



قوائم المحتويات متاحة على ASJP المنصة الجزائرية للمجلات العلمية
الأكاديمية للدراسات الاجتماعية والإنسانية
الصفحة الرئيسية للمجلة: www.asjp.cerist.dz/en/PresentationRevue/552



إشكالية الموازنة بين متطلبات الأمن السيبراني و ضمان الحقوق الفردية

The Challenge of Balancing Cybersecurity Requirements With the Protection of Individual Rights

د. عروس كوثر^{1*}، د. عروس فوزية².

¹ جامعة طاهري محمد بشار.

² جامعة طاهري محمد بشار.

Key words:	Abstract
Cybersecurity Individual Rights Privacy and Data Protection Freedom of Expression Principle of Proportionality.	This research aims to examine the challenge of balancing cybersecurity requirements with the protection of individual rights, as both represent essential pillars for building a safe and fair digital society. With the growing threat of cybercrime and attacks targeting critical infrastructures, strengthening cybersecurity has become a strategic necessity. However, this approach may endanger citizens' constitutional rights, particularly the right to privacy and freedom of expression. Based on this dilemma, the research adopts a descriptive-analytical methodology supported by comparative analysis of national and international legal frameworks, while relying on the general principles of human rights. The study concludes that achieving the desired balance requires a legislative approach grounded in the principle of proportionality, coupled with effective mechanisms of judicial oversight and good governance. The results emphasize that cybersecurity cannot succeed without respecting fundamental rights, just as the protection of those rights depends on the existence of a secure and trustworthy cyberspace.

ملخص	معلومات المقال
	تاريخ المقال:
	الإرسال: 2025-09-21
	القبول: 2026-01-11
	الكلمات المفتاحية:
	الأمن السيبراني
	حقوق الأفراد
	الخصوصية وحماية البيانات
	حرية التعبير
	مبدأ التناسب.
يهدف هذا البحث إلى دراسة إشكالية الموازنة بين متطلبات الأمن السيبراني و ضمان الحقوق الفردية، باعتبار أن كلاهما يشكلان ركيزة أساسية لبناء مجتمع رقمي آمن وعادل، فمع تنامي الجرائم الإلكترونية والهجمات الموجهة ضد البنى التحتية الحيوية، أصبح تعزيز الأمن السيبراني ضرورة استراتيجية، غير أن هذا التوجه قد يهدد الحقوق الدستورية للمواطنين، خاصة الحق في الخصوصية و حرية التعبير، وانطلاقاً من هذا الإشكال، اعتمد البحث على منهج تحليلي-وصفي قائم على المقارنة بين الأطر القانونية الوطنية والدولية، مع الاستناد إلى المبادئ العامة لحقوق الإنسان، وقد خلصت الدراسة إلى أن تحقيق التوازن المنشود يقتضي تبني مقاربة تشريعية قائمة على مبدأ التناسب، مقرونة بآليات فعالة للرقابة القضائية والحوكمة الرشيدة، وتؤكد النتائج أن الأمن السيبراني لا يمكن أن ينجح في غياب احترام الحقوق الفردية، كما أن حماية هذه الحقوق تظل رهينة بوجود فضاء سيبراني آمن وموثوق.	

1. مقدمة

أفرزت الثورة الرقمية المتسارعة تحولات عميقة مست مختلف مناحي الحياة الإنسانية، حيث أصبح الفضاء السيبراني مكونا أساسيا في النشاط الاقتصادي والاجتماعي والسياسي، وأداة لا غنى عنها في تسير المرافق العامة، وتبادل المعلومات، وممارسة الحقوق والحريات الأساسية.

غير أن هذا التطور التكنولوجي، ورغم ما يحمله من فرص هائلة للتنمية والتقدم، صاحبه بروز تهديدات سيبرانية متزايدة، تمثلت في الجرائم الإلكترونية، والاختراقات المعلوماتية، والهجمات الموجهة ضد البنى التحتية الحيوية، الأمر الذي جعل مسألة الأمن السيبراني إحدى الأولويات الاستراتيجية للدول في العصر الرقمي.

وفي مقابل هذا التوجه المتصاعد نحو تعزيز الأمن السيبراني، برزت إشكالية قانونية وحقوقية لا تقل أهمية، تتعلق بمدى تأثير التدابير الأمنية الرقمية على الحقوق الفردية، ولا سيما الحق في الخصوصية، وحماية المعطيات ذات الطابع الشخصي، وحرية التعبير، والحق في الوصول إلى المعلومات، إذ قد يؤدي التوسع غير المنضبط في آليات المراقبة الرقمية وجمع البيانات، تحت مبرر مكافحة التهديدات السيبرانية، إلى المساس بجوهر هذه الحقوق، وتحويل الفضاء الرقمي إلى مجال للمراقبة والتقييد بدل أن يكون فضاء للحرية والتمكين.

ومن هنا، تبرز إشكالية التوازن بين متطلبات الأمن السيبراني وضمان الحقوق الفردية باعتبارها إحدى أعقد الإشكاليات التي تواجه التشريعات المعاصرة، خاصة في ظل الطابع العابر للحدود الذي يميز الفضاء السيبراني، وصعوبة إخضاعه للقواعد التقليدية للسيادة والاختصاص القضائي، فالتشدد المفرط في التدابير الأمنية قد يؤدي إلى تقويض الثقة بين المواطن والدولة، في حين أن إهمال مقتضيات الأمن السيبراني قد يفتح المجال أمام فوضى رقمية تهدد استقرار المجتمعات وأمنها القومي.

وانطلاقا من ذلك، تتمحور إشكالية هذا البحث حول التساؤل الآتي: إلى أي مدى يمكن تحقيق توازن فعلي بين متطلبات الأمن السيبراني وضمان الحقوق الفردية؟

وما هي الآليات القانونية الكفيلة بضمان عدم تغليب البعد الأمني على حساب الحقوق الفردية في البيئة الرقمية؟

ويتفرع عن هذه الإشكالية عدد من التساؤلات الفرعية المتعلقة بحدود تدخل الدولة في الفضاء السيبراني، ودور التشريع والقضاء في ضبط هذا التدخل، ومدى فعالية الأطر القانونية الوطنية والدولية في تكريس هذا التوازن، وهي كما يلي:

ما حدود تدخل الدولة في الفضاء السيبراني لحماية الأمن دون المساس بجوهر حقوق الأفراد؟

ما هي الآليات القانونية والمؤسسية الكفيلة بضمان هذا التوازن؟

إلى أي مدى نجحت التجارب المقارنة في تحقيق الموازنة بين الأمن السيبراني والحقوق الفردية؟

وما هو واقع الإطار القانوني الجزائري وإمكانات تطويره في هذا المجال؟

وتتجلى أهمية هذا البحث في كونه يعالج موضوعا راهنا يكتسي أبعادا قانونية وحقوقية واستراتيجية، لاسيما بالنسبة للدول النامية، التي تسعى إلى تعزيز أمنها السيبراني وفي الوقت ذاته الالتزام بالمعايير الدولية لحماية حقوق الإنسان.

