كلية العلوم القانونية والسياسية
Faculty of Legal and Political Sciences

جامعة ابن طفيل
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵙⵉ ⵉⵣⵔⵉⴼ
Ibn Tofaïl University

ماستر الدراسات السياسية والدستورية

الفوج الثاني

رسالة لنيل شهادة الماستر في موضوع:

الأمن السيبراني وحماية البنية التحتية الرقمية: المغرب نموذجًا

إعداد الطالب الباحث:

حمزة لحسيني

تحت إشراف الدكتور:

خليل سعدي

لجنة المناقشة:

الأستاذ خليل سعدي.....أستاذ باحث بكلية العلوم القانونية والسياسية بالقنيطرة.....بصفته مشرفا ورئيسا.

الأستاذ يوسف حمومي.....أستاذ باحث بكلية العلوم القانونية والسياسية بالقنيطرة.....بصفته عضوا.

الأستاذ ابراهيم التوري.....أستاذ باحث بكلية العلوم القانونية والسياسية بالقنيطرة.....بصفته عضوا.

السنة الجامعية:

2025/2024


بسم الله الرحمن الرحيم

إهداء

إلى وطني، **المملكة المغربية**، إليك، يا "منبت الأحرار ومشرق الأنوار"، أُهدي هذا البحث المتواضع، وفاءً لما أوليتني من انتماء، وعرفانًا لما غرسته في من قيم الولاء **والمسؤولية والجدية**. لقد جاء هذا العمل ثمرة وعيي العميق بأهمية حماية بنيتك التحتية الرقمية، وإيمانًا مني بأن أمنك السيبراني هو حصن من حصون سيادتك الوطنية. أهديه إليك، بكل صدق، كطالب باحث ينتمي إليك جسدًا وروحًا، ويؤمن أن خدمة الوطن ليست شعارًا، بل التزامًا دائمًا ومسؤولية وجدية.

كلمة شكر

الحمد لله الذي يسّر لي سُبل هذا الإنجاز، ومنَّ عليّ بتوفيقه في كل مرحلة من مراحل هذا البحث. له الشكر والحمد. وإني أتقدم بخالص الشكر والامتنان لأستاذي المشرف **الدكتور خليل سعدي**، على ما بذله من جهدٍ وتوجيه وصبر، أسأل الله أن يحفظ له أهله ومن يُحب، ويبارك له في عمره، وأن يُكرمه في الآخرة برؤية وجهه الكريم، فهي أعظم النعم وأسمى الجزاء. كما أخص بالشكر جميع الطلبة والأساتذة والإداريين وسائر العاملين من تقنيين وحراس، وعمال، وممن يسهمون في خدمة جامعة ابن طفيل القنيطرة ككل.

جدول المختصرات

المصطلح	بالعربية	الشرح
ADD ***Agence de développement du digital***	وكالة التنمية الرقمية	مؤسسة عمومية مغربية تهدف إلى تسريع التحول الرقمي في المغرب
ANSSI ***Agence nationale de la sécurité des systémes d'information***	الوكالة الفرنسية لأمن أنظمة المعلومات	وكالة حكومية فرنسية مسؤولة عن الأمن السيبراني
AUSIM ***Association des utilisateures des systémes d'information au maroc***	جمعية مستخدمي نظم المعلومات بالمغرب	جمعية مهنية تجمع مستخدمي نظم المعلومات في المغرب
BCP ***Banque Centrale Populaire***	البنك الشعبي	مجموعة بنكية مغربية
CCDCOE ***NATO Cooperative Cyber Defence Centre of Excellence***	مركز التميز التعاوني للدفاع السيبراني التابع لحلف الناتو	مركز بحث وتدريب تابع لحلف الناتو مقره إستونيا
CIH ***Crédit Immobilier et Hôtelier***	بنك CIH	بنك مغربي/القرض العقاري والسياحي
CIC ***Cybersecurity Innovation Center***	مركز الابتكار في الأمن السيبراني	مركز للابتكار في مجال الأمن السيبراني بالمغرب

CNDP ***Commission Nationale de contrôle de la protection des Données à caractère Personnel***	اللجنة الوطنية لحماية المعطيات الشخصية ذات الطابع الشخصي	هيئة مغربية مستقلة مكلفة بضمان حماية البيانات الشخصية
CNSS ***Caisse Nationale de Sécurité Sociale***	الصندوق الوطني للضمان الاجتماعي	مؤسسة عمومية مغربية تدير نظام الضمان الاجتماعي
COVID-19 ***Coronavirus Disease 2019***	جائحة كوفيد19	الوباء العالمي الذي تسبب فيه فيروس كورونا
DDoS ***Distributed Denial of Service***	هجمات الحرمان من الخدمة	نوع من الهجمات السيبرانية يهدف إلى تعطيل خدمة أو موقع إلكتروني بإغراقه بالطلبات
DESI ***Digital Economy and Society Index***	مؤشر اقتصاد ومجتمع رقمي	مؤشر أوروبي يقيس الأداء الرقمي للدول
DGSSI ***Direction Générale de la Sécurité des Systèmes d'Information***	المديرية العامة لأمن نظم المعلومات	السلطة الوطنية المغربية المكلفة بالأمن السيبراني، تابعة لإدارة الدفاع الوطني
DHS ***Department of Homeland Security***	وزارة الأمن الداخلي	وزارة أمريكية مسؤولة عن الأمن الداخلي للولايات المتحدة

DMS ***Distribution Management System***	نظم سيطرة ومراقبة	أنظمة تستخدم لمراقبة وإدارة شبكات التوزيع مثل الكهرباء
DNSSI ***Directive Nationale de la Sécurité des Systèmes d'Information***	التوجيه الوطني لأمن نظم المعلومات	وثيقة مرجعية وطنية مغربية تحدد التدابير الأمنية لنظم المعلومات
DOD ***Department of Defense***	وزارة الدفاع	وزارة أمريكية مسؤولة عن القوات المسلحة الأمريكية
DXC.CDG ***DXC Technology – Caisse de Dépôt et de Gestion***	مركز DXC.CDG	مركز للتحول الرقمي والابتكار في المغرب
EDL Cyber Unit ***Estonian Defence League Cyber Unit***	وحدة الدفاع السيبراني التابعة لرابطة الدفاع الإستونية	وحدة تطوعية إستونية متخصصة في الدفاع السيبراني
EGDI ***E-Government Development Index***	مؤشر تنمية الحكومة الإلكترونية	مؤشر عالمي يقيس مستوى تطور الحكومة الإلكترونية
E-ITS ***Estonian Information Security Standard***	معيار أمن المعلومات الوطني الإستوني	معيار وطني لأمن المعلومات في إستونيا
FAR ***Forces Armées Royales***	القوات المسلحة الملكية المغربية	القوات العسكرية للمملكة المغربية

GCI ***Global Cybersecurity Index***	مؤشر الأمن السيبراني العالمي	مؤشر صادر عن الاتحاد الدولي للاتصالات يقيس التزام الدول بالأمن السيبراني
GDPR ***General Data Protection Regulation***	اللائحة العامة لحماية البيانات الأوروبية	قانون أوروبي لحماية البيانات والخصوصية
G7 Hiroshima AI ***G7 Hiroshima Process on Generative AI***	عملية G7 Hiroshima AI	مبادرة لمجموعة الدول السبع حول الذكاء الاصطناعي
IBM ***International Business Machines***	عملية IBM	شركة تكنولوجيا أمريكية متعددة الجنسيات
ICE71 ***Innovation Cybersecurity Ecosystem at BLOCK71***	حاضنة ICE71	حاضنة سنغافورية لشركات الأمن السيبراني الناشئة
ICT Governance ***Information and Communication Technology Governance***	حكامة تكنولوجيا المعلومات والاتصالات	الإطار الذي يحكم استخدام وإدارة تكنولوجيا المعلومات والاتصالات
IEA ***International Energy Agency***	وكالة الطاقة الدولية	منظمة حكومية دولية تركز على سياسات الطاقة
IoT ***Internet of Things***	إنترنت الأشياء	شبكة الأجهزة المادية المدمجة مع أجهزة

		الاستشعار والبرامج والتقنيات الأخرى
IRENA ***International Renewable Energy Agency***	الوكالة الدولية للطاقة المتجددة	منظمة حكومية دولية تدعم التحول العالمي إلى الطاقة المتجددة
ISO/IEC 27001 ***International Organization for Standardization / International Electrotechnical Commission 27001***	معايير ISO/IEC 27001	معيار دولي لنظم إدارة أمن المعلومات
ITU ***International Telecommunication Union***	الاتحاد الدولي للاتصالات	وكالة متخصصة تابعة للأمم المتحدة مسؤولة عن مسائل تكنولوجيا المعلومات
.MA ***Country-code top-level domain for Morocco***	النطاق المغربي الإلكتروني	يُستخدم لتمييز مواقع الإنترنت المرتبطة بالمملكة المغربية
maCERT ***Moroccan Computer Emergency Response Team***	المركز الوطني لرصد الهجمات والتصدي لها	فريق الاستجابة لحوادث الحاسوب الوطني في المغرب، تابع لـ DGSSI
MAP ***Maghreb Arabe Presse***	وكالة المغرب العربي للأنباء	وكالة الأنباء الرسمية للمغرب

Medusa ***Medusa Ransomware***	ميدوسا	سلالة من برامج الفدية الخبيثة
NCCIC ***National Cybersecurity and Communications Integration Center***	مركز التكامل الوطني للأمن السيبراني والاتصالات	مركز أمريكي لتنسيق الأمن السيبراني والاتصالات
NIST ***National Institute of Standards and Technology***	إطار NIST للأمن السيبراني	إطار عمل أمريكي لإدارة مخاطر الأمن السيبراني
NSA ***National Security Agency***	وكالة الأمن القومي الأمريكية	وكالة استخبارات أمريكية متخصصة في التشفير والاستخبارات الإشارات
ONEE ***Office National de l'Electricité et de l'Eau Potable***	المكتب الوطني للكهرباء والماء الصالح للشرب	مؤسسة عمومية مغربية مسؤولة عن قطاعي الكهرباء والماء
OT ***Operational Technology***	التكنولوجيا التشغيلية	أنظمة التحكم الصناعي المستخدمة في البنية التحتية الحيوية
R&D ***Research and Development***	البحث العلمي والتطوير	الأنشطة المبتكرة التي تقوم بها الشركات أو الحكومات لتطوير منتجات أو خدمات جديدة
ROCA ***Return of Coppersmith's Attack***	ثغرة ROCA	ثغرة أمنية تشفيرية

SCADA ***Supervisory Control and Data Acquisition***	نظام تحكم ومراقبة مركزي	نظام تحكم صناعي يستخدم لمراقبة العمليات والتحكم فيها
SOC ***Security Operations Center***	مراكز عمليات أمنية متقدمة	مراكز مسؤولة عن مراقبة وتحليل التهديدات الأمنية
SQL ***Structured Query Language***	لغة الاستعلام الهيكلية	لغة برمجة تستخدم لإدارة قواعد البيانات
UNSCF ***United Nations Cybersecurity Fellowship***	زمالة UNSCF	برنامج زمالة للأمن السيبراني تابع للأمم المتحدة
VPN ***Virtual Private Network***	شبكة افتراضية خاصة	تقنية تتيح إنشاء اتصال آمن عبر شبكة عامة
X-road ***Estonian Data Exchange Layer***	إكس-رود	نظام تبادل بيانات حكومي إستوني آمن
P/Pp/page/s	ص/الصفحة	ص34
No/ Number	العدد/الرقم	لتحديد رقم العدد في الدورية(No. 3)
Vol/ Volume	المجلد	لتحديد رقم المجلد في الدورية أو السلسلة (Vol. 41)

Op. cit ***Opere citato***	في العمل المذكور سابقًا	تشير إلى مصدر ذُكر سابقاً
Ibidem/Ibid	نفس المصدر	تُحيل إلى نفس المصدر والصفحة الواردين في الإحالة السابقة

المقدمة

شهد العالم خلال العقود الأخيرة تحولًا رقميًا متسارعًا أصبح فيه الأمن السيبراني ضرورة ملحّة لحماية استقرار الدول وسيادتها الوطنية. فقد تزايد الاعتماد على الأنظمة الرقمية في مختلف مناحي الحياة، من إدارة الخدمات الحكومية إلى تشغيل البنى التحتية الحيوية (كشبكات الطاقة والاتصالات والقطاعات المالية)، مما جعل هذه البنى عرضة لتهديدات إلكترونية متطورة ومتنامية. وفي ظل تصاعد الهجمات السيبرانية عبر الحدود – التي باتت أكثر تعقيدًا واستهدافًا للبنى الحيوية للدول – أدرجت العديد من الدول الأمن السيبراني ضمن أولويات سياساتها العمومية باعتباره مكوّنًا أساسيًا من مكونات أمنها القومي. هكذا أصبح الفضاء الرقمي ساحة جديدة للصراع وحماية الأمن الوطني، مما دفع المجتمع الدولي إلى تعزيز التعاون ووضع الأطر القانونية لمواجهة الجرائم السيبرانية وحماية السيادة الرقمية للدول. ويمكن تتبع الجذور التاريخية لأمن المعلومات إلى فترات مبكرة من عصر الحوسبة، حيث ظهرت أولى محاولات تأمين البيانات مع بدايات استخدام الحواسيب في الستينيات والسبعينيات. لكن مفهوم الأمن السيبراني بمضمونه الحديث تبلور بشكل أوضح منذ انتشار الإنترنت وشبكات المعلومات في أواخر القرن العشرين. شهدت الثمانينيات ظهور فيروسات الحاسوب الأولى وحوادث اختراق لأنظمة حكومية وخاصة، ما نبه الدول إلى خطورة ترك الأنظمة الرقمية دون حماية كافية. ومع ثورة الإنترنت في التسعينيات، تنامى الاهتمام الدولي بأمن الشبكات؛ فشهدنا مثلاً إصدار معايير وبروتوكولات أمان (مثل بروتوكولات التشفير *SSL* في 1994[1]) وظهور فرق الاستجابة لطوارئ الحاسوب (*CERTs*[2]) في عدة دول. تصاعدت أهمية الأمن السيبراني أكثر مع حادثة الهجمات الإلكترونية على إستونيا سنة 2007 – والتي اعتُبرت من أولى الحروب السيبرانية التي استهدفت دولة بشكل شامل – ما شكل جرس إنذار عالمي حول قدرة الهجمات الرقمية على شل مؤسسات الدولة. تلا ذلك هجوم فيروس *Stuxnet* 2010[3] الذي استهدف منشآت نووية، مؤكّدًا أن التهديدات السيبرانية قد تُستخدم كسلاح جيوستراتيجي. بناءً

[1] Oppliger, Rolf. *SSL and TLS: Theory and Practice*. 3rd ed. Norwood, MA: Artech House, 2023, p. 13.
[2] Stallings, William, and Lawrie Brown. *Computer Security: Principles and Practice*. 2nd ed. Boston: Pearson Education, 2012, p. 251.
[3] Ibid., p193.

على هذه التطورات، بادرت العديد من الدول والقوى الدولية إلى تبني استراتيجيات وطنية للأمن السيبراني وإنشاء هيئات متخصصة لمواجهة الأخطار الجديدة. كما أبرمت اتفاقيات دولية لمكافحة الجريمة الإلكترونية (مثل اتفاقية بودابست 2001[4]) ووُضعت أطر للتعاون المعلوماتي بين الدول لملاحقة القراصنة وتعزيز تبادل المعلومات. بحلول العقد الثالث من القرن الحادي والعشرين، بات الأمن السيبراني حجر الزاوية في سياسات الأمن القومي للدول المتقدمة والنامية على حد سواء، وأُنشئت وكالات وطنية متخصصة وفرق دفاع سيبراني عسكرية، فضلاً عن إدماج بعد الأمن السيبراني في تحالفات دفاعية (مثل حلف الناتو الذي اعتبر الفضاء السيبراني مجالاً عملياتيًا للحرب[5]). هذا التطور التاريخي السريع يبرز أن تأمين الفضاء الرقمي أصبح مهمة مشتركة عالميًا، وتحديًا عابرًا للحدود يتطلب يقظة جماعية وأطرًا تشريعية مرنة لمجاراة أساليب التهديد المستحدثة. ومن ناحية المغرب فقد بدأ الوعي بأمن المعلومات يظهر بشكل متزايد مع انخراط الدولة في مشاريع الرقمنة الحكومية منذ أوائل الألفية. ومع إطلاق مبادرات وطنية مثل خطة "المغرب الرقمي 2010[6]" ثم "المغرب الرقمي 2020[7]"، تعاظمت الحاجة إلى تأمين البنية التحتية المعلوماتية المرافقة لهذه المشاريع. ويمكن القول إن عام 2011 شكّل منعطفًا حاسمًا في تطور الأمن السيبراني بالمغرب؛ إذ تم خلاله إنشاء إطار مؤسساتي حكومي مكلف بأمن المعلومات. صدر المرسوم رقم 2.11.509 بتاريخ 21 شتنبر 2011 الذي أحدث المديرية العامة لأمن نظم المعلومات (*DGSSI*[8]) لتكون الهيئة المركزية لتأمين أنظمة الدولة المعلوماتية. أُنيط بهذه المديرية دور وضع وتنفيذ الإستراتيجية الوطنية للأمن السيبراني، ورصد المخاطر والتحذير منها على المستوى الوطني. كما تم إنشاء اللجنة الإستراتيجية لأمن نظم المعلومات كهيئة عليا تُعنى بتحديد السياسات الاستراتيجية في المجال السيبراني وحماية المعطيات الرقمية السيادية. وفي العام نفسه،

---

[4] هلالي، عبداللاه أحمد. *اتفاقية بودابست لمكافحة جرائم المعلوماتية: معلقًا عليها*. الطبعة الأولى. القاهرة: دار النهضة العربية، 2011.

