

الأمن السيبراني كمدخل أساسي لتحقيق الأمن القانوني في المجتمع الرقمي

Cybersecurity as a Fundamental Pillar for Achieving Legal Security in the Digital Society

د. بن عمار حنان^{1*}، د. ساعد العقون²¹ جامعة زيان عاشور الجلفة، benammarhann@gmail.com² جامعة زيان عاشور الجلفة، saad.lagoun@univ-djelfa.dz

تاريخ النشر: 2026/10/27

تاريخ القبول: 2026/10/03

تاريخ الاستلام: 2026/08/28

ملخص:

يُعتبر الأمن السيبراني أحد الركائز الجوهرية لتحقيق الأمن القانوني في المجتمع الرقمي المعاصر، حيث أفرزت الثورة الرقمية تحديات قانونية وأمنية جديدة تمس الخصوصية، والمعاملات الإلكترونية، وحماية البيانات. ويهدف الأمن السيبراني إلى ضمان سلامة الفضاء الإلكتروني واستقراره، من خلال آليات تقنية وتشريعية متكاملة تحافظ على الثقة الرقمية وتعزز سيادة القانون في البيئة الافتراضية. ومن خلال التحليل يتضح أن تحقيق الأمن القانوني لم يعد مرتبطاً فقط بوضوح النصوص واستقرارها، بل بمدى قدرة الدولة على تأمين بنيتها المعلوماتية ضد التهديدات والهجمات الإلكترونية. كما أن التكامل بين الإطارين القانوني والتقني أصبح ضرورة استراتيجية لبناء مجتمع رقمي تسوده الشفافية والعدالة والثقة. وتخلص الدراسة إلى أن تفعيل الأمن السيبراني كمدخل لتحقيق الأمن القانوني يتطلب تحديث المنظومة التشريعية، وإنشاء هيئات وطنية متخصصة، وتعزيز التعاون الدولي في مكافحة الجريمة المعلوماتية. بذلك، يشكل الأمن السيبراني الركيزة الأساسية لاستدامة سيادة القانون في العصر الرقمي.

الكلمات المفتاحية: الأمن السيبراني، الأمن القانوني، المجتمع الرقمي، الثقة الإلكترونية، الحوكمة الرقمية.

Abstract:

Cybersecurity has emerged as a fundamental pillar for achieving legal security within the modern digital society. The digital revolution has created complex legal and security challenges concerning privacy, electronic transactions, and data protection. Cybersecurity aims to ensure the stability and integrity of cyberspace through integrated technical and legal mechanisms that strengthen digital trust and uphold the rule of law in virtual environments. The study reveals that legal security is no longer guaranteed solely by the clarity of laws but also by the state's capacity to protect its digital infrastructure against cyber threats. Therefore, the integration between legal and

technological frameworks has become essential to building a transparent, fair, and trust-based digital society. It concludes that implementing cybersecurity as a foundation for legal security requires modernized legislation, specialized national institutions, and strengthened international cooperation against cybercrime. Thus, cybersecurity stands as the cornerstone for sustaining the rule of law in the digital era.

Keywords: Cybersecurity, Legal Security, Digital Society, Digital Trust, E-Governance.

مقدمة

العالم اليوم يشهد تحولاً رقمياً كبيراً، أحدثت تغييرات جذرية في كيفية التفاعل الاجتماعي والاقتصادي. أصبح لدينا فضاء رقمي مفتوح لا يعترف بالحدود التقليدية للدول، ولكن مع هذه الثورة الرقمية ظهرت تهديدات سيبرانية تهدد الأمن الوطني والاقتصادي وحتى القانوني الجرائم الإلكترونية باتت تتحدى القوانين القديمة، مما يتطلب إعادة النظر في وسائل الحماية والردع الأمن السيبراني الآن هو جزء أساسي لضمان الأمن القانوني وسط التحولات الكبرى في العالم الرقمي، ومع تسارع الرقمنة وانتقال الأنشطة الاقتصادية والإدارية والاجتماعية إلى الإنترنت، أصبح من الضروري إنشاء نظام قانوني وأمني شامل يحمي الحقوق ويحافظ على الخصوصية ويضمن استقرار المعاملات الرقمية.

في الواقع مفهوم الأمن القانوني داخل المجتمع الرقمي لم يعد كما كان سابقاً في الماضي كان التركيز على وضوح النصوص القانونية وثباتها اليوم أصبح الأمر يتعلق بقدرة الدولة على حماية الفضاء السيبراني من التهديدات التي تهدد الثقة في النظام القانوني الإلكتروني الأمن السيبراني الآن هو الأساس لترسيخ سيادة القانون في العالم الرقمي فهو يحمي البنى التحتية الرقمية للمؤسسات ويمنع التلاعب بالمعلومات الحساسة إضافة إلى ذلك، يحد من الجرائم الإلكترونية التي تؤثر سلباً على الاقتصاد والعدالة أيضاً يعزز الثقة الرقمية بين الأفراد والمؤسسات مما يعتبر ضرورياً لتحقيق الأمن القانوني الفعلي. لأن غياب الأمان التقني يجعل القوانين غير قادرة على ضمان استقرار العلاقات القانونية عبر الإنترنت بشكل فعال.

حيث يجب أن يكون هناك تكامل بين الجانبين القانوني والتقني لضمان نجاح النظام الرقمي القانوني بالكامل تحقيق الأمن في المجتمع الرقمي الحديث يعتمد بشكل أساسي على فهم العلاقة بين الأمن السيبراني والأمن القانوني هذا الفهم يمثل خطوة استراتيجية لفهم التغيرات القانونية في العصر الرقمي، خصوصاً للدول التي تسعى لبناء إدارة إلكترونية وحكومة رقمية فعالة، ومن الضروري وضع التشريعات الملائمة، وتحديث المؤسسات، وتطوير مهارات الأفراد في مجال أمن المعلومات لتحقيق مجتمع رقمي يسوده القانون والشفافية والثقة.

ويمكن القول إن ضمان الأمن القانوني في العصر الرقمي يتطلب تأسيس نظام أمن سيبراني متوازن يحافظ على الحقوق والحريات من جهة، ويلبي متطلبات الأمن الوطني من جهة أخرى، مما يضمن استمرار سيادة القانون في العالم الافتراضي.

إشكالية البحث

كيف يساهم الأمن السيبراني في تحقيق الأمن القانوني داخل المجتمع الرقمي؟ وما هي الآليات القانونية والتقنية التي تضمن حماية الحقوق والحريات في الفضاء السيبراني دون الإخلال بمبادئ الشرعية القانونية؟

فرضيات البحث

1. إن تحقيق الأمن القانوني في المجتمع الرقمي لا يمكن أن يتم دون منظومة أمن سيبراني فعّالة.
2. يشكل الأمن السيبراني إطاراً وقائياً وتنظيمياً لحماية المعاملات الإلكترونية والبيانات الشخصية.
3. تحتاج التشريعات الوطنية إلى التكيف مع التطورات السيبرانية لضمان الأمن القانوني والرقمي معاً.

أهداف البحث

1. توضيح المفهوم القانوني للأمن السيبراني وأبعاده في ظل التحول الرقمي.
2. بيان العلاقة بين الأمن السيبراني والأمن القانوني في حماية الحقوق الرقمية.
3. تحليل التحديات القانونية الناجمة عن الجرائم السيبرانية وضعف الحماية التقنية.
4. اقتراح آليات قانونية وتشريعية لتعزيز الأمن القانوني في المجتمع الرقمي.

منهجية البحث

يعتمد البحث على مزيج من المنهج الوصفي التحليلي لدراسة المفاهيم والنصوص القانونية ذات الصلة، والمنهج المقارن لتحليل التجارب الدولية في الأمن السيبراني (مثل الاتحاد الأوروبي والولايات المتحدة). كما يوظف المنهج الاستنباطي لاقتراح حلول قانونية عملية لتطوير المنظومة الجزائية والعربية في المجال الرقمي.

خطة البحث

حيث تطرقنا في المبحث الأول: الإطار المفاهيمي والنظري للأمن السيبراني والأمن القانوني، و أما المبحث الثاني: التفاعل بين الأمن السيبراني والأمن القانوني في المجتمع الرقمي، وفي المبحث الثالث: آليات تحقيق الأمن القانوني من خلال الأمن السيبراني

المبحث الأول: الإطار المفاهيمي والنظري للأمن السيبراني والأمن القانوني

المطلب الأول: ماهية الأمن السيبراني

الفرع الأول: تعريف الأمن السيبراني وأبعاده التقنية والقانونية

أولاً : تعريف الأمن السيبراني

يُنظر إلى الأمن السيبراني بدرجة كبيرة على أنه أحد أهم الأفكار التي ظهرت في خضم تسارع الثورة الرقمية، إذ يوفر أساساً حاسماً للدفاع في الفضاء السيبراني، كما يساعد على الاستمرار في ضمان وحماية عمل تلك الأنظمة الرقمية العديدة التي يقوم عليها نخط الحياة اليوم، ويشير الأمن السيبراني إلى: "قوة التقنيات والعمليات المصممة لحماية الشبكات

وأجهزة الحاسوب والبرامج والبيانات من الهجمات أو الأضرار أو الوصول غير المصرّح به¹، ومن هذا التعريف تحديداً، لم يعد الأمن السيبراني مجرد مسألة تقنية فحسب، بل أصبح نظاماً متكاملًا يجمع بين تكنولوجيا القانون والتنظيمات. ومع ازدياد اعتماد أصحاب المصلحة في البنى التحتية الحيوية مثل الطاقة والتمويل والتعليم والإدارة على التكنولوجيا، أصبح صون الفضاء السيبراني غير منفصل عن الأمن القومي للدولة، بسبب آثاره المباشرة على الاستقرار الاقتصادي والاجتماعي والسياسي².