كما تبرز أهمية الدراسة من خلال محاولتها تقديم قراءة تحليلية نقدية للإطار القانوني الجزائري، في ضوء التجارب المقارنة، بما يسمح باستخلاص آليات عملية يمكن أن تسهم في بناء نموذج وطني متوازن للأمن السيبراني.

ولتحقيق أهداف البحث والإجابة عن إشكاليته، تم الاعتماد على المنهج الوصفي التحليلي، المدعوم بالمنهج المقارن، من خلال تحليل النصوص القانونية الوطنية والدولية، والاتفاقيات ذات الصلة، إلى جانب استعراض بعض التجارب المقارنة البارزة، ولا سيما النموذج الأوروبي والأمريكي والصيني، بهدف إبراز أوجه التباين في مقاربات الموازنة بين الأمن والحقوق.

وبناء على ذلك، تم تقسيم البحث إلى محورين رئيسيين، يتناول الأول الإطار المفاهيمي والنظري للأمن السيبراني والحقوق الفردية كمدخل لفهم إشكالية الموازنة، في حين يخصص المحور الثاني لدراسة إشكالية التوازن بينهما من خلال التجارب المقارنة، ثم تحليل الإطار الوطني الجزائري وإمكانات تطويره بما يضمن تحقيق التوازن المنشود.

1. الإطار المفاهيمي للأمن السيبراني والحقوق الفردية كمدخل لفهم إشكالية الموازنة

يشكل الأمن السيبراني في الوقت الراهن أحد أبرز التحديات التي تواجه الدول، وذلك بالنظر إلى ما يشهده العالم من توسع غير مسبوق في استخدام التكنولوجيا الرقمية والاعتماد المتزايد على شبكات المعلومات في مختلف القطاعات، وهذا الواقع الجديد أفرز تهديدات سيبرانية عابرة للحدود، تطل الأفراد والمؤسسات وحتى الأمن القومي للدول.

وعليه فإن تناول إشكالية التوازن بين الأمن السيبراني والحقوق الفردية تقتضي الوقوف بداية عند الإطار المفاهيمي المنظم لهذين المفهومين، باعتبار أن غياب الدقة في تحديد مدلولاتهما يؤدي إلى اضطراب في المقاربة القانونية للموازنة بينهما، إلى جانب استيعاب مضمون الحقوق الفردية في البيئة الرقمية، يشكل مدخلا ضروريا لتحديد نطاق التوازن الممكن بين متطلبات الحماية الأمنية وضمانات الحقوق والحريات.

2. 1. مفهوم الأمن السيبراني وأبعاده القانونية

مع تزايد الاعتماد على الفضاء الرقمي تزايدت أيضا المخاطر المرتبطة بالاخترقات والجرائم الإلكترونية، ما فرض على الدول وضع أطر قانونية تحكم كيفية التصدي لهذه التهديدات دون الإخلال بحقوق الأفراد الأساسية.

ومن هنا يكتسي البحث في مفهوم الأمن السيبراني وأبعاده أهمية بالغة، لأنه يشكل الأساس الذي تبنى عليه السياسات العمومية والآليات التشريعية لتحقيق التوازن بين متطلبات الحماية والالتزام بالمعايير الحقوقية.

أ/ تعريف الأمن السيبراني:

يعد الأمن السيبراني من المفاهيم الحديثة نسبيا التي برزت نتيجة التحول الرقمي العالمي والاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات في جميع القطاعات الحيوية، بدءا من الإدارة الحكومية مروراً بالقطاع المالي وصولاً إلى الأمن القومي.

ويعرف الأمن السيبراني بأنه: " وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة " (العمارات، 2022، صفحة 15)

وهناك من عرفه بأنه: " ممارسة الدفاع عن أجهزة الكمبيوتر، والخوادم، والأجهزة المحمولة، والأنظمة الإلكترونية، والشبكات، والبيانات، من الهجمات الخبيثة " (اللقاني، 2022، صفحة 162)

ويعرف أيضا بأنه: " مجموعة من العمليات التفاعلية المصممة لحماية الفضاء السيبراني والأنظمة الممكنة تقنيا من التهديدات التي تؤثر على نزاهتها وتؤدي إلى التدخل في حقوق الملكية، مما يؤدي إلى بعض الخسارة " (Schiliro, 2023).

وتكتسي هذه التعريفات أهمية خاصة في إطار بحث إشكالية الموازنة، لأنه يحدد نطاق التدخل الأمني الذي يجب ألا يتجاوز الحدود اللازمة لحماية الحقوق الفردية.

وأما في السياق القانوني، فقد تبنت العديد من التشريعات تعريفات مختلفة للأمن السيبراني، لكنها تتقاطع في عناصر أساسية هي: حماية سرية المعلومات، ضمان سلامة الأنظمة، واستمرارية الخدمات الرقمية.

فالقانون الأوروبي للأمن السيبراني (Cybersecurity Act 2019) مثلاً عرفه باعتباره:

" قدرة الشبكات والأنظمة على مقاومة الأحداث السيبرانية التي قد تؤثر على توافر الخدمات أو مصداقية البيانات أو سريتها " (Commission, 2023)

بينما عرفته بعض التشريعات العربية، مثل القانون المغربي رقم 05-20 المتعلق بالأمن السيبراني، نص في المادة 02 منه:

"الأمن السيبراني هو مجموع التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكوينات وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات أن يقاوم أحداثاً مرتبطة بالفضاء السيبراني، من شأنها أن تمس بتوافر وسلامة وسرية المعطيات المخزنة أو المعالجة أو المرسل، والخدمات ذات الصلة التي يقدمها هذا النظام أو تسمح بالتولوج إليه" (05، 20، 25 يوليو 2020)

كما تضمنت نفس المادة تعريفا لمفاهيم أخرى مهمة مثل البنيات التحتية ذات الأهمية الحيوية الجرمية السيبرانية و التهديد السيبراني.

وعرفه القانون الأردني رقم 16 لسنة 2019 المتعلق بالأمن السيبراني بأنه :

"الإجراءات المتخذة لحماية الأنظمة والشبكات والمعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني، والقدرة على استعادة عملها واستمراريته سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الإخلال باتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك " (16، 2019).

وبالرجوع للتشريع الجزائري فلا نجد حتى الآن نص قانوني صريح يعرف "الأمن السيبراني" تعريفا قانونيا شاملا.

وانطلاقا مما تقدم يمكن القول أن تعريف الأمن السيبراني وإن كان قد حظي باهتمام متزايد في التشريعات المقارنة والفقه، إلا أن تعدد التعريفات يكشف عن إشكالية حقيقية في توحيد الرؤية، فالتعريف الأوروبي الوارد في لائحة 2019 يعد من أكثر التعريفات دقة وشمولا، إذ جمع بين الجوانب التقنية والتنظيمية، وركز على حماية سرية وسلامة وتوافر الأنظمة والمعلومات، غير أن هذا التعريف يظل تقنيا بالأساس، ولا يولي أهمية كافية للبعد الحقوقي المتعلق بحماية الأفراد وحقوقهم الرقمية.