[5] في قمة وارسو (*Warsaw Summit*) بتاريخ 8-9 يوليوز 2016، أعلن حلف شمال الأطلسي (*NATO*) أن الفضاء السيبراني أصبح مجالًا عملياتيًا رابعًا إلى جانب البر والبحر والجو.

[6] Centre National de Documentation. Maroc Numeric Cluster. Rabat : Haut-Commissariat au Plan. Consulté le 20 juin 2025 à 10h00, à : https://cnd.hcp.ma.

[7] المجلس الاقتصادي والاجتماعي والبيئي. *نحو تحول رقمي مسؤول ومدمج*. رأي في إطار إحالة ذاتية، الدورة العادية الحادية والعشرون بعد المائة، 29 أبريل 2021.

[8] *مرسوم رقم 509-11-2* الصادر في 22 شوال 1432 (21 شتنبر 2011) المتمم للمرسوم رقم 673-82-2 الصادر في 28 ربيع الأول 1403 (13 يناير 1983) المتعلق بتنظيم إدارة الدفاع الوطني وإحداث المديرية العامة لأمن نظم المعلومات.

وُضعت أسس التعاون بين المؤسسات الأمنية والتقنية للتصدي للهجمات الإلكترونية وحماية البنى الحرجة. سبق ذلك أيضًا بعض الخطوات التشريعية المهمة، حيث اعتمد المغرب في 2003 القانون رقم 07.03 الذي أدرج الجرائم المعلوماتية ضمن مجموعة القانون الجنائي، مما مثل أول اعتراف تشريعي بخطورة الجرائم الإلكترونية[9]. ثم جاء القانون رقم 09.08 لسنة 2009 المتعلق بحماية المعطيات ذات الطابع الشخصي لإنشاء إطار قانوني لحماية البيانات الشخصية للمواطنين، من خلال إحداث اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (*CNDP*) المناط بها حصريًا التأكد من احترام معالجات البيانات للقانون وعدم انتهاكها لخصوصية الأفراد[10]. وقد تواصل البناء التشريعي والمؤسساتي في العقد الماضي بوتيرة متسارعة لمجاراة التهديدات السيبرانية. فتم إحداث وكالة التنمية الرقمية بموجب القانون 61.16 لعام 2017 لتعزيز التحول الرقمي وتنسيق الجهود التقنية بين مؤسسات الدولة[11]. وتتوج هذا المسار بإصدار القانون رقم 05.20 المتعلق بالأمن السيبراني في يوليو 2020[12]، والذي شكل قفزة نوعية في تأطير أمن نظم المعلومات بالمغرب. هذا القانون الشامل وضع المتطلبات الأساسية لحماية الأنظمة المعلوماتية الحساسة، وأسّس هيئة وطنية مكلفة بالأمن السيبراني (اللجنة الاستراتيجية للأمن السيبراني) لتنسيق الجهود ورسم الاستراتيجيات. كما عزز القانون العقوبات على مرتكبي الجرائم السيبرانية، وألزم المؤسسات الوطنية باحترام معايير الأمن المعلوماتي لضمان صمود البنى التحتية الرقمية أمام الهجمات. وعلى صعيد الإستراتيجيات، عملت المملكة على صياغة الإستراتيجية الوطنية للأمن السيبراني التي تم تحيينها مؤخرًا لعام 2030[13]، مركزة على تطوير القدرات التقنية وبناء الكفاءات الوطنية والتعاون الدولي. وقد أثمرت هذه الجهود تحسّنًا ملحوظًا في مكانة المغرب الدولية في مجال

---

[9] الظهير الشريف *رقم 1.03.197* الصادر في 16 رمضان 1424 (الموافق لـ 11 نوفمبر 2003)، القاضي بتنفيذ القانون رقم 07.03 القاضي بتتميم مجموعة القانون الجنائي فيما يخص الجرائم المرتبطة بنظم المعالجة الآلية للمعطيات.

[10] Bassime, Lamya. *"Application en droit marocain des normes de protection des personnes physiques à l'égard du traitement des données à caractère personnel."* REMSES 9, no. 2 (2024): pp. 360.

[11] صدر الظهير الشريف رقم 1.17.27 بتاريخ 8 ذي الحجة 1438 (الموافق لـ14 سبتمبر 2017)، والذي نُشر في العدد 6604 من الجريدة الرسمية، ليؤسس وكالة التنمية الرقمية (ADD) بموجب القانون رقم 61.16 تُصاغ هذه الوكالة كمؤسسة عمومية ذات شخصية معنوية وذاتيّة مالية، مهمتها تنظيم وتنسيق جهود الدولة في مجال التحول الرقمي، والتحسيس باستخدام التكنولوجيا الرقمية بين الإدارات والهيئات والقطاع الخاص والمواطنين .

[12] المملكة المغربية. *"القانون رقم 05.20 المتعلق بالأمن السيبراني."* الجريدة الرسمية، عدد 6904 (30 يوليوز 2020): 4160. الظهير الشريف رقم 1.20.69 بتاريخ 4 ذو الحجة 1441 (25 يوليوز 2020).

[13] المديرية العامة لأمن نظم المعلومات. الاستراتيجية الوطنية للأمن السيبراني 2030. المملكة المغربية، 2023. تم الاطلاع عليه بتاريخ 30 يونيو 2025، على الساعة 13:00، على الرابط: https://www.dgssi.gov.ma.

الأمن السيبراني؛ إذ اعترف الاتحاد الدولي للاتصالات في تقريره لعام 2020 و2024 بأداء المغرب المتميز، الذي حقق درجة 100/97.5 في مؤشر الأمن السيبراني العالمي لسنة 2024، وأُدرج ضمن الدول الرائدة (المستوى 1) عالميًا[14]. ويعكس هذا الإنجاز الإرادة المشتركة والالتزام القوي لجميع الفاعلين الوطنيين بتأمين الفضاء السيبراني المغربي وتعزيز قدرته على الصمود. ورغم ذلك، يظل التطور التقني متسارعًا، ما يتطلب استمرار المغرب في تحديث إستراتيجيته وتنمية موارده البشرية وتقنياته لمواجهة التحديات السيبرانية المستجدة.

أمام هذا السياق، برز اهتمام خاص في المغرب بموضوع الأمن السيبراني وحماية البنية التحتية الرقمية كجزء من التوجه العالمي نحو تأمين الفضاءات الرقمية. وقد اعتمدت المملكة المغربية خلال السنوات الأخيرة مقاربة متعددة الأبعاد لتعزيز أمنها السيبراني، شملت تطوير ترسانة قانونية وتنظيمية حديثة، وإنشاء مؤسسات وهيئات متخصصة، إضافة إلى الانخراط في تعاون دولي لحماية البنية التحتية الرقمية الوطنية. وتأتي هذه الجهود انسجامًا مع تزايد التهديدات السيبرانية التي قد تمس استقرار المغرب وسيادته الرقمية. وبذلك يشكّل المغرب نموذجًا لدراسة كيف يمكن لدولة ذات سيادة أن تواجه التحديات السيبرانية ضمن إطار سياسي ودستوري يحفظ أمنها القومي. إن اختيار المغرب نموذجًا يعكس الرغبة في تحليل التجربة الوطنية في هذا المجال، ومدى فاعلية الإجراءات المغربية في تحصين الفضاء السيبراني الوطني وتعزيز القدرة على الصمود أمام الهجمات الرقمية.

تنبع أهمية هذا الموضوع من تداخله مع عدة جوانب حيوية أمنية وقانونية وعلمية. فمن الجانب الأمني، يتصل الأمن السيبراني اتصالًا مباشرًا بالأمن القومي وسيادة الدولة؛ إذ أصبح الفضاء السيبراني بعدًا جديدًا من أبعاد السيادة الوطنية التي يجب حمايتها. إن قدرة الدولة على حماية بياناتها وأنظمتها الرقمية وصون بنيتها التحتية الحيوية من الهجمات الإلكترونية باتت شرطًا لضمان استقرارها الداخلي وحماية أمن المجتمع. أي إخلال بأمن الفضاء الرقمي قد يعرّض سيادة الدولة وسلامتها للخطر، خاصة في ظل ما يشهده العالم من تهديدات سيبرانية غير متماثلة قد تستهدف البنى الحيوية أو البيانات السيادية.

---

[14] الاتحاد الدولي للاتصالات. المؤشر العالمي للأمن السيبراني – النسخة الخامسة. الاتحاد الدولي للاتصالات، 2024. تم الاطلاع عليه بتاريخ 20 يونيو 2025، على الساعة 00:00، على الرابط: https://www.itu.int.

اما على الصعيد القانوني فتبرز ضرورة توفر الدولة على إطار تشريعي وتنظيمي محكم يساير التطور التقني المتسارع. ويأتي القانون رقم 05.20 المتعلق بالأمن السيبراني[15] ليرسخ قواعد حماية النظم المعلوماتية ذات الاهمية الحيوية ويحدد مسؤوليات الفاعلين ويمكن السلطات المختصة من آليات المراقبة والتدخل عند وقوع تهديدات سيبرانية. ويكتمل هذا الإطار بقوانين معززة مثل القانون رقم 53.05 الخاص بالتبادل الالكتروني للمعطيات القانونية[16] والقانون رقم 09.08 المتعلق بحماية المعطيات ذات الطابع الشخصي[17] بما يعزز الثقة في البيئة الرقمية ويحافظ على الحقوق والحريات الدستورية للمستخدمين.

ومن الزاوية الاقتصادية يكتسي الأمن السيبراني مكانة محورية لأنه يمثل خط الدفاع الأول عن الاستثمارات الرقمية والمعاملات المالية الإلكترونية التي أصبحت ركيزة للنمو الحديث. فكل اختراق قد يشل أنظمة الدفع ويعرقل سلاسل التوريد ويكبّد المؤسسات خسائر مباشرة في المداخيل، فضلاً عن كلفة السمعة التي ترغم الشركات والحكومة معاً على إنفاق مبالغ طائلة لاستعادة الثقة. كما يُمكّن إطار الحماية السيبرانية من جذب الاستثمارات الأجنبية، إذ يفضّل المستثمرون البيئات الآمنة القادرة على حماية أصولهم الرقمية وبياناتهم الحساسة، وهو ما ينعكس إيجاباً على خلق فرص الشغل وتعزيز الناتج الداخلي الإجمالي. إضافة إلى ذلك، يحدّ الأمن السيبراني المتين من كلفة الجرائم الإلكترونية التي قد تستنزف ميزانيات القطاعات البنكية والتجارية، ويوفّر بيئة مستقرة لنمو التجارة الإلكترونية والخدمات السحابية، بما يعزّز مسار التحول الرقمي ويضاعف القيمة المضافة لاقتصاد المعرفة.

وعلى الصعيد العلمي (الأكاديمي)، تبرز أهمية البحث في كونه يُسهم في سد فجوة معرفية في أدبيات الدراسات السياسية والقانونية العربية. يُعد ربط الأمن السيبراني بحماية البنية التحتية الرقمية في إطار السياسات العمومية والسيادة الوطنية طرحًا حديثًا نسبيًا، مما يضفي على الدراسة قيمة علمية. فمن جهة، يساعد البحث صنّاع القرار على فهم التحديات التقنية الحديثة ضمن إطار نظري سياسي وقانوني؛ ومن جهة أخرى، يثري الأدبيات الأكاديمية عبر مقاربة

---

[15] مرجع سابق، *"القانون رقم 05.20 المتعلق بالأمن السيبراني"*.

[16] القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية كما تم تعديله: القانون رقم 43.20. الصادر بتنفيذه الظهير الشريف رقم 1.20.100 بتاريخ 16 من جمادى الأولى 1442 (31) ديسمبر 2020؛ الجريدة الرسمية عدد 6951 بتاريخ 27 .271 جمادى الأولى 1442 (11) يناير (2021) ص 271.

[17] القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذه الظهير الشريف رقم 1.09.15 بتاريخ 18 فبراير 2009.

موضوع يجمع بين الحقل التقني والحقلين القانوني والأمني. وبذلك، تتيح هذه الدراسة فهمًا أعمق لكيفية تكييف النظريات التقليدية للأمن والسيادة مع واقع التحول الرقمي، مما يدعم تطوير سياسات عمومية رشيدة في مجال الأمن السيبراني.

لضمان وضوح الدراسة ودقة التحليل، من الضروري تحديد المفاهيم والمحاور الأساسية نظريًا وإجرائيًا، وعلى رأسها مصطلحات: الأمن السيبراني والبنية التحتية الرقمية.

الأمن السيبراني: من ناحية النظرية يمكن القول انه يشير إلى مجموعة الإجراءات والتدابير التقنية والإدارية الرامية إلى حماية الأنظمة الحاسوبية والشبكات والبيانات من الهجمات الإلكترونية والاختراقات والتخريب. فهو يركز على ضمان ثلاثة مبادئ أساسية في أمن المعلومات: سرية المعطيات وسلامتها وتوافرها، من خلال التصدي لمختلف التهديدات السيبرانية كالفيروسات وهجمات القرصنة وغيرها. ويُعد الأمن السيبراني اليوم جزءًا لا يتجزأ من الأمن القومي للدول، نظرًا لتأثير الهجمات على البنى التحتية الرقمية في سيادة الدول واستقرارها. أما إجرائيًا في السياق المغربي، مجموعة متكاملة من التدابير والإجراءات والتقنيات الحديثة المصممة لحماية أنظمة المعلومات وتمكينها من الصمود أمام التهديدات المرتبطة بالفضاء السيبراني، بما يضمن الحفاظ على سريّة المعطيات وسلامتها وتوافرها واستمرارية الخدمات. هذا التعريف القانوني يبيّن نهجًا شاملًا يتجاوز الحماية التقنية البحتة ليشمل الأبعاد التنظيمية والإدارية بهدف إنشاء بيئة رقمية آمنة قادرة على التصدي للهجمات.

البنية التحتية الرقمية: نظريًا، تُعرّف البنية التحتية الرقمية بأنها مجموعة المكونات التقنية (الأجهزة، الشبكات، البرمجيات، مراكز البيانات) والخدمات التي تتيح تدفق البيانات ومعالجة المعلومات وتقديم الخدمات الرقمية بشكل مستدام. بعبارة أخرى، تشمل البنية التحتية الرقمية جميع الأنظمة والمنشآت التكنولوجية الضرورية لتشغيل المجتمع الرقمي الحديث، من خوادم الحكومة الإلكترونية وقواعد البيانات الوطنية إلى شبكات الاتصالات ومنصات الخدمات العامة على الإنترنت. وإجرائيًا، يقصد بهذا المفهوم في بحثنا كل العناصر الرقمية الحيوية التي يعتمد عليها تسيير المرافق العمومية والقطاعات الحيوية في المغرب – مثل أنظمة الاتصالات الحكومية، وشبكات المصارف، وأنظمة التحكم في الطاقة والنقل – والتي قد يؤدي تعطلها أو اختراقها إلى شلل في الخدمات الأساسية وانتهاك للأمن الوطني. وعليه، فإن حماية البنية

التحتية الرقمية تعني تأمين هذه المكونات ضد الأخطار التقنية والبشرية المحتملة، وضمان استمرارية عملها بأمان.

انبثقت فكرة اختيار هذا الموضوع لدى الباحث من مجموعة اعتبارات ودوافع علمية وشخصية. أولًا، جاء الاختيار مدفوعًا بالاشتغال العملي والتقني للباحث في ميدان ذا صلة بموضوع البحث؛ فقد مكنه العمل في هذا المجال من ملامسة واقع التهديدات الرقمية عن قرب والإحساس بأهمية حماية الأنظمة الحساسة. هذا الاحتكاك العملي عزّز الوعي بضرورة معالجة موضوع الأمن السيبراني من زاوية العلوم السياسية والقانونية، نظرًا لتأثير القرارات التقنية على السياسات العمومية وأمن الدولة. ثانيًا، يلاحظ قلة الدراسات الأكاديمية العربية – وخاصة المغربية – التي تناولت الأمن السيبراني بشكل شمولي يربطه بالسيادة الوطنية. فمعظم الأدبيات المتوفرة تركز إما على الجوانب التقنية البحتة، أو على الجرائم الإلكترونية من منظور جنائي ضيق. ورغم وجود بعض المساهمات السابقة في المغرب، إلا أنها تظل محدودة في ربط الأمن السيبراني بالسياسات العمومية والبنية المؤسساتية للدولة. هذا النقص في الأدبيات شكّل حافزًا للباحث لسدّ هذه الفجوة ومحاولة تقديم إضافة علمية تربط بين التقنيات الحديثة وإطارها القانوني والمؤسساتي في المغرب. كما أن التطورات السريعة التي يشهدها العالم الرقمي اليوم – سواء من حيث تزايد حوادث الاختراق الكبرى عالميًا، أو من حيث استجابة الدول بسنّ استراتيجيات أمن سيبراني جديدة – تجعل من دراسة هذا الموضوع أمرًا ملحًا وذي راهنية، لضمان مواكبة الباحثين وصنّاع القرار لهذه التحولات المتسارعة.