ثانياً. أبعاده التقنية والقانونية

من الناحية التقنية، يشمل الأمن السيبراني عدداً من الإجراءات الوقائية التي تهدف إلى حماية الأنظمة الرقمية من الاختراقات أو الهجمات التخريبية. وتتمثل أهم هذه الإجراءات في استخدام أنظمة التشفير لحماية المعلومات الحساسة، واعتماد جدران نارية وأنظمة كشف التسلل، إضافة إلى تطوير برمجيات مضادة للفيروسات والبرامج الخبيثة. كما أصبح الذكاء الاصطناعي وتقنيات التعلم الآلي من الأدوات الحديثة التي توظفها الدول والمؤسسات لتوقع التهديدات السيبرانية قبل وقوعها. وفي السياق الجزائري، كشفت الدراسات الأكاديمية أن تعزيز القدرات التقنية للأمن السيبراني يمثل ضرورة إستراتيجية لضمان "السيادة الرقمية"، وهو ما دفع السلطات إلى إنشاء الهيئة الوطنية للأمن السيبراني سنة 2021، لتنسيق الجهود في مجال حماية الفضاء الإلكتروني الوطني³، هذه المقاربة التقنية تُظهر أن الأمن السيبراني لم يعد ترفاً تكنولوجياً، بل مكوناً أساسياً من مكونات البنية التحتية للأمن القومي في الجزائر⁴.

أما من الناحية القانونية، فقد سعى المشرّع الجزائري إلى وضع إطار تشريعي يُنظّم الفضاء الإلكتروني ويحمي المستخدمين من الجرائم المعلوماتية. فقد جاء الأمر رقم 04-09 ليُجرّم الأفعال التي تمس سلامة الأنظمة المعلوماتية، مثل الدخول غير المشروع أو تدمير البيانات أو اعتراض الاتصالات⁵، كما أتى القانون رقم 04-18 ليكرّس بعداً آخر من أبعاد الأمن السيبراني يتمثل في حماية الخصوصية والهوية الرقمية⁶، وبهذا، يجمع الأمن السيبراني بين الأبعاد التقنية والقانونية في إطار واحد، حيث لا يمكن تحقيق الحماية التقنية دون إطار قانوني يضبط المسؤوليات والعقوبات. هذا

¹ - عبد المالك فريد، مدخل إلى الأمن السيبراني وإدارة المخاطر الرقمية، دار الهدى، الجزائر، 2020، ص. 22.

² - زروقي كمال، "الأمن السيبراني كأداة لحماية البنية التحتية المعلوماتية"، مجلة العلوم القانونية والسياسية، جامعة باتنة، العدد 11، 2021، ص. 15.

³ - بن يوسف محمد، "التهديدات السيبرانية في الجزائر: واقع وآفاق"، مجلة الدراسات الأمنية، جامعة الجزائر 3، العدد 5، 2022، ص. 44.

⁴ - وزارة الرقمنة والإحصائيات، الاستراتيجية الوطنية للأمن السيبراني في الجزائر، الجزائر، 2021، ص. 7.

⁵ - الأمر رقم 04-09 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، 2009، ص. 3.

⁶ - القانون رقم 04-18 المؤرخ في 10 ماي 2018 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 27، 2018، ص. 5.

التداخل بين التقنية والقانون يؤكد أن الأمن السيبراني يمثل رؤية شمولية تُجسّد حماية الدولة والمجتمع والفرد في آن واحد¹.

الفرع الثاني: عناصر ومجالات الأمن السيبراني في الفضاء الرقمي

يُعدّ الأمن السيبراني من الركائز الأساسية في بناء المجتمع الرقمي الآمن، حيث تتجسّد أهميته في حماية مختلف مكونات الفضاء الإلكتروني من الأخطار التقنية والتنظيمية والجرائم المعلوماتية. ويمكن القول إن عناصر الأمن السيبراني تتوزع بين أبعاد تقنية، بشرية، وإدارية، تتكامل فيما بينها لتحقيق الحماية الشاملة للبيئة الرقمية. فالجانب التقني يمثل حجر الزاوية في منظومة الأمن السيبراني، إذ يشمل مجموعة من الأدوات والآليات مثل التشفير، والجدران النارية، وأنظمة كشف التسلل، ومراقبة حركة البيانات. وتُعدّ هذه العناصر التقنية ضرورية لمنع الاختراقات وتأمين سرية وسلامة وتوافر المعلومات داخل الشبكات الرقمية²، كما أكد الباحث فريد عبد المالك أن نجاح منظومة الأمن السيبراني يعتمد على التكامل بين "التقنيات الوقائية والبرمجيات الذكية والسياسات التقنية المعتمدة في إدارة المخاطر الرقمية"³، وهو ما يجعل البعد التقني الأساس الذي تبنى عليه بقية العناصر.

أما العنصر البشري فيُعدّ من أكثر الجوانب حساسية في مجال الأمن السيبراني، إذ تشير الدراسات إلى أن نسبة كبيرة من الاختراقات الأمنية تعود إلى أخطاء بشرية، سواء كانت ناتجة عن ضعف الوعي الأمني أو الإهمال أو سوء استخدام التكنولوجيا⁴، لذا، يُعتبر بناء ثقافة أمنية رقمية بين المستخدمين خطوة محورية في الحد من المخاطر، وهو ما تسعى الجزائر إلى تحقيقه من خلال برامج التكوين والتوعية التي تشرف عليها وزارة الرقمنة والإحصائيات بالتعاون مع مؤسسات الأمن الوطني⁵، كما يدخل ضمن العناصر الإدارية وضع سياسات أمنية مؤسسية تنظم طرق الوصول إلى المعلومات، وإجراءات الاستجابة للحوادث الرقمية، وخطط استمرارية العمل في حال وقوع هجمات إلكترونية.

وفيما يخص مجالات الأمن السيبراني، فهي تمتد لتشمل حماية البنية التحتية المعلوماتية الحيوية كأنظمة الطاقة، والمياه، والاتصالات، والمؤسسات المالية، إلى جانب أمن الشبكات الحكومية التي تمثل العمود الفقري للإدارة الإلكترونية⁶، كما يتسع مفهومه ليشمل أمن البيانات الشخصية وحماية الخصوصية الرقمية، وهو ما كرسه القانون

¹ - بوعزيز عبد القادر، "الأمن السيبراني في التشريع الجزائري بين الحاجة والتطبيق"، مجلة السياسة والأمن، جامعة الجزائر 3، العدد 6، 2022، ص. 31

² - زروقي كمال، "الأمن السيبراني كأداة لحماية البنية التحتية المعلوماتية"، مجلة العلوم القانونية والسياسية، جامعة باتنة، العدد 11، 2021، ص. 19

³ - عبد المالك فريد، مدخل إلى الأمن السيبراني وإدارة المخاطر الرقمية، دار الهدى، الجزائر، 2020، ص. 41

⁴ - بن يوسف محمد، المرجع السابق، ص. 46

⁵ - وزارة الرقمنة والإحصائيات، الاستراتيجية الوطنية للأمن السيبراني في الجزائر، الجزائر، 2021، ص. 12

⁶ - بوعزيز عبد القادر، المرجع السابق، ص. 29.

الجزائري رقم 18-04 لسنة 2018 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي¹، إضافة إلى ذلك، يشمل الأمن السيبراني مجال الحوكمة الرقمية، أي وضع الأطر القانونية والتنظيمية التي تضمن الاستخدام الآمن والمسؤول للتكنولوجيا. ومن ثمّ، فإن الأمن السيبراني لم يعد مجرد تخصص تقني، بل منظومة متعددة الأبعاد تشمل التكنولوجيا، القانون، الإنسان، المؤسسة، بهدف حماية الفضاء الرقمي وضمان استدامة التنمية الإلكترونية في الدولة.²

المطلب الثاني: مفهوم الأمن القانوني في البيئة الرقمية

الفرع الأول: تطور مفهوم الأمن القانوني وأبعاده في الفكر القانوني الحديث

أولاً: تطور مفهوم الأمن القانوني

يُعتبر مفهوم الأمن القانوني من المفاهيم المركزية التي برزت في الفكر القانوني الحديث، بوصفه أحد الأعمدة التي يقوم عليها مبدأ دولة القانون وضمان الثقة في المنظومة التشريعية والمؤسسية. وقد تطور هذا المفهوم تدريجياً ليعبر عن حاجة المجتمع إلى الاستقرار في القواعد القانونية وتوقع نتائج تطبيقها. فالأمن القانوني، في جوهره، يعني أن يكون القانون واضحاً، مستقراً، وقابلاً للتنبؤ، بحيث يستطيع الأفراد والمؤسسات تنظيم سلوكهم في ضوء معرفة مسبقة بحقوقهم وواجباتهم³، وقد نشأ هذا المفهوم في الفكر الأوروبي مع اجتهادات مجلس الدولة الفرنسي والحكمة الدستورية الألمانية في القرن العشرين، قبل أن ينتقل إلى الفقه العربي الحديث الذي أعاد صياغته في ضوء التحولات السياسية والمؤسسية التي شهدتها الدول النامية، ومنها الجزائر.⁴

