عمليات التحقيق في الجرائم الإلكترونية العابرة للحدود، إضافة إلى تطوير آليات التعاون القضائي والتقني في المجال السيبراني.

2- الاتفاقيات الثنائية في مجال الأمن الرقمي

تلجأ العديد من الدول إلى إبرام اتفاقيات ثنائية للتعاون في مجالات الأمن السيبراني وحماية البيانات، خاصة في ظل تزايد المخاطر المرتبطة بالاختراقات الإلكترونية والهجمات الرقمية.[2]

وتشمل هذه الاتفاقيات تبادل المعلومات المتعلقة بالتهديدات السيبرانية، وتنظيم التدريبات المشتركة، وتطوير أنظمة الحماية الإلكترونية، إضافة إلى التعاون في مجال مكافحة الجرائم الرقمية والإرهاب الإلكتروني.

3- التعاون الإقليمي في حماية الفضاء الرقمي

برزت خلال السنوات الأخيرة عدة مبادرات إقليمية تهدف إلى تعزيز الأمن الرقمي بين الدول المتجاورة، خاصة في ظل تشابه التحديات المرتبطة بالبنية التحتية الرقمية والجرائم السيبرانية.

---

[1]- عبد القادر عابد، "الأمم المتحدة وقضايا الأمن السيبراني"، مجلة العلوم السياسية والعلاقات الدولية، العدد 17، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3 إبراهيم سلطان شيبوط، الجزائر، 2021، ص 59 .

[2]- سمير لعريبي، "الاتفاقيات الدولية ودورها في مكافحة الجرائم الإلكترونية"، مجلة الفكر القانوني والسياسي، المجلد 06، العدد 02، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، الجزائر، 2022، ص 201 .

وفي هذا الإطار، تعمل الدول العربية والإفريقية على تطوير استراتيجيات مشتركة للأمن السيبراني وتبادل الخبرات التقنية، بما يساعد على تعزيز حماية الفضاء الرقمي الإقليمي ومواجهة التهديدات الإلكترونية المتزايدة.[1]

الفرع الثاني: التحديات المستقبلية للسيادة الرقمية

يشهد العالم اليوم تطورًا متسارعًا في مجالات التكنولوجيا الرقمية، خاصة مع بروز تقنيات حديثة كالذكاء الاصطناعي والحوسبة السحابية وإنترنت الأشياء والبيانات الضخمة، الأمر الذي أدى إلى ظهور تحديات جديدة تمس سيادة الدول وأمنها الرقمي. فهذه التقنيات، رغم ما توفره من فرص للتطور الاقتصادي والعلمي، قد تُشكل في الوقت نفسه مصدرًا لتهديد الاستقلال الرقمي للدول إذا لم تتمكن من التحكم في استخدامها وتأمين بنيتها التحتية الرقمية.[2]

كما أن التحول نحو الاقتصاد الرقمي العالمي زاد من حدة المنافسة الدولية في مجال التكنولوجيا، حيث أصبحت الدول الكبرى والشركات الرقمية العملاقة تتحكم في جزء كبير من البيانات والخدمات الإلكترونية، وهو ما يثير مخاوف متزايدة حول مستقبل السيادة الرقمية للدول، خاصة النامية منها.[3]

وفي هذا الإطار، تسعى الدول إلى تطوير استراتيجيات جديدة تهدف إلى مواكبة التطور التكنولوجي وحماية فضائها الرقمي من مختلف المخاطر المستقبلية، وذلك عبر تعزيز الأمن السيبراني، ودعم الصناعات الرقمية الوطنية، وتطوير التشريعات المتعلقة بحماية البيانات والذكاء الاصطناعي.

[1]– سمير لعريبي، المرجع السابق ، ص204

[2]– عبد الحميد زيد، الذكاء الاصطناعي والسيادة الرقمية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2023، ص 49 .

[3]– كريمة بن داود، الأمن الرقمي والتحديات المستقبلية للدولة الحديثة، أطروحة دكتوراه في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة الجزائر 3 إبراهيم سلطان شيبوط، الجزائر، السنة الجامعية 2022–2023، ص 118 .

أولا : تأثير الذكاء الاصطناعي والتقنيات الناشئة على السيادة الرقمية

ساهمت الثورة التكنولوجية الحديثة في بروز تقنيات رقمية متطورة غيرت طبيعة العلاقات الدولية وأساليب إدارة الدول لمؤسساتها ومواردها. ويُعد الذكاء الاصطناعي من أبرز هذه التقنيات، بالنظر إلى قدرته على تحليل البيانات والتحكم في الأنظمة الرقمية واتخاذ القرارات بشكل سريع ودقيق.[1]

غير أن الاعتماد المتزايد على هذه التكنولوجيا يثير العديد من الإشكالات المتعلقة بالأمن الرقمي والسيادة الوطنية، خاصة في ظل احتكار بعض الدول والشركات العالمية للتكنولوجيا الحديثة والبنية التحتية الرقمية.[2]

1- الذكاء الاصطناعي وتغير مفهوم القوة الرقمية

أصبح الذكاء الاصطناعي يمثل أحد أهم مظاهر القوة في العصر الرقمي، بعدما دخل في مجالات متعددة تشمل الأمن والدفاع والاقتصاد والإدارة الإلكترونية. كما سمح هذا التطور للدول بتحسين قدراتها في تحليل البيانات وإدارة الأنظمة الرقمية وتطوير أدوات المراقبة والحماية السيبرانية[3].

