ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

السياسة الوطنية للأمن السيبراني بالمغرب: بين متطلبات السيادة الرقمية وتحديات التهديدات السيبرانية المعاصرة

Morocco's National Cybersecurity Policy: Between the Requirements of Digital Sovereignty and the Challenges of Contemporary Cyber Threats.

الباحث سفيان لوطي

طالب باحث بسلك الدكتوراه، جامعة الحسن الثاني

ملخص:

يعد الأمن السيبراني من أبرز القضايا الاستراتيجية التي فرضتها التحولات الرقمية المتسارعة، بالنظر إلى ارتباطه بحماية نظم المعلومات والبنيات التحتية الحيوية والمعطيات الرقمية، فضلاً عن دوره المتنامي في تعزيز السيادة الرقمية للدول. وفي هذا السياق، انخرط المغرب في بناء سياسة وطنية للأمن السيبراني من خلال تطوير إطار تشريعي ومؤسساتي يهدف إلى مواجهة التهديدات السيبرانية وضمان أمن الفضاء الرقمي الوطني.

تهدف هذه الدراسة إلى تحليل مكونات السياسة الوطنية للأمن السيبراني بالمغرب وتقييم مدى فعاليتها في مواجهة التهديدات الرقمية المعاصرة، وذلك من خلال الوقوف على الأسس التشريعية المنظمة للمجال، واستعراض البنية المؤسساتية المكلفة بحماية الأمن الرقمي، مع إبراز أهم التحديات القانونية والعملية التي تواجه هذه المنظومة في ظل التطور المتسارع للتكنولوجيا الرقمية.

واعتمدت الدراسة على المنهج التحليلي المدعوم بالمقاربة الوصفية والنقدية، من أجل دراسة مختلف النصوص القانونية والمؤسسات المتدخلة في مجال الأمن السيبراني. وقد خلصت إلى أن المغرب نجح في إرساء منظومة قانونية ومؤسساتية متطورة نسبياً، غير أن فعالية هذه المنظومة تظل رهينة بمواصلة تحيين التشريعات، وتعزيز التنسيق المؤسساتي، وتطوير الكفاءات البشرية المتخصصة، فضلاً عن دعم التعاون الدولي في مواجهة التهديدات السيبرانية العابرة للحدود.

الكلمات المفتاحية: الأمن السيبراني، السيادة الرقمية، الجرائم الإلكترونية، الأمن الوطني، حماية المعطيات الشخصية، التحول الرقمي، المغرب.

Abstract

Cybersecurity has emerged as one of the most significant strategic challenges resulting from rapid digital transformation, given its close connection to the protection of information systems, critical digital infrastructures, and data security. Beyond its technical dimension, cybersecurity has become a key component of national security and digital sovereignty in contemporary states. In this context, Morocco has undertaken substantial legislative and institutional reforms aimed at establishing a comprehensive national cybersecurity framework capable of addressing emerging cyber threats and ensuring the security of its digital environment.

This study seeks to analyze the components of Morocco's national cybersecurity policy and assess its effectiveness in confronting contemporary cyber threats. It examines the legal framework governing cybersecurity, the institutional architecture responsible for protecting cyberspace, and the major legal and operational challenges facing this policy in light of rapid technological developments.

Relying on an analytical approach supported by descriptive and critical perspectives, the study concludes that Morocco has succeeded in establishing a relatively advanced legislative and institutional framework in the field of cybersecurity.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

Nevertheless, the effectiveness of this framework remains dependent on the continuous adaptation of legislation to technological change, the strengthening of institutional coordination, the development of specialized human resources, and the enhancement of international cooperation in combating transnational cyber threats.

Keywords: Cybersecurity, Digital Sovereignty, Cybercrime, National Security, Personal Data Protection, Digital Transformation, Morocco.

مقدمة

أدى التطور المتسارع لتكنولوجيا المعلومات والاتصال خلال العقود الأخيرة إلى إحداث تحولات عميقة في بنية المجتمعات المعاصرة، حيث أصبحت الرقمنة أحد المرتكزات الأساسية للإدارة الحديثة والاقتصاد الرقمي والخدمات العمومية والتعاملات المالية والتجارية.[669] وقد أسهمت هذه التحولات في تعزيز كفاءة المؤسسات وتوسيع نطاق الوصول إلى المعرفة والخدمات، غير أنها أفرزت في المقابل تحديات أمنية جديدة تمثلت أساسًا في تنامي التهديدات السيبرانية وما يرتبط بها من جرائم إلكترونية تستهدف الأفراد والمؤسسات والدول على حد سواء[670].

ولم يعد الأمن السيبراني في الوقت الراهن مجرد قضية تقنية مرتبطة بحماية الأنظمة والشبكات المعلوماتية، بل أضحى رهانًا استراتيجيًا متصلًا بالأمن القومي والسيادة الرقمية والتنمية الاقتصادية المستدامة.[671] فمع توسع استخدام الإنترنت وتزايد الاعتماد على البنيات التحتية الرقمية في تدبير المرافق العمومية والخدمات الحيوية، أصبحت الهجمات السيبرانية قادرة على إحداث آثار اقتصادية وأمنية واجتماعية جسيمة،[672] الأمر الذي دفع مختلف الدول إلى تطوير سياسات وطنية متكاملة تهدف إلى حماية فضائها السيبراني وتعزيز قدرتها على مواجهة المخاطر الرقمية المستجدة.

وفي هذا السياق، برزت أهمية الأمن السيبراني باعتباره أحد المكونات الأساسية للأمن الشامل للدولة، خاصة في ظل تصاعد الجرائم الإلكترونية العابرة للحدود، وتنامي مخاطر الاختراقات المعلوماتية، وسرقة المعطيات الشخصية، والهجمات الموجهة ضد البنيات التحتية الحيوية.[673] كما ساهمت التطورات الحديثة المرتبطة بالذكاء الاصطناعي والحوسبة السحابية وإنترنت الأشياء في تعقيد المشهد الأمني الرقمي،[674] بما فرض على التشريعات الوطنية ضرورة مواكبة هذه التحولات من خلال تطوير آليات قانونية ومؤسساتية أكثر فعالية ومرونة.

وقد انخرط المغرب مبكرًا في هذا التوجه من خلال اعتماد مجموعة من الإصلاحات التشريعية والمؤسساتية الرامية إلى بناء منظومة وطنية للأمن السيبراني. فمن الناحية التشريعية، عمل المشرع المغربي على إدراج مقتضيات خاصة بمكافحة الجرائم المعلوماتية ضمن مجموعة القانون الجنائي،[675] كما سنّ قوانين متعلقة بحماية المعطيات ذات الطابع الشخصي والتبادل الإلكتروني للمعطيات القانونية وخدمات الثقة المتعلقة بالمعاملات الإلكترونية.[676] أما على المستوى المؤسساتي، فقد تم إحداث مجموعة

669 عبد الفتاح بيومي حجازي، *الحكومة الإلكترونية وحمايتها جنائياً ومدنياً وإدارياً*، دار الفكر الجامعي، الإسكندرية، 2021، ص 25.

670 Scott J. Shackelford, *Cybersecurity Law and Policy*, 3rd ed., Cambridge University Press, Cambridge, 2023, pp. 7–12.

671 Peter Warren Singer & Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, New York, 2024, pp. 15–18.

672 Paul Cornish, Cyber Security and Cyber Power, Routledge, London, 2022, pp. 31–36.

673 Jonathan Rosenoer, Cyber Law: The Law of the Internet, Springer, Cham, 2021, pp. 95–101.

674 OECD, *Digital Security Risk Management for Economic and Social Prosperity*, Paris, 2023, pp. 22–29.

675 القانون رقم 03.07 المتمم لمجموعة القانون الجنائي فيما يتعلق بالجرائم المرتبطة بنظم المعالجة الآلية للمعطيات، الجريدة الرسمية عدد 5584 بتاريخ 6 ديسمبر 2007.