من الناحية النظرية، يُعدّ الأمن القانوني أحد تجليات مبدأ الشرعية وسيادة القانون، إذ يهدف إلى تحقيق الطمأنينة القانونية للأفراد تجاه تصرفات السلطات العامة. فالقانون، كي يحقق غايته، يجب ألا يكون متقلباً أو غامضاً، بل ثابتاً ومعلوماً للجميع. وقد أشار الدكتور محمد الصغير بعلي إلى أن الأمن القانوني "يُترجم في الممارسة القانونية عبر استقرار التشريعات، وضمان عدم رجعية القوانين، واحترام مبدأ الثقة المشروعة للمواطنين في النصوص القانونية"⁵، هذا البعد المفاهيمي جعل الأمن القانوني يتجاوز مجرد الحماية القانونية الشكلية، ليصبح مفهوماً يلامس جوهر العدالة الإجرائية

¹ - القانون رقم 18-04 المؤرخ في 10 ماي 2018 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 27، 2018، ص. 6

² - منصوري سمير، "حوكمة الأمن السيبراني وأثرها على حماية الفضاء الرقمي"، مجلة البحوث القانونية المعاصرة، جامعة وهران، العدد 9، 2023، ص. 55

³ - الخالدي أحمد، الأمن القانوني ومبدأ استقرار القواعد القانونية، دار الفكر الجامعي، القاهرة، 2019، ص. 24

⁴ - بن ناصر عبد الرزاق، "تطور مفهوم الأمن القانوني في الفقه الدستوري الحديث"، مجلة البحوث القانونية والسياسية، جامعة باتنة، العدد 10، 2021، ص. 41

⁵ - بعلي محمد الصغير، النظام القانوني للأمن القانوني في التشريع الجزائري، دار هومة، الجزائر، 2020، ص. 33

والموضوعية. وفي السياق الجزائري، أكدت المحكمة الدستورية في عدة قراراتها على ضرورة احترام مبدأ الأمن القانوني كشرط لضمان المشروعية الدستورية للقوانين¹.

ثانياً: أبعاده في الفكر القانوني الحديث

أما من حيث الأبعاد، فإن الأمن القانوني يُجسّد ثلاثة مستويات مترابطة: البعد التشريعي الذي يقتضي وضوح النصوص واستقرارها وتكاملها، البعد القضائي الذي يضمن تفسيراً موحداً ومتوقفاً للقانون من قبل القضاء، والبعد الإداري الذي يرتبط بتصرفات الإدارة في إطار الشريعة والشفافية²، وقد بيّن الباحث عبد القادر بوعزيز أن غياب الأمن القانوني يؤدي إلى انعدام الثقة في الدولة ومؤسساتها، ويخلق بيئة قانونية مضطربة تُعيق الاستثمار والتنمية³، لذلك تبنت الجزائر، في إطار الإصلاحات التشريعية والإدارية، مقاربة جديدة لترسيخ الأمن القانوني من خلال تحديث النصوص، وتبسيط الإجراءات، وضمان الشفافية القانونية⁴، إن تطور مفهوم الأمن القانوني في الفكر القانوني الحديث يعكس تحوُّلاً نحو دولة القانون الفعلية، التي لا تكتفي بإصدار القوانين، بل تضمن تطبيقها بعدالة واستقرار، بما يعزز الثقة بين المواطن والسلطة العامة.

الفرع الثاني: علاقة الأمن القانوني بالتحول الرقمي وسيادة القانون الإلكتروني

تتجسد علاقة الأمن القانوني بالتحول الرقمي وسيادة القانون الإلكتروني في كونها علاقة تفاعلية تتأسس على ضرورة التوفيق بين مقتضيات التطور التكنولوجي ومتطلبات استقرار القاعدة القانونية. فالأمن القانوني في البيئة الرقمية يعني ضمان وضوح النصوص التشريعية واستقرارها وقابليتها للتطبيق على الوقائع الجديدة التي تفرزها التكنولوجيا، بما يحفظ ثقة الأفراد في المنظومة القانونية ويعزز سيادة القانون الإلكتروني بوصفه الامتداد الرقمي لمبدأ المشروعية التقليدي. ويظهر هذا الترابط جلياً في حاجة الدولة إلى تحديث بنيتها التشريعية لمواكبة التحول الرقمي، خصوصاً في مجالات التوقيع الإلكتروني، حماية المعطيات الشخصية، والأدلة الرقمية، إذ إن أي فراغ أو غموض تشريعي في هذه الميادين يُضعف من اليقين القانوني ويخلق مخاطر تتعلق بانتهاك الخصوصية أو المساس بالمصالح الاقتصادية للأفراد والمؤسسات. ومن ثم، فإن التحول الرقمي لا يمكن أن يحقق أهدافه التنموية إلا إذا ارتكز على منظومة قانونية رقمية تضمن الشفافية والعدالة وتكافؤ الفرص في الوصول إلى الخدمات الإلكترونية⁵.

¹ - القرار رقم 01/د.ع/2022 بشأن الرقابة الدستورية على القوانين، الجريدة الرسمية رقم 12، 2022، ص. 5

² - زواوي عبد الكريم، "الأمن القانوني كضمانة للثقة في النظام القانوني"، مجلة الحقوق والعلوم السياسية، جامعة الجزائر 1، العدد 8، 2022، ص. 28

³ - بوعزيز عبد القادر، المرجع السابق، ص. 39

⁴ - وزارة العدل الجزائرية، تقرير حول إصلاح المنظومة القانونية وتعزيز مبدأ الأمن القانوني، الجزائر، 2023، ص. 11

⁵ - معمر فراق وفهيم بلحمزي، "البيئة الإلكترونية والأمن القانوني"، مجلة العلوم القانونية والسياسية، جامعة ورقلة، العدد 12، 2017، ص. 45

لقد أبرزت التجربة الجزائرية أن التحول الرقمي يحتاج إلى مقارنة قانونية متكاملة تتضمن إصلاح التشريعات الإدارية والجزائية والمدنية على السواء، لتتلاءم مع متطلبات الفضاء الإلكتروني. وقد شكل صدور القانون رقم 07-18 خطوة مهمة نحو تكريس الأمن القانوني في البيئة الرقمية، إذ أرسى مبادئ احترام الحياة الخاصة، وفرض التزامات قانونية على الجهات المسؤولة عن معالجة البيانات، كما منح للمواطنين حق الاعتراض والوصول إلى المعلومات، وهو ما يعزز سيادة القانون الإلكتروني من خلال حماية الحقوق الأساسية للمستخدمين¹، لكن تطبيق هذا القانون عملياً ما زال يواجه تحديات تتعلق بضعف التنسيق المؤسسي، وغياب هيئات رقابية رقمية متخصصة، الأمر الذي يجعل الأمن القانوني في العالم الافتراضي هشاً أمام الجرائم الإلكترونية².

إن تحقيق سيادة القانون الإلكتروني يستوجب تطوير قدرات القضاء والإدارة في التعامل مع الأدلة الرقمية والعقود الإلكترونية، وضمان الشفافية في استخدام الذكاء الاصطناعي في المعاملات الحكومية، لأن ذلك يعزز الثقة في المنظومة الرقمية ويحد من التعسف في استعمال السلطة في الفضاء الإلكتروني. فالأمن القانوني في ظل التحول الرقمي لم يعد مجرد مبدأ قانوني جامد، بل أصبح شرطاً جوهرياً لاستدامة التنمية الرقمية، وضمان أن تكون التكنولوجيا في خدمة الإنسان لا أداة للمساس بحقوقه الأساسية³.

المبحث الثاني: التفاعل بين الأمن السيبراني والأمن القانوني في المجتمع الرقمي

المطلب الأول: الأمن السيبراني كضمانة لتحقيق الأمن القانوني

الفرع الأول: دور الحماية التقنية في استقرار المعاملات القانونية الرقمية

يشكل دور الحماية التقنية في استقرار المعاملات القانونية الرقمية أحد الركائز الجوهرية لضمان الأمن القانوني في البيئة الرقمية، إذ لم تعد النصوص القانونية وحدها كافية لتحقيق الثقة في المعاملات الإلكترونية دون وجود آليات تقنية مؤمنة تدعم مصداقيتها وسلامتها. فالتوقيع الإلكتروني، والتشفير، وأنظمة التحقق من الهوية الرقمية تمثل أدوات أساسية لحماية المعطيات وضمان حجية التصرفات القانونية في الفضاء الإلكتروني. إن الحماية التقنية تُعدّ بمثابة "الضمان

¹ - القانون رقم 07-18 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، ص. 12

² - بوجمعة بوشارب، "تأثير التطور التكنولوجي وتقنيات المعلومات على تحقيق الأمن القانوني"، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، جامعة الجزائر 1، العدد 3، 2022، ص. 78

³ - مسقمين نفيسة، "الإدارة الإلكترونية القانونية: تحديات وآفاق في الجزائر"، مجلة جامعة تموشنت للدراسات القانونية والإدارية، العدد 5، 2025، ص. 61

الرقمي" الذي يُمكن من استقرار المعاملات الإلكترونية ويمنع التلاعب بالمعلومات أو تزوير الوثائق الرقمية، مما يساهم في تحقيق مبدأ اليقين القانوني ويدعم سيادة القانون في البيئة الافتراضية¹

وقد أدرك المشرع الجزائري أهمية هذه الحماية، فعمل على تقنين الوسائل التقنية التي تضمن سلامة المبادلات الإلكترونية، من خلال القانون رقم 04-15 الذي وضع الإطار القانوني لاستخدام التوقيع الإلكتروني كوسيلة لإثبات المعاملات الرقمية، وجعل منه أداة توازي التوقيع الخطي التقليدي من حيث القوة الثبوتية. ويُعتبر هذا القانون خطوة هامة نحو تعزيز الثقة في الاقتصاد الرقمي، حيث نصّ على ضرورة اعتماد هيئات تصديق معتمدة تشرف على تأمين المعاملات الإلكترونية وضمان نزاهتها²، غير أن التطبيق العملي لهذا القانون ما زال يواجه عراقيل تقنية ومؤسسية تتعلق بضعف جاهزية البنية التحتية الرقمية، وغياب ثقافة قانونية رقمية لدى المتعاملين في السوق، مما يجعل الحماية التقنية لا تحقق أهدافها إلا جزئياً³.

