

السيادة الرقمية والأمن السيبراني: نحو مقاربة قانونية لحماية الدولة في البيئة الرقمية

Digital Sovereignty and Cybersecurity: Towards a Legal Framework for State Protection in the Digital Environment

لعجال منيرة^{1*}، علي محمد²

جامعة أحمد درايعية، أدرار (الجزائر)، ladjalmounira@univ-adrar.edu.dz

جامعة أحمد درايعية، أدرار (الجزائر)، ali.mohammed@univ-adrar.edu.dz

تاريخ الاستلام: 2026/06/11 تاريخ القبول: 2026/09/29 تاريخ النشر: 2026/09/30

ملخص

تهدف هذه الدراسة إلى إبراز أهم التهديدات التي تواجه السيادة الرقمية في ظل التحول الرقمي المتسارع وما صاحبه من توسع في استخدام تكنولوجيات الإعلام والاتصال، الأمر الذي جعل الفضاء السيبراني مجالاً استراتيجياً تتداخل فيه المصالح الأمنية والاقتصادية والسياسية للدول. كما تسعى إلى تحليل الآليات القانونية والمؤسسية المعتمدة لحماية السيادة الرقمية وتعزيز الأمن القومي.

وقد خلصت الدراسة إلى أن الجرائم الإلكترونية والهجمات السيبرانية والتبعية التكنولوجية تمثل أبرز مهددات السيادة الرقمية، وأن مواجهتها تقتضي اعتماد مقاربة شاملة تقوم على تكامل التدابير القانونية والتقنية والمؤسسية، فضلاً عن تعزيز التعاون الدولي وتطوير استراتيجيات وطنية فعالة لحماية الفضاء الرقمي وضمان الأمن والاستقرار.

الكلمات المفتاحية: السيادة الرقمية؛ الأمن القومي؛ الأمن السيبراني؛ الجرائم الإلكترونية؛ حماية المعطيات الشخصية؛ الهجمات السيبرانية.

Abstract:

This study highlights the major threats to digital sovereignty in the context of rapid digital transformation and the widespread use of information and communication technologies, which have transformed cyberspace into a strategic domain where states' security, economic, and political interests

* المؤلف المرسل

increasingly intersect. It also analyzes the legal and institutional mechanisms adopted to protect digital sovereignty and strengthen national security.

The study concludes that cybercrime, cyberattacks, and technological dependence represent the most significant threats to digital sovereignty. Addressing these challenges requires a comprehensive approach that integrates legal, technical, and institutional measures, along with the enhancement of international cooperation and the development of effective national strategies to safeguard cyberspace and ensure security and stability.

Keywords: Digital sovereignty; national security; cybersecurity; cybercrime; personal data protection; cyberattacks.

مقدمة:

أبرزت التحولات التكنولوجية المتسارعة التي عرفها العالم خلال العقود الأخيرة واقعا جديدا أصبحت فيه التكنولوجيا الرقمية والبيانات والمعلومات من المقومات الأساسية لقوة الدول وممارسة اختصاصاتها السيادية. فقد أدى التوسع في استخدام شبكات الاتصال والأنظمة المعلوماتية واعتماد الإدارة الإلكترونية والتعاملات الرقمية إلى انتقال جانب مهم من مظاهر السلطة والسيادة إلى الفضاء الرقمي، الأمر الذي أسهم في ظهور مفهوم السيادة الرقمية بوصفه امتدادا حديثا لمفهوم السيادة في القانون العام.

يقصد بالسيادة الرقمية سلطة الدولة على فضاءها الرقمي وما يتصل به من بيانات ومعلومات وبني تحتية رقمية، بما يكفل لها ممارسة اختصاصاتها وحماية مصالحها الحيوية وضمان أمنها القومي في البيئة الإلكترونية. غير أن الطبيعة العابرة للحدود للفضاء السيبراني وما يتسم به من انفتاح وتشابك قد أبرزت تحديات قانونية وأمنية متزايدة، تمثلت في تنامي الهجمات السيبرانية، وجرائم الاختراق المعلوماتي، والتجسس الإلكتروني، وسرقة البيانات، والإرهاب السيبراني، وغيرها من الممارسات التي من شأنها المساس باستقلال الدول وقدرتها على التحكم في مواردها الرقمية ومرافقها الحيوية.

تتجلى أهمية دراسة هذا الموضوع في ارتباطه المباشر بحماية الأمن القومي للدول والحفاظ على استقرار مؤسساتها وضمان استمرارية المرافق والخدمات العامة المعتمدة على الأنظمة الرقمية، فضلا عن تنامي الحاجة إلى تطوير أطر قانونية ومؤسسية قادرة على مواجهة المخاطر المستجدة

التي أفرزها التحول الرقمي المتسارع. كما تكتسب هذه الدراسة أهميتها من تزايد الجهود الوطنية والدولية الرامية إلى إرساء قواعد فعالة لحوكمة الفضاء الرقمي وضمان الاستخدام الآمن للتكنولوجيا الحديثة.

تهدف هذه الدراسة إلى بيان طبيعة التهديدات التي تواجه السيادة الرقمية وتحليل آثارها على الدولة المعاصرة، وكذا الوقوف على مختلف الآليات والاستراتيجيات القانونية والمؤسسية والتقنية المعتمدة لمواجهتها وتعزيز حماية الفضاء الرقمي الوطني. وفي ضوء ذلك تثار الإشكالية الآتية: ما أثر التهديدات السيبرانية على السيادة الرقمية للدولة، وما الآليات القانونية والمؤسسية الكفيلة بحمايتها؟

وللإجابة عن هذه الإشكالية تم الاعتماد على المنهج التحليلي من خلال تحليل المفاهيم القانونية المرتبطة بالسيادة الرقمية، ودراسة أبرز المهددات التي تعترضها، فضلاً عن تحليل التدابير والآليات المعتمدة على المستويين الوطني والدولي لتعزيز حمايتها. وعليه، تم تقسيم هذا المقال إلى محورين رئيسيين:

المبحث الأول: مظاهر المساس بالسيادة الرقمية في الفضاء السيبراني.

المبحث الثاني: آليات حماية السيادة الرقمية ومواجهة التهديدات السيبرانية.

المبحث الأول: مظاهر المساس بالسيادة الرقمية في الفضاء السيبراني

يشكل الفضاء السيبراني مجالاً لتهديدات متزايدة تمس أمن الدولة وسيادتها الرقمية، من خلال الإرهاب الإلكتروني والجرائم المرتكبة باستخدام تقنيات المعلومات وما تسببه من أضرار للأنظمة والبيانات الرقمية (المطلب الأول). كما تفرض الطبيعة العابرة للحدود للفضاء الرقمي تحديات إضافية تتمثل في الجريمة المنظمة الإلكترونية وحروب المعلومات التي تؤثر على استقرار الدول وتماسك مجتمعاتها وقدرتها على ممارسة سيادتها الرقمية (المطلب الثاني).

المطلب الأول: التهديدات السيبرانية الموجهة لأمن الدولة وسيادتها الرقمية

تتخذ التهديدات السيبرانية الموجهة لأمن الدولة وسيادتها الرقمية صورا متعددة، أبرزها الإرهاب الإلكتروني (الفرع الأول) والجرائم المرتكبة باستخدام تقنيات المعلومات (الفرع الثاني).