وفي المقابل، أدى السباق الدولي نحو امتلاك تقنيات الذكاء الاصطناعي إلى ظهور نوع جديد من التنافس بين الدول، خاصة بين القوى الكبرى التي تسعى إلى فرض هيمنتها التكنولوجية على المستوى العالمي. ولهذا أصبحت التكنولوجيا الحديثة عنصرًا مؤثرًا في ميزان القوى والعلاقات الدولية.

[1]- سمير قسوم، "التحولات الرقمية وأزمة السيادة الوطنية"، مجلة الدراسات السياسية المعاصرة، العدد 12، جامعة وهران 2 محمد بن أحمد، الجزائر، 2023، ص 91 .

[2]- نسرين بوقرة، التحول الرقمي وإشكالية التبعية التكنولوجية، أطروحة دكتوراه في العلاقات الدولية، كلية العلوم السياسية، جامعة قسنطينة 3 صالح بوبنيدر، الجزائر، السنة الجامعية 2021-2022، ص 105 .

[3]- نسرين بوقرة،المرجع السابق ، ص107

2- التحديات التي تفرضها التقنيات الناشئة

تواجه الدول اليوم مجموعة من التحديات الناتجة عن التطور السريع للتكنولوجيا الرقمية، من أبرزها تزايد مخاطر الاختراقات الإلكترونية والهجمات السيبرانية التي تستهدف المؤسسات الحيوية وقواعد البيانات الوطنية. كما أن الاعتماد على الخدمات السحابية والمنصات الأجنبية قد يؤدي إلى فقدان جزء من السيطرة على البيانات والمعلومات الوطنية.[1]

ومن جهة أخرى، ساهمت البيانات الضخمة في تعقيد مسألة حماية الخصوصية والسيادة الرقمية، خاصة بعدما أصبحت الشركات العالمية قادرة على جمع وتحليل كميات هائلة من المعلومات المتعلقة بالمستخدمين والدول.

كما يُعتبر الاعتماد المتزايد على البرمجيات والتطبيقات الأجنبية من أبرز التحديات التي تواجه الدول النامية، لأن ذلك قد يجعلها أكثر عرضة للتبعية التكنولوجية والضغوط السياسية والاقتصادية الخارجية.

3- انعكاسات التطور الرقمي على العلاقات الدولية

أدى التقدم في مجالات الذكاء الاصطناعي والتكنولوجيا الحديثة إلى بروز أشكال جديدة من الصراع الدولي، ترتبط بالتحكم في البيانات والتكنولوجيا والبنية التحتية الرقمية. ولهذا ظهر ما يُعرف بالحرب التكنولوجية، التي تسعى من خلالها الدول الكبرى إلى تعزيز نفوذها الرقمي والاقتصادي.

كما ساهم هذا الواقع في تصاعد المنافسة الدولية حول شبكات الاتصالات والأنظمة الذكية وأشباه الموصلات، باعتبارها من أهم العناصر التي تتحكم في مستقبل الاقتصاد الرقمي العالمي.

[1]- عبد العزيز لعمامرة، "الحرب التكنولوجية وأثرها على العلاقات الدولية"، ضمن أعمال الملتقى الدولي حول التكنولوجيا والتحولات الجيوسياسية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، الجزائر، 2023، ص 58 .

ثانيا: الاستراتيجيات المقترحة للدول للحفاظ على سيادتها الرقمية مستقبليًا

أمام التحديات المتزايدة التي يفرضها التطور التكنولوجي، أصبحت الدول مطالبة بوضع استراتيجيات فعالة تضمن حماية فضائها الرقمي وتعزيز استقلالها التكنولوجي. ولم يعد الحفاظ على السيادة الرقمية يقتصر على الجانب الأمني فقط، بل أصبح يشمل أيضًا تطوير الاقتصاد الرقمي ودعم البحث العلمي وتحديث التشريعات المرتبطة بالتكنولوجيا الحديثة.[1]

ولهذا تتجه الحكومات نحو تبني سياسات رقمية شاملة تقوم على تعزيز الأمن السيبراني، وتشجيع الابتكار، وتقوية الصناعات الرقمية الوطنية، بما يسمح بمواجهة التحديات المستقبلية المرتبطة بالعولمة الرقمية.[2]

1- تطوير الأمن السيبراني والبنية التحتية الرقمية

تُعتبر حماية البنية التحتية الرقمية من أهم الخطوات التي تساعد الدول على الحفاظ على سيادتها الرقمية، وذلك من خلال تحديث شبكات الاتصالات وتطوير أنظمة الحماية الإلكترونية ومراكز تخزين البيانات الوطنية.

كما أصبح الاستثمار في تقنيات الأمن السيبراني ضرورة أساسية لمواجهة التهديدات الإلكترونية المتزايدة، خاصة مع تطور أساليب الاختراق والهجمات الرقمية التي تستهدف المؤسسات الحكومية والاقتصادية.