كما تُساهم الحماية التقنية في استقرار المعاملات القانونية الرقمية من خلال اعتماد أنظمة التشفير القوية، والجدران النارية، وآليات التحقق المتعدد، التي تمنع الوصول غير المشروع إلى البيانات وتحافظ على سلامة الوثائق الإلكترونية أثناء نقلها أو تخزينها. هذه التقنيات تُوفّر مستوى عالٍ من الثقة الرقمية، وهو ما يُترجم قانونياً في استقرار المعاملات وازدياد الاعتماد على المنصات الإلكترونية الرسمية في التعاقد والتقاضي والدفع. إن استقرار المعاملات لا يتحقق إلا بتكامل بين الحماية التقنية والحماية القانونية، لأن كل ضعف في أحدهما ينعكس على الآخر؛ فالتكنولوجيا من دون إطار قانوني حاكم قد تتحول إلى أداة للمخاطر، في حين أن القوانين من دون حماية تقنية فعالة تبقى مجرد نصوص نظرية⁴، وعليه، فإن بناء منظومة حماية تقنية متطورة يُعتبر شرطاً لضمان استقرار المعاملات القانونية الرقمية وتعزيز الثقة في الاقتصاد الرقمي الجزائري، وتحقيق الأمن القانوني في عالم رقمي سريع التغير.

الفرع الثاني: الأمن السيبراني كآلية لتكريس الثقة في البيئة القانونية الإلكترونية

يُعدّ الأمن السيبراني أحد أهم الآليات الحديثة لتكريس الثقة في البيئة القانونية الإلكترونية، إذ يشكّل الإطار الوقائي الذي يضمن حماية الأنظمة الرقمية من الاختراقات والتلاعبات، ويحافظ على سرية وسلامة المعطيات المتبادلة في

¹ - مراد بن عتو، "الأمن القانوني في المعاملات الإلكترونية: مقارنة تكنولوجية"، مجلة العلوم القانونية والسياسية، جامعة الجزائر 1، العدد 8، 2021، ص. 37

² - القانون رقم 04-15 المؤرخ في 1 فبراير 2015 المتعلق بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 11، ص. 5

³ - حديجة بوشامة، "الحماية التقنية للمعاملات الإلكترونية في التشريع الجزائري"، مجلة الدراسات القانونية المعاصرة، جامعة سطيف 2، العدد 6، 2022، ص. 64

⁴ - سامية بن شريف، "التوقيع الإلكتروني وأثره في استقرار المعاملات القانونية الرقمية"، مجلة القانون والتكنولوجيا، جامعة تلمسان، العدد 4، 2023، ص. 59

المعاملات الإلكترونية. فالثقة في الفضاء الإلكتروني لا يمكن أن تُبنى دون وجود منظومة أمنية سيبرانية قوية تؤمّن البيانات والمراسلات والمعاملات القانونية التي تتم عبر الشبكات الرقمية. ويُترجم الأمن السيبراني من الناحية القانونية في مبدأ حماية الحقوق الرقمية للأفراد والمؤسسات، بما يضمن استقرار العلاقات القانونية القائمة على الوسائط الإلكترونية ويُعزّز مبدأ الأمن القانوني في العالم الرقمي¹، إن هذه الثقة تمثل الركيزة الأساسية لأي اقتصاد أو إدارة رقمية ناجحة، لأن فقدانها يؤدي إلى عزوف الأفراد عن التعامل عبر الوسائط الإلكترونية، مما يفرغ التحول الرقمي من محتواه القانوني والمؤسسي.

وقد أدرك المشرّع الجزائري هذه الحقيقة، فعمد إلى سنّ القانون رقم 05-23 الذي جاء ليضع إطاراً قانونياً متكاملًا لحماية الفضاء السيبراني الوطني من التهديدات والهجمات الإلكترونية، من خلال إنشاء الهيئة الوطنية للأمن السيبراني، وتحديد مهامها في الوقاية والرصد والتدخل عند وقوع الهجمات. ويُعد هذا القانون نقلة نوعية في تأمين البنية التحتية للمعلومات الحساسة التابعة للمؤسسات العمومية والخاصة، كما يرسّخ الثقة في المعاملات الإلكترونية من خلال تعزيز مسؤولية مقدمي الخدمات الرقمية وضبط التزاماتهم تجاه حماية البيانات والمستخدمين²، غير أن تفعيل هذا القانون يحتاج إلى موارد بشرية وتقنية مؤهلة، وتنسيق مؤسسي فعّال بين القطاعات الأمنية والقضائية والتقنية لضمان نجاعة منظومة الحماية³.

ومن الناحية العملية، يسهم الأمن السيبراني في تكريس الثقة القانونية الإلكترونية من خلال تأمين القنوات التي تُجرى عبرها العقود الرقمية، وحماية أنظمة التوقيع الإلكتروني، وضمان سرية المراسلات القضائية والإدارية الرقمية. كما يُساهم في الحد من الجرائم الإلكترونية التي تمسّ المعاملات القانونية، مثل الاحتيال الرقمي أو سرقة الهوية الإلكترونية، مما ينعكس إيجاباً على استقرار النظام القانوني الرقمي وفعالية العدالة الإلكترونية. إن الأمن السيبراني ليس مجرد إجراء تقني، بل هو مفهوم قانوني مؤسسي يُجسّد التزام الدولة بحماية الحقوق الرقمية للمواطنين والمستثمرين، ويعزز مبدأ سيادة القانون في الفضاء السيبراني⁴، وبذلك، فإن ترسيخ الثقة في البيئة القانونية الإلكترونية يمرّ حتماً عبر بناء منظومة سيبرانية وطنية متكاملة، تُوازن بين حماية الأمن المعلوماتي وصون الحقوق والحريات في العصر الرقمي.

¹ - عبد القادر بن قانة، "الأمن السيبراني ودوره في حماية البيئة القانونية الإلكترونية"، مجلة العلوم القانونية والسياسية، جامعة ورقلة، العدد 10، 2022، ص. 41.

² - القانون رقم 05-23 المؤرخ في 27 أبريل 2023 المتعلق بالأمن السيبراني، الجريدة الرسمية، العدد 30، ص. 7.

³ - زروقي سميرة، "تحديات الأمن السيبراني في الجزائر: مقارنة قانونية ومؤسسية"، مجلة الدراسات القانونية والإدارية، جامعة تلمسان، العدد 5، 2024، ص. 53.

⁴ - سارة بن عمار، "الثقة الرقمية والأمن السيبراني كدعامات للحكومة الإلكترونية"، المجلة الجزائرية للبحوث القانونية والاقتصادية، جامعة الجزائر 1، العدد 9، 2023، ص. 68.

المطلب الثاني: التحديات القانونية للأمن السيبراني

الفرع الأول: قصور التشريعات الوطنية في مواجهة الجرائم الإلكترونية

يشكل قصور التشريعات الوطنية في مواجهة الجرائم الإلكترونية أحد أبرز التحديات التي تُقوّض فاعلية المنظومة القانونية في البيئة الرقمية، إذ إن التطور السريع للتكنولوجيا يقابله غالباً بطء في استجابة المشرّع لسنّ النصوص القانونية المناسبة. فالكثير من القوانين الجزائرية ما زالت تستند إلى مفاهيم تقليدية للجريمة والعقوبة، دون أن تستوعب بالكامل الخصائص التقنية للجرائم السيبرانية التي تتميز بالطابع العابر للحدود وصعوبة التتبع الرقمي. إن هذا القصور التشريعي يُفرز ثغرات خطيرة في مبدأ الشرعية الجنائية، حيث تبقى العديد من الأفعال الإلكترونية غير مجرّمة بشكل صريح، أو تفتقر إلى نصوص إجرائية واضحة تضمن الإثبات والتحقيق والمحاكمة العادلة في الجرائم الرقمية¹.