676 القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي؛ القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية؛ القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

من الهيئات والأجهزة المتخصصة التي تضطلع بمهام حماية الفضاء السيبراني الوطني وتأمين نظم المعلومات ومراقبة معالجة المعطيات الشخصية والتصدي للتهديدات الرقمية.[677]

ورغم أهمية هذه الجهود، فإن التطور المستمر للجرائم السيبرانية وتعدد صورها وأساليب ارتكابها يثير تساؤلات جوهرية حول مدى كفاية المقاربة التشريعية والمؤسساتية المعتمدة بالمغرب لمواجهة التهديدات الرقمية المعاصرة.[678] فالتحديات المرتبطة بالتنسيق المؤسساتي، والتطور السريع للتقنيات الرقمية، وصعوبة اثبات الجرائم الإلكترونية، والطابع العابر للحدود الذي يميز العديد من الهجمات السيبرانية، كلها عوامل تفرض إعادة تقييم فعالية السياسة الوطنية للأمن السيبراني ومدى قدرتها على تحقيق التوازن بين متطلبات الأمن الرقمي وضمان الحقوق والحريات الأساسية.

وتنبع أهمية هذا الموضوع من كونه يلامس أحد أكثر المجالات حيوية في الدراسات القانونية المعاصرة، بالنظر إلى ارتباطه المباشر بحماية الأمن الوطني الرقمي وصيانة الحقوق الرقمية للأفراد وضمان استمرارية المرافق والخدمات الحيوية. كما يكتسي أهمية عملية بالنظر إلى الحاجة المتزايدة إلى تطوير السياسات العمومية المرتبطة بالأمن السيبراني في ظل التحولات التكنولوجية المتسارعة.

و انطلاقًا من ذلك، تتمحور إشكالية الدراسة حول التساؤل الرئيس الآتي:

إلى أي حد نجحت السياسة الوطنية للأمن السيبراني بالمغرب في بناء منظومة تشريعية ومؤسساتية فعالة لمواجهة التهديدات الرقمية المعاصرة، وما حدود هذه الفعالية في ظل التحولات التكنولوجية المتسارعة؟

ويتفرع عن هذه الإشكالية عدد من التساؤلات الفرعية:

- ما الأسس التشريعية التي اعتمدها المشرع المغربي لتأطير الأمن السيبراني ومكافحة الجرائم الإلكترونية؟
- ما طبيعة الأدوار التي تضطلع بها المؤسسات الوطنية المكلفة بالأمن السيبراني؟
- ما مدى فعالية المقاربة المؤسساتية في مواجهة التهديدات الرقمية المستجدة؟
- وما أبرز التحديات القانونية والعملية التي تواجه السياسة الوطنية للأمن السيبراني في المغرب؟

وللإجابة عن هذه التساؤلات، تنطلق الدراسة من فرضية مؤداها أن المغرب استطاع بناء إطار تشريعي ومؤسساتي متطور نسبيًا في مجال الأمن السيبراني، غير أن فعالية هذه المنظومة ما تزال رهينة بقدرتها على مواكبة التطور المتسارع للتهديدات الرقمية وتعزيز التنسيق بين مختلف الفاعلين المؤسساتيين وتحيين التشريعات ذات الصلة بشكل مستمر.

واعتمادًا على المنهج التحليلي المدعوم بالمقاربة الوصفية والنقدية، ستسعى هذه الدراسة إلى تحليل مكونات السياسة الوطنية للأمن السيبراني بالمغرب وتقييم مدى فعاليتها في مواجهة التهديدات الرقمية الراهنة، وذلك من خلال التطرق في المبحث الأول إلى المقاربة التشريعية للأمن السيبراني، قبل الانتقال في المبحث الثاني إلى دراسة المقاربة المؤسساتية وتقييم فعاليتها في ضوء التحديات المعاصرة.

المبحث الأول: المقاربة التشريعية للأمن السيبر اني بالمغرب

يشكل الإطار التشريعي أحد المرتكزات الأساسية التي تقوم عليها السياسة الوطنية للأمن السيبراني، ذلك أن فعالية التدابير التقنية والمؤسساتية تظل رهينة بوجود منظومة قانونية قادرة على استيعاب التحولات المتسارعة التي يعرفها الفضاء الرقمي. فمع تزايد الاعتماد على نظم المعلومات في تدبير المرافق العمومية والأنشطة الاقتصادية والخدمات الحيوية، لم يعد من الممكن مواجهة

677 القانون رقم 05.20 المتعلق بالأمن السيبراني؛ والنصوص التنظيمية المتعلقة بالمديرية العامة لأمن نظم المعلومات؛ وتقارير اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي.

678 International Cybersecurity Law Review, Vol. 5, No. 2, 2024, pp. 113–129.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

المخاطر السيبرانية بالاعتماد على القواعد التقليدية للقانون الجنائي أو التجاري، بل أصبح الأمر يقتضي بناء منظومة قانونية متخصصة تستجيب لخصوصيات البيئة الرقمية وما تفرضه من تحديات جديدة.

وقد أدرك المغرب مبكراً أهمية هذا التحول، فانخرط منذ بداية الألفية الثالثة في مسار تشريعي متدرج يهدف إلى تأطير مختلف الجوانب المرتبطة بالأمن السيبراني، سواء من خلال تجريم الأفعال الماسة بنظم المعالجة الآلية للمعطيات، أو من خلال إرساء قواعد لحماية المعطيات الشخصية والمعاملات الإلكترونية والبنيات التحتية الرقمية الحساسة. ويمثل هذا المسار التشريعي انعكاساً لتحول الأمن السيبراني من مجرد قضية تقنية إلى رهان استراتيجي يرتبط بحماية الأمن الوطني والسيادة الرقمية للدولة.

المطلب الأول: تطور الإطار القانوني المنظم للأمن السيبراني بالمغرب

لم تتشكل المنظومة التشريعية للأمن السيبراني بالمغرب دفعة واحدة، وإنما جاءت نتيجة تراكمات قانونية ومؤسساتية واكبت التطور التدريجي للمجتمع الرقمي المغربي. ويمكن تمييز مرحلتين أساسيتين في هذا التطور؛ مرحلة التجريم المعلوماتي، ثم مرحلة بناء منظومة قانونية متكاملة للأمن السيبراني.

الفقرة الأولى: مرحلة التجريم المعلوماتي وتأسيس الحماية الجنائية للفضاء الرقمي

شهدت نهاية القرن العشرين وبداية القرن الحادي والعشرين تزايداً ملحوظاً في استخدام الوسائط الرقمية وشبكات الاتصال الحديثة، الأمر الذي أفرز أنماطاً جديدة من السلوك الإجرامي لم تكن القواعد التقليدية للقانون الجنائي قادرة على استيعابها بصورة كاملة.[679] فقد ظهرت جرائم الولوج غير المشروع إلى الأنظمة المعلوماتية، والاعتداء على سلامة البيانات الإلكترونية، والقرصنة المعلوماتية، والتلاعب بالمعطيات الرقمية، وهي أفعال تتسم بخصوصيات تقنية تجعل من الصعب إخضاعها للأوصاف الجنائية التقليدية.[680]

في هذا السياق، تدخل المشرع المغربي بموجب القانون رقم 03.07 المتمم لمجموعة القانون الجنائي فيما يتعلق بالجرائم المرتبطة بنظم المعالجة الآلية للمعطيات.[681] وقد شكل هذا القانون نقطة الانطلاق الحقيقية لبناء الحماية الجنائية للفضاء السيبراني بالمغرب، إذ أقر مجموعة من الأفعال المجرمة المرتبطة بالولوج الاحتيالي إلى الأنظمة المعلوماتية أو تعطيل سيرها أو تغيير البيانات المخزنة بها أو إتلافها أو تزوير الوثائق الإلكترونية.[682]

وتكمن أهمية هذا القانون في كونه تجاوز المفهوم التقليدي للجريمة الذي كان يرتبط أساساً بالاعتداء على الأشخاص أو الأموال المادية، ليعترف بالحماية القانونية للمعلومات والبيانات باعتبارها قيماً قانونية مستقلة تستحق الحماية الجنائية.[683] كما ساهم في تعزيز الثقة في البيئة الرقمية من خلال توفير إطار قانوني يسمح بملاحقة مرتكبي الجرائم المعلوماتية ومعاقبتهم.

غير أن هذه المرحلة اتسمت بطابعها الزجري بالأساس، إذ انصب اهتمام المشرع على تجريم الأفعال الضارة ومعاقبة مرتكبيها دون أن يتطور الأمر بعد إلى بناء تصور شامل للأمن السيبراني بمختلف أبعاده الوقائية والتنظيمية والمؤسساتية.