وأما بخصوص التعريفات الفقهية، فهي منقسمة بين اتجاه تقني ضيق ينظر إلى الأمن السيبراني كوسائل وبرامج دفاعية لمواجهة الهجمات، واتجاه آخر موسع يراه منظومة قانونية ومؤسسية تتجاوز الجانب الأمني لتشمل السياسات العامة والوقاية والتثقيف الرقمي.

وقوة هذه التعريفات تكمن في إظهار شمولية الأمن السيبراني كإطار متكامل، لكن ضعفها يتجلى في غياب معيار موحد، مما قد يخلق التباسا عند التطبيق العملي.

وفي السياق العربي، نجد أن معظم التشريعات لم تصغ تعريفا واضحا، بل اكتفت بذكره ضمنيا في قوانين مكافحة الجريمة الإلكترونية، باستثناء بعض التجارب كالمغرب والأردن التي حاولت تقديم تعريفات صريحة، لكنها بدورها إما كانت تقنية بحتة أو عامة وفضفاضة، وأما الجزائر، فلا تزال تفتقر إلى تعريف رسمي، ما يترك فراغا تشريعيا يزيد من صعوبة وضع سياسة وطنية فعالة للأمن السيبراني.

ولمواجهة هذه التحديات، برزت عدة اتجاهات: الأول يتمثل في توسيع الاختصاص الإقليمي للمحاكم الوطنية بحيث ينعقد الاختصاص كلما ظهرت آثار الفعل في إقليمها، وهو ما يطبق مثلا في قضايا الجرائم العابرة للحدود، أما الاتجاه الثاني فيسعى إلى تعزيز التعاون القضائي الدولي من خلال الاتفاقيات الثنائية والمتعددة الأطراف، كاتفاقية بودابست حول الجرائم السيبرانية.

غير أن فعالية هذه الآليات ظلت محدودة، إذ ظل غياب إطار دولي شامل ومتوافق عليه لفترة طويلة يشكل عائقا حقيقيا أمام مكافحة الجريمة السيبرانية.

وانطلاقا مما تقدم فإن تحدي الاختصاص القضائي في الفضاء السيبراني يكشف عن قصور النظم القانونية التقليدية في استيعاب واقع جديد تحكمه التكنولوجيا، ولا يمكن تجاوز هذا التحدي إلا عبر تطوير مقاربة مزدوجة: تحديث التشريعات الوطنية لتكون أكثر شمولاً، وفي الوقت نفسه تعزيز التعاون الدولي لإرساء قواعد واضحة ومشاركة فالفضاء السيبراني بطبيعته لا يعرف الحدود، ومن ثمة فإن معالجته القانونية تتطلب فكرا يتجاوز الحدود التقليدية للسيادة الوطنية.

2. ضعف التنسيق الدولي:

يمثل الفضاء السيبراني مجالا عالميا مفتوحا تتقاطع فيه المصالح الأمنية والاقتصادية والسياسية للدول، غير أن ما يميزه أيضا هو هشاشة الإطار القانوني والمؤسسي المنظم له على المستوى الدولي، فضعف التنسيق بين الدول في مواجهة التهديدات السيبرانية يعد من أخطر التحديات، إذ يكشف عن قصور في النظام الدولي القائم وعجزه عن التعامل مع فضاء لا تحده الجغرافيا ولا تعترف به الحدود.

أول أبعاد هذا الضعف يتمثل في غياب معاهدة دولية شاملة وملزمة فحتى الآن، لا يوجد إطار موحد يحكم سلوك الدول في الفضاء السيبراني، باستثناء بعض المبادرات الجزئية مثل اتفاقية بودابست لسنة 2001 الخاصة بالجرائم الإلكترونية.

ولكن ورغم الأهمية البالغة لاتفاقية بودابست لسنة 2001 في تعزيز التعاون القضائي الدولي لمكافحة الجرائم السيبرانية، إن محدودية نطاقها الجغرافي وعدم انضمام عدد معتبر من الدول إليها، خاصة من العالم النامي، ظل يشكل عائقا أمام بناء إطار دولي شامل وموحد لمواجهة الجريمة السيبرانية.

وفي هذا السياق، جاءت اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية (Nations, 2024) تشكل تحولا نوعيا في الجهود الدولية الرامية إلى وضع إطار عالمي أكثر شمولاً وتوازناً، يقوم على احترام مبدأ السيادة الوطنية، ويؤكد في الوقت ذاته على ضرورة مراعاة حقوق الإنسان أثناء اتخاذ تدابير مكافحة الجريمة السيبرانية.

وتكتسي هذه الاتفاقية أهمية خاصة بالنسبة للجزائر، التي انضمت إليها رسميا في أكتوبر 2025، وهو ما يعكس توجه

وعليه، فإن أفضل تعريف هو ذلك الذي يجمع بين البعد التقني والبعد القانوني ويتيح إطارا متكاملًا يتماشى مع التوجهات الدولية، وفي الوقت ذاته يفتح المجال أمام الدول لصياغة سياسات وطنية تتناسب مع خصوصياتها.

ب/ التحديات القانونية المرتبطة بالفضاء السيبراني

يطرح الفضاء السيبراني إشكاليات قانونية عميقة نظرا لطبيعته العابرة للحدود وصعوبة إخضاعه للسيادة التقليدية للدول، فهو مجال افتراضي غير مادي، تتداخل فيه المصالح الاقتصادية والسياسية والأمنية على نحو يجعل أي تنظيم قانوني يواجه معضلة الموازنة بين حماية الأمن الوطني وضمان حرية تداول المعلومات، ومن بين أبرز التحديات القانونية المرتبطة بالفضاء السيبراني ما يلي:

1. إشكالية الاختصاص القضائي:

يعد الاختصاص القضائي من أهم القضايا القانونية التي يواجهها الفضاء السيبراني، إذ يرتبط مباشرة بحق الأفراد في الوصول إلى قاضيهم الطبيعي وضمان عدم إفلات المجرمين من العقاب.

ولكن الطبيعة العابرة للحدود للشبكات الرقمية تطرح معضلة حقيقية أمام الأنظمة القانونية الوطنية التي وضعت في الأصل للتعامل مع نزاعات محلية أو إقليمية، لا مع فضاء افتراضي لا يعترف بالحدود الجغرافية.

وأول مظاهر هذه الإشكالية يتمثل في تحديد مكان ارتكاب الفعل الضار أو الجريمة الإلكترونية، ففي الفضاء المادي، مكان الجريمة أو النزاع واضح ومحدد، بينما في الفضاء الرقمي قد يكون الجاني في دولة، والضحية في دولة أخرى، والخواص المستعملة في دولة ثالثة، وهذا التوزيع الجغرافي يجعل من الصعب على أي محكمة وطنية أن تدعي اختصاصا حصريا، ويفتح المجال أمام تضارب الاختصاصات أو على العكس إنكار العدالة بحجة غياب جهة مختصة.