[1]- فاطمة بن قانة، الصناعات الرقمية الوطنية ودورها في تحقيق السيادة الرقمية، أطروحة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة سطيف 1 فرحات عباس، الجزائر، السنة الجامعية 2022-2023، ص 134 .

[2]- محمد الصالح بوزيد، استراتيجيات الأمن السيبراني وحماية السيادة الوطنية، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2022، ص 96 .

2- دعم البحث العلمي والصناعات التكنولوجية

تسعى العديد من الدول إلى تقوية استقلالها الرقمي عبر الاستثمار في البحث العلمي وتشجيع الصناعات الرقمية المحلية، خاصة في مجالات الذكاء الاصطناعي والبرمجيات والأمن السيبراني.[1]

كما يُساهم دعم المؤسسات الناشئة ومراكز الابتكار في تطوير القدرات التكنولوجية الوطنية وتقليل الاعتماد على التكنولوجيا الأجنبية، الأمر الذي يعزز السيادة الرقمية للدولة على المدى الطويل.

3- تحديث التشريعات وتعزيز التعاون الدولي

فرضت التحولات الرقمية الحديثة ضرورة مراجعة التشريعات القانونية المتعلقة بحماية البيانات والجرائم الإلكترونية والذكاء الاصطناعي، بهدف مواكبة التطور التكنولوجي وضمان حماية الحقوق الرقمية للأفراد والدول.[2]

وفي السياق نفسه، أصبح التعاون الدولي عنصرًا أساسيًا لمواجهة المخاطر السيبرانية، خاصة من خلال تبادل المعلومات والخبرات وتعزيز التنسيق بين الدول والمنظمات الدولية المختصة بالأمن الرقمي.

4- الاستثمار في العنصر البشري والتكوين الرقمي

يمثل العنصر البشري حجر الأساس في نجاح السياسات الرقمية الحديثة، لذلك تعمل الدول على تطوير برامج التكوين والتعليم الرقمي لإعداد كفاءات قادرة على التعامل مع التحديات المرتبطة بالتكنولوجيا الحديثة.[3]

---

[1]- سعاد قريشي، "التكوين الرقمي كآلية لتعزيز الأمن السيبراني"، مجلة العلوم الاجتماعية والإنسانية، العدد 14، جامعة محمد خيضر بسكرة، الجزائر، 2023، ص 109 .

[2]- القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، الجزائر، الصادرة بتاريخ 10 جوان 2018 .

[3]- محمد الصالح بوزيد، المرجع السابق ، ص97

كما أن نشر الثقافة الرقمية داخل المجتمع يساهم في رفع مستوى الوعي بالمخاطر الإلكترونية وتعزيز الاستخدام الآمن للتكنولوجيا، وهو ما يساعد على حماية الفضاء الرقمي الوطني وضمان استقراره مستقبلاً.

من خلال دراسة تطبيقات السيادة الرقمية في العلاقات الدولية، يتضح أن التحول الرقمي أصبح من أبرز العوامل المؤثرة في قوة الدول ومكانتها الدولية، حيث لم تعد السيادة مرتبطة فقط بالحدود الإقليمية، بل أصبحت تشمل التحكم في الفضاء الرقمي وحماية البيانات الوطنية وتأمين البنية التحتية المعلوماتية. وقد دفعت هذه التحولات الدول إلى تبني استراتيجيات وطنية متنوعة تهدف إلى تعزيز استقلالها الرقمي، من خلال تطوير التشريعات، ودعم الأمن السيبراني، والاستثمار في الاقتصاد الرقمي والتكنولوجيا الحديثة.

كما أظهرت الدراسة أن الفضاء الرقمي أصبح مجالًا جديدًا للصراعات الدولية، خاصة في ظل تزايد الهجمات السيبرانية وعمليات التجسس الرقمي والنزاعات المتعلقة بالبيانات والخدمات العابرة للحدود، الأمر الذي جعل الأمن السيبراني عنصرًا أساسيًا في حماية الأمن القومي للدول. وفي المقابل، برزت أهمية التعاون الدولي من خلال دور المنظمات الدولية والاتفاقيات الثنائية والإقليمية في تنظيم الفضاء الرقمي وتعزيز الأمن الرقمي العالمي.

الخاتمة

في ختام هذه الدراسة، يتضح أن السيادة الرقمية أصبحت من أبرز القضايا التي تشغل الدول في العصر الحديث، نتيجة التطور السريع للتكنولوجيا الرقمية واتساع استخدام الفضاء السيبراني في مختلف المجالات السياسية والاقتصادية والأمنية. فلم يعد مفهوم السيادة يقتصر على الحدود الجغرافية التقليدية، بل امتد ليشمل قدرة الدولة على التحكم في بياناتها الوطنية وحماية بنيتها التحتية الرقمية وضمان أمنها السيبراني.

كما أظهرت الدراسة أن التحولات الرقمية أفرزت تحديات جديدة فرضت على الدول ضرورة تطوير استراتيجيات رقمية متكاملة تقوم على تعزيز الأمن السيبراني، وتحديث التشريعات القانونية، ودعم الصناعات الرقمية الوطنية، إلى جانب تعزيز التعاون الدولي لمواجهة التهديدات الإلكترونية العابرة للحدود.