الفقرة الثانية: الانتقال نحو بناء منظومة قانونية متكاملة للأمن السيبراني

مع اتساع نطاق التحول الرقمي وتزايد أهمية الاقتصاد الرقمي والخدمات الإلكترونية، برزت الحاجة إلى تجاوز المقاربة الزجرية الضيقة نحو بناء منظومة قانونية متكاملة قادرة على توفير الحماية للمعاملات الإلكترونية والمعطيات الشخصية والبنيات التحتية الرقمية.[684]

---

679 عبد الفتاح بيومي حجازي، *الدليل الجنائي وتقنيات التحقيق في جرائم الكمبيوتر والإنترنت*، دار الفكر الجامعي، الإسكندرية، 2020، ص 17.

680 أحمد إبراهيم أحمد، *المسؤولية الجنائية عن الجرائم الإلكترونية*، دار الجامعة الجديدة، الإسكندرية، 2021، ص 42.

681 القانون رقم 03.07 المتمم لمجموعة القانون الجنائي فيما يتعلق بالجرائم المرتبطة بنظم المعالجة الآلية للمعطيات، الجريدة الرسمية عدد 5584 بتاريخ 6 ديسمبر 2007.

682 المواد 607-3 إلى 607-11 من مجموعة القانون الجنائي المغربي.

683 محمد الإدريسي العلمي المشيشي، "السياسة الجنائية المغربية في مواجهة الجريمة الإلكترونية"، *مجلة الحقوق المغربية*، العدد 15، 2021، ص 113.

684 حمد أمين البشري، *الأمن السيبراني والتحديات القانونية المعاصرة*، دار النهضة العربية، القاهرة، 2023، ص 54.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

وفي هذا الإطار صدر القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، والذي شكل خطوة مهمة في إرساء الثقة القانونية في المعاملات الرقمية من خلال الاعتراف بالحجية القانونية للمحررات الإلكترونية والتوقيع الإلكتروني.[685] وقد ساهم هذا القانون في توفير الأساس القانوني اللازم لتطوير الإدارة الإلكترونية والتجارة الإلكترونية والخدمات الرقمية.

كما تعززت هذه الحماية بصدور القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي،[686] الذي يعد من أهم النصوص القانونية المرتبطة بالأمن السيبراني في بعده الحقوقي. فقد أرسى هذا القانون مجموعة من المبادئ الأساسية المتعلقة بمشروعية معالجة البيانات الشخصية وضرورة الحصول على موافقة أصحابها واحترام حقوقهم في الولوج والتصحيح والاعتراض،[687] كما أحدث اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي باعتبارها سلطة مستقلة مكلفة بالسهر على احترام مقتضياته.[688]

ويلاحظ أن هذا القانون نقل الاهتمام التشريعي من مجرد حماية الأنظمة المعلوماتية إلى حماية الإنسان الرقمي ذاته، وذلك من خلال تكريس الحق في الخصوصية المعلوماتية باعتباره أحد الحقوق الأساسية المرتبطة بالكرامة الإنسانية في العصر الرقمي.

وقد عرف المسار التشريعي المغربي تطوراً نوعياً إضافياً مع صدور القانون رقم 05.20 المتعلق بالأمن السيبراني، الذي يمثل أول إطار تشريعي متخصص يكرس الأمن السيبراني كمجال قانوني مستقل.[689] ويهدف هذا القانون إلى تعزيز أمن نظم المعلومات الحساسة وحماية البنيات التحتية ذات الأهمية الحيوية ووضع قواعد للحكامة الأمنية الرقمية وتدبير المخاطر السيبرانية.[690] وقد شكل هذا النص نقلة نوعية من منطق الحماية الجزئية إلى منطق الأمن السيبراني الشامل القائم على الوقاية والاستباق وإدارة المخاطر.

وفي الاتجاه نفسه، جاء القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية ليعزز البنية القانونية للثقة الرقمية من خلال تنظيم خدمات التوقيع الإلكتروني والختم الإلكتروني والتأريخ الإلكتروني والخدمات المرتبطة بالتصديق الإلكتروني،[691] مع إسناد اختصاصات تنظيمية ورقابية مهمة إلى المديرية العامة لأمن نظم المعلومات باعتبارها السلطة الوطنية المختصة في هذا المجال. وقد وسع هذا القانون نطاق الحماية القانونية للمعاملات الرقمية وأدخل آليات جديدة لتعزيز الأمن القانوني للفضاء الرقمي.

ومن خلال استقراء هذا التطور التشريعي يتضح أن السياسة التشريعية المغربية انتقلت من مرحلة مكافحة الجريمة المعلوماتية إلى مرحلة بناء منظومة قانونية متكاملة للأمن السيبراني تقوم على ثلاثة أبعاد مترابطة: البعد الزجري المتمثل في مكافحة الجرائم السيبرانية، والبعد الوقائي المرتبط بتدبير المخاطر الرقمية، والبعد الحقوقي المتعلق بحماية المعطيات الشخصية والخصوصية الرقمية. ويعكس هذا التحول وعياً متزايداً بأهمية الأمن السيبراني باعتباره ركيزة أساسية للأمن الوطني والتنمية الرقمية المستدامة.[692]

685 القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، الجريدة الرسمية عدد 5584 بتاريخ 6 ديسمبر 2007.

686 القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 5714 بتاريخ 5 مارس 2009.

687 عمر الكتاني، "حماية المعطيات الشخصية في التشريع المغربي على ضوء القانون 09.08"، *مجلة القانون والأعمال الدولية*، العدد 37، 2022، ص 88.

688 المادة 27 من القانون رقم 09.08.

689 القانون رقم 05.20 المتعلق بالأمن السيبراني، الجريدة الرسمية عدد 6996 بتاريخ 24 يونيو 2021.

690 المواد 2 و3 و4 من القانون رقم 05.20 المتعلق بالأمن السيبراني.

691 القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية، الجريدة الرسمية عدد 7006 بتاريخ 19 يوليوز 2021.

692 محمد عبد النباوي، *السياسة الجنائية والتحول الرقمي: تحديات العدالة في العصر الرقمي*، منشورات وزارة العدل، الرباط، 2022، ص 61.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

المطلب الثاني: الآليات التشريعية لحماية الفضاء السيبراني الوطني

إذا كانت السياسة الجنائية التقليدية تقوم أساساً على تجريم الأفعال الضارة ومعاقبة مرتكبيها بعد وقوع الجريمة، فإن خصوصية المخاطر السيبرانية تفرض اعتماد مقاربة وقائية واستباقية قوامها منع التهديدات قبل تحقق آثارها. فالهجمات السيبرانية لا تستهدف فقط المصالح الفردية للأشخاص، بل قد تمس الأمن الاقتصادي والاجتماعي للدولة، بل وقد تؤثر على استمرارية المرافق العمومية والبنيات التحتية الحيوية المرتبطة بالطاقة والنقل والاتصالات والقطاع المالي.

ومن هذا المنطلق، عمل المشرع المغربي على إرساء مجموعة من الآليات القانونية الرامية إلى تعزيز أمن الفضاء السيبراني الوطني، سواء من خلال توفير الحماية الجنائية لنظم المعلومات أو عبر إرساء قواعد قانونية لضمان أمن المعطيات الشخصية والمعاملات الرقمية.

الفقرة الأولى: الحماية الجنائية لنظم المعلومات والبنيات الرقمية

تشكل الحماية الجنائية أحد المرتكزات الأساسية للأمن السيبراني، بالنظر إلى الدور الردعي الذي تؤديه القواعد الزجرية في مواجهة الأفعال الماسة بنظم المعلومات.[693] وقد استند المشرع المغربي في هذا المجال إلى مقاربة قائمة على تجريم مختلف صور الاعتداء على الأنظمة المعلوماتية، سواء تعلق الأمر بالولوج غير المشروع إلى نظم المعالجة الآلية للمعطيات أو عرقلة سيرها أو تغيير البيانات المخزنة بها أو إتلافها أو تزوير الوثائق الإلكترونية[694].