وإضافة إلى ذلك، يبرز تحدي تعدد النظم القانونية وتفاوتها فبينما تبنت بعض الدول تشريعات متقدمة في مجال مكافحة الجرائم السيبرانية (كالاتحاد الأوروبي أو الولايات المتحدة)، ما زالت دول أخرى تعتمد نصوصا عامة لا تغطي خصوصيات الجرائم الرقمية، وهذا التفاوت يؤدي إلى إشكالات عملية، مثل اختلاف تعريف الجريمة الإلكترونية أو تفاوت العقوبات، ما يصعب التعاون القضائي الدولي ويخلق ملاذات أمان للمجرمين السيبرانيين.

كما أن قواعد القانون الدولي التقليدية، خاصة المتعلقة بالسيادة وعدم التدخل، تجد نفسها في مواجهة تحديات جديدة، فالدولة التي يقع فيها ضحايا هجوم إلكتروني قد تسعى لمباشرة اختصاصها حتى لو انطلق الهجوم من خارج حدودها، بينما قد تعترض دولة أخرى على ذلك باعتباره مساسا بسيادتها، هذا يطرح سؤالا عميقا حول مدى كفاية القواعد التقليدية لحل نزاعات سيبرانية تتسم بالتعقيد والتداخل.

ومن هنا يطرح الإشكال الجوهرى: كيف يمكن الحفاظ على جوهر الحقوق الفردية، مثل الحق في الخصوصية وحرية التعبير، ضمن بيئة رقمية متسارعة التطور؟ وهو ما يستوجب معالجة دقيقة تجمع بين مقتضيات الأمن وضمانات الحقوق.

أ/ الخصوصية وحماية البيانات الشخصية

أضحت الخصوصية من أكثر الحقوق عرضة للانتهاك في العصر الرقمي، حيث تتضاعف عمليات جمع البيانات الشخصية من قبل الشركات والهيئات الحكومية لأغراض أمنية أو تجارية.

ولعل أبرز مثال عالمي على تنظيم هذا الحق يتمثل في اللائحة الأوروبية العامة لحماية البيانات (GDPR) التي أُرست مبدأ "الموافقة الصريحة" كشرط أساسي لمعالجة البيانات، ومنحت الأفراد حق الوصول والتصحيح والنسيان (27، Union, april 2016).

في السياق الجزائري، صدر القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي المدلل والمتمم، وهو خطوة مهمة لتأطير هذا الحق (18-07، 10 يونيو 2018).

غير أن التطبيق العملي ما يزال يواجه تحديات مرتبطة بضعف الثقافة القانونية الرقمية لدى المواطنين، وبغياب هيئة فعالة للمراقبة على غرار النموذج الأوروبي.

إذن، حماية الخصوصية لم تعد مسألة أخلاقية أو اجتماعية فحسب، بل تحولت إلى مطلب قانوني يفرض على المشرع إيجاد آليات تضمن التوازن بين مقتضيات الأمن السيبراني ومتطلبات احترام الحياة الخاصة للأفراد.

ب/ حرية التعبير وضمانات المحاكمة العادلة

يمثل الفضاء السيبراني مجالا واسعا لممارسة حرية التعبير، لكنه في الوقت نفسه فضاء يثير تهديدات جديدة مثل خطاب الكراهية، الأخبار المضللة، والتحرش على العنف، ما يفرض تحديا قانونيا يتمثل في كيفية ضبط هذا الحق دون المساس بجوهره.

والقانون الدولي لحقوق الإنسان، خاصة العهد الدولي للحقوق المدنية والسياسية، نص صراحة على أن حرية التعبير يمكن أن تقتيد في حالات الضرورة لحماية الأمن الوطني أو النظام العام، لكن القيود يجب أن تكون متناسبة ومؤقتة.

إلا أن الواقع يظهر ميل العديد من الحكومات إلى التوسع في الرقابة الرقمية بذريعة مواجهة الجرائم السيبرانية، مما يثير مخاطر انتهاك حقوق الأفراد.

إضافة إلى ذلك، فإن المحاكمات المتعلقة بالجرائم السيبرانية كثيرا ما تطرح فيها إشكالية ضمانات الدفاع، خاصة عندما تعتمد السلطات على أدلة رقمية قد يشوبها الغموض أو صعوبة التحقق من مصداقيتها، وهو ما يجعل من مبدأ

الدولة نحو تعزيز التعاون الدولي في المجال السيبراني ضمن مقاربة متعددة الأطراف، والسعي إلى تحقيق توازن دقيق بين متطلبات الأمن السيبراني وضمان الحقوق الأساسية، ولاسيما الحق في الخصوصية وضمانات المحاكمة العادلة.

ورغم الأهمية التي تكتسيها اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية لسنة 2024 في تعزيز التنسيق الدولي، فإن تفعيلها العملي يظل رهينا بجملة من العوامل التي تحد من فعاليتها، وعلى رأسها تباين الأولويات الوطنية بين الدول، فالدول المتقدمة تركز على حماية بنيتها التحتية الحساسة، وضمان أمن سلاسل الإمداد الرقمية، وحماية حقوق الملكية الفكرية، بينما تنشغل الدول النامية أساسا بمكافحة الجرائم البسيطة مثل الاحتيال والاختراق الفردي، نظرا لضعف إمكانياتها التقنية، وهذا الاختلاف في الرؤى يجعل من الصعب صياغة أجندة موحدة للتعاون الدولي.

إلى جانب ذلك فإن غياب آليات ملزمة لتسوية النزاعات السيبرانية يمثل عقبة أخرى، فعندما تتعرض دولة لهجوم من مصدر خارجي، لا توجد جهة قضائية أو آلية دولية مختصة للفصل في النزاع بشكل ملزم، وهذا الفراغ القانوني يدفع بعض الدول إلى تبني إجراءات أحادية قد تؤدي إلى تصعيد النزاعات بدل احتوائها.

وفي ضوء ما سبق، يتضح أن ضعف التنسيق الدولي في الفضاء السيبراني ليس مجرد خلل عرضي، بل هو انعكاس مباشر لبنية النظام الدولي ذاته، وإذا كان الهدف هو بناء فضاء سيبراني أكثر أمانا وعدالة، فإن تجاوز هذا الضعف يتطلب إرادة سياسية صادقة لتوحيد القواعد والمعايير، وتطوير آليات تعاون مرنة تجمع بين تبادل المعلومات، ووضع أطر قانونية مشتركة، وتعزيز الثقة المتبادلة بين الدول.

وعليه فإن غياب التنسيق الدولي لا يعني فقط قصورا في مكافحة الجريمة الإلكترونية، بل يهدد أيضا الأمن الرقمي العالمي، ويترك الفضاء السيبراني ساحة مفتوحة أمام الفاعلين غير الشرعيين.

وانطلاقا مما تقدم يمكن القول بأن هذه التحديات تجعل من الضروري تطوير مقاربة قانونية متوازنة تعترف بخصوصية الفضاء السيبراني وتراعي حقوق الأفراد الأساسية في الوقت ذاته.

2.2. الحقوق الفردية في ظل البيئة الرقمية

أحدثت الثورة الرقمية نقلة نوعية في ممارسة الحقوق الفردية، إذ أصبح الفضاء السيبراني مجالا جديدا للتعبير والتواصل وتداول المعلومات.