وقد تبين كذلك أن التطور المتسارع للذكاء الاصطناعي والتقنيات الحديثة يمثل في الوقت نفسه فرصة لتعزيز التنمية والتطور، وتهديدًا محتملًا للسيادة الوطنية إذا لم تتمكن الدول من التحكم في هذه التكنولوجيا وتأمين استخدامها. ولهذا أصبحت السيادة الرقمية أحد المقومات الأساسية لحماية الأمن القومي وضمان الاستقلال السياسي والاقتصادي للدول في المستقبل.

وعليه، فإن الحفاظ على السيادة الرقمية يتطلب رؤية استراتيجية شاملة تجمع بين التطور التكنولوجي، والحماية القانونية، والتعاون الدولي، والاستثمار في العنصر البشري، بما يسمح للدول بمواجهة التحديات الرقمية المتزايدة وتعزيز مكانتها في النظام الدولي المعاصر.

-النتائج

- ✓ أصبحت السيادة الرقمية امتدادًا لمفهوم السيادة التقليدية في ظل التحولات التكنولوجية الحديثة .
- ✓ يشكل الأمن السيبراني أحد أهم الركائز الأساسية لحماية سيادة الدول في الفضاء الرقمي .
- ✓ أدت الهجمات السيبرانية والتجسس الرقمي إلى ظهور أنماط جديدة من الصراعات الدولية .
- ✓ تساهم البيانات الرقمية في تعزيز القوة الاقتصادية والسياسية للدول، مما جعل التحكم فيها مسألة سيادية .
- ✓ فرض التطور السريع للذكاء الاصطناعي والتقنيات الحديثة تحديات جديدة تتعلق بحماية الأمن الرقمي والخصوصية .
- ✓ تلعب المنظمات الدولية والاتفاقيات الإقليمية دورًا مهمًا في تعزيز التعاون الدولي لمواجهة التهديدات السيبرانية .
- ✓ لا يمكن تحقيق السيادة الرقمية دون تطوير البنية التحتية الرقمية ودعم الصناعات التكنولوجية الوطنية .

-الاقتراحات

- ✓ ضرورة تطوير استراتيجيات وطنية شاملة للأمن السيبراني لحماية البنية التحتية الرقمية والبيانات الوطنية .
- ✓ تعزيز الاستثمار في البحث العلمي والتكنولوجيا الحديثة، خاصة في مجالات الذكاء الاصطناعي والأمن الرقمي .

- ✓ تحديث التشريعات الوطنية المتعلقة بحماية البيانات والجرائم الإلكترونية بما يواكب التطورات التكنولوجية .
- ✓ دعم الصناعات الرقمية الوطنية وتقليل الاعتماد على البرمجيات والخدمات الأجنبية .
- ✓ تكثيف التعاون الدولي والإقليمي في مجال الأمن السيبراني وتبادل الخبرات والمعلومات المتعلقة بالتهديدات الرقمية .

قائمة المراجع

أولا: المصادر

1- الاتفاقيات الدولية

1. **اتفاقية مجلس أوروبا بشأن الجريمة المعلوماتية**، بودابست، 23 نوفمبر 2001، المواد 2-11 المتعلقة بتجريم الأفعال المعلوماتية، والمواد 23 وما بعدها المتعلقة بالتعاون الدولي .
2. **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**، القاهرة، 21 ديسمبر 2010، المادة 1 المتعلقة بهدف الاتفاقية، والمادة 2 المتعلقة بالمصطلحات، والمواد المتعلقة بالتعاون القضائي .
3. **اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية**، مالابو، 27 جوان 2014، المواد المتعلقة بالأمن السيبراني وحماية البيانات الشخصية والمعاملات الإلكترونية .
4. **اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية**، المعتمدة بموجب قرار الجمعية العامة للأمم المتحدة رقم 243/79، نيويورك، 24 ديسمبر 2024، المواد 2 وما بعدها المتعلقة بالمصطلحات، والمواد المتعلقة بالتعاون الدولي والأدلة الإلكترونية .

2- القوانين

1. القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، 16 أوت 2009 .
2. القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق 1 فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 6، 10 فبراير 2015 .

3. القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 28، الصادرة بتاريخ 16 ماي 2018 .
4. القانون رقم 18-07 المؤرخ في 10 جوان سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 34، الصادرة بتاريخ 10 جوان 2018 .

3-المراسيم الرئاسية

1. المرسوم الرئاسي رقم 14-252 المؤرخ في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 57، 28 سبتمبر 2014 .
2. المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي سنة 2020، المتعلق بإنشاء منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 04، الصادرة بتاريخ 22 جانفي 2020 .

ثانيا: المراجع

1-الكتب

1-1- الكتب العامة

1. سعيد بوشعير، **القانون الدولي والتحولات الرقمية الحديثة**، الطبعة الأولى، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2021 .
2. عبد الله الأشعل، **القانون الدولي والسيادة الرقمية**، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2021 .
3. عبد الواحد محمد الفار، **القانون الدولي العام**، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2005 .

4. محمد بن عيسى، **الصناعات الرقمية ودورها في التنمية الاقتصادية**، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2020 .
5. مصطفى يوسف كافي، **الاقتصاد الرقمي والتجارة الإلكترونية**، الطبعة الأولى، دار رسلان للطباعة والنشر والتوزيع، دمشق، سوريا، 2017 .
6. ياسر عبد العزيز، **عصر ما بعد العولمة: السيادة الرقمية وصراع التحكم في البيانات**، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، مصر، 2022 .