وعلى الرغم من إدراج بعض التعديلات ضمن قانون العقوبات الجزائري بموجب القانون رقم 04-15 الذي أضاف مواد تجرّم الدخول غير المشروع إلى الأنظمة المعلوماتية وتزوير المعطيات الإلكترونية، إلا أن هذه النصوص تبقى محدودة النطاق ولا تغطي كل صور الجرائم الإلكترونية المعاصرة مثل الاحتيال عبر العملات الرقمية أو الابتزاز الإلكتروني. كما أن القانون لم يتناول بعمق مسألة المسؤولية الجنائية للأشخاص المعنويين في الفضاء الإلكتروني، ولا نظم الإثبات الرقمي المعتمد أمام القضاء، ما يضعف الملاحقة القضائية ويجعل العديد من القضايا تُحفظ لغياب الأدلة التقنية الكافية²، هذا القصور ينعكس أيضاً على التنسيق المؤسسي بين الأجهزة الأمنية والقضائية، حيث يفتقر القضاء الجزائري إلى كوادرات تقنية متخصصة قادرة على التعامل مع الأدلة الرقمية وتحليلها وفق المعايير الدولية³.

ومن الناحية العملية، فإن غياب استراتيجية تشريعية شاملة لمكافحة الجريمة الإلكترونية يُؤثر سلباً على الأمن القانوني والثقة الرقمية، إذ يشعر المواطن والمستثمر بعدم كفاية الحماية القانونية في البيئة الإلكترونية. ورغم صدور القانون رقم 05-23 الذي نص على آليات للوقاية من الهجمات الإلكترونية، إلا أنه بقي ذا طابع وقائي وأمني أكثر منه جزائي، مما يستدعي مراجعة شاملة للمنظومة القانونية لتضمين نصوص ردعية واضحة تتلاءم مع تطور التهديدات الرقمية⁴، وبالتالي، فإن معالجة هذا القصور تستوجب تطوير تشريعات متخصصة في الجريمة السيبرانية، وتعزيز قدرات

¹ - بن عطية محمد، "القصور التشريعي في مواجهة الجرائم الإلكترونية في الجزائر"، مجلة العلوم القانونية والسياسية، جامعة بسكرة، العدد 7، 2021، ص. 29.

² - القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، الجريدة الرسمية، العدد 71، ص. 4.

³ - بن ساسي فاطمة الزهراء، "التحديات التقنية في الإثبات الجنائي للجرائم الإلكترونية"، مجلة البحوث القانونية المعاصرة، جامعة الجزائر 1، العدد 9، 2022، ص. 63.

⁴ - القانون رقم 05-23 المؤرخ في 27 أبريل 2023 المتعلق بالأمن السيبراني، الجريدة الرسمية، العدد 30، ص. 7.

القضاء والشرطة الرقمية، وإنشاء محاكم مختصة في قضايا الجرائم الإلكترونية، لضمان تطبيق القانون بفعالية وتحقيق الردع القانوني في البيئة الرقمية الحديثة.

الفرع الثاني: إشكاليات الإثبات والمسؤولية القانونية في الفضاء الرقمي

تُعدّ إشكاليات الإثبات والمسؤولية القانونية في الفضاء الرقمي من أعقد القضايا التي تواجه المنظومات القضائية الحديثة، إذ أدّت الرقمنة إلى تغيير عميق في طبيعة الأدلة القانونية وطرق جمعها وحجيتها أمام القضاء. ففي البيئة الإلكترونية، لم تعد الوثائق الورقية ولا التوقيعات التقليدية هي السائدة، بل حلت محلها الأدلة الرقمية مثل الرسائل الإلكترونية، والسجلات الرقمية، وبيانات الخوادم، والتوقيع الإلكتروني. وهذا التحوّل أوجد تحدياً مزدوجاً: أولاً، صعوبة التأكد من مصداقية الدليل الرقمي وثبوته؛ وثانياً، تحديد المسؤولية القانونية عند وقوع الضرر في فضاء يتسم باللامادية والتعقيد التقني. فإثبات الجريمة أو التصرف القانوني في العالم الرقمي يتطلب خبرة تقنية متقدمة وقدرة على تتبع البصمات الإلكترونية، وهو ما يفرض على القضاء تكييف قواعد الإثبات التقليدية مع خصوصية الأدلة الرقمية¹.

في السياق الجزائري، حاول المشرّع معالجة هذه الإشكاليات عبر القانون رقم 15-04 الذي اعترف بالحاجة القانونية للتوقيع الإلكتروني متى تم وفق إجراءات تقنية مؤمنة تضمن هوية الموقع وسلامة الوثيقة. كما نصّ قانون الإجراءات المدنية والإدارية في بعض تعديلاته على إمكانية اعتماد النسخ الإلكترونية كوسيلة إثبات، إلا أن الإطار العملي لا يزال يعاني من غياب معايير تقنية موحدة للاعتراف بالأدلة الرقمية أمام القضاء، وهو ما يجعل القاضي يعتمد في كثير من الأحيان على السلطة التقديرية دون وجود توجيهات قانونية دقيقة²، هذا النقص التشريعي يفتح المجال لتفاوت الأحكام وضعف توحيد الاجتهاد القضائي في القضايا ذات الطابع الإلكتروني³.

أما على مستوى المسؤولية القانونية في الفضاء الرقمي، فإن التحدي الأكبر يكمن في تحديد من يتحمّل المسؤولية عند وقوع ضرر إلكتروني: هل هو المستخدم، أم مزوّد الخدمة، أم الجهة التي تدير المنصة الرقمية؟ إذ أن غياب النصوص الصريحة يخلق تداخلاً بين المسؤولية المدنية والجنائية، خاصة في حالات الاختراق أو تسريب البيانات أو الأعطال البرمجية. وفي ظل عدم وجود تشريعات دقيقة تُحدّد معايير الخطأ والإهمال في المجال الرقمي، يصبح من الصعب ترتيب المسؤولية القانونية بشكل عادل ومتوازن. لذلك، فإن تطوير منظومة الإثبات والمسؤولية في الجزائر يتطلب تحديث القوانين

¹ - بن يوسف أمينة، "الإثبات في المعاملات الإلكترونية: بين النص القانوني والتطبيق القضائي"، مجلة العلوم القانونية والسياسية، جامعة الجزائر 1،

العدد 11، 2021، ص. 56

² - القانون رقم 15-04 المؤرخ في 1 فبراير 2015 المتعلق بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 11، ص. 5.

³ - بوزيد عبد النور، "الإشكالات العملية لإثبات الجرائم الإلكترونية في القانون الجزائري"، مجلة البحوث القانونية المعاصرة، جامعة سطيف 2،

العدد 8، 2022، ص. 72

الإجرائية، وتكوين قضاة وخبراء تقنيين في مجال الأدلة الرقمية، وإنشاء وحدات قضائية متخصصة في الجرائم والالتزامات الإلكترونية¹.

المبحث الثالث: آليات تحقيق الأمن القانوني من خلال الأمن السيبراني

المطلب الأول: الأطر التشريعية والتنظيمية للأمن السيبراني

الفرع الأول: القوانين الوطنية المنظمة للأمن السيبراني (دراسة حالة: الجزائر وبعض الدول العربية)

يُعدّ الإطار التشريعي الوطني المنظم للأمن السيبراني في الجزائر وبعض الدول العربية محوراً أساسياً في بناء منظومة حماية رقمية شاملة، لما له من دور في ضمان سلامة الفضاء الإلكتروني، وحماية الحقوق الرقمية، وتعزيز الثقة في المعاملات الإلكترونية. ففي الحالة الجزائرية، يُعتبر القانون رقم 05-23 أول نص تشريعي شامل يُؤطر حماية الفضاء السيبراني الوطني، إذ نصّ على إنشاء الهيئة الوطنية للأمن السيبراني، وحدّد مهامها في الوقاية، والرصد، والتدخل، وحماية البنى التحتية الحيوية للمعلومات. كما وضع القانون أسس التعاون بين السلطات الإدارية والأمنية والتقنية، في سبيل مواجهة التهديدات الإلكترونية المحلية والعابرة للحدود. ومع ذلك، فإن تطبيقه يواجه تحديات مؤسسية وتقنية تتعلق بضعف الكفاءات المتخصصة ونقص التجهيزات، ما يجعل الأمن السيبراني في الجزائر في مرحلة تأسيسية تتطلب مزيداً من تفعيل والتنسيق بين مختلف القطاعات المعنية².

في المقابل، تُظهر التجارب العربية المقارنة نماذج مختلفة في التعامل مع الأمن السيبراني. فالمملكة المغربية اعتمدت القانون رقم 05.20 المتعلق بالأمن السيبراني سنة 2020، الذي أرسى إطاراً مؤسسياً متطوراً عبر "المديرية العامة لأمن نظم المعلومات"، وركّز على حماية شبكات الدولة والمؤسسات الحساسة، مع إقرار آليات إلزامية للإبلاغ عن الحوادث السيبرانية. أما في جمهورية مصر العربية، فقد سنّ القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الذي يُعدّ أكثر تركيزاً على الجانب الجزري، حيث نصّ على عقوبات جزائية مشددة على الأفعال التي تمسّ أمن الدولة أو الخصوصية الرقمية، مع الاعتراف بالأدلة الرقمية كوسيلة إثبات أمام القضاء. هذه القوانين تُمثل تجارب رائدة في العالم العربي، إذ سعت إلى إيجاد توازن بين حماية الأمن السيبراني وصون الحقوق والحريات الرقمية³.