الفرع الأول: الإرهاب الإلكتروني

يتكون مصطلح (Cyber Terrorisme) من اندماج كلمتين: "Cyber" الفضاء الإلكتروني و "Terrorisme" الإرهاب. وأول محاولة لظهور هذا المصطلح كانت عام 1997 من قبل موظف مكتب التحقيقات الفدرالي الأمريكي T. Pollitt. يعرف الإرهاب الإلكتروني على أنه كل استخدام لأجهزة الكمبيوتر كسلاح أو هدف للهجوم من قبل مجموعات دولية أو عرقية أو عملاء سريين ذوي دوافع سياسية، يهددون أو يتسببون في العنف ويغرسون الخوف من أجل التأثير أو إجبار الحكومة على تغيير سياستها (ناصر، 2021، صفحة 30).

يعتبر التعريف الذي قدمته "دوروثي دينينغ" للإرهاب السيبراني، سنة 2000 أمام لجنة القوات المسلحة بمجلس النواب الأمريكي، من أكثر التعريفات وضوحاً وأهمية. فوفقاً لهذا التعريف، فإن الإرهاب السيبراني يتمثل في التقاء الفضاء السيبراني بالإرهاب، ويشير إلى الهجمات غير المشروعة أو التهديدات الموجهة ضد الحواسيب والشبكات والمعلومات المخزنة فيها، متى كان الهدف منها ترهيب حكومة أو مجتمع أو إكراهه لتحقيق أهداف سياسية أو اجتماعية معينة. كما يشترط لاعتبار الفعل إرهاباً سيبرانياً أن يترتب عليه عنف ضد الأشخاص أو الممتلكات، أو أن يحدث ضرراً جسيماً من شأنه إثارة الخوف والذعر. وتشمل أمثلة ذلك الهجمات التي تؤدي إلى الوفاة أو الإصابات الجسدية أو الانفجارات أو الخسائر الاقتصادية الجسيمة، فضلاً عن الهجمات الخطيرة التي تستهدف البنى التحتية الحيوية. أما الهجمات التي تقتصر آثارها على تعطيل خدمات غير أساسية أو إحداث إزعاج محدود فلا تُعد إرهاباً سيبرانياً وفق هذا المفهوم.

كما يمكن أن يندرج ضمن الإرهاب السيبراني أي هجوم إلكتروني محدود من حيث النطاق لكنه يؤدي إلى نتائج خطيرة، مثل الوفيات أو الإصابات أو انقطاع الكهرباء لفترات طويلة أو حوادث الطيران أو تلوث المياه أو فقدان الثقة في قطاعات اقتصادية مهمة. هذا المفهوم لا يشمل أنشطة "الهاكتيفيزم" أو القرصنة ذات الدوافع السياسية، رغم وجود بعض أوجه التشابه بينهما، لأن الهدف الأساسي للهاكتيفيزم غالباً ما يكون الاحتجاج السياسي أو التعبير عن موقف معين، وليس إحداث أضرار جسيمة أو نشر الرعب بين السكان. ومع ذلك، قد تصبح الحدود الفاصلة بين الظاهرتين غير واضحة في بعض الحالات، خاصة إذا استعانت الجماعات الإرهابية بقرصنة

محترفين أو إذا تطورت أنشطة "الهاكتيفيزم" لتستهدف البنى التحتية الحيوية للدولة (John J, 2015, p. 22).

الفرع الثاني: الجرائم السيبرانية المرتكبة باستخدام تقنية المعلومات

تتسم جرائم تقنية المعلومات بنفس سمات الجرائم العادية من حيث إلحاق الضرر بالآخرين، ويمكن حصر أهم أوجهها فيما يلي:

أولاً: الجرائم المرتكبة ضد التقنية ومستخدميها

تعد الاختراقات الإلكترونية من أبرز التهديدات التي تواجه الأمن السيبراني والسيادة الرقمية، إذ يمكن أن ترتكبها جهات متعددة تشمل التنظيمات الإرهابية، والجماعات الإجرامية المنظمة، ومجموعات القرصنة الإلكترونية، بل وحتى بعض الجهات المدعومة من الدول. وتتم هذه الهجمات بالاعتماد على إمكانيات تقنية متطورة تتيح استهداف الأنظمة المعلوماتية والمواقع الإلكترونية وقواعد البيانات الحساسة. ومن بين الأساليب الأكثر شيوعاً في هذا المجال الاستيلاء على البيانات السرية والرموز الخاصة بالأنظمة المعلوماتية، أو تصميم ونشر البرمجيات الخبيثة والفيروسات عبر شبكات الاتصال والبريد الإلكتروني، بما يؤدي إلى إتلاف البيانات أو تعطيل الأنظمة الحاسوبية أو إضعاف كفاءتها التشغيلية. وتتميز هذه الجرائم بطابعها العابر للحدود، إذ يمكن تنفيذها عن بُعد من أي مكان في العالم دون الحاجة إلى التواجد داخل إقليم الدولة المستهدفة، الأمر الذي يجعل البعد الجغرافي غير ذي أثر في الحد من مخاطر الاختراقات الإلكترونية (مباركة، 2017، صفحة 347، 2017).

لا تقتصر التهديدات السيبرانية على اختراق الأنظمة المعلوماتية فحسب، بل تمتد إلى الاعتداء على حقوق الملكية الفكرية وسرقة الأسرار التجارية والمعلومات الاستراتيجية وقواعد بيانات العملاء وخطط التسويق، بما يترتب عليه الإضرار بالمصالح الاقتصادية والإنتاج الفكري للأفراد والمؤسسات. كما قد تستهدف هذه الأفعال السجلات الحكومية والعسكرية والأنظمة الأمنية الحساسة بغرض الحصول على معلومات استخباراتية أو استخدامها في الابتزاز والضغط أو تحقيق أهداف سياسية واقتصادية وأمنية (ليلي، 2021، صفحة 18).

ثانيا: الجرائم التي ترتكب باستخدام تقنية المعلومات:

يتسع حيز الجرائم التي ترتكب باستخدام تقنية المعلومات لتشمل:

- جرائم الاحتيال المالي: تتم هذه الجرائم عن طريق استعمال أجهزة الصرف الآلي وحسابات مزورة وسرقة بطاقات الائتمان، وتشمل السرقات المالية من حساب البنوك ومراكز التعامل المالي. في هذا الإطار تلقى مركز شكاوى احتيال الانترنت الأمريكي في عام 2000م ما يقارب 4.6 مليار دولار، وبلغ حجم خسائر الشركة الأمريكية حوالي 450 مليون دولار بسبب الاحتيال المالي وسوء الاستخدام لبطاقات الائتمان.

- جرائم استخدام النظم الحاسوبية لإنتاج أو توزيع صور أو نصوص أو معلومات مخالفة للقانون الجنائي.

- جرائم الاختطاف ذات الصلة بالانترنت مثل إغراء الأطفال عبر مواقع الدردشة واستدراجهم ليتم اختطافهم واستغلالهم جنسيا.

- جرائم المخدرات عن طريق نشر كيفية زراعتها وأساليب ترويجها وطرق تصنيعها واستعمالها (القحطاني، 2008، الصفحات 28-30).