1-2- الكتب الخاصة

1. إيهاب خليفة، **القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت؟ الولايات المتحدة نموذجًا**، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، مصر، 2017 .
2. إيهاب خليفة، **مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي**، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، مصر، 2019 .
3. جمال الدين شيخي، **القانون الدولي للاتصالات وتحديات الفضاء السيبراني**، الطبعة الأولى، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2019 .
4. زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دون طبعة مذكورة، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011 .
5. عبد الحميد زيد، **الذكاء الاصطناعي والسيادة الرقمية**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2023 .
6. عبد الرحمان خلفي، **القانون الإداري الرقمي والتحول الإلكتروني للإدارة**، الطبعة الأولى، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2021 .
7. عبد الرزاق السنهوري، **الأمن السيبراني والتعاون الدولي**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2022 .

8. عبد الرؤوف منصور، **الأمن السيبراني وحروب الجيل الجديد**، الطبعة الأولى، دار الأيام للنشر والتوزيع، عمان، الأردن، 2021 .

9. عبد العزيز سعد، **القانون الرقمي وحماية البيانات الشخصية**، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2021 .

10. عبد الفتاح بيومي حجازي، **الحكومة الإلكترونية وحماية الأمن المعلوماتي**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2010 .

11. عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي: دراسة متعمقة في القانون المعلوماتي**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2006 .

12. عبد القادر بوزيان، **الأمن الرقمي والسياسات الحكومية الحديثة**، الطبعة الأولى، دار هومة، الجزائر، 2022 .

13. فارس محمد العمارات، إبراهيم محمد الحمامصة، **الأمن السيبراني: المفهوم وتحديات العصر**، الطبعة الأولى، دار الخليج للنشر والتوزيع، عمان، الأردن، 2022 .

14. محمد الصالح بوزيد، **استراتيجيات الأمن السيبراني وحماية السيادة الوطنية**، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2022 .

15. محمد سامي الشوا، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 1994 .

16. محمد عبد الحميد، **الأمن المعلوماتي والأمن السيبراني**، الطبعة الثانية، دار الجامعة الجديدة، الإسكندرية، مصر، 2020 .

17. محمد عبد الواحد، **الأمن المعلوماتي والجرائم الإلكترونية**، الطبعة الثانية، دار الجامعة الجديدة، الإسكندرية، مصر، 2020 .

18. نبيل صقر، **الحروب السيبرانية وتحولات الصراع الدولي**، الطبعة الأولى، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2022 .

19. هشام محمد بدر، **الحماية الجنائية للتعاملات الإلكترونية**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2012.

2- المذكرات والرسائل والأطروحات

2-1- رسائل الماجستير

1. أسماء بوقرة، **الفضاء السيبراني وتحول مفهوم السيادة الدولية**، رسالة ماجستير في العلاقات الدولية، كلية العلوم السياسية، جامعة قسنطينة 3 صالح بوبنيدر، الجزائر، السنة الجامعية 2019-2020 .

2. نور الدين بوطبة، **الأمن السيبراني في التشريع الجزائري**، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة الجزائر 1 يوسف بن خدة، الجزائر، السنة الجامعية 2018-2019 .

3. محمد قسوم، **دور الأمم المتحدة في تقديم المساعدات الإنسانية: الصومال نموذجًا**، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أمحمد بوقرة، بومرداس، الجزائر، 2015 .

2-2- أطروحات الدكتوراه

1. خولة رحموني، **الأمن السيبراني والسيادة الرقمية في العلاقات الدولية المعاصرة**، أطروحة دكتوراه في العلوم السياسية والعلاقات الدولية، كلية الحقوق والعلوم السياسية، جامعة الجزائر 3 إبراهيم سلطان شيبوط، الجزائر، السنة الجامعية 2022-2023 .

2. سومية قلات، **الأحكام الإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2024 .

3. طوايبية أحمد، **تطبيقات الاقتصاد الرقمي وأثرها على النمو الاقتصادي**، أطروحة دكتوراه علوم في العلوم الاقتصادية، تخصص التخطيط والتنمية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر، السنة الجامعية 2008-2009 .
4. عبد الحكيم بوزيدي، **الدبلوماسية الرقمية وأثرها على العلاقات الدولية**، أطروحة دكتوراه في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة وهران 2 محمد بن أحمد، الجزائر، السنة الجامعية 2020-2021 .
5. فاطمة الزهراء بوعلام، **السيادة الرقمية في ظل التحولات التكنولوجية الحديثة**، أطروحة دكتوراه لنيل شهادة الدكتوراه في العلوم السياسية والعلاقات الدولية، تخصص تنظيمات سياسية وإدارية، كلية الحقوق والعلوم السياسية، جامعة وهران 2 محمد بن أحمد، الجزائر، السنة الجامعية 2021-2022 .
6. فاطمة بن قانة، **الصناعات الرقمية الوطنية ودورها في تحقيق السيادة الرقمية**، أطروحة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة سطيف 1 فرحات عباس، الجزائر، السنة الجامعية 2022-2023 .
7. كريمة بن داود، **الأمن الرقمي والتحديات المستقبلية للدولة الحديثة**، أطروحة دكتوراه في العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة الجزائر 3 إبراهيم سلطان شيبوط، الجزائر، السنة الجامعية 2022-2023 .
8. ليلى بن سالم، **الاقتصاد الرقمي وأثره على سيادة الدولة**، أطروحة دكتوراه في العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجزائر 3 إبراهيم سلطان شيبوط، الجزائر، 2022 .
9. نسرين بوقرة، **التحول الرقمي وإشكالية التبعية التكنولوجية**، أطروحة دكتوراه في العلاقات الدولية، كلية العلوم السياسية، جامعة قسنطينة 3 صالح بوبنيدر، الجزائر، السنة الجامعية 2021-2022 .