في نطاق الدراسات السابقة حول الأمن السيبراني تبرز دراسة أساسية تشكل مرجعًا أوليًا في هذا المجال لـ ياسين مليح ويونس مليح بعنوان *Cybersecurity in Morocco* (الأمن السيبراني بالمغرب[18])، وهو كتاب موجز صادر سنة 2022، استعرضَ تطوّر الإستراتيجية الوطنية منذ إحداث المديرية العامة لأمن نظم المعلومات سنة 2011، وحلّل موقع المغرب في المؤشرات الدولية، وقارن معايير الحوكمة الوطنية (كالقانون 05.20) بالمعايير العالمية

[18] Maleh, Yassine, and Youness Maleh. *Cybersecurity in Morocco*. 1st ed. Cham, Switzerland: Springer Nature Switzerland AG, 2022 p. 13.

(NIST ،ISO 27001)، مُختتمًا بتوصيات لتعزيز الصمود السيبراني عبر تقوية القدرات البشرية وتنسيق عمل الهيئات المختصّة.

واجه إعداد هذا البحث عدة صعوبات وعراقيل، كان أبرزها ندرة المادة العلمية المتخصصة في موضوع يربط بين الأمن السيبراني والدراسات الدستورية والسياسية في السياق المغربي. فعلى الرغم من توافر معلومات تقنية وأمنية عامة، إلا أن العثور على مصادر أكاديمية تجمع بين الجانبين القانوني والتقني للموضوع تطلب جهدًا واسعًا في البحث والترجمة والاستقراء. واجه الباحث صعوبة في الحصول على مراجع حديثة باللغة العربية تعالج موضوع السيادة الرقمية أو الإطار المؤسساتي للأمن السيبراني، مما اضطره للاعتماد على بعض المصادر الأجنبية والتقارير الدولية وترجمتها لسد الفجوة. كما أن حداثة الموضوع نسبيًا في البيئة الأكاديمية العربية جعلت الكثير من المفاهيم التقنية بحاجة إلى تأصيل نظري ضمن الحقل القانوني. ومن الصعوبات كذلك محدودية البيانات العلنية حول الحوادث السيبرانية في المغرب نظرًا لحساسية هذا المجال أمنيًا؛ إذ تفتقر المراجع إلى إحصاءات مفصلة حول الهجمات الإلكترونية التي استهدفت البنى التحتية الوطنية أو الخسائر الناجمة عنها، وهو ما صعّب مهمة التحليل الكمّي. إضافة إلى ذلك، تطلب الطبيعة البينمناهجية للموضوع من الباحث الإلمام بجوانب تقنية معقدة في أمن المعلومات حتى يتسنى له مناقشتها ضمن إطار قانوني وسياسي سليم. ورغم هذه الصعوبات، سعى الباحث لتجاوزها عبر توسيع نطاق البحث ليشمل مصادر متعددة (قانونية، تقنية، إستراتيجية)، والاستعانة ببعض الخبرات الميدانية المكتسبة من العمل في القطاع التقني، مما ساعد في تقديم قراءة شمولية ومتوازنة قدر الإمكان لهذا الموضوع الحديث.

ينطلق هذا البحث من تساؤل جوهري حول مدى قدرة المنظومة القانونية والمؤسساتية المعتمدة في المغرب على تأمين الفضاء السيبراني الوطني وحماية البنية التحتية الرقمية بشكل يكرّس السيادة الرقمية للدولة ويصونها من التهديدات المتسارعة والمتعددة الأبعاد. فهل استطاعت هذه المنظومة مجاراة التحولات التقنية المتلاحقة والاستجابة لمتطلبات الحماية الحديثة؟ وهل وفّرت الأطر التنظيمية والمؤسساتية الحالية مستوى كافيًا من التنسيق

والجاهزية لضمان أمن المعلومات والخدمات الحيوية في مواجهة التحديات السيبرانية المتنامية؟

للتعمق في جوانب الإشكالية المذكورة وتغطية مختلف محاورها، تفرعت عنها مجموعة من الأسئلة الفرعية التي ترتبط كل منها بجزء محدد من الدراسة. من قبيل هذه الأسئلة: ما هي المفاهيم الأساسية للأمن السيبراني والبنية التحتية الرقمية؟ كيف يساهم الأمن السيبراني في حماية السيادة الوطنية للدولة؟ هل الإطار القانوني المغربي كافٍ لحماية الفضاء الرقمي الوطني؟ ما دور المؤسسات الوطنية المختصة في تعزيز الأمن السيبراني وحماية البنية الرقمية؟ ما أبرز التهديدات السيبرانية التي تواجه البنية التحتية الرقمية في المغرب حاليًا؟ ما هي نقاط الضعف والثغرات في المنظومة الرقمية الوطنية التي قد تستغلها التهديدات السيبرانية؟ كيف يمكن الاستفادة من التجارب الدولية الرائدة في مجال الأمن السيبراني لتعزيز النموذج المغربي؟ ما هي سُبل تعزيز الأمن السيبراني في المغرب مستقبلًا؟

في ضوء الإشكالية المحورية، ومع الأخذ في الاعتبار سياق البحث وأهدافه، يوجَّه التحليل بفرضيتين متقابلتين تستقرئان مدى فاعلية المنظومة القانونية والمؤسّساتية المغربية في حقل الأمن السيبراني. ترتكز الفرضية الأولى على تصورٍ يُقرّ بكفاية الإطار القائم ـ وفي طليعته القانون رقم 05.20 والهيئات المختصة التابعة له ـ لتحقيق حماية شاملة للبنية التحتية الرقمية، بما يجعل هذا الإطار قادرًا بذاته على مجابهة التهديدات السيبرانية المتجددة من غير حاجة إلى تعديلات جوهرية أو تدابير إضافية. أمّا الفرضية الثانية فتفترض أن المنظومة الراهنة، على الرغم من أهميتها، ما زالت تتطلّب تطويرًا تشريعيًا وتنظيميًا وتقنيًا متواصلًا، فضلًا عن تعميق التنسيق بين الجهات المعنية، وبناء قدرات بشرية متخصصة، وتوطين التكنولوجيا عبر تحفيز البحث والتطوير والتصنيع المحلي للأدوات والحلول السيبرانية، حتى تؤمّن حماية فعّالة ومستدامة للبنية الرقمية وتكرّس السيادة الوطنية في مواجهة وتيرة المخاطر السيبرانية المتسارعة.

يعتمد هذا البحث مقاربة منهجية متعدّدة؛ إذ يرتكز أوّلًا على المنهج الوصفي–التحليلي لعرض الإطار القانوني والمؤسّساتي للأمن السيبراني في المغرب ثم تفكيك عناصره واستنتاج نقاط قوّته وضعفه، ويستعين ثانيًا بالتحليل الكمي لاستثمار المؤشّرات والإحصاءات الدولية في

قياس مستوى الجاهزية السيبرانية ومقارنته زمنيًا، كما يوظّف المنهج البنيوي–الوظيفي لفحص أداء الهيئات المختصّة من قبيل المديرية العامة لأمن نظم المعلومات واللجنة الوطنية لحماية المعطيات الشخصية وطرائق تفاعلها في ما بينها. علاوة على ذلك، يُفعَّل المنهج المقارن لاستجلاء التجارب الدولية الرائدة واستنباط الممارسات الملائمة للبيئة المغربية، بينما تشكّل دراسة الحالة إطارًا جامعًا يُسلّط الضوء على المغرب كنموذج لفهم التحديات والسياسات السيبرانية في دولة نامية تسعى إلى ترسيخ سيادتها الرقمية. هكذا تتكامل هذه المناهج لتوفير تحليل شامل يجمع بين البعد النظري والبعد التطبيقي، ويُفضي إلى تقييمٍ علميٍّ لمستوى فاعلية المنظومة المغربية في حماية البنية التحتية الرقمية.

ينتظم هذا البحث في فصلين مترابطين، يتكاملان في معالجة الإشكالية المطروحة. يتناول ***الفصل الأول: الإطار النظري والمؤسساتي للأمن السيبراني وحماية البنية التحتية الرقمية*** *المفاهيم الأساسية المرتبطة بالأمن السيبراني والبنية التحتية الرقمية، ويستعرض الإطارين القانوني والمؤسساتي اللذين يشكّلان الأساس الوطني لحماية الفضاء الرقمي. أما* ***الفصل الثاني: التحديات السيبرانية واستراتيجيات الحماية في المغرب،*** *فيُكرَّس لتحليل التهديدات التقنية والاختلالات البنيوية التي تواجه المنظومة السيبرانية المغربية، مع استعراض الاستراتيجيات الوطنية المعتمدة، والدروس المستخلصة من بعض التجارب المقارنة، بهدف تقديم مقترحات لتعزيز فعالية الحماية وتعزيز السيادة الرقمية.*

الفصل الأول: الإطار النظري والمؤسساتي للأمن السيبراني وحماية البنية التحتية الرقمية

في ظل التحولات الرقمية المتسارعة، أصبح الأمن السيبراني يشكّل أحد المرتكزات الأساسية لحماية السيادة الوطنية، لاسيما مع تزايد الاعتماد على البنية التحتية الرقمية في تسيير المرافق الحيوية، وتزايد التهديدات الإلكترونية الموجهة للدول. وقد بات من الضروري التأسيس لنظرة علمية ومؤسساتية شاملة تُمكّن من فهم تحديات هذا المجال وتعزيز آليات حمايته، سواء من الناحية القانونية أو التقنية أو الاستراتيجية. بناءً على ذلك، سنعالج في هذا الفصل الأول الإطار النظري والمؤسساتي للأمن السيبراني وحماية البنية التحتية الرقمية. حيث سيتم تخصيص المبحث الأول لتحليل المفاهيم العامة المرتبطة بالأمن السيبراني والبنية التحتية الرقمية وأبعادها السيادية، في حين يُعنى المبحث الثاني بدراسة المنظومة القانونية والمؤسساتية المؤطرة لهذا المجال في السياق المغربي. وسيتم تفكيك هذه القضايا عبر مطالب وفقرات دقيقة تُبرز تلازم البعدين النظري والتطبيقي في حماية الفضاء السيبراني الوطني.

المبحث الأول: المفاهيم العامة للأمن السيبراني والبنية التحتية الرقمية

يمثل الأمن السيبراني والبنية التحتية الرقمية اليوم حجر الزاوية في بناء الدولة الحديثة، خصوصًا مع تنامي التهديدات الرقمية التي تستهدف استقرار الأنظمة والمؤسسات. ويعد فهم هذه المفاهيم مدخلًا ضروريًا لأي مقاربة فعالة تهدف إلى تأمين الفضاء السيبراني الوطني وتعزيز السيادة الرقمية. لذلك، يهدف هذا المبحث إلى وضع الأسس النظرية الضرورية لاستيعاب الرهانات التقنية والسيادية المرتبطة بالأمن السيبراني والبنية التحتية الرقمية، في أفق ربطها لاحقًا بالإطار المؤسساتي والقانوني المنظِّم لها في السياق المغربي. وفي هذا السياق، سيتم ضمن المطلب الأول تحليل مفهوم الأمن السيبراني من مختلف زواياه، مع التوقف عند أبعاده السيادية والمكونات النظرية والتقنية المرتبطة به، بينما يتناول المطلب الثاني أهمية البنية التحتية الرقمية وأدوارها الحيوية في دعم وظائف الدولة، مع إبراز علاقتها المباشرة بتعزيز الاستقرار الوطني والسيادة الرقمية.

المطلب الأول: مفهوم الأمن السيبراني وأبعاده السيادية

يعد الأمن السيبراني من المفاهيم الحديثة التي فرضتها التحولات الرقمية العالمية، وأصبح يشكّل ركيزة أساسية لحماية الفضاء المعلوماتي للدول، بالنظر إلى التهديدات المتزايدة التي

تستهدف البنية التحتية الرقمية ومصادر القرار السيادي. وقد أضحى هذا المفهوم يُمثل أحد أبعاد الأمن القومي، من حيث وظيفته الوقائية وقدرته على تعزيز سيادة الدولة في المجال الرقمي. وفي هذا الإطار، يتناول هذا المطلب الأول تحليلًا دقيقًا لمفهوم الأمن السيبراني، من خلال تحديد دلالاته اللغوية، التقنية، والاستراتيجية، مع إبراز أبعاده السيادية في ظل التحديات الرقمية المتصاعدة. وسيتم ذلك عبر فقرتين متكاملتين؛ سنخصص الأولى لتحديد المفهوم ومكوناته الأساسية، أما الفقرة الثانية سنخصصها لعلاقته بالسيادة الوطنية والأمن القومي.

الفقرة الاولى: تحديد المفهوم ومكوناته الأساسية

يشكل الأمن السيبراني مفهومًا مركبًا يتقاطع فيه البعد اللغوي، بما يحمله من دلالات على الحماية والاطمئنان، مع الجوانب التقنية المرتبطة بتأمين النظم المعلوماتية، إلى جانب أبعاده الاستراتيجية التي تجعل منه أداة مركزية في صون السيادة الرقمية وحماية المصالح الوطنية في الفضاء السيبراني.

اولا: تحديد المفهوم

في اللغة العربية، يُعبر مصطلح "الأمن" عن حالة الاطمئنان والحماية من المخاطر، مشيرًا إلى شعور الأفراد أو المجتمعات بالسلامة لأنفسهم وممتلكاتهم[19]. أما مصطلح "السيبراني" فينبع من كلمة "*Cyber*" الإنجليزية، التي تدل على ما يرتبط بالحواسيب، تكنولوجيا المعلومات، أو الفضاء الافتراضي. وقد استُخدم هذا المصطلح لأول مرة عام 1948 بواسطة عالم الرياضيات نوربرت وينر[20] للدلالة على علم التحكم والاتصال في الأنظمة الحاسوبية، مما مهد لتكوين مفهوم الفضاء السيبراني كبيئة تشمل الشبكات والبيانات[21].

مفاهيميًا، يُعرف الأمن السيبراني بأنه مجموعة الإجراءات والتدابير التقنية والتنظيمية التي تسعى لحماية الأنظمة الحاسوبية، الشبكات، البرمجيات، والبيانات من التهديدات الإلكترونية، بما في ذلك الهجمات الضارة والاختراقات. ويركز هذا المجال على ضمان سرية المعلومات،

---

[19] الأصفهاني، الحسين بن علي، *المفردات في غريب القرآن*، دار المعرفة، بيروت، لبنان، 2005، ص 34.

[20] نوربرت وينر (1894–1964): عالم رياضيات أمريكي، *يُعدّ مؤسس علم السيبرنطيقا*، وهو من أوائل من تناولوا مفاهيم التحكم والاتصال في الأنظمة الآلية والبيولوجية.

[21] بكيل بن محمد البراشي، *دور الأمن الفكري في الوقاية من الإرهاب*، رسالة ماجستير، *قسم العلوم الشرطية*، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2010، ص 83.

سلامتها، وتوافرها، مع مواجهة محاولات التخريب أو التلاعب، كما يتضمن الأمن السيبراني حماية مادية للأجهزة والبرمجيات، وحماية معنوية للبيانات من السرقة أو التلف، مع إيلاء أهمية لضبط الوصول إلى الأنظمة للحد من المخاطر[22].

يُعتبر الأمن السيبراني جزءًا أساسيًا من الأمن القومي، حيث تؤثر الهجمات على البنية التحتية الرقمية، مثل الاتصالات والأنظمة الإلكترونية، على سيادة الدول واستقرارها. ومع تزايد الاعتماد على هذه البنية، أصبحت التهديدات السيبرانية تهديدًا للأمن الاستراتيجي، مما يجعل الأمن السيبراني محط اهتمام عالمي. يستند هذا المجال إلى مبادئ تشمل حماية البيانات من الوصول غير المصرح به، ووضع سياسات أمنية فعالة لمواجهة التهديدات، مثل البرمجيات الخبيثة والهجمات الهجينة – من خلال مقاربة تجمع بين الأبعاد التقنية والتنظيمية[23].

وفقًا للمادة 2 من القانون رقم 05.20 المتعلق بالأمن السيبراني، يُعرف الأمن السيبراني بأنه مجموعة متكاملة من التدابير، الإجراءات، المفاهيم الأمنية، استراتيجيات إدارة المخاطر، الأنشطة العملية، التكوينات التقنية، أفضل الممارسات، والتكنولوجيات الحديثة التي تُصمم لحماية أنظمة المعلومات. يهدف هذا الإطار إلى تمكين هذه الأنظمة من الصمود أمام التهديدات والأحداث المرتبطة بالفضاء السيبراني التي قد تُعرض للخطر توافر المعطيات، سلامتها، أو سريتها، سواء كانت هذه المعطيات مخزنة، قيد المعالجة، أو يتم إرسالها. كما يشمل الهدف ضمان استمرارية الخدمات المرتبطة بالنظام وتأمين إمكانية الوصول إليها بشكل آمن. يتضمن هذا التعريف مقاربة شاملة تتجاوز الحماية التقنية البحتة لتشمل أبعادًا تنظيمية، إدارية، ومفاهيمية. فالمصطلح يشير إلى نظام بيئي متكامل يهدف إلى تعزيز مرونة أنظمة المعلومات ضد التهديدات السيبرانية. على سبيل المثال، تشمل "التدابير والإجراءات" وضع سياسات أمنية، مثل بروتوكولات التشفير أو أنظمة كشف التسلل، بينما تُركز "مفاهيم الأمن" على بناء إطار فكري يوجه هذه السياسات، كمبدأ الدفاع المتعدد الطبقات. أما "إدارة المخاطر"

---

[22] إدريس عطية، *مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري*، جامعة العربي التبسي، الجزائر، 2019، ص 56.