- جرائم غسيل الأموال: تعد الانترنت الأداة المثالية لغسل الأموال نظرا لطبيعتها الافتراضية وسرعة التحويل وتحررها من القيود الإقليمية (طبيعتها العابرة للحدود، وتعارض الاختصاصات والولايات القضائية)، فشبكة الانترنت تجعل من الممكن تحويل الأموال ذات المنشأ الإجرامي إلى دوائر اقتصادية قانونية وذلك باستخدام الحوالات المالية والاستثمار والرملة، فالاستثمارات والمقامرة والتجارة على شبكة الانترنت كبيع سلع وخدمات خيالية مقابل نقود حقيقية، تجعل في المستطاع توليد مداخيل تبدو مشروعة ويصعب رصدها ويكاد أن يكون من المستحيل مقاضاتها، فالعمليات المصرفية الالكترونية والعمليات العقارية عبر الشبكة، واستخدام شركات كواجهات خيالية والنقد الالكتروني كلها عمليات يتم استخدامها في غسل غنائم الجريمة. وقد أشار تقرير صادر عن الأمم المتحدة وصندوق النقد الدولي إلى أن 28.5 مليار دولار من الأموال القذرة تطير سنويا عبر الانترنت لتخترق حدود 67 دولة لغسلها (فتيحة، 2011-2012، صفحة 83). وعليه تشكل جريمة غسل الأموال أحد أهم مهددات السيادة الرقمية خصوصا في الدول النامية،

ومنها البنوك الجزائرية لعدم توفرها على نظام معلوماتي متطور من شأنه عرقلة عملية مكافحة تبييض الأموال التي تتم عبر الوسائط الإلكترونية (رقية، حورية، 2020، صفحة 131، 130).

- التهديد والابتزاز المعلوماتي: تتمثل التهديدات السيبرانية الموجهة ضد الأفراد، في الاختراقات التي تقوم بها من خلال وسائل التكنولوجيا (الإنترنت، الهاتف، الفاكس) مهما كان نوعها أو حجمها ضد الشخص الطبيعي، ومن بين أهم مخاطر التهديدات السيبرانية على الأفراد نجد التهديد والابتزاز المعلوماتي، حيث شهدت شبكة الانترنت حالات للابتزاز المعلوماتي من قبل أشخاص تمكنوا بوسيلة أو بأخرى من اختراق نظام الأمن للبريد الإلكتروني، أو التنصت أو التجسس على حلقات الدردشة عبر مواقع التواصل الاجتماعي.

وفي الغالب تستهدف التهديدات السيبرانية الشخصيات المعروفة سواء الحكومية أو العسكرية أو الفنية، حيث تتيح الأنترنت والتكنولوجيا وسائل مبتكرة للابتزاز منها: انتحال شخصية الأفراد من أجل الاستفادة من سمعتهم أو أموالهم أو صلاحياتهم أو نشر أسرارهم، من خلال إنشاء حسابات مزورة من أجل التعارف ثم استغلالهم وتشويه سمعتهم، ونشر المعلومات السرية والصور الشخصية عنهم بهدف المساس بكرامتهم وتهديدهم. ومن الأمثلة على ابتزاز الشخصيات المعروفة ما حدث في أمريكا، حيث نفذ قراصنة إلكترونيون (Hackers) من مجموعة Revil تهديداتهم للرئيس الأمريكي "دونالد ترامب" بتسريب 169 رسالة إلكترونية تتحدث عن ترامب إذا لم يدفع فدية تقدر بـ 42 مليون دولار، وحسب تصريحاتهم تحصلوا على هذه المعلومات الخطيرة باختراق مكتب محاماة شهير يمثل العديد من المشهورين، وقد صنفها مكتب التحقيقات الفيدرالي (أف، بي، آي) أنها عمل إرهابي سيبراني أي إلكتروني (محمود، 2023، صفحة 15).

المطلب الثاني: التهديدات العابرة للحدود وأثرها على السيادة الرقمية

تتجلى التهديدات العابرة للحدود في الفضاء الرقمي من خلال الجريمة المنظمة الإلكترونية (الفرع الأول) وحروب المعلومات وما تفرضه من تحديات على السيادة الرقمية للدول (الفرع الثاني).

الفرع الأول: الجريمة المنظمة الإلكترونية العابرة للحدود

تعد الجريمة المنظمة العابرة للحدود من أبرز التهديدات الأمنية المعاصرة. وقد عرّفها مؤتمر الإنترنت الأول حول الإجرام المنظم المنعقد بفرنسا سنة 1988 بأنها "جماعة من الأشخاص

ترتكب أفعالا غير مشروعة بصورة مستمرة بهدف تحقيق الربح، دون التقيد بالحدود الوطنية"، قبل أن يضاف لاحقاً لهذا التعريف عنصر التنظيم للتمييز بينها وبين غيرها من الأنماط الإجرامية (أحمد، 2020، صفحة 565). وتؤكد التطورات الراهنة أن عناصر الاستمرارية والربح والتنظيم والطابع العابر للحدود لم تعد تقتصر على صورتها التقليدية، بل اكتسبت أبعاداً جديدة بفعل التحول الرقمي. فوفقاً لتقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة، أصبحت الشبكات الإجرامية تستغل الفضاء الرقمي والعملات المشفرة لتنفيذ أنشطتها غير المشروعة واستهداف ضحايا في مناطق جغرافية متعددة انطلاقاً من مراكز نشاط بعيدة عن أماكن وقوع الجريمة. كما أفرزت البيئة الرقمية أنماطاً أكثر تعقيداً من التنظيم الإجرامي، تقوم على تقسيم دقيق للأدوار وتوظيف خدمات متخصصة تشمل الاحتيال الإلكتروني وغسل الأموال والابتكار التكنولوجي. أما البعد الربحي، فقد تجسد في العائدات الضخمة التي تحققها هذه الشبكات، والتي تتراوح وفق التقرير ذاته بين 27.4 و 36.5 مليار دولار سنوياً (UNODC, 2024).

الفرع الثاني: حروب المعلوماتية والتأثير على التماسك المجتمعي

تلعب وسائل الاتصال الحديثة دوراً هاماً في إثارة النزعات القبلية والطائفية التي تعد أشد خطراً على وحدة البلاد من الإرهاب، فهذا الأخير ينحصر في فئة يمكن تحديدها والقضاء عليها، بينما تتسع دائرة مصادر إثارة الفتن وتنوع بحيث يصعب التحكم فيها، ومما يزيد الأمر خطورة هو انتقال المناوشات المتعلقة بإثارة النزعات الطائفية والمذهبية من العوالم الافتراضية في ثنايا الشبكات الاجتماعية إلى أرض الواقع، فقد انتشر على الصعيد المصري مقطع فيديو على العديد من المواقع الرقمية يدعو إلى مواجهة نصارى مصر وحرق جميع الكنائس "بإمبابة" وذلك بعد الأحداث التي وقعت في شهر ماي 2011، وأسفرت عن مقتل 12 شخصاً وكان هناك من نسب المقطع إلى الموساد الإسرائيلي بغرض إشعال الفتنة الطائفية في مصر (الغفيلي، صفحة 25، 26). كما يمكن استغلال الفضاء المعلوماتي لنشر المعلومات المضللة والتأثير على الرأي العام وإضعاف الشعور بالانتماء والوحدة المجتمعية، مما يجعل حرب المعلومات أداة فعالة للإكراه والتأثير السياسي والاجتماعي دون الحاجة إلى استخدام القوة العسكرية التقليدية. في هذا الإطار استخدمت جهات مرتبطة بروسيا القراصنة الإلكترونيين (Hackers) وحسابات التضليل والتأثير

(Trolls) للتأثير في الانتخابات الرئاسية الأمريكية سنة 2016 من خلال نشر رسائل موجهة والتلاعب بالنقاش العام واستهداف فئات اجتماعية معينة، بما في ذلك تعبئة بعض النخبين وإحباط مشاركة آخرين في العملية الانتخابية. كما استغلت وسائل التواصل الاجتماعي للتأثير في الرأي العام وتوجيه الأجندة الإعلامية عبر تسريب رسائل البريد الإلكتروني والوثائق السياسية، بما أثر في التغطية الإعلامية والنقاش السياسي خلال الحملة الانتخابية (Crilly, 2019, p. 1).