10. نصيرة بوحزمة، **التحقيق الجنائي في الجرائم الإلكترونية: دراسة مقارنة**، أطروحة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس، الجزائر، 2022 .

11. نوال زروقي، **السيادة الرقمية في ظل العولمة التكنولوجية**، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 1 يوسف بن خدة، الجزائر، السنة الجامعية 2022-2023 .

12. ياسين بن حمادي، **التحديات القانونية للسيادة الرقمية في ظل العولمة الرقمية**، أطروحة دكتوراه في القانون الدولي العام، كلية الحقوق، جامعة مولود معمري تيزي وزو، الجزائر، السنة الجامعية 2021-2022 .

13. يوسف بن عدة، **السيادة الرقمية والأمن السيبراني في القانون الدولي المعاصر**، أطروحة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1 يوسف بن خدة، الجزائر، السنة الجامعية 2021-2022 .

3-المقالات العلمية

1. ابن زرارة أمينة، أعراب فطيمة، "الحلول الرقمية الابتكارية في مجال حماية الهوية والخصوصية والأمن السيبراني خلال جائحة كوفيد-19"، مجلة رقمنة للدراسات الإعلامية والاتصالية، الجزائر، المجلد 3، العدد 1، عدد خاص، مارس 2023 .
2. أحمد بن ناصر، "تحديات السيادة الرقمية في ظل العولمة التكنولوجية"، مجلة الباحث للدراسات الأكاديمية، العدد 14، جامعة باتنة 1، الجزائر، 2020 .
3. أحمد شحيرط، مراد قريبيز، "تحديات الإنترنت لسيادة الدول: السيادة الرقمية"، مجلة البحوث القانونية والاقتصادية، الجزائر، المجلد 5، العدد 1، 2022 .
4. أحمد مومن، "التعاون الدولي في مجال الأمن السيبراني"، مجلة الحقوق والعلوم السياسية، المجلد 08، العدد 01، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، 2023 .

5. أمينة إيجر، "السيادة الرقمية في العالم المعولم: التحديات والرهانات"، مجلة الدراسات القانونية والسياسية، المجلد 10، العدد 02، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي بالأغواط، الجزائر، 2024 .
6. سمير بارة، "الأمن السيبراني (Cyber Security) في الجزائر: السياسات والمؤسسات"، المجلة الجزائرية للأمن الإنساني، المجلد 02، العدد 02، جامعة قاصدي مرباح ورقلة، الجزائر، 2017 .
7. بلحاج خالدية، فرعون محمد، "السيادة الرقمية"، مجلة البحوث في الحقوق والعلوم السياسية، جامعة ابن خلدون تيارت، الجزائر، المجلد 11، العدد 1، 2025 .
8. بن برغوث ليلى، "الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي: التهديدات، التقنيات، التحديات وآليات التصدي"، المجلة الدولية للاتصال الاجتماعي، المجلد 10، العدد 01، جامعة عبد الحميد بن باديس مستغانم، الجزائر، مارس 2023 .
9. بن دعاس سهام، بن عثمان فوزية، "ضمانات حماية المعطيات الشخصية في البيئة الرقمية في التشريع الجزائري"، مجلة الحقوق والعلوم الإنسانية، جامعة محمد لمين دباغين، سطيف 2، الجزائر، المجلد 15، العدد 1، 2022 .
10. بن قطاط خديجة، "تداعيات الحروب السيبرانية على السيادة الرقمية"، مجلة القانون العام الجزائري والمقارن، الجزائر، المجلد 10، العدد 2، 2024 .
11. بوازدية جمال، "الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية"، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمه لخضر الوادي، الجزائر، المجلد 10، العدد 1، أفريل 2019 .
12. بوعزة حكيمة، "معايير تحديد الاختصاص القضائي للجريمة المعلوماتية"، مجلة القانون والعلوم السياسية، الجزائر، المجلد 11، العدد 2، 2025 .