غير أن هذه التحولات أفرزت في المقابل تحديات عميقة تتعلق بكيفية حماية هذه الحقوق من انتهاكات قد تنشأ عن المراقبة الواسعة، أو جمع البيانات الشخصية، أو التضيق على حرية التعبير بدعوى مواجهة التهديدات الأمنية.

يقوم عليه أي مشروع وطني للأمن السيبراني يحترم في الوقت ذاته الحقوق الفردية.

2. 1. التجارب المقارنة في تحقيق التوازن بين متطلبات الأمن السيبراني وضمان الحقوق الفردية.

تتباين مقاربات الدول في تنظيم الأمن السيبراني باختلاف خلفياتها السياسية والقانونية وأولوياتها الاستراتيجية، الأمر الذي انعكس على طبيعة العلاقة التي تقيمها بين متطلبات الحماية الأمنية وضمان الحقوق الفردية في البيئة الرقمية، فبين دول تغلب الاعتبارات الأمنية بدعوى حماية الأمن القومي، وأخرى تعتمد رقابة مركزية صارمة على الفضاء السيبراني، برزت تجارب تسعى إلى بناء مقاربة قانونية أكثر توازناً تقوم على إدماج حماية الحقوق والحريات ضمن السياسات الأمنية الرقمية.

ومن هذا المنطلق، تكتسي دراسة التجارب المقارنة أهمية بالغة في فهم الكيفية التي تعاملت بها الأنظمة القانونية المختلفة مع إشكالية الموازنة بين الأمن السيبراني والحقوق الفردية، من حيث الأسس القانونية المعتمدة، وحدود تدخل الدولة، والضمانات المقررة لحماية الحقوق، كما تسمح هذه المقارنة باستخلاص الدروس والعبر التي يمكن الاستفادة منها في تطوير الأطر القانونية الوطنية، ولا سيما في الدول التي تسعى إلى بناء منظومة متكاملة للأمن السيبراني تحترم في الوقت ذاته حقوق الإنسان ومبادئ دولة القانون.

أ/ النموذج الأمريكي: أولوية الأمن القومي على حساب حقوق الإنسان.

يعتمد النموذج الأمريكي في تنظيم الفضاء السيبراني على مقاربة أمنية تضع حماية الأمن القومي في مقدمة الأولويات، خاصة في أعقاب الهجمات الإرهابية التي شهدتها الولايات المتحدة، وهو ما انعكس بوضوح في التوسع في صلاحيات أجهزة الأمن والاستخبارات في مجال المراقبة الرقمية وجمع البيانات.

وقد كرس هذا التوجه صدور قانون USA PATRIOT Act الذي منح السلطات صلاحيات واسعة في تتبع الاتصالات الإلكترونية، وجمع البيانات الشخصية، بدعوى مكافحة الإرهاب والجرائم السيبرانية.

ورغم أن هذا الإطار القانوني أسهم في تعزيز قدرة الدولة على مواجهة التهديدات الأمنية، إلا أنه أثار انتقادات واسعة من قبل منظمات حقوق الإنسان، بسبب ما ينطوي عليه من مساس بالحقوق الخصوصية وحرية التعبير (congress, 2015).

ومن نقاط قوة النموذج الأمريكي قدرته على الاستجابة السريعة للتهديدات السيبرانية، واعتماده على بنية تقنية متقدمة وأجهزة أمنية ذات كفاءة عالية، غير أن نقطة ضعفه الأساسية تتمثل في غياب إطار شامل لحماية البيانات الشخصية على المستوى الفيدرالي، ما يؤدي إلى تباين مستوى حماية الحقوق بين الولايات، ويجعل الموازنة تميل لصالح الأمن على حساب الحقوق الفردية.

المحاكمة العادلة ركنا أساسيا في أي تنظيم قانوني متوازن للأمن السيبراني.

بعد أن تبين لنا في المحور الأول أن الأمن السيبراني يمثل ضرورة استراتيجية لحماية الدول والمجتمعات، وفي الوقت ذاته أن الحقوق الفردية تمثل جوهر أي نظام قانوني يحترم الكرامة الإنسانية، يصبح من اللازم معالجة الإشكالية المركزية: كيف يمكن تحقيق توازن عادل بين متطلبات الأمن ومتطلبات الحقوق؟.

هذا التوازن لا يعد مسألة تقنية فحسب، بل هو قضية قانونية وأخلاقية تتعلق بموقع الفرد داخل المنظومة الرقمية، ومن هنا تأتي أهمية استعراض بعض التجارب المقارنة من جهة، ثم تحليل الواقع الجزائري من جهة أخرى.

2. نحو تحقيق توازن بين الأمن السيبراني والحقوق الفردية.

إن معالجة موضوع الأمن السيبراني بمعزل عن الحقوق الفردية يجعل الصورة مبثورة وغير مكتملة، لأن أي سياسة أو تدبير أمني لا يكتسب شرعيته إلا إذا كان متوافقا مع القيم والمبادئ التي يقوم عليها النظام القانوني، فالحقوق الفردية ليست امتيازاً يمنح للأفراد بل هي مكتسبات دستورية وإنسانية واجبة الاحترام حتى في أحلك الظروف.

غير أن البيئة الرقمية فرضت معادلة معقدة، فمن جهة، تواجه الدول تهديدات سيبرانية متنامية تهدد بنيتها التحتية الحيوية وأمنها القومي، ومن جهة أخرى، يتعين عليها الالتزام بضمان الخصوصية وحماية البيانات وحرية التعبير وحقوق المحاكمة العادلة.

ويبرز هذا الواقع أن إشكالية التوازن بين الأمن السيبراني والحقوق الفردية ليست مسألة نظرية بقدر ما هي إشكال عملي يومي ينعكس في التشريعات والسياسات العمومية، فالتشدد المفرط في التدابير الأمنية قد يؤدي إلى انتهاكات خطيرة تمس جوهر الحقوق، بينما يؤدي التراخي في الضبط القانوني إلى هشاشة في حماية الأفراد والمؤسسات من الجرائم الإلكترونية، ومن هنا، فإن تحقيق التوازن يصبح خياراً استراتيجياً لضمان أمن رقمي فعال وعدالة رقمية مستدامة.

ولأجل ذلك، يعني المحور الثاني من هذا البحث بدراسة الكيفية التي سعت من خلالها التجارب المقارنة إلى بناء هذا التوازن، حيث يستعرض النموذج الأوروبي القائم على مبدأ حماية الحقوق في قلب الاستراتيجيات الأمنية، ثم النموذج الأمريكي الذي أعطى الأولوية للأمن القومي، وأخيراً النموذج الصيني الذي ركز على الرقابة المركزية الصارمة، وبعد ذلك، يتم الانتقال إلى قراءة الواقع الجزائري الذي يشهد جهوداً تشريعية متفرقة تحتاج إلى التنسيق والتكامل من أجل صياغة إطار وطني شامل.

وعليه، فإن هذا المحور يهدف إلى إبراز أن التوازن هو الضامن الحقيقي لبناء ثقة المواطن في الفضاء الرقمي، والأساس الذي

البنية التحتية للمعلوماتية، بهدف تحقيق التنمية المستدامة والانخراط في الاقتصاد العالمي.