المبحث الثاني: آليات حماية السيادة الرقمية ومواجهة التهديدات السيبرانية

تفرض حماية السيادة الرقمية اعتماد تدابير وطنية قانونية ومؤسساتية لمواجهة التهديدات السيبرانية وتعزيز أمن الفضاء الرقمي (المطلب الأول). كما تقتضي الاستفادة من آليات التعاون الدولي والتجارب المقارنة التي أفرزتها الممارسات الدولية في مجال حماية السيادة الرقمية (المطلب الثاني).

المطلب الأول: آليات حماية السيادة الرقمية على المستوى الوطني

تعتمد حماية السيادة الرقمية على المستوى الوطني على إرساء إطار قانوني يجرّم التهديدات السيبرانية وينظم الفضاء الرقمي (الفرع الأول)، إلى جانب إنشاء مؤسسات متخصصة تتولى الوقاية من هذه التهديدات ومكافحتها (الفرع الثاني).

الفرع الأول: الإطار القانوني لحماية السيادة الرقمية

استحدثت الجزائر العديد من التشريعات والقوانين الكفيلة بمحاربة التهديدات والجرائم السيبرانية وذلك من خلال ما يلي:

- عمد المشرع الجزائري إلى تعزيز الحماية القانونية للأنظمة المعلوماتية والمعطيات الإلكترونية من خلال تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، الذي أدرج ضمن قانون العقوبات أحكاماً خاصة تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، ثم عرفت هذه الأحكام تعديلات لاحقة بهدف مواكبة تطور صور الجرائم المعلوماتية ووسائل ارتكابها. وقد كرس المشرع ضمن القسم الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

مجموعة من النصوص التي تجرم الاعتداء على سلامة الأنظمة والمعطيات المعلوماتية، من بينها المواد 394 مكرر وما يليها، بما يوفر حماية جنائية للأنظمة المعلوماتية والبيانات الإلكترونية.

وقد تعززت هذه الحماية بموجب القانون رقم 24-06 المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، حيث مسّ التعديل أحكاما متعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تضمنت تجريم مختلف الأفعال الماسة بالأنظمة المعلوماتية والبيانات الإلكترونية، مع تحديد العقوبات المقررة لها بهدف توفير حماية قانونية فعالة للفضاء الرقمي. ويمكن إجمالها فيما يلي:

- **جرائم إدخال أو حذف أو تعديل المعطيات في نظام المعالجة الآلية:** نصت المادة 394 مكرر، وفق تعديلها بموجب القانون رقم 24-06، على معاقبة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها، بالحبس من سنة إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج. ويستهدف هذا التجريم حماية سلامة المعطيات المعلوماتية من أفعال التغيير أو الإتلاف غير المشروع، بما يضمن المحافظة على موثوقية الأنظمة المعلوماتية وسلامة البيانات التي تتضمنها.

- **جرائم تصميم أو تجميع أو نشر أو الاتجار في المعطيات ذات الصلة بالجرائم المعلوماتية وحيازتها أو إفشائها أو نشرها أو استعمالها:** عزز المشرع هذه الحماية من خلال المادة 394 مكرر 2، التي قررت عقوبة الحبس من سنة إلى خمس سنوات والغرامة من 1.000.000 دج إلى 5.000.000 دج على الأفعال المتعلقة عمدا أو عن طريق الغش بتصميم أو تجميع أو نشر أو الاتجار في المعطيات المخزنة أو المعالجة أو المراسلة عن طريق منظومة معلوماتية، متى كانت قابلة لأن تستعمل في ارتكاب الجرائم المنصوص عليها في هذا القسم، كما تشمل الحماية الأفعال المتعلقة بالمعطيات المتحصلة من إحدى الجرائم المعلوماتية، من حيازة أو إفشاء أو نشر أو استعمال.

ويكتسي هذا التوجه أهمية خاصة في إطار حماية السيادة الرقمية، باعتبار أن سلامة الأنظمة المعلوماتية وحماية المعطيات من التغيير أو الإتلاف أو التداول غير المشروع تمثلان أحد المقومات

الأساسية للأمن الرقمي للدولة. كما أن تشديد العقوبات بموجب القانون رقم 24-06 يعكس اتجاهها نحو تعزيز الحماية الجنائية للبيئة الرقمية، ولا سيما في مواجهة الأفعال التي تهدد سلامة المعطيات والأنظمة المعلوماتية، وهو ما يمكن إدراجه ضمن الآليات القانونية التي تساهم بصورة غير مباشرة في حماية السيادة الرقمية للدولة.

- القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (القانون 09-04، 2009)، ويقصد بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وقد منح القانون السلطات المختصة صلاحيات قانونية لمراقبة الاتصالات الإلكترونية وتسجيلها، فضلا عن إجراء التفتيش والحجز داخل الأنظمة المعلوماتية وفق ضوابط محددة. كما نظم أحكام التعاون والمساعدة القضائية الدولية، وأقر اختصاص القضاء الجزائري بالنظر في بعض الجرائم الإلكترونية المرتكبة خارج الإقليم الوطني متى استهدفت مصالح الدولة الجزائرية أو أمنها أو اقتصادها الاستراتيجي (هشام، 2017، صفحة 200).

- القانون رقم 18-04 (القانون رقم 18-04، 2018) المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية: حيث استحدث هذا القانون سلطة ضبط، من بين مهامها السهر على احترام متعاملي البريد والاتصالات الإلكترونية للأحكام القانونية والتنظيمية المتعلقة بالبريد والاتصالات الإلكترونية والأمن السيبراني، كما نص على تجريم انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه، أو الإخبار بوجودها وتجرىم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة، ورصد القانون مجموعة من العقوبات ضمن المواد من 164 إلى 188 (مهدي، 2021، صفحة 121).

- القانون المتعلق بحماية المعطيات الشخصية للأشخاص الطبيعيين (القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين، 2018)، تمثلت أهداف هذا القانون في تحديد قواعد حماية الأشخاص

الطبيعيين ذات الطابع الشخصي في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة، وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم، وقد شددت أحكام هذا القانون على عدم إمكانية القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني الذي يمكنه التراجع عن ذلك في أي وقت. استثنى هذا القانون حسب المادة السادسة منه المعالجة من طرف شخص طبيعي لغايات لا تتجاوز الاستعمال الشخصي أو العائلي، شرط عدم إحالتها للغير أو نشرها، وكذا المعالجة لمصلحة الدفاع الوطني والوقاية من الجرائم ومتابعة مرتكبيها، وتميز هذا القانون بطابع تقني حيث نص على إنشاء سلطة وطنية لحماية المعطيات ذات الطابع الشخصي (يوسف، محمد، 2018، صفحة 117).