¹ - رحامي سميرة، "المسؤولية القانونية في الفضاء الرقمي بين الفاعل والمزود"، مجلة القانون والتكنولوجيا، جامعة تلمسان، العدد 6، 2023، ص. 67

² - قانون رقم 05-23 المؤرخ في 27 أبريل 2023 المتعلق بالأمن السيبراني، الجريدة الرسمية، العدد 30، ص. 7

³ - عبد الله الشريف، "القوانين العربية المنظمة للأمن السيبراني: دراسة مقارنة بين الجزائر والمغرب ومصر"، مجلة البحوث القانونية والسياسية، جامعة الجزائر 1، العدد 12، 2024، ص. 42

ورغم اختلاف المقاربات بين الجزائر والدول العربية الأخرى، إلا أن القاسم المشترك بينها هو السعي إلى إرساء منظومة تشريعية تستجيب لمخاطر الفضاء السيبراني وتنسجم مع المعايير الدولية، مثل اتفاقية بودابست لعام 2001 بشأن الجريمة الإلكترونية. ومع ذلك، يظل التحدي الأكبر في المنطقة العربية مرتبطاً بضعف التنسيق الإقليمي، وغياب استراتيجيات وطنية متكاملة للأمن السيبراني، وتعدد الجهات المسؤولة عن التنفيذ. لذا، فإن تطوير القوانين الوطنية يجب أن يواكبه بناء مؤسسات قوية، وتدريب كوادر متخصصة، وتبني مقاربة تشاركية تجمع بين التشريع والتكنولوجيا والسياسات العامة، لضمان فعالية الحماية السيبرانية في العالم العربي¹.

الفرع الثاني: الأطر الدولية والإقليمية (الاتحاد الأوروبي - مجلس أوروبا - الأمم المتحدة)

يشكّل الأمن السيبراني اليوم أحد أبرز القضايا التي استقطبت اهتمام المنظمات الدولية والإقليمية، بالنظر إلى تزايد التهديدات التي تستهدف البنى التحتية الرقمية للدول والمؤسسات. فقد أضحت تطوير أطر قانونية وتنظيمية شاملة في هذا المجال ضرورة استراتيجية لضمان حماية الفضاء السيبراني، وصون سيادة الدول الرقمية، وتعزيز الثقة في الاقتصاد الرقمي العالمي. ويُعدّ الاتحاد الأوروبي من أبرز الفاعلين في صياغة سياسات متقدمة في هذا المجال، حيث تبنت التوجيه الأوروبي للأمن السيبراني لعام 2016 المعروف بـ (NIS Directive)، الذي وضع معايير ملزمة لتأمين الشبكات والأنظمة المعلوماتية، وأرسى قواعد للتعاون بين الدول الأعضاء في مواجهة الحوادث السيبرانية الكبرى²، كما أنشئت وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) لتنسيق الجهود التقنية والقانونية وتقديم الدعم للدول الأعضاء في بناء قدراتها الوطنية³.

أما على مستوى مجلس أوروبا، فقد برز دوره من خلال اتفاقية بودابست لعام 2001 حول الجريمة المعلوماتية، التي تُعد أول وثيقة دولية ملزمة تعالج الأفعال الإجرامية في الفضاء الإلكتروني من قبيل الاختراق، وتزوير البيانات، والإرهاب السيبراني⁴، وقد مكّنت الاتفاقية من توحيد المفاهيم القانونية بين الدول الأطراف، كما ألزمتها بتجريم سلوكيات محددة وتبادل المعلومات في إطار التعاون القضائي الدولي. وبالرغم من أن الجزائر والدول العربية لم تصادق جميعها على الاتفاقية، إلا أن مضمونها أثر في التشريعات الوطنية، لاسيما من حيث تبني مبدأ التعاون القضائي الدولي ومواءمة القوانين مع المعايير الأوروبية⁵.

¹ - بن عتو مراد، "الحوكمة التشريعية للأمن السيبراني في الوطن العربي"، مجلة القانون والتكنولوجيا، جامعة تلمسان، العدد 5، 2023، ص. 64

² - الاتحاد الأوروبي، توجيه البرلمان والمجلس الأوروبي رقم (1148/2016) بشأن أمن الشبكات ونظم المعلومات، بروكسل، 2016، ص. 5

³ - الوكالة الأوروبية للأمن السيبراني (ENISA)، تقرير حول تنفيذ التوجيه الأوروبي للأمن السيبراني، أتبنا، 2020، ص. 12

⁴ - مجلس أوروبا، اتفاقية بودابست بشأن الجريمة المعلوماتية، بودابست، 2001، ص. 3

⁵ - بن ناصر، عبد الحكيم، "انعكاسات اتفاقية بودابست على التشريعات العربية"، مجلة القانون والتكنولوجيا، جامعة الجزائر 1، العدد 6، 2022، ص. 45

وفي الإطار الأممي، تعمل الأمم المتحدة من خلال عدة هيئات، أبرزها "فريق الخبراء الحكوميين بشأن التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي" (GGE)، و"مجموعة العمل المفتوحة العضوية" (OEWG)، على تطوير قواعد السلوك المسؤول للدول في الفضاء السيبراني¹، وقد أسهمت تقارير الأمم المتحدة في ترسيخ مبدأ أن القواعد القانونية الدولية، وعلى رأسها ميثاق الأمم المتحدة، تسري على الفضاء السيبراني، بما في ذلك احترام سيادة الدول وعدم التدخل في شؤونها الداخلية²، كما تشجع المنظمة على بناء القدرات الوطنية والإقليمية في مجالات الوقاية والاستجابة للهجمات السيبرانية، بما يعزز الأمن الجماعي في البيئة الرقمية.

وعلى الرغم من هذا الزخم الدولي، لا تزال الفجوة قائمة بين الأطر المعيارية العالمية والواقع العملي في العديد من الدول النامية، ومنها الجزائر والدول العربية، بسبب محدودية الإمكانيات التقنية وضعف التنسيق الإقليمي. لذا بات من الضروري إدماج هذه الأطر في التشريعات الوطنية، عبر إنشاء هيئات وطنية متخصصة وتفعيل التعاون الدولي، لضمان بيئة رقمية آمنة ومتوازنة بين الحريات الفردية ومتطلبات الأمن الوطني³.

المطلب الثاني: مقترحات لتعزيز الأمن القانوني في الفضاء الرقمي

الفرع الأول: نحو حوكمة رقمية شاملة قائمة على الثقة والأمن

تُعدّ الحوكمة الرقمية من أهم الركائز الحديثة التي تقوم عليها إدارة الشأن العام في عصر التحول الرقمي، إذ تهدف إلى تحقيق توازن بين متطلبات الكفاءة والشفافية من جهة، وضمان حماية الحقوق الرقمية والأمن المعلوماتي من جهة أخرى. فالتحول نحو الحوكمة الرقمية لا يقتصر على رقمنة الخدمات والإجراءات الإدارية فحسب، بل يتطلب بناء منظومة مؤسسية وتشريعية شاملة تكرّس مبادئ الثقة والأمن السيبراني كعنصرين أساسيين لضمان استدامة النظام الرقمي الوطني⁴، فالثقة الرقمية تُبنى عبر توفير ضمانات قانونية لحماية البيانات الشخصية والمعاملات الإلكترونية، بينما يشكّل الأمن السيبراني السياج الوقائي ضد الاختراقات والتهديدات الإلكترونية التي قد تمسّ استقرار المؤسسات والدولة⁵.

¹ - الأمم المتحدة، تقرير فريق الخبراء الحكوميين بشأن الأمن السيبراني، نيويورك، 2015، ص. 7.

² - بوزيدي، سامية، "القانون الدولي وتحديات الأمن السيبراني"، مجلة الدراسات القانونية والسياسية، جامعة قسنطينة، العدد 8، 2021، ص. 33.

³ - الاستراتيجية الوطنية للأمن السيبراني 2022-2025، وزارة الرقمنة والإحصائيات، الجزائر، 2022، ص. 18.

⁴ - بن يحيى عبد الرؤوف، الحوكمة الإلكترونية وأثرها على تحديث الإدارة العامة، دار الهدى للنشر، الجزائر، 2020، ص. 25.

⁵ - زروقي نادية، "الأمن السيبراني كدعامة للحكومة الرقمية"، مجلة دراسات قانونية وسياسية، جامعة الجزائر 1، العدد 10، 2021، ص. 54.

وفي السياق الجزائري، بدأت معالم الحوكمة الرقمية تتجلى من خلال إصدار مجموعة من النصوص القانونية التي تؤسس للإدارة الإلكترونية الآمنة، على غرار القانون رقم 07-18 والذي أرسى أسس الثقة في البيئة الرقمية¹، كما أطلقت الدولة الاستراتيجية الوطنية للأمن السيبراني (2022-2025) لتعزيز منظومة الوقاية والاستجابة للحوادث المعلوماتية، وتكريس مبدأ "التحكم في الفضاء الرقمي الوطني"²، غير أن تحقيق حوكمة رقمية فعالة يظل مرهوناً بمدى التنسيق بين مختلف الفاعلين: المؤسسات الحكومية، والقطاع الخاص، والمجتمع المدني، ضمن إطار شفاف يقوم على المساءلة الرقمية والتدبير الرشيد للمخاطر³.