غير أن هذا الانفتاح على التكنولوجيا يرافقه بروز تهديدات سيبرانية متنامية، مثل الهجمات الإلكترونية، والاختراقات، وسرقة البيانات، وهي تهديدات قد تمس الأمن الوطني وتضع الحقوق الفردية في موضع الخطر.

ومن هنا يبرز التحدي الأكبر: كيف يمكن صياغة إطار وطني متكامل يوازن بين ضرورات الأمن السيبراني ومتطلبات حماية الحقوق الفردية؟

فمن الناحية التشريعية، أولت الجزائر اهتماما ملحوظا بتنظيم الفضاء الرقمي عبر إصدار نصوص متعددة.

وقد شكل القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي المعدل والمتمم (07.18، 10 يونيو 2018)، الإطار التشريعي الأساسي لتنظيم حماية البيانات في الجزائر، إذ سعى المشرع من خلاله إلى تكريس الحق في الخصوصية وضبط عمليات جمع ومعالجة المعطيات الشخصية، لاسيما في ظل تنامي استخدام الوسائط الرقمية وتزايد مخاطر الاستغلال غير المشروع للبيانات.

غير أن التطورات المتسارعة في مجال الأمن السيبراني، وظهور أنماط جديدة من التهديدات الرقمية، إلى جانب التوسع الكبير في المعالجة الآلية للمعطيات، كشفت عن بعض النقائص العملية في أحكام هذا القانون، سواء من حيث فعالية آليات الرقابة أو من حيث ملاءمته لمتطلبات الحماية الرقمية الحديثة، الأمر الذي استدعى تدخل المشرع لإعادة النظر في بعض أحكامه وتحسينها بما ينسجم مع المستجدات التقنية والأمنية.

وقد عرف الإطار القانوني الجزائري المتعلق بحماية المعطيات ذات الطابع الشخصي تطورا تشريعا هاما بصور القانون رقم 11-25 المؤرخ في 24 جويلية 2025، المعدل والمتمم للقانون رقم 07-18 (07-18، 11-25، 2025)

ويهدف هذا التعديل إلى تعزيز حماية الأشخاص الطبيعيين في ظل تصاعد التهديدات السيبرانية، من خلال تشديد الالتزامات المفروضة على مسؤولي المعالجة، وتوسيع صلاحيات السلطات الوطنية لحماية المعطيات ذات الطابع الشخصي، ولاسيما في مجال الرقابة والجزاءات.

كما كرس المشرع مبدأ التناسب بين متطلبات الأمن السيبراني واحترام الحقوق الأساسية، خاصة الحق في الخصوصية، بما ينسجم مع المعايير الدولية لحماية البيانات، ويعكس توجهها تشريعا نحو تحقيق توازن أدق بين الضرورات الأمنية وضمان الحريات الرقمية.

ويُعد هذا التعديل خطوة نوعية في سد بعض الثغرات التي كشف عنها التطبيق العملي للقانون 07-18، ويؤكد وعي المشرع الجزائري بضرورة مواكبة التحولات الرقمية المتسارعة.

وعليه، يمكن القول إن النموذج الأمريكي يعكس مقاربة أمنية فعالة من حيث الحماية، لكنها تعاني من اختلال في التوازن القانوني لصالح البعد الأمني، مما يضع الحقوق الفردية في مرتبة ثانوية.

ب/النموذج الأوروبي: مقارنة قانونية قائمة على التوازن وحماية الحقوق الفردية.

يعتبر الاتحاد الأوروبي رائدا في مجال محاولة إيجاد معادلة متوازنة بين الأمن السيبراني والحقوق الفردية، فقد اعتمد اللائحة العامة لحماية البيانات (GDPR 2016) التي منحت الأفراد سلطة حقيقية على بياناتهم

ثم جاء قانون الاتحاد الأوروبي للذكاء الاصطناعي (EU AI Act 2024) ليؤكد أن الأمن السيبراني لا يجب أن يكون ذريعة للمساس بالحقوق، بل ينبغي أن يبنى على أساس تصنيف المخاطر (Parliament, 13 June 2024)

وإلى جانب ذلك، تبنى الاتحاد استراتيجيّة الأمن السيبراني 2020 التي ركزت على مبادئ الشفافية، والمساءلة، واحترام الخصوصية، وهو ما يعكس رؤية متقدمة ترى أن الثقة الرقمية لا تتحقق إلا إذا شعر المواطن أن حقوقه محفوظة (commission, 2020)

ج/النموذج الصيني: تغليب الرقابة المركزية على الحقوق الفردية

في الصين يعتمد النموذج على مقاربة أمنية مشددة، حيث تفرض الدولة رقابة صارمة على الفضاء الرقمي، من خلال "قانون الأمن السيبراني 2017" الذي يمنح السلطات صلاحيات واسعة في مراقبة المحتوى وتخزين البيانات داخل الحدود الوطنية (china, 2017)

ورغم أن هذا النظام يوفر مستوى عالٍ من السيطرة الأمنية، إلا أنه يتعرض لانتقادات دولية بسبب تأثيره السلبي على حرية التعبير والحق في الخصوصية.

وانطلاقا مما تقدم يمكن أن القول التجارب المقارنة تظهر أن المقاربة الأوروبية هي الأكثر توازنا بين الأمن والحقوق، بينما تميل المقاربة الأمريكية إلى تعزيز الأمن على حساب الحرية، أما المقاربة الصينية فتعتبر مثالا على تغليب الأمن الكلي على الحقوق الفردية، وبالنسبة للدول النامية، فإن الاستفادة من هذه التجارب يقتضي صياغة تشريعات تراعي الخصوصيات الوطنية وتوازن بين الضرورات الأمنية والمبادئ الحقوقية.

2. 2. الإطار القانوني الجزائري وامكانات تحقيق التوازن بين الأمن السيبراني والحقوق الفردية.

يشهد العالم في العقود الأخيرة طفرة رقمية واسعة، جعلت الفضاء السيبراني ميدانا رئيسيا للتفاعل الاقتصادي والاجتماعي والسياسي.

وفي هذا السياق، لم تكن الجزائر بمنأى عن هذه التحولات، إذ شرعت الدولة في بناء إستراتيجيات للتحويل الرقمي وتعزيز

شرطا لضمان فعالية السياسات الوطنية للأمن السيبراني.

كما أن الاستثمار في تكوين الكفاءات الوطنية وتطوير البنى التحتية المعلوماتية يساهم في تقليص الاعتماد على الحلول الأجنبية، وبالتالي يعزز السيادة الرقمية للدولة.

ومن ناحية أخرى، تفرض البيئة الرقمية الحديثة تحديات جديدة تتعلق بحقوق الأفراد في ظل الرقمنة المتسارعة للخدمات العمومية، فمع انتشار الحكومة الإلكترونية، والعدالة الرقمية، والتعليم عن بعد، والصحة الإلكترونية، أصبح الاعتماد على البيانات الشخصية ضرورة حتمية لتسيير هذه الخدمات.