عزز المشرع الجزائري منظومة الحماية القانونية للمعطيات الشخصية من خلال القانون رقم 25-11 المؤرخ في 24 جويلية 2025 المعدل والمتمم للقانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. وقد جاء هذا التعديل لمواكبة التحولات التكنولوجية المتسارعة وما أفرزته من مخاطر جديدة على خصوصية الأفراد وأمن المعلومات، حيث استحدثت مجموعة من المفاهيم القانونية الحديثة، على غرار المعطيات البيومترية، والتنميط، واستعارة الهوية أو إخفاءها، وانتهاك المعطيات الشخصية، بما يسمح بتأطير قانوني أدق للمعاملات الرقمية الحديثة والتقنيات المعتمدة على الذكاء الاصطناعي وتحليل البيانات الضخمة.

كما استحدث المشرع منصب مندوب حماية المعطيات الشخصية الذي يتولى مراقبة مدى امتثال الجهات المعالجة لأحكام القانون، وتقديم المشورة القانونية والتقنية بشأن معالجة البيانات، والتنسيق مع السلطة الوطنية لحماية المعطيات الشخصية، وهو ما يعكس توجهها نحو تعزيز الحوكمة الرقمية وترسيخ ثقافة الامتثال داخل المؤسسات العمومية والخاصة.

ومن أهم المستجدات التي جاء بها التعديل استحداث نظام دراسة أثر المعالجة على حماية المعطيات الشخصية، والذي يفرض على المسؤول عن المعالجة تقييم المخاطر المحتملة التي قد تمس حقوق الأشخاص وحياتهم قبل الشروع في عمليات المعالجة عالية الخطورة أو المرتبطة

بتكنولوجيات جديدة. ويشكل هذا الإجراء آلية وقائية مهمة لتفادي الانتهاكات المحتملة وتقليل المخاطر المرتبطة بالأمن السيبراني .

وعلاوة على ذلك، فرض القانون التزاما بالإبلاغ عن خروقات المعطيات الشخصية، حيث يتعين على المسؤول عن المعالجة إخطار السلطة الوطنية المختصة خلال أجل لا يتجاوز خمسة أيام من تاريخ العلم بالخرق، مع إعلام الأشخاص المعنيين عندما يشكل هذا الخرق خطرا مرتفعا على حقوقهم وحرياتهم. ويجسد هذا الإجراء توجهها حديثا نحو تعزيز الثقة الرقمية ورفع مستوى الحماية ضد الهجمات السيبرانية وتسرب البيانات. كما أولى المشرع أهمية خاصة لمعالجة المعطيات ذات الطابع الشخصي لأغراض الوقاية من الجرائم والكشف عنها والتحقيق فيها ومتابعتها وتنفيذ العقوبات، واضعا إطاراً قانونياً يوازن بين متطلبات الأمن القومي ومقتضيات حماية الحياة الخاصة والحقوق الأساسية للأفراد.

وعلى صعيد السيادة الرقمية، وضع التعديل ضوابط أكثر دقة لنقل المعطيات الشخصية إلى الدول الأجنبية أو المنظمات الدولية، واشترط توفير مستوى كاف من الحماية القانونية والأمنية للبيانات المنقولة، بما يحد من مخاطر الاستغلال غير المشروع للمعطيات الوطنية ويعزز قدرة الدولة على التحكم في تدفقات البيانات العابرة للحدود.

وعليه، يمكن القول إن تعديل سنة 2025 يمثل خطوة نوعية في مسار تعزيز السيادة الرقمية الجزائرية، من خلال إرساء آليات أكثر فعالية لحماية المعطيات الشخصية، ورفع مستوى الأمن السيبراني، وتدعيم الثقة في البيئة الرقمية، بما يساهم في حماية المصالح الاستراتيجية للدولة وضمان ممارسة الحقوق والحريات الأساسية في الفضاء الرقمي.

الفرع الثاني: الحماية المؤسسية للسيادة الرقمية

في هذا الجانب عمدت الجزائر إلى استحداث مؤسسات متخصصة في مواجهة التهديدات السيبرانية بغية تعزيز أمنها القومي ومن ذلك نجد:

- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته

أنشئت هذه الهيئة بموجب المرسوم الرئاسي رقم 15-261 (المرسوم الرئاسي رقم 15-261، 2015) الذي حدد تشكيلتها وتنظيم سيرها للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتعتبر هذه الهيئة بموجب المادة الثانية من المرسوم المذكور أعلاه سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي وتوضع لدى الوزير المكلف بالعدل. تكلف الهيئة طبقاً لنص المادة 14 من القانون 09-04 تحت رقابة السلطة القضائية بالمهام التالية:

- اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- مساعدة السلطات القضائية ومصالح الشرطة في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

- القيام بموجب إذن من السلطات القضائية بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات كمساعدة لمصالح الشرطة القضائية المختصة بتحقيقات لجرائم خاصة ارتكبت أو سهل ارتكابها استعمال تكنولوجيا الإعلام والاتصال (هشام، 2017، الصفحات 203-204).

- مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية للدرك الوطني

تتمثل أهداف هذا المركز في تأمين منظومة المعلومات لخدمة الأمن العمومي، وهو بمثابة مركز توثيق يقوم بتحليل المعطيات والبيانات للجرائم المعلوماتية المرتكبة ومحاولة تحديد أصحابها مما يؤمن الأنظمة المعلوماتية للمؤسسات والبنوك والشركات، ويعمل على التنسيق الأمني بين الأجهزة الأمنية الأخرى (يوسف، 2018، صفحة 111).

-مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة

استحدثت القيادة العليا للجيش مصلحة الدفاع السيبراني ومراقبة الأنظمة بمحدف حماية الدولة من كافة التهديدات التي يشكلها الدفاع السيبراني على الأمن وعلى السيادة الرقمية للجزائر، مهمتها تخطيط وإدراج ومتابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية، التي تستهدف أنظمة المعلومات ومنظومة الاتصال وكذا منظومة الأسلحة للجيش. وتتمحور استراتيجية الدفاع السيبراني للجيش حول سبعة محاور وهي جانب وظيفي وتنظيمي، حتى تكون أعمال الدفاع السيبراني ضمن الجيش موجهة ومنفذة في إطار سلسلة وظيفية أو تنظيمية مكرسة لضمان تجانس وفعالية هذه الأعمال، والجانب القانوني المكلف بتحيين وتعزيز الإطار القانوني المتعلق باستعمال تكنولوجيا الإعلام والاتصال عموما وتأمين منظومات الإعلام خصوصا. كما تتضمن استراتيجية الدفاع السيبراني للجيش أيضا جانب الموارد البشرية، الذي يتطلب جاهزية مورد بشري تقني معتبر وذو كفاءة عالية في مجال الدفاع السيبراني هدفا أساسيا لكي تضمن نجاح إدخال هذا المجال في النشاطات العملياتية والتسيير للجيش، وأيضا الجانب التقني المكلف بتقوية وتكثيف القدرات التقنية للحماية والكشف والرد على الهجمات السيبرانية باستمرار، مع ضمان يقظة دائمة فيما يخص الطرق والوسائل المستعملة من طرف المهاجمين. أما الجانب الرابع للاستراتيجية فهو يتعلق بوقاية وتحسيس مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات التي تنجر عن استعمال تكنولوجيا الإعلام والاتصال في الإطار المهني أو الشخصي بطريقة مستمرة، فيما تضمن الجانب الخامس شق البحث والتطوير باستعمال وسائل تقنية خاصة ومشخصة من طرف هياكل البحث والتطوير للجيش الوطني الشعبي، لاسيما تلك المستعملة للحماية ضد التهديدات السيبرانية عنصرا حاسما في إستراتيجية الدفاع السيبراني، إلى جانب تعزيز التعاون في هذا المجال مع جيوش الدول الشريكة من أجل السماح لقوات الجيش الجزائري من الاستفادة من الخبرات والوسائل التكنولوجية المتقدمة، وبلغة الأرقام تجهض وزارة الدفاع الوطني يوميا 3500 محاولة اختراق لمواقع قيادات قواتها ومديرياتها المركزية، بمعدل 130 ألف محاولة اختراق في السنة، من قبل عصابات "الهacker" (نجمة، 2023، صفحة 82).