وتكمن أهمية هذه الحماية في أنها لا تقتصر على حماية المكونات المادية للأنظمة المعلوماتية، وإنما تمتد لتشمل البيانات الرقمية ذاتها باعتبارها محل حماية قانونية مستقلة.[695] فالبيانات أصبحت تمثل أحد أهم الأصول الاستراتيجية للدولة والمؤسسات والأفراد، وأضحى الاعتداء عليها يوازي في خطورته الاعتداء على الأموال أو الممتلكات المادية.[696]

وقد تبنى المشرع المغربي في هذا الصدد سياسة جنائية تقوم على توسيع نطاق التجريم ليشمل مختلف الأفعال التي من شأنها المس بسلامة نظم المعلومات أو بسرية البيانات أو بتوافرها. ويعكس هذا التوجه استيعاباً لخصوصية الجريمة السيبرانية التي تتسم بسرعة التطور وتعدد الوسائل التقنية المستعملة في ارتكابها.[697]

غير أن فعالية الحماية الجنائية تظل مرتبطة بمجموعة من الإكراهات العملية، من أبرزها صعوبة اكتشاف الجريمة الإلكترونية في مراحلها الأولى، وتعقيد إجراءات الاثبات الرقمي، والطابع العابر للحدود الذي يميز العديد من الجرائم السيبرانية. فمرتكب الجريمة قد يوجد خارج الإقليم الوطني، بينما توجد الضحية والخوادم المستهدفة في دول مختلفة، الأمر الذي يفرض تطوير آليات التعاون القضائي والأمني الدولي لمواجهة هذه التحديات.

كما أن الاعتماد المتزايد على تقنيات التشفير والذكاء الاصطناعي والتخزين السحابي يفرض على المشرع مواصلة تحيين المنظومة الجنائية لمواكبة التحولات التقنية المتسارعة، إذ إن النصوص القانونية مهما بلغت درجة تطورها قد تصبح غير كافية إذا لم تواكب الابتكارات التكنولوجية الحديثة.

وإلى جانب الحماية الجنائية التقليدية، اتجه المشرع المغربي نحو تبني مقاربة وقائية قائمة على تدبير المخاطر السيبرانية، وهو ما تجسد بشكل واضح في القانون المتعلق بالأمن السيبراني الذي ألزم عدداً من الجهات العمومية والخاصة باتخاذ تدابير أمنية وتنظيمية لحماية نظم المعلومات الحساسة من مختلف التهديدات السيبرانية.

---

693 عبد الفتاح بيومي حجازي، *الحماية الجنائية للتجارة الإلكترونية والجرائم المرتبطة بالإنترنت*، دار الفكر الجامعي، الإسكندرية، 2021، ص 37.

694 المواد من 607-3 إلى 607-11 من مجموعة القانون الجنائي المغربي.

695 أحمد شوقي الشلقاني، *جرائم الاعتداء على نظم المعلومات*، دار النهضة العربية، القاهرة، 2020، ص 84.

696 Scott J. Shackelford, *Cybersecurity Law and Policy*, Cambridge University Press, 2023, pp. 41–46.

697 NIST, *Cybersecurity Framework 2.0*, National Institute of Standards and Technology, 2024.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

ويكتسي هذا التوجه أهمية خاصة لأنه ينقل الأمن السيبراني من منطق رد الفعل إلى منطق الوقاية والاستباق، وذلك من خلال فرض معايير أمنية وتدابير للحكامة الرقمية وإدارة المخاطر قبل وقوع الهجمات.

الفقرة الثانية: الحماية القانونية للمعطيات الشخصية والمعاملات الرقمية

لم يعد الأمن السيبراني يقتصر على حماية الأنظمة التقنية فحسب، بل أصبح يشمل كذلك حماية الحقوق الرقمية للأفراد وضمان الثقة في البيئة الإلكترونية.[698] وفي هذا الإطار، شكلت حماية المعطيات الشخصية إحدى الركائز الأساسية للسياسة التشريعية المغربية في مجال الأمن السيبراني.

فقد جاء القانون رقم 09.08 ليؤسس لنظام قانوني متكامل لحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، وذلك من خلال تكريس مجموعة من المبادئ الأساسية المرتبطة بالشفافية والشرعية والتناسب والغاية المشروعة من المعالجة.[699] كما منح للأفراد مجموعة من الحقوق، من بينها الحق في الإعلام والولوج والتصحيح والاعتراض، بما يضمن حماية خصوصيتهم الرقمية من مختلف أشكال الاستغلال غير المشروع.[700]

وتكتسي هذه الحماية أهمية متزايدة في ظل التحول نحو الاقتصاد الرقمي القائم على جمع البيانات الضخمة وتحليلها واستثمارها لأغراض تجارية وأمنية وإدارية. فالمعطيات الشخصية أصبحت تمثل مورداً استراتيجياً لا يقل أهمية عن الموارد الاقتصادية التقليدية، الأمر الذي يفرض ضمان توازن دقيق بين متطلبات الاستغلال المشروع للبيانات وضرورة حماية الحقوق والحريات الفردية.

كما عزز المشرع المغربي الثقة في البيئة الرقمية من خلال تنظيم المعاملات الإلكترونية ومنح الحجية القانونية للمحررات والتوقيعات الإلكترونية.[701] وقد شكل القانون رقم 53.05 خطوة مهمة في هذا الاتجاه من خلال إقرار المساواة القانونية بين الوثيقة الورقية والوثيقة الإلكترونية متى استوفت الشروط القانونية اللازمة.[702]

وتعزز هذا المسار بصدور القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية، والذي جاء استجابة للتطورات المتسارعة التي شهدها مجال الاقتصاد الرقمي. فقد أرسى هذا القانون إطاراً قانونياً حديثاً لخدمات الثقة الرقمية، بما يشمل التوقيع الإلكتروني والختم الإلكتروني وخدمات التأريخ الإلكتروني والمصادقة الرقمية.

وتكمن أهمية هذا القانون في كونه يعالج أحد أهم الإشكالات المرتبطة بالأمن السيبراني، والمتمثل في بناء الثقة داخل البيئة الرقمية. فنجاح الإدارة الإلكترونية والتجارة الإلكترونية والخدمات الرقمية يظل رهيناً بوجود ضمانات قانونية وتقنية تكفل سلامة المعاملات وتحمي المتعاملين من مخاطر التزوير والانتحال والاختراق.[703]

ومع ذلك، فإن فعالية هذه المنظومة القانونية تظل مرتبطة بمدى انتشار الثقافة الرقمية لدى الأفراد والمؤسسات، وبمدى قدرة الفاعلين الاقتصاديين والإداريين على احترام المقتضيات القانونية المتعلقة بحماية البيانات وأمن المعاملات الإلكترونية. كما أن التوسع المتزايد في استخدام تطبيقات الذكاء الاصطناعي والبيانات الضخمة يطرح تحديات قانونية جديدة تستدعي مراجعة مستمرة للنصوص التشريعية بما يضمن مواكبة التطورات المستقبلية.

وعليه، يتبين أن المقاربة التشريعية المغربية للأمن السيبراني لم تعد تقتصر على تجريم الأفعال الضارة، بل أصبحت ترتكز على منظومة متكاملة تجمع بين الحماية الجنائية والوقاية التقنية وحماية الحقوق الرقمية وتعزيز الثقة في المعاملات الإلكترونية، وهو

---

698 محمد أمين البشري، *الأمن السيبراني والتحديات القانونية المعاصرة*، مرجع سابق، ص 119.

699 القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

700 اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، *الدليل العملي لحماية المعطيات الشخصية*، الرباط، 2023، ص 15.

701 القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية.

702 المواد 417-1 إلى 417-3 من قانون الالتزامات والعقود كما تم تعديلها بموجب القانون 53.05.

703 المديرية العامة لأمن نظم المعلومات، *دليل خدمات الثقة للمعاملات الإلكترونية*، الرباط، 2022، ص 9.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

ما يعكس تطوراً ملحوظاً في فلسفة المشرع المغربي تجاه الأمن السيبراني باعتباره أحد مقومات الأمن الوطني والتنمية الرقمية المستدامة.[704]

خاتمة جزئية للمبحث الأول

يمكن استخلاص أن السياسة التشريعية المغربية في مجال الأمن السيبراني شهدت تطوراً ملحوظاً انتقلت معه من مرحلة التجريم المحدود للجرائم المعلوماتية إلى مرحلة بناء منظومة قانونية متكاملة تستهدف حماية الفضاء السيبراني بمختلف مكوناته. وقد تجسد هذا التطور من خلال تعدد النصوص القانونية المنظمة للجرائم الإلكترونية والمعطيات الشخصية والمعاملات الرقمية والأمن السيبراني، بما يعكس وعياً متزايداً بأهمية الأمن الرقمي في حماية المصالح الحيوية للدولة والمجتمع.