وهذا الواقع يزيد من مخاطر المساس بالخصوصية إذا لم يرفق بآليات قوية لحماية المعطيات وضمان شفافيتها، وفي غياب هذه الآليات، قد يفقد المواطن ثقته في الخدمات الرقمية، مما يعرقل مسار التحول الرقمي برمته.

إن التوازن بين الأمن السيبراني والحقوق الفردية في الجزائر لا يمكن فهمه بمعزل عن السياق الدولي، فالمعايير والتجارب المقارنة، مثل النظام الأوروبي لحماية البيانات (GDPR) أو التشريعات الأمريكية والصينية، توفر نماذج مختلفة يمكن استلهاها مع مراعاة الخصوصيات الوطنية.

ولكن التحدي يكمن في صياغة نموذج وطني قادر على التوفيق بين مقتضيات الأمن ومتطلبات الحقوق، دون استنساخ آليات خارجية قد لا تتلاءم مع البنية القانونية والاجتماعية للجزائر.

وفي الأخير يمكن القول بأن الإطار الوطني الجزائري في مجال الأمن السيبراني وحماية الحقوق الفردية يشكل منظومة في طور التشكل، تتسم بوجود إرادة سياسية وتشريعية واضحة لمواجهة التهديدات الرقمية، لكنها ما تزال بحاجة إلى المزيد من التكييف والتكامل حتى تحقق التوازن المنشود، فالمسألة لا تتعلق بمجرد إصدار نصوص قانونية أو إنشاء مؤسسات، بل تقتضي مقارنة شاملة تدمج البعد القانوني بالتقني والاجتماعي، وتجعل المواطن في صميم العملية بوصفه المستفيد الأول من الحماية والضمانات.

خاتمة

لقد أظهر البحث في موضوع التوازن بين الأمن السيبراني والحقوق الفردية مدى تعقيد العلاقة بين بعدين متداخلين:

البعد الأمني الذي يسعى لحماية الدولة والمجتمع من المخاطر المتزايدة في الفضاء الرقمي، والبعد الحقوقي الذي يتمثل في صون الحريات الفردية والحقوق الدستورية التي تمثل جوهر دولة القانون، هذا التداخل لا يمكن التعامل معه بسطحية أو بإجراءات جزئية، بل يتطلب مقاربة شمولية تستحضر الجوانب القانونية والتقنية والاجتماعية والأخلاقية.

إن التطور الهائل في مجال تكنولوجيا المعلومات أفرز واقعا

وإضافة إلى ذلك، تضمن قانون العقوبات مواد تجرم الأفعال المرتبطة بالأنظمة المعلوماتية، مثل الدخول غير المشروع إلى قواعد البيانات، أو عرقلة النظم الإلكترونية، وهو ما يعكس إدراك المشرع لخطورة التهديدات الرقمية على النظام العام.

وإلى جانب ذلك، أصدر المشرع الجزائري نصوصا تنظيمية مرتبطة بالأمن السيبراني، من أبرزها المرسوم الرئاسي الذي يتضمن إنشاء المدرسة الوطنية العليا للأمن السيبراني (24-181، 2024)

كما أدرجت الحكومة الأمن السيبراني ضمن إستراتيجية التحول الرقمي التي تستهدف تحديث الإدارة والخدمات العمومية، الأمر الذي يبرز رغبة الدولة في جعل الأمن السيبراني ركيزة للتنمية الاقتصادية والاجتماعية.

غير أن هذه المنظومة التشريعية والمؤسسية، رغم أهميتها، لا تزال تواجه تحديات عملية، إذ يلاحظ وجود تشتت في النصوص القانونية، ما يجعل الإطار التنظيمي غير متكامل بالشكل المطلوب.

ضف لذلك أن تطبيق القوانين على أرض الواقع يعترضه نقص في الإمكانيات البشرية والتقنية، وهو ما قد يحد من فعالية الرقابة والوقاية من الهجمات السيبرانية.

وعليه تتجلى إشكالية التوازن في كون التدابير الأمنية قد تتعارض أحيانا مع حقوق الأفراد المكفولة دستوريا، فالدستور الجزائري يضمن حرية الرأي والتعبير، وحق حماية الحياة الخاصة، وحرية الاتصال.

غير أن الإجراءات المتعلقة بمراقبة الفضاء الرقمي أو جمع البيانات من أجل مكافحة الجريمة الإلكترونية قد تؤدي، في بعض الحالات، إلى تقييد تلك الحقوق أو المساس بسرية الاتصالات.

وهنا تبرز الحاجة إلى إطار قانوني يحدد بدقة حدود تدخل السلطات العامة، ويضع ضمانات تحول دون تجاوز التدابير الأمنية لجوهر الحقوق الفردية.

وفي هذا السياق، يظهر دور القضاء الدستوري والهيئات المستقلة كعوامل أساسية في تحقيق التوازن، إذ يمكن لهذه المؤسسات أن تراقب مدى احترام التشريعات والإجراءات لمبادئ الدستور، بما يمنع الانزلاق نحو التضيق على الحريات باسم حماية الأمن السيبراني.

كما يشكل تعزيز استقلالية الهيئات الرقابية، مثل السلطة الوطنية لحماية البيانات، خطوة ضرورية لإعطاء المصداقية لجهود الدولة في هذا المجال، وضمان أن تكون الرقابة متوازنة وشفافة.

وإلى جانب البعد القانوني، يظل البعد المؤسسي والتقني محوريا في بناء التوازن، فالتسيق بين مختلف الفاعلين، سواء الأجهزة الأمنية أو المؤسسات الإدارية أو الهيئات المستقلة، يعد

على المستوى التشريعي:

-إعداد قانون وطني شامل للأمن السيبراني يجمع بين الجوانب الأمنية والحقوقية، على نحو يستلهم من التجارب المقارنة، خصوصاً النظام الأوروبي القائم على تصنيف المخاطر.

-مراجعة القوانين الحالية بما يضمن التكامل بين قانون العقوبات، قانون حماية البيانات، وقانون التجارة الإلكترونية، مع سد الثغرات التي تستغلها الجرائم السيبرانية.

-دسترة صريحة لمبدأ حماية البيانات الشخصية كحق أساسي، بما يكرس الالتزام الدستوري بحماية الحياة الخاصة.

على المستوى المؤسسي:

-تعزيز استقلالية وفعالية الهيئات الرقابية، مثل الهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي، وتمكينها من الموارد والصلاحيات لمراقبة الفضاء الرقمي بفعالية.

-دعم الهيئة الوطنية للأمن السيبراني لتكون مركزاً محورياً للتنسيق بين مختلف الفاعلين (الأمنية، التقنية، الإدارية).

-إشراك المجتمع المدني والجامعات في صياغة السياسات العمومية المتعلقة بالأمن السيبراني.

على المستوى التقني والبشري:

-الاستثمار في التكوين العالي للخبراء في الأمن السيبراني، وتشجيع البحث العلمي في مجالات التشفير، الحماية الرقمية، والذكاء الاصطناعي.

- تطوير بنية تحتية رقمية وطنية مؤمنة تقلل الاعتماد على الحلول المستوردة، بما يعزز السيادة الرقمية.

على المستوى الحقوقي والاجتماعي:

-تكثيف برامج التوعية والتحسيس لتعريف المواطن بحقوقه الرقمية وطرق حمايتها.