- المصلحة المركزية لمكافحة الجريمة المعلوماتية

أنشأت مصالح الأمن المصلحة المركزية لمكافحة الجريمة المعلوماتية سنة 2011، استجابة لمطلب الأمن المعلوماتي، وتعتمد هذه المصلحة على موارد بشرية لها الكفاءة المهنية ما يؤهلها لتنفيذ مهامها على المستوى الدولي من خلال التعامل مع المصالح المختصة (انتربول-أفريكوم) أو مصالح الشرطة لكبرى الدول، وعلى المستوى الوطني تتواصل هذه الهيئة مع الشرطة العلمية والمكاتب اللامركزية المختصة في الإجرام (الشرطة القضائية) (نجمة، 2023، صفحة 83).

من خلال ما سبق، يتضح أن حماية السيادة الرقمية لم تعد مسألة تقنية بحتة، بل أصبحت رهانا قانونيا وأمنيا واستراتيجيا يقتضي تضافر الجهود التشريعية والمؤسسية والتقنية. ورغم الخطوات التي اتخذتها الجزائر في هذا المجال، فإن تحقيق سيادة رقمية فعالة يظل مرتبطا بمدى القدرة على مواكبة التحولات التكنولوجية المتسارعة وتعزيز التنسيق بين مختلف الفاعلين المعنيين بحماية الفضاء السيبراني.

المطلب الثاني: الآليات الدولية والتجارب المقارنة في حماية السيادة الرقمية

تفرض الطبيعة العابرة للحدود للفضاء السيبراني تعزيز التعاون الدولي لمواجهة التهديدات الرقمية (الفرع الأول)، مع الاستفادة من التجارب المقارنة التي طورت نماذج مختلفة لحماية السيادة الرقمية (الفرع الثاني).

الفرع الأول: التعاون الدولي في مواجهة التهديدات السيبرانية

إن مسألة الحفاظ على السيادة الوطنية واسترجاعها في مواجهة النشاطات غير المشروعة هي مسألة معترف بها من طرف الجميع، وهي تفوق الحدود الوطنية وتتخطاها ولا يمكن التصدي لها إلا بالتعاون الدولي، لذلك عملت الدول على إيجاد آليات تشريعية ومؤسسية من أجل تحقيق مواجهة فعالة لمهددات السيادة الرقمية.

أولاً: جهود منظمة الأمم المتحدة للدفاع عن السيادة الرقمية

بذلت الهيئة الأمية جهوداً في سبيل العمل على مكافحة الجرائم المعلوماتية وذلك لما تسببه هذه الجرائم من خسائر اقتصادية ومشاكل سياسية واجتماعية خطيرة، حيث أصدرت منظمة الأمم المتحدة عبر جمعيتها العامة عدداً من القرارات التي توضح مدى تصاعد الاهتمام العالي باستخدام تكنولوجيا الإعلام والاتصال استخداماً غير سلمي إلى جانب عقدتها لمجموعة من المؤتمرات لذات الغرض.

- جهود منظمة الأمم المتحدة للدفاع عن السيادة الرقمية من خلال قراراتها

أعربت الجمعية العامة للأمم المتحدة من خلال القرار رقم 54/49 عن قلقها من احتمال استخدام تكنولوجيا المعلومات والاتصالات السلوكية واللاسلكية في أغراض لا تتفق وأهداف صون الاستقرار والأمن الدولي. حيث ترى الجمعية العامة ضرورة تكثيف التعاون الدولي من أجل منع إساءة استخدام موارد أو تكنولوجيا المعلومات أو استغلالها في تحقيق أغراض إجرامية أو إرهابية. ثم جاء القرار رقم 65/63 يحمل مجموعة من التدابير الرامية إلى مكافحة هذا النوع من إساءة الاستعمال نذكر منها:

أ- ينبغي على الدول أن تكفل عدم توفير قوانينها وممارساتها ملاذاً للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية.

ب- ينبغي أن تتبادل الدول المعلومات المتعلقة بالمشاكل التي تواجهها في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

ج- ينبغي تدريب العاملين في مجال إنفاذ القوانين وتجهيزهم بما يمكن من مكافحة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

- جهود منظمة الأمم المتحدة للدفاع عن السيادة الرقمية من خلال مؤتمراتها

ظهرت جهود المنظمة الأمية في حماية السيادة الرقمية من خلال مؤتمراتها بدءاً بالمؤتمر السابع عام 1985 المنعقد في إيطاليا والذي انبثقت عنه مجموعة من القواعد التوجيهية التي

اكتملت صياغتها في الاجتماعات الإقليمية التحريرية للمؤتمر الثامن، تدور حول وجوب حماية الانسان في حياته الخاصة، وتحسين أمن الحاسب الآلي وزيادة التعاون الدولي من أجل مكافحة هذه الجرائم (مراد، 2022، صفحة 1597).

ثانيا: دور الاتفاقيات الدولية في مكافحة الجرائم السيبرانية.

من أهم الاتفاقيات الدولية التي تم إبرامها في هذا الإطار "اتفاقية بودابست" في 23 نوفمبر 2001، حيث أكد من خلالها مجلس أوروبا والدول الأخرى الموقعة عليها على التغيرات العميقة التي أدت إلى ظهور فضاء جديد يسمى بالفضاء المعلوماتي الذي يستخدم لأغراض مشروعة، غير أنه بالإمكان استخدامه في ارتكاب أعمال إجرامية، الأمر الذي يتطلب مواكبة هذا التطور بقوانين جنائية تواكب هذه التكنولوجيات واستخداماتها في البيئة الرقمية. إلى جانب ذلك تناولت الاتفاقية الإرهاب الإلكتروني وحددت أفضل الطرق الواجب اتباعها في جرائم الانترنت التي تعهدت الدول الموقعة بالتعاون من أجل محاربتها (حكيم، 2021، صفحة 661).

الفرع الثاني: التجارب المقارنة في حماية السيادة الرقمية

شهدت العديد من الدول تجارب متباينة في حماية السيادة الرقمية، اختلفت باختلاف تصوراتها لمتطلبات الأمن والسيادة الرقمية وطبيعة بنيتها التكنولوجية، وهو ما يبرز من خلال النماذج الصينية والروسية والإستونية.