غير أن فعالية هذه المنظومة التشريعية تبقى رهينة بمدى قدرة المؤسسات المكلفة بتنفيذها على مواكبة التحولات التقنية المتسارعة، وهو ما يقتضي الانتقال إلى دراسة البعد المؤسساتي للأمن السيبراني بالمغرب باعتباره الحلقة الأساسية في تفعيل المقتضيات القانونية وتحويلها إلى آليات عملية لحماية الأمن الرقمي الوطني، وهو ما سنعالجه في المبحث الثاني.

المبحث الثاني: المقاربة المؤسساتية للأمن السيبراني بالمغرب وتحديات تعزيز الأمن الرقمي

إذا كانت النصوص القانونية تمثل الإطار المعياري المنظم للأمن السيبراني، فإن فعاليتها تبقى رهينة بوجود مؤسسات قادرة على تنزيلها وتفعيل مقتضياتها على أرض الواقع. فالتجارب المقارنة أثبتت أن نجاح السياسات الوطنية للأمن السيبراني لا يقاس فقط بجودة التشريعات المعتمدة، وإنما كذلك بمدى قدرة المؤسسات المختصة على تدبير المخاطر الرقمية والتنسيق فيما بينها والاستجابة السريعة للتهديدات السيبرانية المتجددة.[705]

وقد أدرك المغرب مبكراً هذه الحقيقة، فعمل على إرساء بنية مؤسساتية متخصصة في مجال الأمن السيبراني، تجمع بين المؤسسات ذات الطابع الأمني والتقني والرقابي والقضائي، بما يسمح بمقاربة شمولية تتجاوز البعد الزجري التقليدي نحو منطق الحكامة الرقمية الشاملة.[706] غير أن تعدد الفاعلين المؤسساتيين يثير في المقابل تساؤلات حول فعالية التنسيق بينهم ومدى قدرتهم على مواكبة التطورات التقنية المتسارعة.

المطلب الأول: البنية المؤسساتية للأمن السيبراني بالمغرب

تتسم المنظومة المؤسساتية للأمن السيبراني بالمغرب بتعدد الفاعلين وتنوع اختصاصاتهم، وهو ما يعكس الطبيعة المركبة للتهديدات السيبرانية التي تجمع بين الأبعاد الأمنية والتقنية والقانونية والاقتصادية.

الفقرة الأولى: المؤسسات التقنية والأمنية المكلفة بحماية الفضاء السيبراني

تحتل المديرية العامة لأمن نظم المعلومات موقعاً محورياً داخل منظومة الأمن السيبراني المغربية، باعتبارها الجهة الوطنية المكلفة بتنسيق السياسة العمومية في مجال أمن نظم المعلومات.[707] وقد تعزز دور هذه المؤسسة مع تزايد المخاطر المرتبطة بالتحول الرقمي وارتفاع عدد الهجمات السيبرانية الموجهة ضد المؤسسات العمومية والخاصة.[708]

وتضطلع المديرية العامة لأمن نظم المعلومات بمجموعة من المهام الاستراتيجية، من بينها وضع المعايير الوطنية للأمن السيبراني، وتتبع مستوى أمن الأنظمة المعلوماتية الحساسة، وتقديم التوجيهات التقنية للجهات العمومية والخاصة، فضلاً عن المساهمة في إعداد وتنفيذ الاستراتيجية الوطنية للأمن السيبراني.

---

704 محمد عبد النباوي، *السياسة الجنائية والتحول الرقمي*، مرجع سابق، ص 73.

705 Scott J. Shackelford, *Cybersecurity Law and Policy*, 3rd ed., Cambridge University Press, Cambridge, 2023, pp. 145-162.

706 القانون رقم 05.20 المتعلق بالأمن السيبراني، الجريدة الرسمية عدد 6996 بتاريخ 24 يونيو 2021.

707 المديرية العامة لأمن نظم المعلومات، *الاستراتيجية الوطنية للأمن السيبراني*، الرباط، 2023، ص 11 .

708 القانون رقم 05.20 المتعلق بالأمن السيبراني: المرسوم المتعلق باختصاصات المديرية العامة لأمن نظم المعلومات.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

كما يندرج ضمن هذه المنظومة مركز اليقظة والرصد والاستجابة للهجمات المعلوماتية، الذي يشكل الآلية الوطنية المختصة في الكشف المبكر عن التهديدات السيبرانية وتحليلها والاستجابة للحوادث الأمنية.[709] [710]وتكمن أهمية هذا المركز في كونه يجسد الانتقال من المقاربة التقليدية القائمة على رد الفعل إلى مقاربة استباقية تعتمد على الرصد المستمر للمخاطر الرقمية وتدبيرها قبل تحولها إلى تهديدات فعلية.[711]

ويكتسي هذا الدور أهمية خاصة بالنظر إلى الطبيعة الديناميكية للهجمات السيبرانية الحديثة، التي أصبحت تعتمد على تقنيات متطورة يصعب اكتشافها بالوسائل التقليدية، مما يفرض تطوير آليات الرصد والتحليل والاستجابة بشكل مستمر.

إلى جانب ذلك، تضطلع مختلف الأجهزة الأمنية الوطنية بأدوار مهمة في مكافحة الجرائم السيبرانية، سواء تعلق الأمر بالأبحاث الجنائية أو بتتبع الشبكات الإجرامية المتخصصة في الجرائم المعلوماتية أو بالتعاون الدولي في مجال مكافحة الجريمة الإلكترونية العابرة للحدود.

ويعكس هذا التنوع المؤسسي إدراك المشرع المغربي للطابع متعدد الأبعاد للأمن السيبراني، غير أنه يطرح في المقابل إشكالية التنسيق المؤسساتي وتحديد حدود الاختصاصات بين مختلف الفاعلين.[712]

الفقرة الثانية: المؤسسات الرقابية والقضائية في مجال الأمن السيبراني

إلى جانب المؤسسات الأمنية والتقنية، تضم المنظومة الوطنية للأمن السيبراني هيئات رقابية وقضائية تضطلع بأدوار أساسية في حماية الحقوق الرقمية وضمان احترام التشريعات ذات الصلة.[713]

وتعد اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي إحدى أهم هذه المؤسسات، حيث أوكل إليها المشرع مهمة السهر على احترام مقتضيات قانون حماية المعطيات الشخصية، وضمان التوازن بين متطلبات معالجة البيانات وحماية الحياة الخاصة للأفراد.[714]

وتتجلى أهمية هذه المؤسسة في كونها تمثل الآلية القانونية الأساسية لحماية الخصوصية الرقمية في المغرب، خاصة في ظل التوسع المتزايد في استخدام البيانات الشخصية من قبل الإدارات العمومية والشركات الخاصة ومنصات الخدمات الرقمية.[715]

كما تضطلع النيابة العامة بدور محوري في تنفيذ السياسة الجنائية المتعلقة بالجرائم السيبرانية، من خلال الإشراف على الأبحاث والمتابعات المرتبطة بالجرائم المعلوماتية وتنسيق الجهود بين مختلف الأجهزة المختصة.[716] وقد أفرزت طبيعة الجريمة الإلكترونية الحاجة إلى تطوير قدرات متخصصة لدى القضاة وأعضاء النيابة العامة وضباط الشرطة القضائية لمواكبة الخصوصيات التقنية لهذا النوع من الجرائم.[717]

وتبرز كذلك أهمية التعاون بين المؤسسات القضائية والأمنية والتقنية في مجال جمع الأدلة الرقمية والحفاظ عليها وتحليلها وفق الضوابط القانونية، بالنظر إلى ما تطرحه هذه الأدلة من إشكالات تتعلق بالمشروعية والحجية والاثبات.[718]

---

709 المديرية العامة لأمن نظم المعلومات، دليل تدبير الحوادث السيبرانية، الرباط، 2022، ص 17.

710 المديرية العامة لأمن نظم المعلومات، *الاستراتيجية الوطنية للأمن السيبراني*، الرباط، 2023، ص 12.

711 ENISA, Cyber Crisis Management Framework, European Union Agency for Cybersecurity, 2023, p. 21.

712 OECD, Digital Security Risk Management for Economic and Social Prosperity, Paris, 2023, p. 44.

713 Paul Cornish, Cyber Security and Cyber Power, Routledge, London, 2022, pp. 72-79.

714 المواد 27 إلى 35 من القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

715 اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، التقرير السنوي لسنة 2024، الرباط، ص 6.