[23] السمحان منى عبد الله ، *متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية*، مجلة كلية التربية، جامعة المنصورة، المجلد 111، العدد1، المملكة العربية السعودية، 2020، ص 2-29.

فتعكس عملية تحديد التهديدات المحتملة، تقييم تأثيرها، ووضع خطط للحد منها، مثل تحليل المخاطر السيبرانية للبنية التحتية الحيوية[24].

تشير "الأعمال والتكوينات" إلى الأنشطة العملية، مثل تدريب الموظفين على التعامل مع الهجمات السيبرانية أو تهيئة الأنظمة بإعدادات أمنية متقدمة. وتعكس "أفضل الممارسات" الاستفادة من المعايير الدولية، مثل إطار *NIST* للأمن السيبراني أو معايير *ISO/IEC 27001*، لضمان فعالية التدابير المتخذة. أما "التكنولوجيات" فتشمل الأدوات المتقدمة، مثل جدران الحماية، برامج مكافحة الفيروسات، أو تقنيات الذكاء الاصطناعي للكشف عن التهديدات[25].

الهدف الأساسي لهذا التعريف هو حماية ثلاث ركائز أساسية للمعطيات: **التوافر** (ضمان إمكانية الوصول إلى المعطيات والخدمات عند الحاجة)، **السلامة** (الحفاظ على دقة المعطيات وخلوها من التلاعب)، و**السرية** (منع الوصول غير المصرح به). هذه الركائز تُعد جوهرية لضمان عمل الأنظمة الحيوية، مثل شبكات الاتصالات، الأنظمة المصرفية، أو منصات الحكومة الإلكترونية، التي قد تتعرض لتهديدات مثل هجمات البرمجيات الخبيثة، القرصنة، أو هجمات الحرمان من الخدمة (*DDoS*[26]). كما يُبرز التعريف أهمية حماية الخدمات المرتبطة بالنظام، مثل التطبيقات السحابية[27]، وتأمين قنوات الوصول إليها لمنع الاختراقات.

يُظهر التعريفان للأمن السيبراني – الأول كمفهوم عام متعدد الأبعاد يجمع الدلالات اللغوية، التقنية، والاستراتيجية، والثاني وفق المادة 2 من القانون 05.20 كإطار تنظيمي شامل –

---

[24] المادة 2 الفقرة الاولى من *القانون رقم 05.20 المتعلق بالأمن السيبراني*- الصادر بتنفيذه ظهير شريف رقم 1.20 .69 بتاريخ 4 ذي الحجة 1441 (25 يوليو 2020).

[25] إطار *NIST* للأمن السيبراني هو مجموعة معايير من المعهد الوطني للمعايير والتكنولوجيا بالولايات المتحدة، يهدف لإدارة المخاطر السيبرانية عبر وظائف: التعرف، الحماية، الكشف، الاستجابة، والاستعادة. أما معايير *ISO/IEC 27001* فهي معايير دولية من المنظمة الدولية للتوحيد القياسي (*ISO*) واللجنة الكهروتقنية الدولية (*IEC*) لإدارة أمن المعلومات وحماية البيانات.

[26] Ali El Azzouzi, *La Cybercriminalité au Maroc* (Casablanca : Bishops Solutions, 2010), p. 51.

[27] التطبيقات السحابية *(Cloud Applications)* هي برامج أو تطبيقات يتم تشغيلها وتخزينها على خوادم بعيدة متصلة عبر الإنترنت، بدلاً من تخزينها وتشغيلها على جهاز المستخدم المحلي (مثل الحاسوب أو الهاتف). بمعنى آخر، هي تطبيقات تعتمد على تقنية الحوسبة السحابية لتقديم خدماتها، حيث يمكن الوصول إليها من أي مكان وفي أي وقت طالما يوجد اتصال بالإنترنت.

رؤية متكاملة تركز على حماية أنظمة المعلومات من التهديدات السيبرانية، مع ضمان سرية المعطيات، سلامتها، وتوافرها، إلى جانب استمرارية الخدمات.

ثانيا: المفاهيم المرتبطة بالأمن السيبراني

يُعتبر الأمن السيبراني أحد المجالات الحديثة التي تتطلب فهمًا عميقًا لمجموعة من المفاهيم الأساسية التي تُشكل إطاره النظري والتطبيقي، والتي تُساهم في تعزيز قدرة الدول على حماية بنيتها التحتية الرقمية والحفاظ على سيادتها الوطنية في مواجهة التحديات السيبرانية المتزايدة. وبشكل عام، تتعدد المفاهيم المرتبطة بالأمن السيبراني، ومن أبرزها ما يلي:

أ – الفضاء السيبراني:

عُرف هذا المصطلح من قبل الوكالة الفرنسية لأمن أنظمة المعلومات (*ANSSI*) بأنه "فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[28]. ويُمثل الفضاء السيبراني بيئة رقمية تفاعلية تجمع بين عناصر مادية مثل الأجهزة الرقمية (الحواسيب، الهواتف الذكية، الخوادم) وعناصر غير مادية مثل البرمجيات والبيانات، ويشمل أنظمة الشبكات والمستخدمين، سواء كانوا مشغلين أو مستفيدين. فعلى سبيل المثال، يُعتبر الإنترنت جزءًا من الفضاء السيبراني الذي يربط بين المؤسسات الحكومية والخاصة، مما يجعله هدفًا محتملاً للهجمات التي قد تُهدد الأمن القومي.

ب – الردع السيبراني:

يُعرف بأنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء السيبراني والأصول التي تدعم العمليات الفضائية". ويُعد الردع السيبراني استراتيجية حيوية للحفاظ على السيادة الوطنية، حيث يهدف إلى ردع الجهات المعادية عن تنفيذ هجمات قد تُعطل البنية التحتية الحيوية، مثل أنظمة الاتصالات أو الشبكات الكهربائية. على سبيل المثال، يمكن لدولة أن تتبنى سياسات ردع سيبراني من خلال تعزيز دفاعاتها الرقمية وإظهار قدراتها الهجومية لتثبيط المهاجمين[29].

---

[28] Kempf, Olivier. *Introduction à la Cyberstratégie*. Paris: Economica, 2012, p. 9.

[29] Nye Jr., Joseph S. *Deterrence and Dissuasion in Cyberspace*. Article in International Security, Vol. 41, No. 3, 2017, p. 46.

ج – الهجمات السيبرانية:

تُعرف بأنها "فعل يقوّض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام". وتُشكل هذه الهجمات تهديدًا مباشرًا للأمن القومي، حيث يمكن أن تستهدف مؤسسات حيوية مثل البنوك أو الوزارات الحكومية. فعلى سبيل المثال، قد يستغل المهاجمون ثغرة في نظام حكومي لسرقة بيانات المواطنين أو تعطيل خدمات أساسية، مما يُعرض الاستقرار الوطني للخطر[30].

د – الجريمة السيبرانية:

تُشير إلى "مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تُبث عبرها محتوياتها". وتشمل الجرائم السيبرانية أفعالًا مثل القرصنة، سرقة الهوية، والاحتيال الإلكتروني. على سبيل المثال، قد يُنفذ مجرمو الإنترنت هجومًا على بنك لسرقة بيانات العملاء، مما يُسبب أضرارًا اقتصادية واجتماعية تؤثر على الأمن القومي[31].

يُمكن القول إن الأمن السيبراني يُشكل مجموعة من الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية الفضاء السيبراني –بما في ذلك البرمجيات وأجهزة الكمبيوتر– من مختلف الهجمات والاختراقات والتهديدات السيبرانية التي قد تُهدد الأمن القومي للدول. وفي ظل الاعتماد المتزايد على الأنظمة الرقمية في إدارة البنية التحتية الحيوية، يُصبح الأمن السيبراني عنصرًا أساسيًا للحفاظ على السيادة الوطنية والاستقرار السياسي والاقتصادي والاجتماعي. فعلى سبيل المثال، تعطيل نظام كهربائي أو شبكة اتصالات بسبب هجوم سيبراني قد يؤدي إلى أزمات وطنية تُهدد الأمن العام.

هـ – الأمن المعلوماتي:

يُعتبر الأمن المعلوماتي إطارًا شاملًا يسعى لحماية البيانات والمعلومات بغض النظر عن وسيلة تخزينها أو معالجتها (ورقية، إلكترونية، صوتية...)، مركّزًا على ثلاث ركائز أساسية: السريّة (منع الوصول غير المصرّح)، النزاهة (ضمان دقة المعلومات وعدم التلاعب بها)،

---

[30] International Committee of the Red Cross (ICRC). *Cyber warfare and international humanitarian law: The ICRC's position*. Geneva: ICRC, 2013, p. 2.

[31] الأشقر جبور، منى. *السيبرانية هاجس العصر*. بيروت: المركز العربي للبحوث القانونية والقضائية، 2017، ص 50.

والتوافر إتاحتها في الوقت المناسب للمستخدمين المصرَّح. أما الأمن السيبراني، فهو جزء فرعي متخصص ضمن الأمن المعلوماتي، يتعامل حصريًا مع حماية الأنظمة الرقمية والشبكات من الهجمات الإلكترونية مثل البرمجيات الخبيثة، التصيد، والهاكرز[32].

ثالثا: المفاهيم الأساسية المرتبطة بالأمن السيبراني وفق القانون المغربي 05.20

أدرك المشرع المغربي أهمية وضع إطار قانوني واضح لتنظيم الأمن السيبراني وحماية الفضاء الرقمي، وهو ما تجسد في القانون رقم 05.20 المتعلق بالأمن السيبراني. وقد حددت المادة 2 من هذا القانون مجموعة من المفاهيم الأساسية التي تُشكل مرجعية قانونية لفهم التحديات السيبرانية ووضع الاستراتيجيات اللازمة لمواجهتها. يُعرض الجدول التالي لتوضيح المفاهيم مع شرحها وأمثلة تطبيقية[33]:

المصطلح	شرح المفهوم	مثال توضيحي
الجرائم السيبرانية	الأفعال غير المشروعة التي تُرتكب ضد الأنظمة الرقمية أو تُستخدم كوسيلة لأغراض إجرامية، سواء بموجب القوانين الوطنية أو الدولية.	اختراق موقع حكومي لسرقة بيانات المواطنين أو استخدام الإنترنت لنشر برمجيات خبيثة[34].
التهديد السيبراني	أي نشاط يهدف إلى تعطيل عمل الأنظمة الرقمية أو المساس بأمنها من حيث التوافر، السلامة، أو السرية.	هجمات الحرمان من الخدمة (*DDoS*) التي تُغرق موقعًا إلكترونيًا بحركة مرور وهمية لتعطيله[35].
الأخلاقيات السيبرانية	المبادئ التي تُنظم السلوكيات في الفضاء الرقمي لضمان الاستخدام المسؤول والملتزم.	تجنب مشاركة بيانات شخصية دون موافقة أو الامتناع عن نشر محتوى مسيء عبر الإنترنت.

[32] Kobetitsch, Katarina. Information Security vs. Cyber Security: Are They the Same? St. John's University, March 25, 2024. Accessed July 10, 2025, at 14:47. *https://www.stjohns.edu*

[33] مرجع سابق، *المادة 2* الفقرة الاولى من القانون رقم 05.20 المتعلق بالأمن السيبراني.

[34] Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* 1st ed. New York: Oxford University Press, 2014, p. 13.

[35] Référence précédente: Ali El Azzouzi, *La Cybercriminalité au Maroc* p. 51.

البنيات التحتية ذات الأهمية الحيوية	الأنظمة والتجهيزات الأساسية التي يعتمد عليها المجتمع لضمان استمرارية وظائفه الحيوية كالأمن والصحة.	شبكات الكهرباء أو أنظمة الاتصالات التي تُدير خدمات الطوارئ والمستشفيات.
قطاع الأنشطة ذات الأهمية الحيوية	الأنشطة الجوهرية غير القابلة للاستبدال التي تُساهم في تلبية الاحتياجات الأساسية أو الحفاظ على الأمن الوطني.	توزيع المياه الصالحة للشرب أو إدارة الأنظمة المصرفية التي تُشرف على المعاملات المالية الحيوية.
نظام المعلومات	الموارد المنظمة التي تُستخدم لتجميع المعلومات ومعالجتها ونشرها ضمن بيئة محددة.	نظام إلكتروني يُدير سجلات المرضى في مستشفى، يشمل الأجهزة، البرامج، والبيانات.
نظام معلومات حساس	الأنظمة التي تحتوي على بيانات حساسة قد يتسبب أي خلل فيها بأضرار كبيرة لهيئة أو بنية حيوية.	قاعدة بيانات تحتوي على معلومات عسكرية سرية قد تُعرض الأمن الوطني للخطر إذا تم اختراقها.
خدمة الأمن السيبراني	الخدمات التي تُراقب وتُحلل الحوادث السيبرانية وتُعزز أمن الأنظمة لصالح هيئة أو بنية حيوية.	تقديم خدمة كشف التسلل لنظام بنكي لمنع هجمات القرصنة الإلكترونية.
مقدم الخدمات الرقمية	الجهة التي تُوفر خدمات إلكترونية عبر الإنترنت تشمل التجارة الإلكترونية أو الحوسبة السحابية.	منصة مثل "أمازون" التي تُتيح البيع عبر الإنترنت أو خدمات جوجل السحابية لتخزين البيانات.
الإيواء	خدمة تخزين البيانات بمختلف أشكالها، تُقدمها مزودات الخدمات الرقمية سواء مجانًا أو بعوض.	استضافة موقع إلكتروني على خادم يُديره مزود خدمة مثل *Hostinger*.

إسناد نظام المعلومات لجهة خارجية	تكليف جهة خارجية بإدارة نظام معلومات بشكل جزئي أو كلي وفق عقد يحدد الالتزامات والمدة.	تكليف شركة تكنولوجيا بإدارة نظام تكنولوجيا المعلومات لمؤسسة حكومية لمدة 5 سنوات.
المصادقة على نظم المعلومات	وثيقة تُثبت التزام البنية الحيوية بالتدابير الأمنية مع تحمل المسؤول عنها للمخاطر المتبقية.	شهادة تُثبت أن نظام معلومات لمطار قد خضع لتدابير أمنية مع تحمل المسؤول عن أي مخاطر متبقية.
حادث الأمن السيبراني	واقعة غير متوقعة تُهدد أمن الأنظمة الرقمية وتؤثر على عمل هيئة أو بنية حيوية.	اختراق برمجية خبيثة تُعطل نظام دفع إلكتروني لبنك[36].
أزمة الأمن السيبراني	حالة خطيرة ناتجة عن أحداث سيبرانية تؤثر على الأفراد أو الاقتصاد أو الأمن الوطني.	هجوم سيبراني واسع يُعطل شبكة الاتصالات الوطنية ويُهدد الأمن القومي.
إدارة حوادث الأمن السيبراني	الأنشطة التي تُراقب الحوادث السيبرانية، تُبلغ عنها، وتتخذ تدابير لمعالجتها.	رصد هجوم قرصنة على موقع حكومي، الإبلاغ عنه، وتطبيق إجراءات لإصلاح الثغرة الأمنية.

يُبرز هذا الجدول أهمية المفاهيم التي حددها المشرع المغربي في تعزيز الإطار القانوني للأمن السيبراني، حيث تُسهم في توضيح التحديات الرقمية ودعم استراتيجيات الحماية. وتُشكل هذه المصطلحات أساسًا نظريًا يُعزز فهم البحث للسياق السيبراني[37].

رابعا: مكونات الأمن السيبراني

يعتمد الأمن السيبراني على مكونات أساسية تُشكل الأهداف العامة لضمان حماية الأنظمة الرقمية، وهي تتضمن أربعة عناصر جوهرية تُعتبر أساسية لتحقيق الأمن الرقمي. أولاً، التوافر (*Availability*)، الذي يضمن إمكانية وصول المستخدمين إلى الأنظمة المعلوماتية دون

[36] *Cybersecurity and Cyberwar: What Everyone Needs to Know*, 2014, op. cit. p. 15.
[37] المديرية العامة لأمن نظم المعلومات. *مذكرة تقديمية للقانون 20-05 بشأن الأمن السيبراني*. الرباط: المديرية العامة لأمن نظم المعلومات، 2020.

انقطاع، مما يعني أن البيانات والخدمات يجب أن تكون متاحة عند الحاجة، كما في حالة الخدمات الحكومية الإلكترونية التي تتطلب توافرًا مستمرًا لتلبية احتياجات المواطنين. ثانيًا، السلامة (*Integrity*)، التي تُركز على الحفاظ على دقة البيانات وسلامتها من التلاعب أو التغيير غير المصرح به، كما يحدث عند حماية السجلات المالية من التعديلات الاحتيالية لضمان موثوقيتها. ثالثًا، السرية (*Confidentiality*)، التي تمنع الوصول غير المشروع أو العرضي إلى المعلومات الحساسة، مثل بيانات العملاء في البنوك، حيث يُعد الحفاظ على خصوصية هذه البيانات أمرًا حيويًا لمنع استغلالها. وأخيرًا، الإثبات (*Proof*)، الذي يضمن عدم التنصل من المعاملات مع إمكانية تدقيق النتائج، كما في المعاملات الإلكترونية التي تتطلب سجلات دقيقة لتأكيد صحة العمليات، مما يعزز الشفافية والمساءلة في العمليات الرقمية. تُشكل هذه المكونات الأربعة أساسًا متكاملًا لتحقيق الأمن السيبراني، حيث تتكامل لتوفير حماية شاملة ضد التهديدات الرقمية في ظل الاعتماد المتزايد على البنية التحتية الرقمية[38].