-وضع ضوابط واضحة ومعلنة لعمليات المراقبة الرقمية حتى لا تتحول إلى أداة للمساس بالحقوق الدستورية.

-ضمان مشاركة القضاء الدستوري في مراقبة توافق الإجراءات الأمنية مع المبادئ الدستورية.

على المستوى الدولي:

-تعزيز التعاون الدولي والإقليمي في مجال مكافحة الجرائم الإلكترونية، مع الاستفادة من الاتفاقيات والمعايير الدولية ذات الصلة.

-تبادل الخبرات مع الدول الرائدة في ميدان الأمن السيبراني وحماية الحقوق الفردية.

ومما تقدم فإن التوصيات السابقة لا تشكل مجرد مقترحات نظرية، بل تمثل خريطة طريق عملية يمكن أن تسهم في بناء نموذج وطني متوازن، هذا النموذج يجب أن يكون قادراً

جديداً يتميز بانتقال الجريمة من الشكل التقليدي إلى الشكل السيبراني، وتنامي الاعتماد على البيانات الشخصية والمعالجة الآلية لها، إلى جانب ظهور ممارسات رقمية مستحدثة مثل الذكاء الاصطناعي، البلوكشين، وإنترنت الأشياء.

وهذه المستجدات تطرح تحديات على المشرع الجزائري من حيث ضرورة وضع قواعد متينة للأمن السيبراني، وفي الوقت نفسه ضمان احترام الحقوق الفردية، بما في ذلك الحق في الخصوصية، وحرية التعبير، وحق الوصول إلى المعلومات.

وقد أبرز البحث أن الإطار القانوني الجزائري، رغم غناه وتنوعه، ما يزال مشتتاً في نصوص متفرقة: قانون العقوبات يتناول التجريم والعقاب، القانون 18-07 يتناول حماية البيانات الشخصية..

غير أن هذا التعدد لا يرقى بعد إلى منظومة متكاملة قادرة على ضمان التوازن المنشود كما أظهر البحث أن غياب ثقافة رقمية مجتمعية، وضعف التنسيق بين المؤسسات، يضاعف من صعوبة التطبيق العملي لهذه القوانين.

ومن خلال تحليل الوضع الوطني ومقارنته بالتجارب الدولية، برزت مجموعة من النتائج الأساسية:

1. أولوية الأمن السيبراني:

يشكل الأمن السيبراني اليوم عنصراً جوهرياً في حماية الأمن القومي الجزائري، لاسيما في ظل التهديدات العابرة للحدود مثل الإرهاب السيبراني والجرائم المنظمة عبر الإنترنت.

2. تنامي قيمة الحقوق الفردية:

إذ أن الحقوق والحريات الأساسية المكرسة في الدستور، مثل الحق في الخصوصية وحرية التعبير، أصبحت تواجه مخاطر مضاعفة بسبب الاستخدام المفرط للتكنولوجيا الرقمية وأساليب المراقبة غير المنضبطة.

3. قصور الإطار القانوني:

رغم وجود قوانين متعددة، فإن عدم تكاملها وتشتتها يجعل من الصعب تحقيق حماية متوازنة، وهو ما يبرز الحاجة إلى إصلاح تشريعي شامل.

4. تحديات تقنية وبشرية:

الأمن السيبراني يتطلب موارد بشرية متخصصة وبنية تحتية قوية، وهو ما لا يزال يمثل نقطة ضعف نسبية في الجزائر.

5. الحاجة إلى مقارنة متعددة الأبعاد:

التوازن لا يمكن تحقيقه بنصوص قانونية فقط، بل يحتاج إلى إشراك التكنولوجيا، التكوين، التوعية المجتمعية، والرقابة المؤسسية.

وانطلاقاً من هذه النتائج، يمكن صياغة مجموعة من التوصيات التي تمثل مخرجات عملية للبحث:

على مواجهة التهديدات السيبرانية بكفاءة، وفي الوقت نفسه ضمان احترام الحقوق والحريات التي تمثل الركيزة الأساسية لشرعية الدولة وثقة المواطن.

- كيفية الإستشهاد بهذا المقال حسب أسلوب APA

عروس كوثر، عروس فوزية (2026)، إشكالية الموازنة بين متطلبات الأمن السيبراني وضمان الحقوق الفردية، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد 18، العدد 01، جامعة حسيبة بن بوعلي بالشلف، الجزائر، ص: 258-267.

كما أن التوازن بين الأمن السيبراني والحقوق الفردية ليس خيارا ثانويا، بل هو شرط أساسي لبناء دولة رقمية حديثة، فإذا غلبت الدولة البعد الأمني على الحقوق، فإنها تخاطر بخلق حالة من انعدام الثقة بين المواطن والمؤسسات، مما يعرقل التنمية الرقمية.

أما إذا أهملت متطلبات الأمن، فإن الفضاء الرقمي قد يتحول إلى ساحة فوضى تهدد الأمن الوطني، ومن ثم، فإن النجاح يكمن في صياغة مقاربة وسطية متكاملة تضع الجزائر في موقع متميز إقليميا ودوليا، قادرة على تحقيق التنمية المستدامة وضمان سيادة القانون في البيئة الرقمية.

قائمة المراجع :

- 1-European commission. (2020). The EU's cybersecurity strategy for the digital decade. 01.
- 2-European Commission. (18 april. 2023). EU Cybersecurity Act. تم الاسترداد من digital-strategy.ec: <https://digital-strategy.ec>
- 3-European Parliament. (13 june 2024). Artificial Intelligence Act. Official journal of the European union (OJL), 01.
- 4-European Union. (27 april 2016). General data protection regulation(GDPR). Official journal of the european union.
- 5-Francesco Schiliro. (05 February. 2023). Towards a contemporary Definition of Cybersecurity. see: [arXiv: https://arXiv.org](https://arXiv.org)
- 6-National people's congress of china. (2017). Cybersecurity law of the people's republic of china
- 7-United nation. (2024),United nations convention against cybercrime.
- 7- القانون 07-18. (10 يونيو 2018). يتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي. الجريدة الرسمية الجزائرية، 11.
- 8- القانون 11-25 . (2025). يعدل ويتم القانون رقم 07-18 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. الجريدة الرسمية الجزائرية، 14.
- 8- القانون الأردني رقم 16. (2019). الأمن السيبراني. الجريدة الرسمية الأردنية، 5143.
- 9- القانون رقم 05-20. (25 يوليو 2020). المتعلق بالأمن السيبراني. الجريدة الرسمية المغربية، 4160.
- 10- المرسوم الرئاسي 181-24. (2024). يتضمن إنشاء المدرسة الوطنية العليا للأمن السيبراني. الجريدة الرسمية الجزائرية.
- 11- عبد الرحمن علي اللقاني. (2022). دور الأمن السيبراني في تعزيز أمن المعلومات المالية الإلكترونية. الأردن : دار اليازوري.
- 12- فارس محمد العمارات. (2022). الأمن السيبراني: المفهوم وتحديات العصر. الأردن: دار الخليج للنشر والتوزيع.