716 رئاسة النيابة العامة، الدليل العملي للجرائم الإلكترونية، الرباط، 2023، ص 12.

717 محمد الكشبور، "إشكالات الاثبات في الجرائم الإلكترونية"، مجلة القضاء والقانون، العدد 188، 2022، ص 95.

718 اتفاقية بودابست بشأن الجريمة المعلوماتية لسنة 2001، المواد 16 إلى 21 .

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

ويلاحظ أن فعالية البنية المؤسساتية المغربية ترتبط بدرجة كبيرة بمدى نجاح مختلف هذه المؤسسات في العمل ضمن إطار تكاملي يضمن تبادل المعلومات والخبرات وتوحيد الجهود لمواجهة المخاطر السيبرانية المتزايدة.719

المطلب الثاني: تقييم فعالية السياسة الوطنية للأمن السيبراني بالمغرب وتحدياتها المستقبلية

إن تقييم فعالية السياسة الوطنية للأمن السيبراني يقتضي تجاوز المقاربة الوصفية التي تكتفي بعرض النصوص القانونية والمؤسسات القائمة، والانتقال إلى تحليل مدى قدرة هذه المنظومة على تحقيق الأهداف التي أنشئت من أجلها، والمتمثلة أساساً في حماية الفضاء السيبراني الوطني، وتأمين البنيات التحتية الرقمية الحيوية، وضمان استمرارية الخدمات الرقمية، وتعزيز الثقة في البيئة الإلكترونية.720

ورغم التطور الملحوظ الذي شهدته المنظومة المغربية خلال السنوات الأخيرة، فإن تقييم فعاليتها يقتضي الوقوف على جوانب القوة التي تميزها من جهة، والإكراهات والتحديات التي ما تزال تحد من مردوديتها من جهة أخرى.721

الفقرة الأولى: مؤشرات فعالية السياسة الوطنية للأمن السيبراني

أفرزت التحولات الرقمية التي عرفها المغرب خلال العقدين الأخيرين دينامية تشريعية ومؤسساتية ساهمت في بناء إطار متكامل نسبياً للأمن السيبراني مقارنة بعدد من التجارب الإقليمية.722 ويتجلى ذلك من خلال تعدد النصوص القانونية المنظمة للمجال، وتخصص المؤسسات المكلفة بالحماية الرقمية، واعتماد مقاربات استباقية في تدبير المخاطر السيبرانية.723

ومن أبرز مؤشرات هذه الفعالية نجاح المغرب في الانتقال من مرحلة التجريم المحدود للجرائم المعلوماتية إلى مرحلة بناء منظومة شاملة للأمن السيبراني تستند إلى مقاربة متعددة الأبعاد تجمع بين الوقاية والحماية والردع والتنسيق المؤسساتي.724 فقد أسهمت النصوص القانونية الحديثة في تعزيز حماية نظم المعلومات والمعطيات الشخصية والمعاملات الإلكترونية، كما ساهمت المؤسسات المختصة في رفع مستوى اليقظة الأمنية وتطوير آليات الرصد والاستجابة للحوادث السيبرانية.725

كما يلاحظ أن الدولة المغربية أولت اهتماماً متزايداً بحماية البنيات التحتية ذات الأهمية الحيوية، باعتبارها من أكثر الأهداف عرضة للهجمات السيبرانية.726 وقد أدى ذلك إلى تطوير معايير أمنية خاصة بالقطاعات الاستراتيجية كقطاع الطاقة والاتصالات والخدمات المالية والنقل، بما يعكس تحول الأمن السيبراني إلى أحد مكونات الأمن الوطني الشامل.727

ومن المؤشرات الإيجابية كذلك تنامي الوعي المؤسساتي بأهمية الأمن السيبراني داخل الإدارات العمومية والمؤسسات الاقتصادية، حيث أصبح تدبير المخاطر الرقمية جزءاً من متطلبات الحكامة الحديثة وإدارة المخاطر المؤسسية.728 كما ساهمت برامج التكوين والتوعية في تعزيز الثقافة الأمنية الرقمية لدى عدد من الفاعلين العموميين والخواص.729

وعلى المستوى الدولي، استطاع المغرب تعزيز حضوره في المبادرات الإقليمية والدولية المتعلقة بالأمن السيبراني، وهو ما ساهم في تطوير قدراته على مواجهة التهديدات العابرة للحدود والاستفادة من الخبرات الدولية في هذا المجال.730

---

719 ENISA, National Cybersecurity Governance Models, 2023, p. 33.

720 OECD, Digital Security Risk Management for Economic and Social Prosperity, OECD Publishing, Paris, 2023, pp. 31-39.

721 Paul Cornish, Cyber Security and Cyber Power, Routledge, London, 2022, pp. 95-99.

722 لقانون رقم 03.07؛ القانون رقم 09.08؛ القانون رقم 53.05؛ القانون رقم 05.20؛ القانون رقم 43.20.

723 الاستراتيجية الوطنية للأمن السيبراني، المديرية العامة لأمن نظم المعلومات، الرباط، 2023، ص 13.

724 محمد عبد النباوي، السياسة الجنائية والتحول الرقمي، منشورات وزارة العدل، الرباط، 2022، ص 78.

725 القانون رقم 05.20 المتعلق بالأمن السيبراني؛ اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، التقرير السنوي 2024.

726 المواد 2 و3 و4 من القانون رقم 05.20 المتعلق بالأمن السيبراني.

727 NIST, Cybersecurity Framework 2.0, National Institute of Standards and Technology, 2024.

728 World Economic Forum, Global Cybersecurity Outlook 2024, Geneva, 2024, pp. 27-29.

729 المديرية العامة لأمن نظم المعلومات، برنامج التوعية بالأمن السيبراني، الرباط، 2023.

730 الاتحاد الدولي للاتصالات، Global Cybersecurity Index 2024.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

غير أن هذه المكتسبات، على أهميتها، لا تعني بلوغ مستوى الكفاية التشريعية والمؤسساتية المطلوبة، خاصة في ظل التطور المتسارع للتهديدات الرقمية وتزايد تعقيدها.

الفقرة الثانية: التحديات القانونية والمؤسساتية للأمن السيبراني في ظل التحولات الرقمية المعاصرة

رغم التطور الذي شهدته السياسة الوطنية للأمن السيبراني، فإنها تواجه مجموعة من التحديات البنيوية التي تفرض إعادة التفكير في عدد من المرتكزات القانونية والمؤسساتية المعتمدة حالياً[731].

ويتمثل أول هذه التحديات في الطبيعة المتحولة للتهديدات السيبرانية ذاتها.[732] فالجريمة الإلكترونية لم تعد تقتصر على الاختراقات التقليدية أو سرقة البيانات، بل أصبحت تعتمد على تقنيات متقدمة تشمل الذكاء الاصطناعي التوليدي، والهجمات الموجهة المعتمدة على التعلم الآلي، وبرمجيات الفدية المتطورة، وتقنيات التزييف العميق[733](Deepfake)، وهي ممارسات تطرح إشكالات قانونية جديدة لا تزال العديد من التشريعات الوطنية غير مهيأة للتعامل معها بصورة كافية.

كما يبرز تحدي الطابع العابر للحدود للجرائم السيبرانية، حيث أصبحت الهجمات الإلكترونية تنطلق من فضاءات جغرافية متعددة وتتجاوز الحدود الوطنية بسهولة كبيرة.[734] ويؤدي ذلك إلى تعقيد عمليات البحث والتحقيق وجمع الأدلة الرقمية وتنفيذ الأحكام القضائية، مما يجعل فعالية المواجهة الوطنية رهينة بمدى تطور آليات التعاون الدولي والإقليمي في المجال السيبراني.[735]

ومن بين التحديات الجوهرية كذلك إشكالية الأمن السيبراني للبنيات التحتية الحيوية.[736] فكلما توسعت الرقمنة داخل القطاعات الاستراتيجية ازدادت احتمالات تعرضها لهجمات قد تؤدي إلى تعطيل خدمات أساسية تمس الأمن الاقتصادي والاجتماعي للدولة. ويقتضي هذا الوضع تطوير منظومات متقدمة لإدارة المخاطر السيبرانية والرفع المستمر من مستويات الحماية التقنية والتنظيمية.