أولا: النموذج الصيني القائم على الرقابة التقنية

تعتبر التجربة الصينية في بناء "جدار الحماية العظيم" أو "الجدار الناري العظيم - Great Firewall of China" نظام رقابة وإنترنت متقدم تستخدمه الحكومة الصينية للتحكم في الوصول إلى الإنترنت داخل البلاد، ويهدف هذا الجدار إلى منع الوصول إلى مواقع إلكترونية أجنبية محددة، وتصفية المحتوى غير المرغوب فيه من منظور السلطات الصينية، بالإضافة إلى مراقبة النشاط على الإنترنت، إذ يقوم بحجب مواقع الإنترنت والعديد من المواقع العالمية مثل غوغل، وفيسبوك، وتويتر، ويوتيوب، وتطبيقات أخرى يعتبر أنها تحتوي على محتوى يتعارض مع سياسات الحكومة الصينية. فضلا عن مراقبة النشاط على الأنترنت وتصفية المحتوى. يقوم

الجدار بمنع ظهور المحتويات التي تعتبر حساسة أو غير ملائمة، بالإضافة إلى تحكم صارم في الاتصالات الخارجية عبر استخدام تقنيات متقدمة مثل التصفية العميقة لحزم البيانات (DPI) لمنع الوصول إلى أدوات تجاوز الرقابة مثل الشبكات الافتراضية الخاصة (VPN) ، لحماية فضائها السيبراني وحماية سيادة الصين الرقمية (Ensafi, Winter, Mueen, Crandall, 2015, p. 61).

بالرغم من أن التجربة الصينية تبرز كنموذج يقوم على تعزيز السيادة الرقمية من خلال التحكم في البنية التحتية الرقمية والبيانات الوطنية، وهو ما مكّن الدولة من تقليص درجة التبعية للمنصات الأجنبية. غير أن هذا النموذج يثير نقاشا حول مدى التوفيق بين متطلبات الأمن والسيادة الرقمية من جهة، وضمان حرية تداول المعلومات والحقوق الرقمية من جهة أخرى، الأمر الذي يجعل الاستفادة منه مشروطة بمراعاة الخصوصيات الدستورية والقانونية لكل دولة.

ثانيا: النموذج الروسي القائم على التحكم في البنية التحتية

قامت روسيا بتنفيذ نظام يعرف بـ"الجدار الناري الروسي" أو "الإنترنت السيادي"، للتحكم في الوصول إلى الإنترنت وتنظيم المحتوى داخل البلاد، وهو عبارة عن منظومة رقابة وسيطرة رقمية تهدف إلى إخضاع فضاء الإنترنت الروسي (Runet) لسيطرة الدولة، من خلال إنشاء بنية تحتية تسمح بالتحكم المركزي في تدفقات البيانات، وتصفية وحجب المحتوى والمواقع، ومراقبة نشاط المستخدمين. شهدت عملية فرض السيطرة على الإنترنت الروسي (Runet) تطورا تدريجيا، حيث سعت السلطات الروسية إلى بناء نموذج يقوم على "السيادة الرقمية" من خلال إنشاء بنية تحتية تسمح بالتحكم المركزي في تدفقات البيانات على الإنترنت. وقد شكّل قانون "الإنترنت السيادي" لسنة 2019 نقطة تحول أساسية، إذ ألزم مشغلي الاتصالات بتطبيق وسائل تقنية لمواجهة التهديدات، تقوم بتصفية وحجب حزم البيانات بشكل مركزي .

وتتولى هيئة الرقابة الفيدرالية الروسية للاتصالات وتقنية المعلومات والإعلام (Roskomnadzor) الدور الرئيسي في تنفيذ الرقابة، بمشاركة مؤسسات أخرى، خاصة أجهزة الأمن وعلى رأسها جهاز الأمن الفيدرالي (FSB) (Domańska, Chawryło, 2025,)

(12. p، يعكس النموذج الروسي إدراكا متزايد لأهمية الفضاء الرقمي باعتباره أحد مكونات السيادة الوطنية. غير أن تحقيق هذا الهدف يتطلب استثمارات ضخمة وقدرات تقنية متقدمة، وهو ما قد يشكل تحدياً بالنسبة للدول النامية.

ثالثا: النموذج الإستوني القائم على الوعي الرقمي والأمن السيبراني

أما إستونيا فتستخدم لحماية سادتها ما تسميه "العدوان الرقمي"، وتعليم "محو الأمية الإعلامية" لمساعدة مواطنيها على اكتشاف المعلومات المضللة والحذر منها. ومنذ عام 2010، تقدم المدارس العامة الإستونية -من روضة الأطفال حتى المدرسة الثانوية- لتلاميذها دروسا في محو الأمية الإعلامية، ويشارك الطلاب في الصف العاشر أيضا في دورة إلزامية مدتها 35 ساعة حول "لإعلام وتأثيره" (أماي، صفحة 173).

إلى جانب ذلك تعتمد إستونيا في مواجهة الهجمات السيبرانية على مجموعة من الآليات الأمنية المتكاملة، أبرزها نموذج الثقة الصفرية (Zero Trust) القائم على التحقق المستمر من هوية المستخدمين والأجهزة وعدم منح الثقة بشكل تلقائي. كما تبني مبدأ الأمن منذ التصميم (Security by Design) من خلال إدماج متطلبات الأمن السيبراني في جميع مراحل تطوير الأنظمة والخدمات الرقمية. وإلى جانب ذلك، تعمل على تعزيز الحماية عبر الدرع السيبراني الوطني (Cyber-Shield) ومركز العمليات الأمنية (SOC) لضمان الرصد المستمر للتهديدات والكشف المبكر عن الهجمات والاستجابة الفعالة لها. (Communications, 2024, pp. 17-20).

خاتمة

ختاما يمكن القول إن حماية السيادة الرقمية أضحت من أهم أولويات الدول لارتباطها الوثيق بأمن المعلومات والمعطيات ذات الطابع السياسي والاقتصادي والاجتماعي، خاصة بعد الانتشار الواسع لاستخدام الانترنت التي تخطت الحدود الجغرافية وما نتج عن هذا التطور التكنولوجي لوسائل الإعلام والاتصال من تهديدات للسيادة الرقمية، فأضحت القرصنة والإرهاب الإلكتروني، سرقة وتدمير المعلومات، والتجسس الإلكتروني، جرائم تشكل خطرا كبيرا

على الأمن القومي للدول. وقد خُطت هذه الأخيرة خطوات هامة في إطار مواجهة هذه التهديدات سواء على المستوى الوطني أو الدولي وما تقدم نخرج بالنتائج التالية:

- أصبحت كل دول العالم مطالبة بإعلان سيادتها الرقمية على كامل أراضيها وحماية البنية الرقمية من كافة أشكال الاختراق لما لذلك من تأثير على الأمن القومي للدول وتحقيق السلم والاستقرار الدوليين.

- يعتبر الفضاء الإلكتروني في الوقت الحالي من أكثر الفضاءات أهمية من الناحية الاستراتيجية والأكثر عرضة للاختراق، فقد باتت الجرائم الإلكترونية تهدد أمن المعلومات للقطاعات الحيوية على رأسها القطاع العسكري، قطاع المال والأعمال والقطاع الاقتصادي، الأمر الذي يستدعي وضع استراتيجيات مضادة لحماية السيادة الرقمية وتحقيق الأمن السيبراني.