من جانب آخر، تشكل الثقة الإلكترونية الإطار المعنوي الذي يضمن قبول المواطنين والمستثمرين للتعامل عبر المنصات الرقمية الحكومية والخاصة. وتحقق هذه الثقة من خلال إرساء أنظمة تشفير قوية، واعتماد آليات التحقق من الهوية الرقمية، وضمان سلامة البنية التحتية التقنية⁴، كما أن بناء الثقة لا ينفصل عن تكوين الموارد البشرية المؤهلة لتسيير الأنظمة الرقمية بأمان، وهو ما شددت عليه النصوص الجزائرية من خلال تشجيع التكوين في مجالات أمن المعلومات والتدبير الإلكتروني للمخاطر⁵.

وعلى الصعيد العربي، تتجه العديد من الدول، مثل الإمارات والسعودية، إلى تبني نماذج متقدمة للحكومة الرقمية تعتمد على التكامل بين الأمن السيبراني والإدارة الذكية، مما جعلها نماذج رائدة في مجال بناء ثقة المستخدمين. ومن ثم، فإن الجزائر مدعوة إلى الاستفادة من هذه التجارب عبر تعزيز البنية التشريعية والتنظيمية وضمان شفافية المعاملات الرقمية، تحقيقاً لغاية استراتيجية تتمثل في بناء حوكمة رقمية شاملة قائمة على الثقة والأمن⁶.

الفرع الثاني: توصيات تشريعية ومؤسسية لتعزيز التكامل بين الأمن القانوني والسيبراني

يشكل التكامل بين الأمن القانوني والأمن السيبراني ضرورة محورية في بناء دولة رقمية آمنة تحترم سيادة القانون وتضمن استقرار المعاملات الإلكترونية. فالتحديات الراهنة التي تفرضها الجرائم السيبرانية والهجمات المعلوماتية تستدعي مقاربة شمولية تدمج بين الأدوات التقنية والحماية القانونية، في إطار منظومة متكاملة تتسم بالفعالية والشفافية. ويُعدّ الإصلاح التشريعي حجر الزاوية في هذا التكامل، إذ يتطلب تحديث القوانين الوطنية لتتوافق مع متغيرات البيئة الرقمية،

¹ - القانون رقم 07-18 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، 2018، ص. 4

² - وزارة الرقمنة والإحصائيات، الاستراتيجية الوطنية للأمن السيبراني 2022-2025، الجزائر، 2022، ص. 11

³ - بوعلام سليم، "الحوكمة الرقمية ومتطلبات الأمن القانوني في الجزائر"، مجلة السياسة والقانون، جامعة قسنطينة، العدد 9، 2022، ص. 67

⁴ - شارف عبد القادر، الثقة الرقمية وحماية المعاملات الإلكترونية، دار المعرفة الجامعية، الجزائر، 2021، ص. 38

⁵ - وزارة التعليم العالي والبحث العلمي، تقرير حول تطوير كفاءات الأمن السيبراني في الجزائر، الجزائر، 2023، ص. 19

⁶ - البخيت فاطمة، "نحو نموذج عربي موحد للحكومة الرقمية الآمنة"، مجلة الفكر الإداري العربي، دبي، العدد 5، 2022، ص. 42

لا سيما في مجالات الإثبات الإلكتروني، وحماية البيانات الشخصية، والمسؤولية القانونية عن الأفعال السيبرانية¹، كما يجب أن تتبنى الجزائر تشريعات خاصة بالأمن السيبراني كقانون مستقل يحدد الأطر القانونية للتدبير الوقائي والتقني، ويكرّس مبدأ التناسب بين الحريات الرقمية ومتطلبات الأمن العام².

ومن الناحية المؤسساتية، تبرز الحاجة إلى إنشاء هيئة وطنية عليا للتكامل بين الأمن القانوني والسيبراني تُعنى بالتنسيق بين مختلف القطاعات الحكومية والأمنية، وتعمل على إعداد سياسات وطنية موحدة لمواجهة المخاطر الرقمية³، ويمكن أن تضطلع هذه الهيئة بوظائف الرقابة، وتقديم الاستشارات القانونية والتقنية، وتطوير آليات الإنذار المبكر ضد التهديدات الإلكترونية. كما يُوصى بتعزيز التعاون بين وزارة العدل ووزارة الرقمنة والإحصائيات في إعداد تشريعات مشتركة، بما يضمن توحيد المرجعية القانونية للفضاء الرقمي⁴.

كذلك ينبغي إدماج موضوع الأمن السيبراني في التكوين القانوني والأمني، من خلال فتح تخصصات جامعية جديدة في القانون الرقمي والعدالة السيبرانية، قصد تكوين قضاة ومحامين وخبراء قادرين على معالجة القضايا التقنية المعقدة. وقد أثبتت التجارب الدولية، مثل تجربة الاتحاد الأوروبي، أهمية الاستثمار في العنصر البشري لتطوير القدرات الوطنية في مواجهة التهديدات الرقمية⁵.

وعلى المستوى الدولي، يُستحسن أن تنخرط الجزائر في الاتفاقيات متعددة الأطراف مثل اتفاقية بودابست حول الجريمة المعلوماتية، لما تتيحه من فرص تعاون قضائي وتبادل للمعلومات بين الدول، مما يعزز الأمن القانوني عبر الحدود⁶، كما ينبغي ترسيخ مبدأ الشفافية الرقمية وتعزيز ثقة المواطنين في المؤسسات من خلال تطوير المنصات الآمنة للخدمات الإلكترونية الحكومية⁷، وفي المحصلة، فإن التكامل بين الأمن القانوني والسيبراني ليس مجرد خيار تقني أو قانوني، بل هو توجه استراتيجي يهدف إلى بناء فضاء رقمي آمن، تسوده الثقة، وتُحترم فيه الحقوق الأساسية في ظل سيادة القانون⁸.

¹ - بن ساسي، فريد، الأمن القانوني في البيئة الرقمية، دار الجامعة الجديدة، الجزائر، 2021، ص. 41

² - بوشامة عبد القادر، الحماية القانونية للأمن السيبراني في التشريع الجزائري، مجلة القانون والتكنولوجيا، جامعة الجزائر 1، العدد 7، 2022، ص. 58

³ - وزارة الدفاع الوطني، تقرير حول الاستراتيجية الوطنية للأمن السيبراني، الجزائر، 2022، ص. 15

⁴ - وزارة العدل، مشروع إصلاح القوانين المتعلقة بالجريمة الإلكترونية، الجزائر، 2023، ص. 9.

⁵ - الاتحاد الأوروبي، تقرير حول القدرات الوطنية في الأمن السيبراني، بروكسل، 2020، ص. 12

⁶ - مجلس أوروبا، اتفاقية بودابست بشأن الجريمة المعلوماتية، بودابست، 2001، ص. 3

⁷ - بوناب أمينة، "الثقة الإلكترونية كدعم للحكومة الرقمية"، مجلة العلوم القانونية والإدارية، جامعة قسنطينة، العدد 10، 2021، ص. 48

⁸ - الاستراتيجية الوطنية للأمن السيبراني 2022-2025، وزارة الرقمنة والإحصائيات، الجزائر، 2022، ص. 20

خاتمة:

يتّضح من خلال التحليل النظري والعملي أنّ الأمن السيبراني لم يعد مجرد مجال تقني أو فرع من فروع تكنولوجيا المعلومات، بل أصبح ركيزة أساسية لتحقيق الأمن القانوني في المجتمع الرقمي. فكل تطور في البنية الرقمية يقابله تحدّ قانوني جديد، يستدعي أدوات تشريعية ومؤسسية قادرة على ضمان الاستقرار والعدالة في فضاء يتسم بالتحوّل المستمر. لقد أثبتت التجربة الرقمية أنّ حماية الحقوق والحريات، وضمان نزاهة المعاملات الإلكترونية، لا يمكن أن يتحققا إلا في ظل منظومة أمن سيبراني فعالة، تُطوّرها نصوص قانونية واضحة وتخضع لمعايير الشفافية والمساءلة.

نتائج:

ومن أبرز النتائج المتوصل إليها أنّ التكامل بين الأمنين القانوني والسيبراني هو الأساس في بناء الثقة الرقمية بين المواطن والدولة، لأن أي خلل في المنظومة التقنية أو القانونية يُفضي إلى تقويض مبدأ سيادة القانون في البيئة الإلكترونية. كما تبين أنّ وجود تشريعات جزئية أو متفرقة لا يكفي لمواجهة الجرائم المعلوماتية المعقدة، مما يفرض ضرورة تبني قانون شامل للأمن السيبراني يُنظّم الوقاية والحماية والعقوبات ضمن مقاربة متكاملة. إضافة إلى ذلك، أظهرت الدراسة أنّ تحقيق الأمن القانوني في الفضاء الرقمي لا يقتصر على النصوص القانونية وحدها، بل يرتبط أيضاً بتفعيل مؤسسات متخصصة في الأمن المعلوماتي، وتطوير البنية التحتية التكنولوجية، وتكوين الكفاءات الوطنية القادرة على التعامل مع المخاطر السيبرانية بفعالية ومسؤولية.