وتطرح مسألة الموارد البشرية المتخصصة بدورها تحدياً حقيقياً أمام فعالية السياسة الوطنية للأمن السيبراني.[737] فنجاح أي استراتيجية رقمية يظل رهيناً بتوفر خبرات تقنية وقانونية قادرة على مواكبة التطور المتسارع للتكنولوجيا. ورغم الجهود المبذولة في مجال التكوين، فإن الطلب المتزايد على الكفاءات السيبرانية ما يزال يفوق العرض المتاح، سواء داخل المؤسسات العمومية أو القطاع الخاص.

كما يثير تعدد المتدخلين المؤسساتيين إشكالات مرتبطة بالحكامة والتنسيق.[738] فالتداخل النسبي بين الاختصاصات في بعض المجالات قد يؤثر على سرعة الاستجابة وفعالية اتخاذ القرار، خاصة في الحالات التي تتطلب تدخلاً عاجلاً ومشتركاً بين مختلف الفاعلين. ولذلك تبرز الحاجة إلى تطوير آليات أكثر نجاعة لتبادل المعلومات والتنسيق العملياتي بين المؤسسات المعنية بالأمن السيبراني.

وفي السياق نفسه، يفرض الذكاء الاصطناعي تحديات قانونية وأخلاقية غير مسبوقة.[739] فالتطبيقات الذكية أصبحت قادرة على إنتاج محتويات مزيفة يصعب التمييز بينها وبين المحتويات الحقيقية، كما يمكن توظيفها في عمليات الاحتيال الرقمي والهندسة

731 International Cybersecurity Law Review, Vol. 5, No. 2, 2024, pp. 113-120.
732 ENISA, Threat Landscape Report 2024, pp. 10-18.
733 World Economic Forum, Global Risks Report 2025, Geneva, 2025, pp. 55-61.
734 اتفاقية بودابست بشأن الجريمة المعلوماتية لسنة 2001، المواد 23-35.
735 Jonathan Rosenoer, Cyber Law, Springer, 2021, pp. 201-210.
736 OECD, Critical Infrastructure Protection and Cybersecurity, Paris, 2023.
737 (ISC)², Cybersecurity Workforce Study 2024, pp. 4-9.
738 ENISA, National Cybersecurity Governance Models, 2023, p. 34.
739 UNESCO, Recommendation on the Ethics of Artificial Intelligence, Paris, 2021.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

الاجتماعية والتأثير على الرأي العام. وهو ما يستدعي تطوير إطار قانوني متجدد يوازن بين تشجيع الابتكار التكنولوجي وضمان الأمن الرقمي وحماية الحقوق والحريات الأساسية.740

ومن ثم، فإن فعالية السياسة الوطنية للأمن السيبراني مستقبلاً لن تتوقف فقط على تطوير النصوص القانونية أو تعزيز البنية المؤسساتية، وإنما ستتطلب تبني رؤية استراتيجية متكاملة تقوم على التحيين المستمر للتشريعات، وتعزيز التعاون الدولي، والاستثمار في رأس المال البشري الرقمي، وتطوير القدرات الوطنية في مجالات الذكاء الاصطناعي والأمن السيبراني المتقدم.741

وعليه، يمكن القول إن السياسة الوطنية للأمن السيبراني بالمغرب حققت خلال السنوات الأخيرة تقدماً ملحوظاً على المستوى التشريعي والمؤسساتي، غير أن المحافظة على هذه المكتسبات وتطويرها تظل رهينة بمدى القدرة على التكيف مع بيئة رقمية تتسم بالتغير المستمر والتعقيد المتزايد، وهو ما يجعل الأمن السيبراني مشروعاً استراتيجياً دائماً لا ينتهي بمجرد سن القوانين أو إحداث المؤسسات، بل يتطلب عملية مستمرة من التقييم والتطوير والاستباق.

السيادة الرقمية والأمن السيبراني: نحو إعادة تعريف الأمن الوطني في المغرب

شهد مفهوم الأمن الوطني خلال العقود الأخيرة تحولات عميقة نتيجة التطور المتسارع للتكنولوجيا الرقمية وتزايد الاعتماد على الفضاء السيبراني في مختلف القطاعات الحيوية للدولة. فبعد أن ظل الأمن الوطني مرتبطاً تقليدياً بحماية الحدود الجغرافية والسيادة الترابية والدفاع العسكري، أصبح يشمل أبعاداً جديدة ترتبط بحماية الفضاءات الرقمية والمعطيات الاستراتيجية والبنيات التحتية المعلوماتية.742 وفي هذا السياق برز مفهوم "السيادة الرقمية" باعتباره أحد المفاهيم المركزية في الأدبيات القانونية والسياسية المعاصرة.743

ويقصد بالسيادة الرقمية قدرة الدولة على التحكم في مواردها الرقمية ومعطياتها الاستراتيجية وبنياتها التحتية المعلوماتية وضمان استقلالية قراراتها في الفضاء الرقمي بعيداً عن أشكال التبعية التقنية أو المعلوماتية الخارجية.744 ويعكس هذا المفهوم تحولاً جوهرياً في إدراك الدول لطبيعة التهديدات الجديدة التي لم تعد تقتصر على الاعتداءات العسكرية التقليدية، وإنما أصبحت تشمل الهجمات السيبرانية والتجسس الرقمي وسرقة البيانات والتأثير على الأنظمة الحيوية للدولة745.

وفي الحالة المغربية، تكتسب السيادة الرقمية أهمية متزايدة في ظل المشاريع الكبرى للتحول الرقمي وتعميم الخدمات الإلكترونية وتوسيع نطاق الاقتصاد الرقمي.746 فكلما ازدادت رقمنة الإدارة والقطاعات الاستراتيجية ازدادت الحاجة إلى ضمان أمن المعطيات الوطنية وحماية البنيات التحتية الرقمية من مختلف أشكال الاختراق أو الاستهداف الخارجي.747

ويبرز ارتباط الأمن السيبراني بالسيادة الرقمية من خلال كون حماية نظم المعلومات لم تعد مجرد وظيفة تقنية، بل أصبحت أداة للحفاظ على استقلال القرار الوطني وضمان استمرارية المرافق العمومية وحماية المصالح الاقتصادية للدولة.748 فالهجمات السيبرانية الموجهة ضد المؤسسات الحكومية أو القطاعات الحيوية قد تترتب عنها آثار تتجاوز الخسائر التقنية المباشرة لتصل إلى التأثير على الأمن الاقتصادي والاجتماعي والسياسي للدولة.749

740 Council of Europe, Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, 2024.

741 World Bank, Digital Development and Cybersecurity Capacity Building, Washington, 2024, pp. 41-47.

742 Joseph S. Nye Jr., The Future of Power, Public Affairs, New York, 2011, pp. 113-121.

743 Francesca Bria, Digital Sovereignty in Europe, European University Institute, Florence, 2022, pp. 7-15.

744 Gaia-X Project, Digital Sovereignty and European Data Governance, Policy Report, 2023, pp. 9-12.

745 Paul Cornish, Cyber Security and Cyber Power, Routledge, London, 2022, pp. 85-91.

746 المملكة المغربية، استراتيجية المغرب الرقمي 2030، الرباط، 2024، ص 6.

747 القانون رقم 05.20 المتعلق بالأمن السيبراني، المواد 2 و3 و4.

748 Scott J. Shackelford, Cybersecurity Law and Policy, Cambridge University Press, 2023, pp. 205-212.

749 World Economic Forum, Global Cybersecurity Outlook 2025, Geneva, 2025, pp. 22-28.

ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

كما أن التوسع المتزايد في استخدام تقنيات الحوسبة السحابية والخدمات الرقمية العابرة للحدود يطرح تحديات جديدة تتعلق بمكان تخزين البيانات الوطنية ومدى خضوعها للقوانين الوطنية أو الأجنبية.[750] وقد أدى ذلك إلى بروز نقاشات متقدمة حول مفهوم "السيادة على البيانات" باعتباره أحد المكونات الأساسية للسيادة الرقمية الحديثة، حيث أصبحت البيانات تمثل مورداً استراتيجياً لا يقل أهمية عن الموارد الاقتصادية أو الطبيعية التقليدية.[751]

وتزداد أهمية هذا النقاش مع التطورات المتلاحقة في مجال الذكاء الاصطناعي، إذ تعتمد النظم الذكية الحديثة على كميات هائلة من البيانات التي أصبحت تشكل أساساً للتنافس الاقتصادي والتكنولوجي بين الدول.[752] ومن ثم فإن امتلاك القدرة على حماية هذه البيانات وضمان استخدامها وفق المصالح الوطنية أصبح جزءاً لا يتجزأ من متطلبات الأمن الوطني المعاصر.[753]