13. حسام الدين قاسمي، "الهيمنة الرقمية وأثرها على سيادة الدول"، مجلة السياسة الدولية، العدد 234، مؤسسة الأهرام، القاهرة، مصر، 2023 .
14. خيدل وردة، "إجراءات جمع الأدلة الرقمية طبقًا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات"، مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بوعلي، الشلف، الجزائر، المجلد 8، العدد 1، 2022 .
15. داود كمال، "حقوق الإنسان في الفضاء الرقمي: التعزيز والحماية"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، الجزائر، المجلد 10، العدد 1، 2025 .
16. رحيم محمد، ابن يحي نبيلة، "الأمن السيبراني في المنشآت الحكومية"، المجلة الجزائرية للدراسات السياسية، الجزائر، المجلد 10، العدد 1، 2023 .
17. سامر محي عبد الحمزة، "موقف جامعة الدول العربية من السيادة على الفضاء السيبراني: دراسة في ضوء أحكام القانون الدولي العام"، مجلة القانون الدولي للدراسات البحثية، المركز الديمقراطي العربي، برلين، ألمانيا، المجلد 4، العدد 12، مارس 2023 .
18. سعاد قريشي، "التكوين الرقمي كآلية لتعزيز الأمن السيبراني"، مجلة العلوم الاجتماعية والإنسانية، العدد 14، جامعة محمد خيضر بسكرة، الجزائر، 2023 .
19. سمير قسوم، "التحولات الرقمية وأزمة السيادة الوطنية"، مجلة الدراسات السياسية المعاصرة، العدد 12، جامعة وهران 2 محمد بن أحمد، الجزائر، 2023 .
20. سمير لعريبي، "الاتفاقيات الدولية ودورها في مكافحة الجرائم الإلكترونية"، مجلة الفكر القانوني والسياسي، المجلد 06، العدد 02، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، الجزائر، 2022 .
21. شرايطية سميرة، "السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي"، المجلة الجزائرية للأمن والتنمية، جامعة باتنة 1، الجزائر، المجلد 9، العدد 1، جانفي 2020 .

22. شيماء بوحفص، "البيانات الضخمة والسيادة الاقتصادية للدول"، مجلة العلوم السياسية والقانون، العدد 12، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3 إبراهيم سلطان شيبوط، الجزائر، 2022 .

23. عبد المجيد قدي، "السيادة الرقمية والرهانات الاقتصادية المعاصرة"، مجلة الاقتصاد والتنمية، المجلد 09، العدد 01، جامعة حسيبة بن بوعلي الشلف، الجزائر، 2021 .

24. علي محفوظ، "التهديدات الإلكترونية وانعكاساتها على الأمن الوطني"، مجلة الباحث الأكاديمي، العدد 15، جامعة بسكرة، الجزائر، 2021 .

25. فاطمة بيرم، "السيادة الوطنية السيبرانية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجًا"، المجلة الجزائرية للأمن الإنساني، جامعة باتنة 1، الجزائر، المجلد 5، العدد 1، 2020 .

26. فرحات علاء الدين، عمروس عمارة، "الفضاء السيبراني وتآكل مفهوم السيادة الوطنية"، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، المجلد 8، العدد 2، 31 ديسمبر 2021 .

27. فوزية لعور، "الشراكة بين القطاعين العام والخاص في مجال الأمن السيبراني"، مجلة الدراسات الأمنية والاستراتيجية، العدد 06، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، الجزائر، 2022 .

28. قطاف سليمان، بوقرين عبد الحليم، "الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي، الأغواط، الجزائر، المجلد 6، العدد 1، 2022 .

29. قونان كهينة، حمليل نوارة، "السلطة الوطنية كهيئة مكلفة برقابة احترام تطبيق قانون حماية المعطيات الشخصية رقم 18-07"، مجلة الدراسات القانونية، الجزائر، المجلد 7، العدد 2، جوان 2021 .

30. كمال رزيق، "التحول الرقمي وتحديات الأمن الاقتصادي"، مجلة الدراسات الاقتصادية المعاصرة، العدد 08، كلية العلوم الاقتصادية، جامعة محمد بوضياف بالمسيلة، الجزائر، 2020 .

31. لسود موسى، "معايير الاختصاص القضائي في جرائم قانون التجارة الإلكترونية الجزائري 18-05"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، الجزائر، المجلد 4، العدد 2، 2020 .

32. ليلى بعوني، "التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الإلكترونية نموذجًا"، مجلة ستراتيجيا، الجزائر، المجلد 8، العدد 16، 2021، ص 22 .

33. محمد العيداني، "حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، الجزائر، المجلد 10، العدد 2، 2018 .

34. محمد بن يحي، "الاقتصاد الرقمي كمدخل لتحقيق السيادة الوطنية"، مجلة العلوم السياسية والقانون، العدد 09، جامعة الجزائر 3، الجزائر، 2022 .

35. محمد شتاتحة، "الأمن السيبراني وأثره على الأمن القومي للدول"، مجلة العلوم القانونية والسياسية، المجلد 11، العدد 02، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، الجزائر، 2020 .

36. مروة خلة، بشرى سلاوي، سارة خلة، عبد النور البلدي، "مستقبل السيادة الرقمية في ظل التكنولوجيات الحديثة: دراسة تحليلية استشرافية"، مجلة بحوث ودراسات في الميديا الجديدة، الجزائر، المجلد 4، العدد 1، 31 مارس 2023 .

37. مصطفى بوعزيز، "دور المنظمات الدولية في تنظيم الفضاء السيبراني"، مجلة الدراسات القانونية المقارنة، العدد 11، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، 2022 .