الفقرة الثانية: علاقة الأمن السيبراني بالسيادة الوطنية والأمن القومي

في ظل التحديات الرقمية المتزايدة، يبرز الأمن السيبراني كأداة استراتيجية لحماية السيادة الوطنية، وضمان استقرار الدولة، مما يستوجب تحليل علاقته بالأمن القومي والقرار السيادي للدول.

أولا: السيادة الوطنية في الفضاء السيبراني المغربي

شهد مفهوم السيادة الوطنية تحولات جوهرية مع الثورة الرقمية وعولمة التكنولوجيا، مما أدى لظهور مفهوم السيادة الرقمية الذي يعني ممارسة الدولة لسيادتها على فضائها السيبراني ومعلوماتها الرقمية على غرار سيادتها على أراضيها[39]. وفي السياق المغربي، أدركت الدولة أن تحقيق التحول الرقمي وتنمية الاقتصاد الرقمي لا ينفصل عن تأمين الفضاء السيبراني

[38] Yassine Maleh and Youness Maleh, *Cybersecurity in Morocco*, op. cit. p. 13.
[39] Agouzoul, Mouad, sous la direction d'Ahmed Azirar, et avec la collaboration de Karim Amor et Victor Pauvert. *Souveraineté Numérique: Pourquoi le Maroc ne Peut y Échapper - Recommandations pour un État-Stratège.* Rabat: Institut Marocain d'Intelligence Stratégique, 2024, p. 8.

الوطني وحماية هذه السيادة الرقمية. وقد أكد المسؤولون المغاربة على ضرورة توفير فضاء سيبراني آمن لدعم الانتقال الرقمي وضمان السيادة الرقمية للمملكة[40]. فالأمن السيبراني بات شرطًا أساسيًا للحفاظ على استقلال القرار الوطني في العصر الرقمي، حيث إن التهديدات السيبرانية عابرة للحدود يمكن أن تؤثر على قدرة الدولة في اتخاذ قراراتها سياديًا دون إملاءات أو ضغوط خارجية. إن التهديدات السيبرانية قد تتخذ شكل هجمات تستهدف البنى التحتية المعلوماتية الحيوية أو سرقة معطيات حساسة بغرض الابتزاز أو التأثير في السياسات الوطنية. وفي الحالة المغربية، برزت أمثلة حديثة توضح هذا الترابط بين الأمن السيبراني والسيادة الوطنية. فخلال أبريل 2025، تعرضت مؤسسات سيادية لهجمات إلكترونية كبيرة استهدفت مواقع حكومية وقواعد بيانات وطنية، وقد اعتبرتها الحكومة المغربية محاولة للتشويش على نجاحات البلاد الدبلوماسية في قضيتها الوطنية. وصرّح الناطق الرسمي باسم الحكومة أن توقيت هذه الهجمات تزامن مع تطورات دبلوماسية مهمة تتعلق بقضية الصحراء المغربية، مما يجعلها في نظر المغرب عملاً عدائيًا ذا بُعد سياسي يهدف إلى تقويض المكاسب السيادية للمملكة. يعكس هذا المثال كيف يمكن لهجوم سيبراني موجَّه من أطراف خارجية أن يشكل تدخلًا غير مباشر في الشؤون الداخلية ومحاولة للتأثير على مسار قرارات سيادية أو إضعاف الموقف الوطني على الساحة الدولية. وبالتالي، فإن تحصين المجال الرقمي المغربي ضد هذه التهديدات يظل ضرورة لحماية استقلالية القرار الوطني وضمان عدم ارتهان سيادة الدولة لأي ابتزاز أو اختراق رقمي خارجي[41].

من الجوانب المهمة أيضًا لمسألة السيادة الرقمية قضية التحكم في البيانات الوطنية. فحماية المعطيات الحساسة والبنى التحتية الرقمية داخل حدود الدولة تعدُّ بعدًا أساسيًا للسيادة في العصر الحديث. اتخذ المغرب إجراءات استراتيجية في هذا الصدد، من أبرزها سنّ القانون رقم 05.20 المتعلق بالأمن السيبراني. يهدف هذا القانون إلى حماية نظم المعلومات والبنى التحتية ذات الأهمية الحيوية، ومن جانب آخر منع تخزين البيانات الحساسة خارج التراب

---

[40] Embassy of the Kingdom of Morocco in the United States. Cyber Security Conclave: Cybersecurity, Digital Sovereignty Are Morocco's Core Concerns (Minister). Washington, 2024. Re-accessed on March 8, 2025, at 14:00, at: https://us.diplomatie.ma.

[41] بوابة المغرب. السيد بايتاس يصف الهجمات السيبرانية التي استهدفت مؤسسات وطنية في هذا التوقيت المشبوه بالفعل الإجرامي. الرباط: بوابة المغرب، 2025. تم الاطلاع عليه بتاريخ 11 أبريل 2025، على الساعة 15:00، على الرابط: www.maroc.ma.

الوطني. وقد جاء ذلك استجابة لواقع تصاعد الهجمات السيبرانية (حيث تم تسجيل 577 هجمة على جهات حكومية عام 2021)، مما نبّه السلطات إلى ضرورة "توطين" البيانات وإلزام استضافتها على خوادم داخلية تحقيقًا للسيادة الرقمية[42].

هذا التدبير التشريعي يعكس إدراك المغرب أن الاعتماد المفرط على خدمات خارجية أو بنية تحتية أجنبية قد يعرّض استقلالية القرار التقني والسيادي للخطر، سواء عبر إمكانية انقطاع تلك الخدمات أو تدخل جهات أجنبية في إدارة البيانات الوطنية. وعليه، فإن تعزيز الأمن السيبراني من خلال السيطرة على البيانات والبنية الرقمية محليًا يسهم مباشرة في صون السيادة الوطنية في بعدها الرقمي ويحول دون فرض أمر واقع خارجي على الدولة في فضائها الإلكتروني.

ثانيا: الأمن السيبراني كعنصر مكوّن للأمن القومي المغربي

أضحى الأمن السيبراني اليوم جزءًا لا يتجزأ من مفهوم الأمن القومي للدول، والمغرب ليس استثناءً. فمع تزايد الاعتماد على النظم الرقمية في القطاعات الحيوية (كالاتصالات والطاقة والقطاع المالي والخدمات الحكومية)، أصبحت الهجمات السيبرانية تهديدًا متصاعدًا لاستقرار الدولة الاقتصادي والسياسي والاجتماعي. وقد بات الأمن السيبراني يشكّل أحد الأعمدة الأساسية لحماية الاستقرار الوطني في إفريقيا[43]، الأمر الذي يستلزم تبنّي مقاربات استراتيجية شاملة لحماية الفضاء الرقمي كجزء من منظومة الأمن الشامل. وفي الحالة المغربية، يتبنّى صناع القرار رؤية تعتبر الأمن السيبراني بعدًا استراتيجيًا من أبعاد أمن الدولة، إلى جانب الأبعاد العسكرية والاقتصادية وغيرها. حيث تشير الدراسات إلى أن تحقيق الأمن القومي للمملكة لا يمكن أن يتم بمعزل عن مجابهة التهديدات الأمنية من الجيل الجديد وفي مقدمتها

---

[42] L'Opinion. Avec Abdellatif Loudiyi: "Le Maroc engagé pour une coopération africaine renforcée contre les cybermenaces". Rabat: L'Opinion, 2025. Consulté le 1 avril 2025 à 17:00, à : www.lopinion.ma.

[43] همام، محمود سامح. *الهجمات السيبرانية في إفريقيا.. قراءة في التحديات والاستجابات*. مقال تحليلي. القاهرة: مجلة السياسة الدولية (مؤسسة الأهرام)، 2025.

التهديدات السيبرانية، لما قد ينجم عنها من مخاطر حقيقية قادرة على إحداث اضطراب عميق يمس الاستقرار السياسي والاقتصادي والاجتماعي[44].

على هذا الأساس، يُنظر إلى تعزيز الأمن السيبراني الوطني بوصفه ضرورة حتمية لتحصين البلاد وحماية مكتسباتها التنموية والسيادية من أي إخلال أو تهديد رقمي. تبنّى المغرب خلال العقد الأخير استراتيجية متعددة المستويات لتعزيز أمنه السيبراني كجزء من أمنه القومي. فعلى الصعيد المؤسسي، أُنشئت هيئات متخصصة لمواجهة المخاطر السيبرانية وفي مقدمتها المديرية العامة لأمن نظم المعلومات (*DGSSI*) بوصفها السلطة الوطنية المكلفة بالأمن السيبراني. كما تم إحداث اللجنة الاستراتيجية العليا للأمن السيبراني، إلى جانب المركز الوطني لرصد الهجمات والتصدي لها (ماسيرت – *maCERT*)، بهدف تحصين البنية التحتية الرقمية للدولة وتأمين استمرارية الخدمات الحيوية. وعلى الصعيد القانوني، وكما سلف ذكره، عزز المشرّع المغربي الترسانة التشريعية بإقرار قانون الأمن السيبراني ولوائحه التنظيمية لضمان توفير الأسس القانونية الصارمة لحماية نظم المعلومات الوطنية. تعكس هذه الخطوات اعترافًا رسميًا بأن الدفاع عن الوطن لم يعد مقصورًا على الحدود البرية والبحرية والجوية فحسب، بل يشمل أيضًا حدود الفضاء السيبراني التي لا تقل أهمية. وقد أكدت المديرية العامة لأمن نظم المعلومات أن المغرب ينتهج سياسة استباقية في هذا المجال من خلال تعزيز مناعة الفضاء الرقمي الوطني ورفع مستوى جاهزية الدفاع السيبراني لحماية الوظائف الحيوية للدولة من أي اختراق قد يهدد استمراريتها[45].

إضافة إلى ذلك، تركز الإستراتيجية المغربية على بناء القدرات البشرية والتعاون الدولي في ميدان الأمن السيبراني كجزء من تأمين الأمن القومي. فالعنصر البشري يُعد خط الدفاع الأول، لذلك تم إطلاق برامج تدريبية وتمارين محاكاة منتظمة لرفع الوعي والجاهزية لدى كوادر المؤسسات الوطنية المختلفة. كما يحرص المغرب على تبادل الخبرات والمعلومات مع الدول الشقيقة والصديقة ضمن اتفاقيات تعاون ثنائي وإقليمي، إدراكًا منه للطبيعة العالمية للتهديدات السيبرانية. هذا التعاون الدولي يندرج أيضًا ضمن مقاربة الأمن القومي الشامل، حيث يعزز

---

[44] جارش، عادل. *مقاربة معرفية حول التهديدات الأمنية الجديدة*. مقال في مجلة العلوم السياسية والقانون، العدد الأول. برلين: المركز الديمقراطي العربي، 2017، ص 11.

[45] *Cyber Security Conclave: Cybersecurity, Digital Sovereignty Are Morocco's Core Concerns (Minister).* Washington: Embassy of the Kingdom of Morocco in the United States. op. cit.

موقع المغرب الاستراتيجي إقليميًا ويمكنه من المساهمة في صياغة معايير وضوابط لسلوك الدول في الفضاء الإلكتروني بما يخدم السلم والأمن الدوليين. ومن جهة أخرى، فإن حماية المعطيات الشخصية وضمان خصوصية المواطنين عبر أطر تنظيمية (مثل جهود اللجنة الوطنية لحماية المعطيات الشخصية[46] – *CNDP*) يشكلان بُعدًا مكملًا للأمن السيبراني الوطني، لما لهما من أثر في ترسيخ ثقة المجتمع في الفضاء الرقمي الوطني وتعزيز الشرعية الرقمية للدولة.

لقد كشفت الحوادث السيبرانية الأخيرة أن أي قصور في الأمن الرقمي قد يستغله الخصوم لضرب الثقة في المؤسسات وإرباك المجتمع[47]، مما يرتب آثارًا تمس الأمن القومي بمفهومه الواسع. بالتالي، فإن مقاربة المغرب تعتبر الأمن السيبراني ركيزة أساسية من ركائز أمنه القومي. فهو عنصر وقائي يهدف إلى منع الاختراقات التي قد تقوّض استقرار الدولة، وعنصر يهيئ المناخ الآمن للتحول الرقمي والتنمية المستدامة. وفي المحصلة، يمثل الأمن السيبراني في المغرب خط دفاع سيادي لحماية الدولة ومؤسساتها ومواطنيها في العالم الرقمي، مما يجعله جزءًا لا غنى عنه من معادلة حفظ السيادة الوطنية وصون الأمن القومي في القرن الحادي والعشرين[48].

المطلب الثاني: البنية التحتية الرقمية وأهميتها في بناء الدولة الحديثة

تُعدّ البنية التحتية الرقمية من الركائز الأساسية في بناء الدولة الحديثة، نظرًا لما توفره من إمكانات تكنولوجية متقدمة تُسهم في تحسين أداء المؤسسات وتعزيز نجاعة المرافق العمومية. ومع التحول المتسارع نحو الرقمنة، أصبحت هذه البنية ضرورة استراتيجية لضمان السيادة الرقمية وتحقيق التنمية المستدامة، خاصة في ظل التحديات المرتبطة بالأمن السيبراني وحماية المعطيات. وعليه، سيعالج هذا المطلب الثاني تطور مفهوم البنية التحتية الرقمية وتوسّع استعمالها في مختلف مجالات الدولة الحديثة، وذلك من خلال فقرتين **نخصص الأولى** لتعريف

---

[46] اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي. المهام. صفحة إلكترونية. الرباط، 2025. تم الاطلاع عليه بتاريخ 5 أبريل 2025، على الساعة 22:00، على الرابط: www.cndp.ma.

[47] Tijani, Yasmine. 4 questions pour comprendre la cyberattaque la plus grave de l'histoire du Maroc. Le Point, 2025. Consulté le 6 avril 2025 à 23:30, à : www.lepoint.fr.

[48] Meeuwisse, Raef. *Cybersecurity for Beginners*. 1st ed. Canterbury, Kent: Icutrain Ltd, 2015, p. 22.

البنية الرقمية وتطور استعمالها في السياق المغربي، ونخصص **الثانية** لتحليل دورها المحوري في استقرار المرافق العمومية وتدبير الشأن العام، وتدعيم الفعل السياسي والدبلوماسي.

الفقرة الأولى: تعريف البنية الرقمية وتطور استعمالها

في ظل التحولات العميقة التي يعرفها العالم، أصبحت البنية التحتية الرقمية عنصرًا مركزيًا في تفعيل وظائف الدولة الحديثة، حيث يتجاوز دورها الأبعاد التقنية ليطال مختلف المجالات السيادية. وفي السياق المغربي، يتجلى هذا الدور بوضوح في مساهمتها في تحديث القدرات الدفاعية، دعم الدينامية الاقتصادية، وتوسيع نطاق الخدمات الاجتماعية، فضلًا عن تعزيز الحضور السياسي والدبلوماسي للمملكة على الصعيدين الإقليمي والدولي. كما تشكل هذه البنية رافعة أساسية في تنزيل مشاريع التحول البيئي والطاقي، من خلال دعم الطاقات المتجددة وتعزيز الاستدامة عبر أدوات رقمية ذكية.

أولاً: تعريف البنية الرقمية

مصطلح "البنية التحتية" يُعبر عن مجموعة العناصر والمكونات الأساسية التي تُشكل الإطار الداعم لتشغيل وتنظيم الأنظمة المختلفة على نطاق واسع، سواء كانت هذه الأنظمة مادية أو غير مادية. تاريخيًا، وقد ظهر هذا المصطلح في بدايات القرن العشرين للإشارة إلى المنشآت العسكرية الثابتة التي تُشكل أساس العمليات الحربية، مثل القواعد والمستودعات. ومع مرور الزمن، تطور المفهوم ليشمل شبكات النقل، وأنظمة توزيع المياه، وشبكات الكهرباء، والاتصالات السلكية واللاسلكية، ليصبح اليوم مصطلحًا شاملًا يُغطي كل ما يُشكل العمود الفقري للخدمات الأساسية في المجتمعات الحديثة[49].

أما الرقمنة، فهي عملية تحويل المعلومات أو المواد التقليدية –سواء كانت مطبوعة أو مخزنة بطرق لا يمكن للحواسيب التعامل معها مباشرة– إلى صيغة رقمية تُمكن الحواسيب من قراءتها ومعالجتها. هذه الصيغة الرقمية تتكون من وحدات بيانات منفصلة تُعرف باسم "البايتات " (*Bytes*[50])، والتي يمكن تخزينها على وسائط رقمية متنوعة مثل الأقراص الصلبة، أو

---

[49] Letellier, Anne-Sophie, et Julien Hocine. *Les infrastructures numériques: quels enjeux en contexte canadien? Dans Infrastructures alternatives*. 2021, p. 51.

[50] (البايتات) هو *وحدة أساسية لقياس البيانات* في مجال الحوسبة والتكنولوجيا الرقمية.