وعلى هذا الأساس، لم يعد الأمن السيبراني مجرد آلية لحماية الأنظمة المعلوماتية من الاختراق، بل أصبح أحد المكونات الجوهرية للسيادة الرقمية وأحد المؤشرات الأساسية على قدرة الدولة على حماية مصالحها الاستراتيجية في البيئة الرقمية.[754] ومن المتوقع أن يشهد هذا المجال خلال السنوات المقبلة مزيداً من التطور، خاصة مع تصاعد الرهانات المرتبطة بالذكاء الاصطناعي والأمن السحابي وحوكمة البيانات الضخمة، وهو ما يفرض على المغرب مواصلة تطوير منظومته التشريعية والمؤسساتية وتعزيز استثماراته في البحث العلمي والابتكار الرقمي لضمان موقع فاعل داخل النظام الرقمي العالمي المتشكل.[755]

ومن ثم، فإن مستقبل الأمن الوطني لن يتحدد فقط بمدى قدرة الدولة على حماية حدودها الترابية، بل أيضاً بمدى قدرتها على حماية فضائها السيبراني وضمان سيادتها الرقمية والتحكم في مواردها المعلوماتية الاستراتيجية، الأمر الذي يجعل الأمن السيبراني أحد أهم رهانات الدولة الحديثة في القرن الحادي والعشرين.[756]

الخاتمة

أفرزت الثورة الرقمية تحولات جوهرية في أنماط ممارسة السلطة والإدارة والاقتصاد والتواصل داخل المجتمعات المعاصرة، الأمر الذي جعل الأمن السيبراني ينتقل من كونه مسألة تقنية محدودة إلى أحد المرتكزات الأساسية للأمن الوطني والسيادة الرقمية للدول. وفي هذا السياق، انخرط المغرب خلال العقدين الأخيرين في مسار إصلاحي متدرج هدف إلى بناء منظومة متكاملة لحماية الفضاء السيبراني الوطني ومواجهة مختلف التهديدات الرقمية المستجدة.

وقد أظهرت الدراسة أن السياسة الوطنية للأمن السيبراني بالمغرب تستند إلى مقاربة مزدوجة تجمع بين البعد التشريعي والبعد المؤسساتي. فمن الناحية التشريعية، عمل المشرع المغربي على تطوير إطار قانوني متنوع يشمل مكافحة الجرائم المعلوماتية، وحماية المعطيات ذات الطابع الشخصي، وتنظيم المعاملات الإلكترونية، وتأمين نظم المعلومات ذات الأهمية الحيوية. ويعكس هذا التوجه وعياً متزايداً بضرورة الانتقال من المقاربة الزجرية التقليدية إلى مقاربة أكثر شمولاً تقوم على الوقاية وإدارة المخاطر وتعزيز الثقة الرقمية.

أما على المستوى المؤسساتي، فقد كشفت الدراسة عن وجود بنية مؤسساتية متخصصة تضم عدداً من الفاعلين العموميين المكلفين بحماية الفضاء السيبراني الوطني، سواء على المستوى الأمني أو التقني أو الرقابي أو القضائي. وقد ساهم هذا التنوع المؤسساتي في تطوير قدرات الدولة على مواجهة المخاطر الرقمية وتدبير الحوادث السيبرانية وتعزيز حماية البنيات التحتية الحيوية والمعطيات الشخصية.

---

750 OECD, Data Governance in the Digital Age, Paris, 2023, pp. 52-58.

751 European Commission, European Strategy for Data, Brussels, 2023, pp. 11-17.

752 UNESCO, Recommendation on the Ethics of Artificial Intelligence, Paris, 2021.

753 World Bank, World Development Report: Data for Better Lives, Washington, 2021, pp. 31-39.

754 International Cybersecurity Law Review, Vol. 5, No. 2, 2024, pp. 121-127.

755 United Nations, Global Digital Compact, New York, 2024.

756 Manuel Castells, The Rise of the Network Society, Updated Edition, Wiley-Blackwell, 2023, pp. 467-472.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/OZSP2793

غير أن التحليل أظهر في المقابل أن فعالية هذه المنظومة ما تزال تواجه مجموعة من التحديات البنيوية والوظيفية. فمن جهة أولى، تفرض الطبيعة المتغيرة للتهديدات السيبرانية ضرورة التحيين المستمر للتشريعات الوطنية بما يسمح باستيعاب الجرائم الرقمية المستحدثة المرتبطة بالذكاء الاصطناعي والبيانات الضخمة والتزييف العميق والأنظمة الذاتية التعلم. ومن جهة ثانية، تبرز الحاجة إلى تطوير آليات أكثر فعالية للتنسيق بين مختلف المتدخلين المؤسساتيين بما يضمن توحيد الجهود وتسريع الاستجابة للحوادث السيبرانية.

كما بينت الدراسة أن الطابع العابر للحدود الذي يميز الجرائم السيبرانية يشكل أحد أبرز التحديات التي تواجه السياسة الوطنية للأمن السيبراني، إذ أصبحت الهجمات الرقمية تتجاوز بسهولة الحدود الجغرافية والسيادية للدول، مما يجعل فعالية المواجهة الوطنية مرتبطة بدرجة كبيرة بمستوى التعاون الدولي والإقليمي في مجالات تبادل المعلومات والمساعدة القضائية والتنسيق العملياتي.

ومن خلال مختلف المعطيات التي تم تحليلها، يمكن تسجيل جملة من النتائج الأساسية:

أولاً: نجح المغرب في إرساء إطار تشريعي متطور نسبياً للأمن السيبراني مقارنة بالعديد من التجارب الإقليمية، من خلال سن نصوص قانونية متخصصة تغطي مختلف جوانب الحماية الرقمية.

ثانياً: أسهمت البنية المؤسساتية الوطنية في تعزيز القدرات الوقائية والاستباقية للدولة في مجال تدبير المخاطر السيبرانية وحماية نظم المعلومات الحساسة.

ثالثاً: ما يزال الأمن السيبراني بالمغرب يواجه تحديات مرتبطة بسرعة التطور التكنولوجي، وصعوبة مواكبة التشريعات للتحولات الرقمية المتسارعة.

رابعاً: يشكل تطوير الكفاءات البشرية المتخصصة أحد الشروط الأساسية لضمان استدامة وفعالية السياسة الوطنية للأمن السيبراني.

خامساً: أصبح الأمن السيبراني جزءاً لا يتجزأ من متطلبات السيادة الرقمية والتنمية المستدامة، ولم يعد مجرد مجال تقني منفصل عن السياسات العمومية.

وانطلاقاً من هذه النتائج، يمكن اقتراح مجموعة من التوصيات:

- مواصلة تحيين المنظومة التشريعية الوطنية بما يواكب التطورات المرتبطة بالذكاء الاصطناعي والجرائم الرقمية الناشئة.
- تعزيز التكامل والتنسيق المؤسساتي بين مختلف الهيئات المتدخلة في مجال الأمن السيبراني.
- تطوير برامج وطنية متخصصة لتكوين الخبرات القانونية والتقنية في المجالات السيبرانية.
- تعزيز التعاون الدولي والإقليمي في مجال مكافحة الجرائم الإلكترونية وتبادل المعلومات المتعلقة بالتهديدات السيبرانية.
- توسيع نطاق الثقافة الرقمية والأمنية داخل الإدارات العمومية والمؤسسات الاقتصادية والمجتمع المدني.
- دعم البحث العلمي المتخصص في الأمن السيبراني والقانون الرقمي باعتباره أحد المداخل الأساسية لتطوير السياسات العمومية الرقمية.

وخلاصة القول، فإن السياسة الوطنية للأمن السيبراني بالمغرب حققت تقدماً ملحوظاً على المستويين التشريعي والمؤسساتي، غير أن المحافظة على هذه المكتسبات وتطويرها تظل رهينة بالقدرة على استباق التهديدات الرقمية المستقبلية وبناء نموذج وطني للأمن السيبراني قائم على الحكامة الرقمية والمرونة التشريعية والتأهيل البشري المستمر. وهو ما يجعل الأمن السيبراني ليس مجرد خيار تنظيمي أو تقني، بل رهاناً استراتيجياً يرتبط مباشرة بحماية السيادة الرقمية وضمان استدامة التنمية في العصر الرقمي.