4- الملتقيات :

1. جميلة قرفي، "الاقتصاد الرقمي كآلية لتعزيز السيادة الوطنية"، ضمن أعمال الملتقى الوطني حول التحول الرقمي والسيادة الإلكترونية، كلية العلوم السياسية والعلاقات الدولية، جامعة قسنطينة 3 صالح بوبنيدر، الجزائر، المنعقد بتاريخ 15 مارس 2023 .
2. سليمان أعراج، "السيادة الرقمية والتحديات الجيوسياسية الجديدة"، مداخلة ضمن أعمال الملتقى الدولي حول السيادة الرقمية والأمن السيبراني، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، الجزائر، المنعقد بتاريخ 06 ديسمبر 2022 .
3. عبد العزيز لعمامرة، "الحرب التكنولوجية وأثرها على العلاقات الدولية"، ضمن أعمال الملتقى الدولي حول التكنولوجيا والتحولات الجيوسياسية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، الجزائر، 2023 .
4. عبد الكريم سلامة، "السياسات الوطنية للأمن السيبراني"، ضمن أعمال الملتقى الدولي حول الأمن الرقمي والتحولات التكنولوجية، جامعة سطيف 2، الجزائر، 2023 .
5. فهد بن محمد الحربي، "الأمن السيبراني كمدخل لحماية السيادة الوطنية"، ضمن أعمال الملتقى العربي للأمن الرقمي والتحول التكنولوجي، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2022 .
6. نعاس صلاح الدين، فاتح بلقاسم أولاد الهدار، "الرقمنة في الجزائر بين تحديات الذكاء الاصطناعي وتعزيز الأمن السيبراني"، ضمن أعمال ملتقى وطني حول الرقمنة في الجزائر، جامعة غرداية، الجزائر، 2025.

ثالثا : المراجع باللغة الأجنبية

1. Herbert Lin & Amy Zegart, *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, First Edition, Brookings Institution Press, Washington DC, United States, 2018,
2. International Telecommunication Union (ITU), *Understanding Cybersecurity*, First Edition, International Telecommunication Union Publishing, Geneva, Switzerland, 2021,
3. Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, First Edition, Houghton Mifflin Harcourt Publishing, New York, United States, 2013,

فهرس المحتويات

العنوان	لصفحة
فهرس المحتويات	
شكر وعرفان	
إهداء	
ملخص الدراسة	-
مقدمة	أ
الفصل الأول الإطار المفاهيمي والسياسي للسيادة الرقمية	
المبحث الأول: مفهوم السيادة الرقمية و أبعادها	09
المطلب الأول: ماهية السيادة الرقمية	10
الفرع الأول: التعريف التقليدي للسيادة ومقارنته بالسيادة الرقمية	10
الفرع الثاني: التعريف الحديث للسيادة الرقمية وخصائصها الأساسية	15
المطلب الثاني: أبعاد السيادة الرقمية وتمييزها عن السيادة التقليدية	19
الفرع الأول: البعد السياسي للسيادة الرقمية: التحكم في البيانات والمعلومات الوطنية	20
الفرع الثاني: البعد التقني والاقتصادي وأثره على استقلال الدولة الرقمي	23
المبحث الثاني: الأسس القانونية والسياسية للسيادة الرقمية	26
المطلب الأول: الإطار القانوني المنظم للسيادة الرقمية	27
الفرع الأول: القوانين الوطنية المنظمة للفضاء الرقمي: التشريع الجزائري نموذجًا	28
الفرع الثاني: الاتفاقيات والمعاهدات الدولية ذات الصلة بالفضاء الرقمي	32
المطلب الثاني: مبدأ استقلال الدولة الرقمي وتحدياته	35
الفرع الأول: حق الدولة في تنظيم وإدارة فضائها الرقمي	36
الفرع الثاني: التحديات القانونية والسياسية بين حماية السيادة وحرية الإنترنت	38
الفصل الثاني تطبيقات السيادة الرقمية في العلاقات الدولية	
المبحث الأول: الاستراتيجيات الوطنية لتحقيق السيادة الرقمية	45
المطلب الأول: السياسات الوطنية للسيادة الرقمية	46
الفرع الأول: إنشاء البنية التحتية الرقمية الوطنية وتأمين البيانات	47
الفرع الثاني: تطوير التشريعات الوطنية لحماية المعلومات والمواطنين	50
المطلب الثاني: الأمن السيبراني والاقتصاد الرقمي كأداة للسيادة الرقمية	52
الفرع الاول :الأمن السيبراني والسيادة الرقمية	53
الفرع الثاني: الاقتصاد الرقمي والسيادة	59

المبحث الثاني: السيادة الرقمية في العلاقات الدولية.	63
المطلب الأول: الصراعات الرقمية بين الدول	64
الفرع الأول: الهجمات السيبرانية والتجسس الرقمي بين الدول	65
الفرع الثاني: النزاعات حول البيانات والخدمات الرقمية العابرة للحدود	67
المطلب الثاني: التعاون الدولي والتحديات المستقبلية للسيادة الرقمية	69
الفرع الأول :دور المنظمات الدولية والاتفقيات التنائية والاقليمية في تنظيم الفضاء الرقمي	70
الفرع الثاني: التحديات المستقبلية للسيادة الرقمية	74
خاتمة	82
قائمة المصادر والمراجع	86