الأقراص المدمجة، أو الأقراص الرقمية متعددة الاستخدام، أو حتى إتاحتها عبر الإنترنت للوصول السهل والسريع. وفي سياق أوسع، تشير الرقمنة أيضًا إلى دمج التقنيات الرقمية الحديثة، مثل الإنترنت والذكاء الاصطناعي، في جميع جوانب الحياة اليومية، مما يُسهم في تحسين الكفاءة وتسهيل التواصل. ومع ذلك، يجب التمييز بين الرقمنة ومصطلح "التحول الرقمي"؛ فالرقمنة تُركز على تحويل المعلومات إلى صيغ رقمية، بينما التحول الرقمي هو مفهوم أشمل يشمل تحسين العمليات الرقمية القائمة، وإعادة تصميم الأنظمة باستخدام التكنولوجيا، وتحليل البيانات لاتخاذ قرارات استراتيجية أكثر فعالية[51].

بالتالي، يُمكن تعريف البنية التحتية الرقمية على أنها مجموعة المكونات والتقنيات التي تُشكل الأساس الداعم لتمكين الأنشطة الرقمية في المجتمع[52]. فهي تضم شبكات الاتصالات السلكية واللاسلكية، مثل شبكات الهاتف والإنترنت، وخدمات الأقمار الصناعية التي تُستخدم في الملاحة والبث، بالإضافة إلى الأجهزة المادية (*Hardware*[53]) مثل الخوادم وأجهزة الحوسبة، والبرمجيات (*Software*[54]) التي تُدير هذه الأنظمة، مثل أنظمة التشغيل والتطبيقات. كما تشمل البنية التحتية الرقمية الخدمات التكميلية مثل مراكز البيانات وأنظمة الحوسبة السحابية، إلى جانب العنصر البشري المتمثل في الكوادر المدربة والمؤهلة القادرة على إدارة وتطوير هذه الأنظمة. بمعنى آخر، البنية التحتية الرقمية تُشكل العمود الفقري الذي يدعم العمليات الرقمية مثل التجارة الإلكترونية، الخدمات الحكومية الإلكترونية، وتبادل المعلومات على نطاق عالمي، مما يجعلها ركيزة أساسية للاقتصادات الحديثة والمجتمعات المترابطة[55].

---

[51] يس، نجلاء أحمد. *الرقمنة ودورها في المكتبات العربية*. القاهرة: العربي للنشر والتوزيع، 2012، ص 21.

[52] Lee, Joonho. *Digital infrastructure for the internationalization of small and medium-sized enterprises in the Republic of Korea.* United Nations publication ECLAC, 2021, p.13.

[53] (المعدات أو الأجهزة المادية) يُستخدم في مجال الحوسبة والتكنولوجيا للإشارة إلى *المكونات المادية* للأنظمة الرقمية.

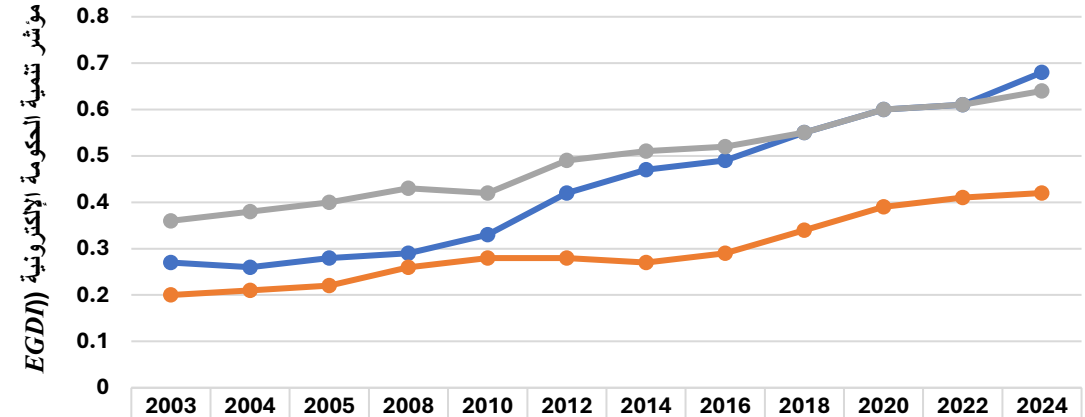
[54] (البرمجيات) يُستخدم في مجال الحوسبة والتكنولوجيا للإشارة إلى *الجزء غير المادي من الأنظمة الرقمية*، أي البرامج والتعليمات التي تُشغل الأجهزة المادية.

[55] صلاح، محمود أحمد عياد، وإبراهيم جابر السيد. *الاقتصاد الرقمي*. القاهرة: دار العلم والإيمان للنشر والتوزيع ودار الجديد للنشر والتوزيع، 2020، ص 9.

ثانيًا: تطور استعمال البنية التحتية الرقمية بالمغرب

لتقييم مدى تطور استعمال البنية التحتية الرقمية بالمغرب، يُعد مؤشر تنمية الحكومة الإلكترونية (*EGDI*[56]) من بين أهم المؤشرات العالمية المعتمدة. ويقيس هذا المؤشر المركب مستوى توفر الخدمات الإدارية عبر الإنترنت، وجودة البنية التحتية الرقمية، ومستوى رأس المال البشري، وهو ما يُمكّن من رصد مدى نجاعة الاستثمار الرقمي في تحسين أداء المؤسسات العمومية. **يوضح المبيان التالي** تطور قيمة هذا المؤشر في المغرب خلال الفترة الممتدة من سنة 2003 إلى 2024[57]، مقارنة بالمعدل الإفريقي والعالمي.

تطور مؤشر تنمية الحكومة الإلكترونية (*EGDI*)
بالمغرب مقارنة بالمعدل الإفريقي والعالمي بين سنتي 2003 و 2024



	2003	2004	2005	2008	2010	2012	2014	2016	2018	2020	2022	2024
المغرب	0.27	0.26	0.28	0.29	0.33	0.42	0.47	0.49	0.55	0.6	0.61	0.68
إفريقيا	0.2	0.21	0.22	0.26	0.28	0.28	0.27	0.29	0.34	0.39	0.41	0.42
العالم	0.36	0.38	0.4	0.43	0.42	0.49	0.51	0.52	0.55	0.6	0.61	0.64

أ – القراءة الكمية لتطور المؤشر

شهد المغرب بين سنتي 2003 و2024 تطورًا ملحوظًا في مؤشر تنمية الحكومة الإلكترونية (*EGDI*)، حيث انتقل من قيمة ضعيفة (0.27) إلى مستوى متقدم (0.68)، متجاوزًا بذلك المتوسط الإفريقي (0.42) ومتقاربًا مع المتوسط العالمي (0.64). هذا الارتفاع السريع لا

---

[56] يُعد مؤشر تنمية الحكومة الإلكترونية (*EGDI*) مؤشرًا مركبًا تصدره الأمم المتحدة كل سنتين لقياس مدى تقدم الدول في تقديم الخدمات العمومية عبر الإنترنت، ويعتمد في تصنيفه على ثلاثة مكونات رئيسية: مستوى الخدمات الإلكترونية، البنية التحتية الرقمية، ورأس المال البشري.

[57] إدارة الشؤون الاقتصادية والاجتماعية بالأمم المتحدة. معلومات عن مؤشر تنمية الحكومة الإلكترونية – المغرب (EGDI)، سنة 2024. تقرير، 2024. تم الاطلاع عليه بتاريخ 12 أبريل 2025، على الساعة 06:15، على الرابط: https://publicadministration.desa.un.org.

يُمكن قراءته فقط كتحسّن إداري، بل يعكس بالأساس توسعًا في استغلال البنية التحتية الرقمية وتزايدًا في الاعتماد المؤسسي على المنصات الإلكترونية في تقديم الخدمات. فالقفزات المسجلة بين سنوات 2012 و2024، خاصة بعد جائحة كوفيد-19، تترجم تحولًا نوعيًا في سياسات الدولة نحو رقمنة الخدمات وتطوير بوابات إلكترونية وطنية متخصصة، مثل المنصات الضريبية، العدلية، والاجتماعية، ما عزز من مؤشر الخدمات عبر الإنترنت، أحد مكونات *EGDI*.[58]

ب – التحليل الكيفي للعوامل المؤثرة

إن تطور *EGDI* لا يرتبط فقط بوجود شبكات أو أجهزة حاسوب، بل هو نتاج تفاعل عدة عوامل بنيوية، منها تقوية شبكات الاتصال وتعميم تغطية الإنترنت، خاصة في المناطق الحضرية وشبه الحضرية، وتحسين كفاءة الخوادم ومراكز البيانات، إضافة إلى الاستثمار في تكوين الكفاءات الرقمية داخل الإدارات. كما أن إدراج المواطن في صلب المنظومة الرقمية، عبر خدمات التصريح الإلكتروني، الأداء عن بُعد، والتسجيل الآلي، يعكس تحول البنية التحتية الرقمية من مجرد وسيلة تقنية إلى أداة لتنظيم العلاقة بين الدولة والمواطن في بعدها السيبراني[59]، مما يفسر ارتفاع المؤشر بشكل واضح مقارنة ببعض الدول الإفريقية التي لا تزال تعاني من ضعف البنية المعلوماتية وقصور الولوج الشامل للخدمات.

ج – العلاقة بين تطور مؤشر *EGDI* والأمن السيبراني

لا يُمكن فهم هذا التطور خارج سياق أوسع يتمثل في الحاجة إلى تأمين هذه البنية التحتية الرقمية المتسعة. فكلما ارتفعت مؤشرات تقديم الخدمات عبر الإنترنت، زادت الحاجة إلى تطوير منظومة الأمن السيبراني لحماية البيانات والمعاملات الرقمية[60]. إن تقدم المغرب في مؤشر *EGDI*، كما يظهر في المبيان، يُعد في حد ذاته مؤشرًا ضمنيًا على تنامي الهجمات المحتملة وارتفاع قيمة الأصول الرقمية، ما يفرض تلازمًا وظيفيًا واستراتيجيًا بين تطوير البنية

---

[58] المديرية العامة للجماعات الترابية. سياق جائحة كورونا: عامل لتسريع الرقمنة بالجماعات الترابية. البوابة الوطنية للجماعات الترابية، بتاريخ 18 يوليوز 2020. تم الاطلاع عليه بتاريخ 3 أبريل 2025، على الساعة 10:55، على الرابط: https://www.collectivites-territoriales.gov.ma.

[59] وزارة الانتقال الرقمي وإصلاح الإدارة، *المغرب الرقمي: الاستراتيجية الوطنية للتحول الرقمي 2030*، المملكة المغربية، 25 شتنبر 2024، تم الاطلاع عليه بتاريخ 13 أبريل 2025، على الساعة 15:33. على الرابط: *www.mmsp.gov.ma*.

[60] Yassine Maleh and Youness Maleh, *Cybersecurity in Morocco*, op. cit. p. 5.

الرقمية وتحصينها. وبالتالي، فإن هذا التحول الكمي والنوعي في *EGDI* يُمهد نظريًا ومؤسساتيًا لما ستتناوله الفصول اللاحقة من هذا البحث، خصوصًا ما يتعلق بتحديات الأمن السيبراني وتطور الترسانة القانونية والمؤسساتية لحماية الفضاء الرقمي الوطني.

الفقرة الثانية: دور البنية الرقمية في استقرار المرافق وتدبير الشأن العام

مع تطور الدولة الحديثة، لم تعد البنية التحتية الرقمية مجرّد أداة تقنية، بل تحولت إلى رافعة استراتيجية متعددة الأبعاد، تؤثر بشكل مباشر على استقرار المؤسسات، نجاعة السياسات العمومية، وتدبير الشأن العام. فقد أصبحت الرقمنة ضرورة حتمية لضمان الأمن المجتمعي، تحفيز التنمية الاقتصادية، وضمان جودة الخدمات العمومية. ومن هذا المنطلق، تسعى الدول، ومن ضمنها المغرب، إلى تعزيز قدراتها الرقمية لتواكب التغيرات المتسارعة التي فرضتها التحديات التكنولوجية، الأمنية، والبيئية.

أ – الدور في تعزيز القدرات الدفاعية

تُشكل البنية التحتية الرقمية ركيزة أساسية لتحديث القدرات الدفاعية للقوات المسلحة الملكية المغربية، حيث تُستخدم لدعم العمليات العسكرية وتعزيز الأمن القومي في مواجهة التهديدات المعاصرة. خلال تمرين *"Arcane Thunder 24"* الذي أُجري في المغرب بالتعاون مع الجيش الأمريكي، تم اختبار تقنيات الحرب الإلكترونية المتقدمة، بما في ذلك الطائرات المسيرة المجهزة بأنظمة جمع المعلومات الاستخباراتية، وأجهزة التشويش التي تُعطل اتصالات العدو وراداراته. تُظهر هذه الأنظمة الاعتماد على شبكات رقمية متطورة لنقل البيانات في الوقت الحقيقي، مما يُتيح اتخاذ قرارات سريعة ودقيقة أثناء العمليات. كما استُخدمت بالونات المراقبة المزودة بتقنيات استشعار إلكترونية لتعزيز الرصد الجوي، مما يُبرز التكامل بين الأنظمة الرقمية والعسكرية لتحسين الوعي الظرفي. يُعد الأمن السيبراني عنصرًا لا غنى عنه لحماية هذه البنية من التهديدات السيبرانية، مثل اختراق الشبكات أو التدخل الإلكتروني، التي قد تُعرقل العمليات العسكرية. يُعزز التعاون مع الولايات المتحدة، من خلال تمارين مثل "**الأسد**

الإفريقي"، قدرات المغرب في تطوير شبكات اتصال مؤمنة وتدريب الكوادر على مواجهة التحديات السيبرانية.[61].

ب – الدور في تعزيز القطاع الاقتصادي

في القطاع الاقتصادي المغربي، البنية التحتية الرقمية تعد ركيزة أساسية حيث تُسهم في تحسين الكفاءة التشغيلية، تعزيز الابتكار، ودعم نمو التجارة الإلكترونية والخدمات الرقمية. تشمل هذه البنية شبكات الاتصال واسع النطاق، مراكز البيانات، والحوسبة السحابية، التي تُمكّن الشركات من إدارة التدفقات المالية والبيانات التجارية بسرعة وأمان. في المغرب، بلغت نسبة انتشار النطاق العريض المتنقل 65% في عام 2019، مما يدعم التجارة الإلكترونية والخدمات المالية الرقمية، لكن انخفاض النطاق العريض الثابت (6.5%) يُحد من الكفاءة في المناطق الريفية. تُعزز البنية التحتية الرقمية الاقتصاد من خلال تمكين الشركات الناشئة الرقمية، مثل *SOWIT* و*Atlan Space*، التي تستفيد من تحليلات البيانات والذكاء الاصطناعي لتقديم خدمات زراعية ومراقبة مبتكرة. كما تدعم برامج مثل "صندوق الابتكار" و"تكنوبارك" ريادة الأعمال الرقمية، مما يُعزز الاستثمار في القطاع الخاص[62].

رغم تركيز البنية الرقمية الرسمية على السياسية والدبلوماسية، إلا أن الحكومة اعتمدت أيضًا حملات رقمية رسمية لتعزيز موقع المغرب الاقتصادي عالميًا، ومنها حملة "*Morocco Now*" للترويج للاستثمار والصادرات. فهذه العلامة التجارية (*Brand*) أطلقتها الوكالة المغربية لتنمية الاستثمارات والصادرات (*AMDIE*) بدعم حكومي، هدفها تقديم المغرب كوجهة جاذبة للاستثمار والأعمال. في إطار هذه الحملة، نظمت وقائع دولية تجسّد الربط بين الرقمنة والترويج الاقتصادي: فعلى سبيل المثال، أقيم حدث ترويجي في لندن (مارس 2022) بإشراف وزاري وعسكري مغربي، وذلك "لتقديم وتسويق العلامة المغربية الخاصة بالاستثمار والتصدير"". وقد شمل أول أيام الحدث عقد ندوة حول أهداف العلامة، أُكد فيها أن منصة "*Morocco Now*" تهدف إلى إبراز مكتسبات وإمكانات المملكة في القطاعات الرائدة

[61] Breaking Defense. Drones, jammers and big balloons: In Morocco, Army's Multi-Domain Task Force tests EW tech. 2024. Accessed on April 15, 2025, at 18:00, at: www.breakingdefense.com.

[62] Zaki B. Khoury, Adele Barzelay *Data Governance Practices in MENA: Case Study - Opportunities and Challenges in Morocco.* World Bank, (2020). pp. 18–19, 36–37, 43–44.

(كالتكنولوجيا) وترويج فرصها الاستثمارية عالمياً. كما امتدت فعاليات الحملة إلى الخارج، فمثلاً أقامت *AMDIE* ندوة في ميونيخ بألمانيا (أبريل 2024) ضمن "الحملة الترويجية الاقتصادية للمغرب بألمانيا" تحت إشراف السلطة التنفيذية المغربية. وعُرض في هذا الحدث التقدم الذي أحرزه المغرب والمزايا التنافسية لديه بهدف تشجيع الاستثمارات الأجنبية وتحفيز الصادرات. وبعبارة أخرى، تم استخدام أدوات رقمية ودبلوماسية تسويقية (موقع الحملة، مادة إعلامية باللغة الإنجليزية، لقاءات مباشرة مع مستثمرين أجانب) للترويج للعرض المغربي الاقتصادي. وقد ساهم ذلك في ربط صور المغرب الاقتصادية بالمنصات الرقمية، وجعل *"Morocco Now"* وسيلة لنشر المواقف والسياسات الاقتصادية للمغرب[63].