قائمة المراجع:

الكتب:

1. بعلي محمد الصغير، النظام القانوني للأمن القانوني في التشريع الجزائري، دار هومة، الجزائر، 2020
2. بن ساسي فريد، الأمن القانوني في البيئة الرقمية، دار الجامعة الجديدة، الجزائر، 2021
3. بن يحي عبد الرؤوف، الحوكمة الإلكترونية وأثرها على تحديث الإدارة العامة، دار الهدى للنشر، الجزائر، 2020
4. الخالدي أحمد، الأمن القانوني ومبدأ استقرار القواعد القانونية، دار الفكر الجامعي، القاهرة، 2019
5. شارف عبد القادر، الثقة الرقمية وحماية المعاملات الإلكترونية، دار المعرفة الجامعية، الجزائر، 2021
6. عبد المالك فريد، مدخل إلى الأمن السيبراني وإدارة المخاطر الرقمية، دار الهدى، الجزائر، 2020

المجلات:

1. البخيت فاطمة، "نحو نموذج عربي موحد للحكومة الرقمية الآمنة"، مجلة الفكر الإداري العربي، دبي، العدد 5، 2022

2. بن ساسي فاطمة الزهراء، "التحديات التقنية في الإثبات الجنائي للجرائم الإلكترونية"، مجلة البحوث القانونية المعاصرة، جامعة الجزائر 1، العدد 9، 2022
3. بن عتو مراد، "الحوكمة التشريعية للأمن السيبراني في الوطن العربي"، مجلة القانون والتكنولوجيا، جامعة تلمسان، العدد 5، 2023
4. بن عطية محمد، "القصور التشريعي في مواجهة الجرائم الإلكترونية في الجزائر"، مجلة العلوم القانونية والسياسية، جامعة بسكرة، العدد 7، 2021
5. بن ناصر عبد الرزاق، "تطور مفهوم الأمن القانوني في الفقه الدستوري الحديث"، مجلة البحوث القانونية والسياسية، جامعة باتنة، العدد 10، 2021
6. بن ناصر، عبد الحكيم، "انعكاسات اتفاقية بودابست على التشريعات العربية"، مجلة القانون والتكنولوجيا، جامعة الجزائر 1، العدد 6، 2022
7. بن يوسف أمينة، "الإثبات في المعاملات الإلكترونية: بين النص القانوني والتطبيق القضائي"، مجلة العلوم القانونية والسياسية، جامعة الجزائر 1، العدد 11، 2021
8. بن يوسف محمد، "التحديات السيبرانية في الجزائر: واقع وآفاق"، مجلة الدراسات الأمنية، جامعة الجزائر 3، العدد 5، 2022
9. بوجمعة بوشارب، "تأثير التطور التكنولوجي وتقنيات المعلومات على تحقيق الأمن القانوني"، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، جامعة الجزائر 1، العدد 3، 2022
10. بوزيد عبد النور، "الإشكالات العملية لإثبات الجرائم الإلكترونية في القانون الجزائري"، مجلة البحوث القانونية المعاصرة، جامعة سطيف 2، العدد 8، 2022
11. بوزيدي، سامية، "القانون الدولي وتحديات الأمن السيبراني"، مجلة الدراسات القانونية والسياسية، جامعة قسنطينة، العدد 8، 2021
12. بوعزيز عبد القادر، "الأمن السيبراني في التشريع الجزائري بين الحاجة والتطبيق"، مجلة السياسة والأمن، جامعة الجزائر 3، العدد 6، 2022
13. بوعلام سليم، "الحوكمة الرقمية ومتطلبات الأمن القانوني في الجزائر"، مجلة السياسة والقانون، جامعة قسنطينة، العدد 9، 2022
14. بوناب أمينة، "الثقة الإلكترونية كدعامة للحكومة الرقمية"، مجلة العلوم القانونية والإدارية، جامعة قسنطينة، العدد 10، 2021

15. خديجة بوشامة، "الحماية التقنية للمعاملات الإلكترونية في التشريع الجزائري"، مجلة الدراسات القانونية المعاصرة، جامعة سطيف 2، العدد 6، 2022
16. رحاني سميرة، "المسؤولية القانونية في الفضاء الرقمي بين الفاعل والمزود"، مجلة القانون والتكنولوجيا، جامعة تلمسان، العدد 6، 2023
17. زروقي سميرة، "تحديات الأمن السيبراني في الجزائر: مقارنة قانونية ومؤسسية"، مجلة الدراسات القانونية والإدارية، جامعة تلمسان، العدد 5، 2024
18. زروقي كمال، "الأمن السيبراني كأداة لحماية البنية التحتية المعلوماتية"، مجلة العلوم القانونية والسياسية، جامعة باتنة، العدد 11، 2021
19. زروقي نادية، "الأمن السيبراني كدعامة للحكومة الرقمية"، مجلة دراسات قانونية وسياسية، جامعة الجزائر 1، العدد 10، 2021
20. زواوي عبد الكريم، "الأمن القانوني كضمانة للثقة في النظام القانوني"، مجلة الحقوق والعلوم السياسية، جامعة الجزائر 1، العدد 8، 2022
21. سارة بن عمار، "الثقة الرقمية والأمن السيبراني كدعامة للحكومة الإلكترونية"، المجلة الجزائرية للبحوث القانونية والاقتصادية، جامعة الجزائر 1، العدد 9، 2023
22. سامية بن شريف، "التوقيع الإلكتروني وأثره في استقرار المعاملات القانونية الرقمية"، مجلة القانون والتكنولوجيا، جامعة تلمسان، العدد 4، 2023
23. عبد القادر بن قانة، "الأمن السيبراني ودوره في حماية البيئة القانونية الإلكترونية"، مجلة العلوم القانونية والسياسية، جامعة ورقلة، العدد 10، 2022
24. عبد القادر بن قانة، الحماية القانونية للأمن السيبراني في التشريع الجزائري، مجلة القانون والتكنولوجيا، جامعة الجزائر 1، العدد 7، 2022
25. عبد الله الشريفي، "القوانين العربية المنظمة للأمن السيبراني: دراسة مقارنة بين الجزائر والمغرب ومصر"، مجلة البحوث القانونية والسياسية، جامعة الجزائر 1، العدد 12، 2024
26. مراد بن عتو، "الأمن القانوني في المعاملات الإلكترونية: مقارنة تكنولوجية"، مجلة العلوم القانونية والسياسية، جامعة الجزائر 1، العدد 8، 2021
27. مسقمين نفيسة، "الإدارة الإلكترونية القانونية: تحديات وآفاق في الجزائر"، مجلة جامعة تموشنت للدراسات القانونية والإدارية، العدد 5، 2025
28. معمر فراق وفهيم بلحمزي، "البيئة الإلكترونية والأمن القانوني"، مجلة العلوم القانونية والسياسية، جامعة ورقلة، العدد 12، 2017

29. منصوري سمير، "حوكمة الأمن السيبراني وأثرها على حماية الفضاء الرقمي"، مجلة البحوث القانونية المعاصرة، جامعة وهران، العدد 9، 2023

القوانين والأوامر

1. القرار رقم 01/د.ع/2022 بشأن الرقابة الدستورية على القوانين، الجريدة الرسمية رقم 12، 2022
2. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، الجريدة الرسمية، العدد 71
3. القانون رقم 04-15 المؤرخ في 1 فبراير 2015 المتعلق بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 11
4. القانون رقم 04-15 المؤرخ في 1 فبراير 2015 المتعلق بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 11
5. الأمر رقم 04-09 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، 2009
6. القانون رقم 04-18 المؤرخ في 10 ماي 2018 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 27، 2018
7. القانون رقم 04-18 المؤرخ في 10 ماي 2018 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 27، 2018
8. القانون رقم 05-23 المؤرخ في 27 أبريل 2023 المتعلق بالأمن السيبراني، الجريدة الرسمية، العدد 30
9. القانون رقم 05-23 المؤرخ في 27 أبريل 2023 المتعلق بالأمن السيبراني، الجريدة الرسمية، العدد 30
10. قانون رقم 05-23 المؤرخ في 27 أبريل 2023 المتعلق بالأمن السيبراني، الجريدة الرسمية، العدد 30
11. القانون رقم 07-18 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، 2018
12. القانون رقم 07-18 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34

تقارير:

1. الاتحاد الأوروبي، تقرير حول القدرات الوطنية في الأمن السيبراني، بروكسل، 2020
2. الاستراتيجية الوطنية للأمن السيبراني 2022-2025، وزارة الرقمنة والإحصائيات، الجزائر، 2022
3. الأمم المتحدة، تقرير فريق الخبراء الحكوميين بشأن الأمن السيبراني، نيويورك، 2015

4. وزارة التعليم العالي والبحث العلمي، تقرير حول تطوير كفاءات الأمن السيبراني في الجزائر، الجزائر، 2023
5. وزارة الدفاع الوطني، تقرير حول الاستراتيجية الوطنية للأمن السيبراني، الجزائر، 2022
6. وزارة الرقمنة والإحصائيات، الاستراتيجية الوطنية للأمن السيبراني 2022-2025، الجزائر، 2022
7. وزارة الرقمنة والإحصائيات، الاستراتيجية الوطنية للأمن السيبراني في الجزائر، الجزائر، 2021
8. وزارة العدل الجزائرية، تقرير حول إصلاح المنظومة القانونية وتعزيز مبدأ الأمن القانوني، الجزائر، 2023
9. وزارة العدل، مشروع إصلاح القوانين المتعلقة بالجريمة الإلكترونية، الجزائر، 2023
10. الوكالة الأوروبية للأمن السيبراني (ENISA)، تقرير حول تنفيذ التوجيه الأوروبي للأمن السيبراني، أثينا، 2020
11. الاتحاد الأوروبي، توجيه البرلمان والمجلس الأوروبي رقم (1148/2016) بشأن أمن الشبكات ونظم المعلومات، بروكسل، 2016