- من أهم معوقات حماية السيادة الرقمية لمعظم الدول غياب استراتيجية وطنية واضحة لحماية الفضاء الإلكتروني.

- بذلت الجزائر جهودا حثيثة لحماية سيادتها الرقمية من خلال استراتيجية تعتمد على جانبين: جانب قانوني مبني على إيجاد منظومة قانونية تعمل على تحقيق الأمن المعلوماتي وتحسين السيادة الرقمية، وجانب مؤسسي يعتمد على مجموعة من الهيئات القانونية والأمنية تعمل على حماية تكنولوجيا الإعلام والاتصال من التهديدات السيبرانية.

- سعت المنظمات الدولية والإقليمية إلى عقد مؤتمرات وإصدار قرارات وإبرام العديد من الاتفاقيات الدولية لغرض حماية الأمن القومي من مختلف التهديدات وتحقيق السيادة الرقمية للدول.

وعليه نوصي بما يلي:

- وضع مقارنة أمنية وقانونية شاملة لحماية السيادة الرقمية تأخذ بعين الاعتبار تنوع مصادر وطرق التهديد الأمني.

- عدم الاقتصار عند التجريم والعقاب على أنماط السلوك التي تشكل تهديدا للأمن القومي المرتكبة في الوقت الحالي بل يجب مراعاة الأبعاد المستقبلية بالاعتماد على الدراسات الاستشرافية، لأن تكنولوجيا المعلومات في تطور سريع.
- تعزيز القدرات التقنية والبشرية للهيئات المكلفة بحماية الفضاء الرقمي وتطوير آليات الرصد والاستجابة للتهديدات السيبرانية .
- نشر الوعي والثقافة الرقمية لدى الأفراد والمؤسسات باعتبارها خط الدفاع الأول في مواجهة المخاطر السيبرانية.
- تشجيع الاستثمار في التكنولوجيات الوطنية والبنى التحتية الرقمية للحد من مظاهر التبعية التكنولوجية الخارجية وتعزيز الاستقلال الرقمي للدولة.
- دعم التعاون الدولي والإقليمي في مجال تبادل المعلومات والخبرات وتنسيق الجهود التشريعية والأمنية لمكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني.
- بالنظر لكون مهددات السيادة الرقمية تتجاوز حدود الدولة الجغرافية، يتعين تعزيز التعاون الدولي في مجال تبادل المعلومات والخبرات الأمنية لمكافحة التهديدات الأمنية، وكذلك تنسيق القوانين الجزائية العالمية بما يؤدي إلى تشديد إحكام قبضة العدالة على المجرمين مهما كان مكان تواجدهم.

-قائمة المراجع

أولاً: النصوص القانونية

- الجزائر. (16 غشت 2009). القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية، العدد 47.
- الجزائر. (8 أكتوبر 2015). المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015. الجريدة الرسمية، العدد 53.
- الجزائر. (13 ماي 2018). القانون رقم 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية. الجريدة الرسمية، العدد 27.
- الجزائر. (10 يونيو 2018). القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المعدل والمتمم. الجريدة الرسمية، العدد 34.
- الجزائر. (2024) القانون رقم 24-06 المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات. الجريدة الرسمية العدد 30.

ثانياً: الكتب

- أحمد مراد. (بلا تاريخ). السيادة الرقمية. دار الفكر للنشر.
- الغفيلي فهد بن عبد العزيز. (بلا تاريخ). الإعلام الرقمي ماهيته أنواعه آثاره.

ثالثاً: المقالات العلمية

أ-باللغة العربية

- إيدابير، أحمد. (2020). استخدام التكنولوجيا للحماية من التهديدات الأمنية الجديدة العابرة للحدود (الحدود الذكية نموذجاً). مجلة آفاق علمية.
- العلي، ناصر. (2021). الجهود الدولية في مكافحة الإرهاب الإلكتروني. مجلة الباحث للدراسات الأكاديمية.

- القحطاني، منصور بن سعيد. (2008). مهددات الأمن المعلوماتي وسبل مواجهتها. السعودية: جامعة نايف العربية للعلوم الأمنية.
- أماني عصام محمد. (2021). استخدام روسيا للقوة السيبرانية في إدارة التفاعلات الدولية . دراسات.
- حسن، محمود. (2023). أثر التهديدات السيبرانية على الأمن القومي: دراسة حالة ماليزيا . (2022-2015)المعهد الوطني الديمقراطي.
- جباب الله، حكيمة. (2021). انعكاسات الجريمة السيبرانية على الجريمة الرقمية: دراسة في آليات واستراتيجيات مكافحتها .حوليات جامعة الجزائر 1.
- مهدي، رضا. (2021). الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري .مجلة إيليزا للبحوث والدراسات.
- عواشيرة رقية، بن سيدهم حورية. (2020). الأمن الفضائي السيبراني: التحديات والحلول . المجلة الجزائرية للأمن الإنساني.
- سنوسي، علي. (2024). السيادة الرقمية والاستقلال التكنولوجي بين تحديات الظروف الوطنية والدولية .المجلة الجزائرية للحقوق والعلوم السياسية.
- رصاع، فتيحة. (2012-2011). الحماية الجنائية للمعلومات على شبكة الإنترنت. تلمسان: جامعة أبي بكر بلقايد.
- بعوني، ليلي. (2021). التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة نموذجا .مجلة استراتيجيا.
- سليمان، مباركة. (2017). الإرهاب الإلكتروني وطرق مكافحته .مجلة الحقوق والعلوم السياسية، 340.355-

-قريبيز، مراد. (2022). تحديات الإنترنت لسيادة الدول (السيادة الرقمية). مجلة البحوث القانونية والاقتصادية.

-شريط، نجمة. (2023). الأمن السيبراني في العقيدة الدفاعية الجزائرية: الفرص والقيود. المجلة الجزائرية للسياسة والأمن.

-بخوش، هشام. (2017). الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في ظل التشريع الجزائري. مجلة الحقوق والعلوم السياسية.

-بوغرارة، يوسف. (2018). الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني. مجلة الدراسات الإفريقية وحوض النيل.

-زروق يوسف، العيداني محمد. (2018). حماية المعطيات الشخصية في الجزائر على ضوء القانون 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. مجلة معالم للدراسات السياسية والقانونية.

ب- باللغة الإنجليزية

-Crilley, R. (2019). *Cyberwar: How Russian Hackers and Trolls Helped Elect aPresident—What We Don't, Can't, and Do Know*. *Journal of Communication*, Vol. 00,, E1–E3.

-John J, K. (2015). *Deterring and Dissuading Cyberterrorism*. *Journal of Strategic Security* 8, no. 4,23-38.

-Ensafi, Winter, Mueen, Crandall, R. (2015). *Analyzing the Great Firewall of China Over Space and Time*. *Proceedings on Privacy Enhancing Technologies*, 61–76.

-Estonian Ministry of Economic Affairs and Communications. *Cybersecurity Strategy 2024–2030: Cyber-Conscious Estonia*. Tallinn: Ministry of Economic Affairs and Communications, 2024.

-Crime, U. N. (2024). *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*. Vienna. UNODC.

-Domańska, M., & Chawryło, K. (2025). *The Great Russian Firewall: The Kremlin's Ultimate Crackdown on Internet Freedom*. Centre for Eastern Studies (OSW).