ج – الدور في تعزيز الخدمات الاجتماعية

ساهمت البنية التحتية الرقمية في المغرب في تمكين الخدمات الاجتماعية الأساسية (التعليم، الصحة، والإدارة الاجتماعية)، وتقليص الفوارق المجالية خاصة بعد جائحة كوفيد-19. ففي التعليم، أطلقت وزارة التربية الوطنية منصة «تلميذ تيس» لتقديم دروس دعم وتمارين تفاعلية لجميع المستويات الدراسية بشكل مجاني، حيث تعزز هذه المبادرة مبدأ تكافؤ الفرص بين التلاميذ (ويمكن الولوج إلى المنصة من المؤسسات التعليمية أو من المنازل دون مقابل)[64] .وفي الإدارة، أُنشِئ موقع «إدارتي» الموحد لتوفير معلومات مفصلة حول المساطر والإجراءات الإدارية، مما يبسط إجراءات الحصول على الوثائق ويخفض العبء البيروقراطي على المواطن[65].

كما شهد القطاع الصحي نقلة رقمية بارزة؛ فقد أُطلِقت منصات تطبيقية مثل «وقايتنا» لمواكبة أزمة كورونا، وتتولى الحكومة تطوير نظام معلومات صحي وطني متكامل يتيح للمواطنين

---

[63] Moroccan Investment and Export Agency. الموقع الرسمي لحملة Morocco Now. تم الاطلاع عليه بتاريخ 21 أبريل 2025، على الساعة 10:25، على الرابط: www.morocconow.com.

[64] وزارة التربية الوطنية والتعليم الأولي والرياضة، *بلاغ صحفي بشأن إطلاق الدعم التربوي الرقمي "عن بُعد" عبر منصة TelmidTICE*، صادر بتاريخ 22 نونبر 2023.

[65] وزارة الاقتصاد والمالية وإصلاح الإدارة – قطاع إصلاح الإدارة، *بلاغ صحفي حول إطلاق البوابة الوطنية للمساطر والإجراءات الإدارية "إدارتي"*، صادر بتاريخ 21 أبريل 2021.

الولوج المتكافئ إلى السجلات والخدمات الصحية عبر الإنترنت. وعززت هذه التقنيات الرقمية مرونة النظام الصحي المغربي في الاستجابة للتحديات الصحية[66].

على صعيد الحماية الاجتماعية، يمثّل «السجل الاجتماعي الموحد» قاعدة بيانات رقمية مركزية، توفر هوية رقمية موحدة للفئات الهشة وتضمن كفاءة توجيه الدعم الاجتماعي، مع استهداف أوسع للمناطق الريفية والنائية بفضل تقديم الطلبات إلكترونيًا وتخفيف الإجراءات الورقية[67].

وقد ربطت الاستراتيجية الوطنية للتحول الرقمي (ضمن رؤى النموذج التنموي الجديد) تحقيق التنمية الاقتصادية بمتطلبات العدالة الاجتماعية، فحددت عام 2030 كأفق زمني لتحقيق رقمنة كاملة للمعاملات الإدارية واعتماد الواجهات الموحدة للخدمات الحكومية[68].

د – تعزيز الفعل السياسي والدبلوماسي للمملكة

مع تنامي أهمية وسائل الاتصال الرقمي وانفتاحها على الجمهور العالمي، اعتمد المغرب بشكل متزايد على بواباته ومنصاته الإلكترونية الحكومية كأدوات رسمية للدبلوماسية العامة والتواصل الاستراتيجي. فهذه المنصات لا تكتفي بنشر الأخبار، بل تتوجه إلى الرأي العام الداخلي والخارجي لتعزيز قضايا وطنية، وترويج مواقف المملكة السياسية والاقتصادية في المحافل الدولية.

ويسلط البحث التالي الضوء على أبرز هذه المنصات – بوابة الصحراء المغربية، موقع وزارة الخارجية، وموقع البوابة الوطنية (*maroc.ma*) – وكيف تم توظيفها في البنية الرقمية للدولة لخدمة قضية الصحراء المغربية وغيرها من القضايا الإستراتيجية، مع إبراز الترابط بين الرقمنة والسياسة الخارجية للمغرب.

ُطلِقت «بوابة الصحراء المغربية» كمشروع رسمي يندرج ضمن استراتيجية التحول الرقمي طويلة المدى في المغرب (حتى 2030). وقد جاء إطلاقها بالشراكة بين وزارة الاتصال و

---

[66] Tchounyabe, Ruben. *Morocco projects national e-health integrated system*. We Are Tech Africa, April 13, 2022. Accessed: April 18, 2025). Available at: *www.wearetech.africa.*

[67] البنك الدولي. *البنك الدولي يعطي الضوء الأخضر لأنظمة الحماية الاجتماعية المبتكرة في المغرب بقيمة 70 مليون دولار.* 4 دجنبر 2024. تم الاطلاع عليه بتاريخ 24 أبريل 2025. متاح على الرابط : *www.albankaldawli.org.*

[68] *التقرير العام للنموذج التنموي الجديد*، اللجنة الخاصة بالنموذج التنموي، الرباط، 2021، ص 135.

الهيئة الوطنية للشباب والديمقراطية بهدف التوعية بقضية الصحراء المغربية وتعزيز الرؤية الملكية حولها عبر الفضاء الرقمي. تُقدم البوابة – وهي منصة متعددة الوسائط متوفرة بعدة لغات – مادة غنية عن الأقاليم الجنوبية: واقعها التاريخي والجغرافي وثقافتها، إضافة إلى إنجازات البرامج التنموية فيها على مدى أربعين عامًا[69].

وتؤكد الجهات الحكومية المغربية، وعلى رأسها وزارة الاتصال والهيئة الوطنية للشباب والديمقراطية أن الهدف هو "التعريف بقضية الصحراء المغربية عن طريق المعطيات والمنجزات التي تتحقق على أرض الواقع، وتعزيز أدوات الدفاع عن الوحدة الوطنية ومواجهة الخطابات ودحض الأطروحات المعادية". وبذلك تشكّل بوابة الصحراء وجهة موثوقة للمعلومة: فهي تجمع بين مواد تاريخية وجغرافية وأكاديمية، وتقارير إخبارية ودراسات قانونية وسياسية واقتصادية تُعرض بشكل موضوعي وكامل. تُستهدف بها الجماهير المحلية والدولية، بمن فيهم الإعلاميون والباحثون والدبلوماسيون؛ لتصبح "مصدرًا موثوقًا لقضية الصحراء المغربية، وإطارًا مرجعيًا لتيسير الاطلاع على مختلف مناحي وجوانب ملف الصحراء بشكل موضوعي وصادق". وهكذا، يُوظّف المغرب هذه المنصة الرقمية لتعزيز روايته حول الصحراء ونقلها إلى المجتمع الدولي، مستفيدًا من انتشار الإنترنت ووسائل التواصل كجزء من قوته الناعمة[70].

الموقع الرسمي لوزارة الشؤون الخارجية (*diplomatie.ma*) له دورًا مركزيًا في نقل المواقف الدبلوماسية للمغرب. فبالإضافة إلى نشر بيانات رسمية وبلاغات صحفية تتعلق بسياسة المملكة في المحافل الدولية، يُعد الموقع نافذةَ الحكومة أمام العالم، متوفرة بعدة لغات ويزوره الجمهور والمهتمون بتطورات العلاقات الخارجية. وقد عملت الوزارة خلال أزمة جائحة كورونا على تعزيز اتصالاتها الرقمية، فاعتمدت على تحديث موقعها الإلكتروني واستمرارية التواصل النشط عبره وبشبكات التواصل الاجتماعي. كما خصصت محتوى رقميًّا متعدد اللغات – العربية والإنجليزية والفرنسية، وأُضيفت الإسبانية حديثًا – لتغطية المواضيع الدبلوماسية

---

[69] وليد خلف الله، *"أثر الدبلوماسية الرقمية في تحسين صورة الدول"*، مجلة علاقات لصناعة العلاقات العامة – بيروت، العدد 15، ماي 2016، ص.33.

[70] وزارة الأوقاف والشؤون الإسلامية. بطاقة حول بوابة الصحراء المغربية. تم الاطلاع عليه بتاريخ 20 أبريل 2025، على الساعة 02:45، على الرابط: www.habous.gov.ma.

المختلفة. واستخدمت الوزارة هذه المنصات الرقمية في بث رسائلها الرسمية، كما وظفت فيسبوك وإنستجرام ويوتيوب للتفاعل مع المواطنين والجالية الدولية[71].

من خلال ذلك، تعزز وزارة الخارجية قدرات المغرب على بث رسائله الدبلوماسية إلى العالم؛ ففيها تنعكس مواقف الرباط حول القضايا الساخنة (كملف الصحراء، والتعاون الإفريقي، والتنسيق الإقليمي) بنص واضح معتمد رسميًا. كما تستضيف صفحات الموقع ملفات سياسية خاصة (مثل ملف الصحراء)، وتتيح الاطلاع على الخطب والمداخلات الرسمية، مما يضمن شفافية أكبر ونقلًا دقيقًا لوجهة نظر المغرب. وبهذه الطريقة، تشكل المنصة الرسمية للوزارة جزءًا أساسيًا من «**الدبلوماسية الرقمية**[72]» للمغرب، إذ تسمح بالتواصل الدائم مع الجماهير الخارجية وحشد الدعم الدولي للسياسات المغربية (سواء بالتنسيق الرسمي أو التفاعل العام عبر الشبكات الاجتماعية).

الموقع الرسمي للبوابة الوطنية المغربية *(maroc.ma)* يتولى الموقع دور المركز الإعلامي الرئيسي، حيث يجمع الأخبار والمستجدات الرسمية وتوجهات السياسات العمومية. فهو مصدر مركزي للنشرات الحكومية، المواثيق الدستورية، ومعلومات حول مؤسسات الدولة. كما يوفر البوابة العامة للخدمات الرقمية، وينظم المحتوى بحسب فئات (المستثمرون، السياح، المغاربة بالخارج، إلخ). يلاحظ أن المغرب استخدم هذا الموقع كمنصة تربط بين مختلف مبادراته الرقمية: فعلى سبيل المثال، تضم صفحة «ملف الصحراء المغربية» في الموقع رابطًا مباشرًا إلى بوابة الصحراء، مما يؤكد تكامل المنصات الرقمية الرسمية. وعليه، يعمل الموقع الحكومي الرسمي كواجهة موحدة تعزّز تماسك البنية الرقمية الوطنية: فهو يجمع بين المحتوى الثقافي، والسياسي، والاقتصادي، ويبرز أهمية الملفات الوطنية (كالصحراء المغربية) من خلال ربطها بالموارد الرقمية المتخصصة. في خلاصة هذه المنصات، نجد أن البوابة الوطنية تترجم التوجه العام للرقمنة في المغرب بإعلام المواطنين ودعم دبلوماسية الحكومة عبر الإنترنت. فهي تنشر بيانات المؤتمر الوطني للوزراء، وتبلغ بإنجازات المشاريع الكبرى، وتحرص على أن يصل خطاب الدولة المنظم إلى جمهور واسع. وعبر تقنيات مثل تطبيقات الهاتف والتوافر

---

[71] وساك، إسماعيل، "*الدبلوماسية المغربية في زمن فيروس كورونا* "، مجلة المنارة للدراسات القانونية والإدارية، دار المنظومة، أكتوبر 2020.

[72] Bridget Verrekia, "*Digital Diplomacy and its Effect on International Relations*," SIT Digital Collections, Spring 2017, p. 11.

اللغوي المتعدد، يعزز هذا الموقع من حضور المغرب الدبلوماسي والاقتصادي على الساحتين الإقليمية والدولية[73].

الترابط بين الرقمنة والسياسة الخارجية من خلال الأمثلة السابقة، يتضح أن المغرب يدمج التقنيات الرقمية بشكل متعمد في أدواته الدبلوماسية والعامة. فالمنصات التي تملكها الدولة (بوابة الصحراء، والمواقع الحكومية والرسمية) تعمل على بث الرسائل الوطنية بأقوى صورة ممكنة، مستغلة الوصول الواسع للشبكات الاجتماعية والأدوات الإلكترونية. وتعكس هذه المنصات رؤية المغرب في ما يسمى بالدبلوماسية الرقمية: فبدلاً من الاكتفاء بالقنوات التقليدية (التصريحات الصحفية والمذكرات)، يستفيد المغرب من الويب في تعزيز روايته حول الصحراء وحول التنمية الاقتصادية، مما يوسع دائرة التأثير إلى جماهير الداخل والخارج. كما أنها تظهر توافقًا مع مفهوم **«القوة الناعمة[74]»**، إذ تُوظف المعلومات والحقائق والأرقام عبر وسائل رقمية لجذب التعاطف الدولي والدفاع عن مصالح المغرب. ويؤكد ذلك ما أكدته دراسات مغربية بأن المغرب خاض معركة دبلوماسية رقمية حول الصحراء واستثمر في تدريب الشباب على الترافع الرقمي عن الوحدة الترابية.

ويتضح أن الرقمنة لا تحل محل الدبلوماسية التقليدية، بل تمدّها بأدوات حديثة: مواقع إلكترونية منظمة متعددة اللغات تسهل الشفافية، ووسائط تواصل اجتماعي قادرة على حشد الرأي العام[75]، فضلًا عن مواد إخبارية مصممة خصيصًا لشرح وجهة نظر المغرب. أكسبت هذه البنية التحتية الرقمية الرسمية الدولة المغربية مرونة وقدرة أكبر على التأثير في الساحة الدولية، فقد أصبحت المنصات الحكومية جزءًا من قواعد اللعبة الدبلوماسية والإعلامية.

ومع ذلك، فإن تعقيد الروابط الرقمية يرفع من أهمية حماية هذه المنصات من التهديدات السيبرانية. فكلما تعاظمت قيمة المواقع الرسمية في بث الرسائل الوطنية، كان لزامًا أن تشكل

---

[73] البوابة الوطنية للمملكة المغربية. تم الاطلاع عليه بتاريخ 20 أبريل 2025، على الساعة 15:00، على الرابط: www.maroc.ma.

[74] ساعد، طيابية، *"مستقبل الممارسة الدبلوماسية في ظل العصر الرقمي"*، أطروحة دكتوراه في تخصص الدبلوماسية، جامعة الجزائر 3، كلية العلوم السياسية والعلاقات الدولية، السنة الجامعية 2018/2017.

[75] العربي، العربي، *"الدبلوماسية الرقمية وتأثيراتها في العلاقات الدولية"*، لباب للدراسات الاستراتيجية والإعلامية، العدد 10، 2021، ص. 147.

الحصانة السيبرانية مدخلاً ضرورياً لضمان أمن المعلومات واستمرارية التواصل الرقمي[76]. ومن ثمّ سيشكل تعزيز الأمن السيبراني على المستوى الوطني مدخلًا رئيسيًا في المراحل التالية من هذه الدراسة، حفاظًا على مصداقية البنية الرقمية الحساسة التي تدعم أجندة المغرب السياسية والدبلوماسية.

هـ – الدور في دعم التحول البيئي والطاقي

تشكل التقنيات الرقمية (مراكز البيانات، شبكات الاستشعار، الأنظمة الذكية وإنترنت الأشياء، والذكاء الاصطناعي) ركيزة أساسية في تعزيز تكامل مصادر الطاقة المتجددة وإدارة الموارد بكفاءة. فقد أشارت الوكالة الدولية للطاقة المتجددة (*IRENA*) إلى أن الرقمنة تحوِّل البيانات إلى قيمة حقيقية في الأنظمة الطاقية، مما يؤدي إلى قطاع طاقي أكثر استدامةً وأقل تكلفة. وتساهم المنصات الرقمية في تعظيم إنتاجية الموارد المتجددة عبر المراقبة اللحظية وتحليل البيانات الضخمة لأحوال الطقس والإنتاج؛ فتدعم اتخاذ قرارات تشغيلية فورية تؤدي إلى سرعة استجابة أفضل للشبكة واضطراب أقل، فضلاً عن تفعيل أنماط عمل ذكية تعتمد على إنترنت الأشياء والذكاء الاصطناعي[77].

كما يوضح تحليل لمشروع تحول الطاقة في المغرب أن تفعيل الشبكة الذكية (*Smart Grid*) يمكن أن يجعل الطاقة أكثر نظافة وكفاءة، ويحافظ على جودة الهواء بتكييف الإنتاج مع الطلب والحدّ من الهدر (مثلاً عبر تمكين توليد طاقة "خضراء" موزعة لدى المستهلكين)[78].

- **دعم مشاريع الطاقة المتجددة:** تستفيد محطات الطاقة الشمسية والريحية الكبرى في المغرب من بنية تحتية رقمية متطورة. فتحتوي محطة «نوّر ورزازات» للطاقة الشمسية المركزة، على سبيل المثال، على نظام تحكم ومراقبة مركزي (*SCADA*) وشبكة حساسات توجه سطح المرايا وتدير تدفق الملح المصهور لتخزين الطاقة، مما يضمن استمرارية

---

[76] المديرية العامة لأمن نظم المعلومات. النسخة السادسة لندوة الأمن السيبراني: Cyber résilience - Nouvelle approche pour relever le défi du cyber risque. منشور على الموقع الرسمي للمديرية، انعقدت بتاريخ 30 أكتوبر 2018. تم الاطلاع عليه بتاريخ 14 أبريل 2025، على الساعة 04:00، على الرابط: www.dgssi.gov.ma.

[77] International Renewable Energy Agency (IRENA). *Digitalisation and the energy transition*, published in 2023. Accessed on 15 April 2025, at 03:47. Available at: *www.irena.org*.

[78] Sana Sahbani, Hassane Mahmoudi, Abdennebi Hasnaoui, Mustapha Kchikach, *"Development Prospect of Smart Grid in Morocco"*, Procedia Computer Science, vol. 83, 2016, pp. 1314.

الإنتاج ليلاً وغيومًا. وبالمثل، تعتمد مزارع الرياح الكبرى (مثل تازة وزاكورة) على حساسات إنترنت الأشياء للتنبؤ بالرياح وضبط زوايا التوربينات أو إيقافها عند الضرورة حفاظًا على السلامة. تعزز هذه التقنيات الرقمية تكامل المتغيرات الحقلية في الوقت الحقيقي مع عملية توليد الطاقة، فتساعد على تحسين استقرار الشبكة وكفاءة الإنتاج الكلي للطاقات المتجددة[79].

أمثلة تطبيقية:

- ✓ محطة نوّر للطاقة الشمسية في ورزازات توظِّف أنظمة تحكم ذكية لمتابعة إنتاج الطاقة الشمسية الشاملة والتحكم في وحدات التخزين الحراري.
- ✓ مزارع الرياح المغربية تستخدم حساسات رقميّة لأداء تحليل بيانات سرعة واتجاه الرياح، ما يساهم في إدارة آلية لتوجيه شفرات التوربين بكفاءة.
- ✓ يجري المكتب الوطني للكهرباء والماء (*ONEE*) تجارب على شبكات ذكية في مرحلة التوزيع: اختبارات نظم سيطرة ومراقبة (*SCADA, DMS*) وتركيب عدادات ذكية في عدة مدن مغربية.

- **الرقمنة وكفاءة استهلاك الطاقة:** تتيح الأنظمة الرقمية تتبع استهلاك الطاقة والتحكم فيه على المستويين الحضري والصناعي. فقد شرع المغرب في تركيب «عدادات ذكية» تمكن المستهلك من رؤية استهلاكه لحظيًا، وتتيح للموزع التحكم في الأحمال عن بُعد للمحافظة على اتزان الشبكة. على سبيل المثال، أفاد تقرير أن *ONEE* قام بتركيب نحو 230 عدادًا ذكيًا مسبق الدفع في الدار البيضاء اعتبارًا من 2014، ضمن جهود لأتمتة التوزيع الكهربائي وإدخال البنية التحتية للقياس المتقدم (*Advanced Metering Infrastructure*) للتحكم في استجابة الطلب. ويعمل هذا النمط الرقمي على تحسين جدولة الأحمال وتشجيع المستهلكين على ترشيد الطاقة عبر تسعير ديناميكي أو معلومات آنية عن الاستهلاك[80]. ويسهم إدخال نظم إنترنت الأشياء (*IoT*) ومراقبة المباني الذكية

[79] Op. cit., S. Sahbani, H. Mahmoudi, A. Hasnaoui, M. Kchikach, *Development Prospect of Smart Grid in Morocco*, p. 1317 - 1320.
[80] *Development Prospect of Smart Grid in Morocco*, Op. cit. p. 1318 – 1320.

في القطاعات الصناعية والمدن في تقليل الهدر الطاقي وخفض الانبعاثات، وفق توصيات *IEA* التي تربط بين الرقمنة وتعزيز كفاءة استخدام الطاقة[81].

- **البنية الرقمية وإدارة الموارد البيئية:** التكنولوجيا الرقمية لها دورًا متزايدًا في رصد وإدارة البيئة والمياه والزراعة. فمثلاً يعمل المغرب على تطوير شبكات ذكية لمراقبة نوعية الهواء والتلوث بتثبيت حساسات رقمية في المدن الكبرى، ما يتيح جمع بيانات فورية عن جودة الهواء. وعبر منصات إنترنت الأشياء، يمكن للسلطات والزراعة الذكية استخدام معلومات المناخ والتربة لتوجيه ري المحاصيل بدقة عالية، مخفضة استعمال المياه. وأفادت مصادر إعلامية أن تقنيات الري الذكي المستندة إلى الطاقة الشمسية (كما نفذتها شركة ناشئة محلية) ساعدت مزارعي منطقة مكناس على تحسين حصادهم وترشيد استعمال المياه عبر نظام يستند إلى حساسات ورقابة مركزية[82]. كما تركز برامج دولية ومحلية حالية على بناء «أنظمة معلومات مائية» رقمية شاملة لمتابعة التدفقات والأراضي المروية وإدارة السدود. فقد ذكر البنك الدولي أن برنامجه لدعم الأمن المائي في المغرب يشمل تطوير «أنظمة معلومات بيانات المياه» لتعزيز الحكامة وكفاءة استخدام الموارد المائية[83].

إنّ البنية التحتية الرقمية تشكل عصبًا حيويًا لدعم الاستدامة البيئية والتحول الطاقي في المغرب. فقد ثبت أنّ دمج الحوسبة والبيانات الضخمة مع المشاريع الخضراء يعزّز كفاءة استغلال الموارد المتجددة وينشر حلول ذكية لتوفير الطاقة والمياه. ومن جهة أخرى، يتطلب هذا التحول الرقمي الحرص على مواجهة المخاطر الأمنية وحماية البيانات لضمان أقصى استفادة منه دون مخاطر إضافية. بفضل السياسات الحكومية الداعمة وتعاون المؤسسات المختصة، يمكن للمغرب أن يستمر في تطوير بنيته الرقمية البيئية والطاقية ليحتل موقع الصدارة في مجال الطاقة المستدامة على المستوى الإقليمي.

المبحث الثاني: المنظومة القانونية والمؤسساتية للأمن السيبراني في المغرب

---

[81] International Energy Agency (IEA). Power Systems in Transition – Cyber Resilience. Published in 2021. Accessed on 5 April 2025, at 04:15, at: www.iea.org.

[82] Saoudi, Oussama, *Morocco adopts smart irrigation amid drought challenges*. Published on 23 July 2024. Accessed on 10 April 2025, at 16:20. Available at: *https://en.hespress.com.*

[83] World Bank. *New World Bank Program in Morocco Supports Efforts to Boost Water Security and Resilience for All*. Published on July 24, 2023. Accessed on 20 April 2025, at 22:25. Available at*: www.worldbank.org.*

يشكّل الأمن السيبراني اليوم أحد أهم ركائز السيادة الوطنية في العصر الرقمي، مما فرض على الدول وضع منظومة قانونية ومؤسساتية متكاملة لمواجهة التهديدات المتزايدة التي تستهدف فضاءاتها المعلوماتية. وفي هذا السياق، انخرط المغرب في بناء إطار تشريعي وتنظيمي قوي، مدعوم بمؤسسات متخصصة، تضمن الاستجابة الفعالة للهجمات السيبرانية، وتعزز ثقة المواطنين والفاعلين الاقتصاديين في البيئة الرقمية. وعليه، يقف هذا المبحث عند مكونات المنظومة القانونية والمؤسساتية للأمن السيبراني بالمغرب، من خلال مطلبين أساسيين: يتناول **الأول** الإطار التشريعي والتنظيمي، فيما يعالج **الثاني** هندسة المؤسسات الوطنية المعنية وتداخل اختصاصاتها.

المطلب الأول: الإطار التشريعي والتنظيمي للأمن السيبراني المغربي

في ظل تصاعد التهديدات السيبرانية وتنامي الاعتماد على البنية الرقمية في مختلف مناحي الحياة، أضحى تأمين الفضاء السيبراني ضرورة وطنية تُحتّم وضع إطار قانوني ومؤسساتي متكامل. وقد عمل المغرب، في هذا السياق، على بلورة منظومة تشريعية وتنظيمية تسعى إلى حماية نظم المعلومات وتعزيز الأمن السيبراني كجزء لا يتجزأ من الأمن القومي. ينصرف هذا المطلب الأول إلى دراسة البنية التشريعية والتنظيمية التي أرساها المغرب لتأطير الأمن السيبراني وحماية الفضاء الرقمي الوطني، من خلال فقرتين رئيستين: تتناول الفقرة الأولى عرض وتحليل القوانين الوطنية ذات الصلة بهذا المجال، بينما تقف الفقرة الثانية عند تقييم مدى نجاعة الترسانة القانونية في مواجهة التهديدات السيبرانية المستجدة.

الفقرة الاولى: عرض وتحليل القوانين الوطنية ذات الصلة

تُشكّل القوانين الوطنية الإطار الأساسي الذي يُنظّم الأمن السيبراني بالمغرب، ويؤطر حماية الفضاء الرقمي من خلال مقتضيات دستورية وتشريعية وتنظيمية متكاملة، تُجسّد رؤية الدولة في مواجهة التهديدات الرقمية وضمان السيادة المعلوماتية.

أولا: الإطار الدستوري:

إن الدستور المغربي لسنة 2011، بما يحمله من منظومة متكاملة من المبادئ والقيم المؤطرة للحياة العامة، لا يقتصر على تنظيم السلطات وضمان الحقوق والحريات فحسب، بل يؤسس،

في عمقه، لنمط من الحماية الشاملة يمتد ليغطي أيضا الفضاءات المستجدة، وفي طليعتها الفضاء السيبراني.

من خلال تصدير الدستور المغربي لسنة 2011، الذي يشكل جزءًا لا يتجزأ من بنية الدستور، تعهدت المملكة بضمان الأمن في معناه الواسع، القائم على صون الحرية والكرامة والمساواة وتكافؤ الفرص[84]. وهي التزامات لا تنفصل، في ظل التحولات الرقمية الراهنة، عن ضرورة حماية المجال السيبراني الذي أضحى امتدادا عضويا للمجال العام التقليدي.

وإذ نص الفصل 24 على ضمان حماية الحياة الخاصة وصيانة سرية الاتصالات وعدم انتهاكها إلا بأمر قضائي[85]، فإنه بذلك يضع لبنة دستورية أصيلة تُحتِّم تأمين الفضاء المعلوماتي ضد كل تهديد أو خرق يمس بالحق في الخصوصية، وهو ما يعد جوهر الأمن السيبراني.

أما الفصل 27، بإقراره الحق في الحصول على المعلومات، فقد قيد هذا الحق بضرورة حماية الدفاع الوطني والأمن الداخلي والخارجي للدولة والحياة الخاصة للأفراد[86]. مما يكشف عن وعي دستوري مبكر بإكراهات العصر الرقمي، ويؤسس لشرعية تنظيم تدفق المعلومات وتأمينها في مواجهة التهديدات السيبرانية.

وتمتد مرتكزات الحماية إلى الفصل 31، الذي ألزم الدولة بتيسير استفادة المواطنين من حق العلاج والتعليم والبيئة السليمة[87]، وهي مجالات لا يمكن ضمانها اليوم دون منظومات معلوماتية مؤمنة ضد مخاطر الاختراق والتعطيل.

أما فصول الحكامة الجيدة، وعلى رأسها الفصلان 154 و156، فقد أرست مبدأ الشفافية والمساءلة في تدبير المرافق العمومية[88]، بما يفترض وجود نظم معلومات آمنة وموثوقة، قادرة على ضمان الخدمة العمومية وحماية المعطيات المرتبطة بها.

---

[84] *توطئة* الدستور المغربي لسنة 2011.
[85] (*الفقرة الاولى والثالثة*) الفصل 24 من دستور المملكة المغربية.
[86] *الفصل 27* من دستور المملكة المغربية.
[87] *الفصل 31* من دستور المملكة المغربية.
[88] *الفصلان 154 و156* من دستور المملكة المغربية لسنة 2011.

وتزداد أهمية هذه الحماية الدستورية بالنظر إلى الفصل 42، الذي يكرس الدور السامي لجلالة الملك باعتباره الضامن لحرمة الدستور وللاختيار الديمقراطي ولسير المؤسسات الدستورية[89]، بما يشمل ضمنيا، في ظل تحولات الدولة الرقمية، ضمان أمن الفضاء السيبراني باعتباره ركيزة من ركائز استقرار الدولة الحديثة.

وهكذا، يتضح أن الدستور المغربي، وإن لم يتناول الأمن السيبراني كمفهوم مستقل، قد بسط من خلال شبكته القيمية والحقوقية الأساس المتين الذي ستنبثق منه لاحقا التشريعات المنظمة للفضاء السيبراني، وعلى رأسها القانون رقم 05.20. "**فالدستور، بما هو المرجعية الأسمى**"[90]، لا يكتفي بتقنين الحياة الواقعية، بل يضفي حماية مبدئية على الامتدادات الرقمية الحديثة، مؤسسا بذلك لنموذج متقدم للأمن السيبراني، مرتبط عضويا بمرتكزات الدولة الديمقراطية الحديثة.

ثانيا: نصوص تشريعية وتنظيمية:

تكمّل النصوص التشريعية والتنظيمية المنظومة القانونية للأمن السيبراني من خلال قوانين ومراسيم تطبيقية تؤطر الجوانب التقنية والمؤسساتية لحماية الفضاء الرقمي.

أ – القانون رقم 05.20 المتعلق بالأمن السيبراني:

القانون رقم 05.20 المتعلق بالأمن السيبراني يشكل القانون رقم 05.20 المتعلق بالأمن السيبراني قفزة نوعية في مسار بناء منظومة وطنية للتحصين الرقمي، من خلال إرسائه لمجموعة من القواعد الإلزامية التي تطال كافة الفاعلين المؤسسيين والاقتصاديين ذوي الصلة بتدبير المعطيات الحساسة أو البنيات التحتية الحيوية، كما يحددها بدقة في مادته الأولى[91].

وقد جاء هذا القانون، في ضوء ما تفرضه التحولات العالمية للتهديدات السيبرانية، ليرسم معالم نظام قانوني مؤسس على إلزامية الالتزام بسياسات أمن المعلومات، وتصنيف الأصول

---

[89] جاء في القانون 05.20 مايلي: *بناء على الدستور ولا سيما الفصلين 42 و 50 منه أصدرنا أمرنا الشريف* بما يلي : ينفذ وينشر بالجريدة الرسمية، عقب ظهيرنا الشريف هذا. القانون رقم 05.20 المتعلق بالأمن السيبراني، كما وافق عليه مجلس النواب ومجلس المستشارين.

[90] حسن مصطفى البحري، *القانون الدستوري: النظرية العامة*، الطبعة الأولى، الجامعة الافتراضية السورية، دمشق، 2009، ص. 27.

[91] *المادة الأولى* من القانون رقم 05.20 المتعلق بالأمن السيبراني.

المعلوماتية بناءً على معايير السرية والتمامية والتوافر، وتعيين مسؤول عن أمن نظم المعلومات داخل كل هيئة، مع فرض منظومات للرصد والتبليغ عن الحوادث السيبرانية[92].

ويتجلى البعد السيادي لهذا القانون من خلال فرض وجوب إيواء المعطيات الحساسة داخل التراب الوطني، وإخضاع نظم المعلومات الحساسة لوجوب المصادقة قبل دخولها حيز الاستغلال، مع إقرار إلزامية الافتحاص الأمني المنتظم من طرف السلطة الوطنية أو من تعهدين مؤهلين وفق معايير محددة [93].

وانطلاقا من أهمية حماية البنيات التحتية ذات الأهمية الحيوية، عمل المشرع على تحديد لائحة هذه البنيات بشكل سري وتجديدي، فارضا على مسؤوليها التزامات صارمة تتعلق بضمان أمن الأنظمة وإعداد خطط لاستمرارية الأنشطة[94].

أما على مستوى القطاع الخاص، فقد ألزم مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت وناشري منصات الإنترنت، وغيرهم من المتعهدين، بالتقيد بتوجيهات السلطة الوطنية، والاحتفاظ بالمعطيات التقنية الضرورية لرصد الحوادث، والإخبار الفوري بالهشاشة والانتهاكات التي قد تطال نظمهم المعلوماتية، مع السماح للسلطة الوطنية بوضع أجهزة للرصد والتحليل داخل شبكاتهم لأغراض وقائية محضة[95].

وفي باب الحكامة، أحدث القانون اللجنة الاستراتيجية للأمن السيبراني باعتبارها الهيئة العليا لتوجيه السياسة العمومية في هذا المجال، مكلفة بإعداد التوجهات الاستراتيجية ومراقبة أنشطة السلطة الوطنية كما تم إنشاء لجنة إدارة الأزمات لمواجهة الأحداث السيبرانية الجسيمة بشكل منسق[96].

---

92 م.س من *المادة 3 الى 8* من القانون رقم 05.20 المتعلق بالأمن السيبراني.
93 م.س *المادة 11 و 19 و 20* من القانون رقم 05.20 المتعلق بالأمن السيبراني.
94 م.س *المادة 14 و 16* من القانون رقم 05.20 المتعلق بالأمن السيبراني.
95 م.س من *المادة 26 الى 28* من القانون رقم 05.20 المتعلق بالأمن السيبراني.
96 م.س المادة 35 من القانون رقم 05.20 المتعلق بالأمن السيبراني.

وأسند القانون إلى السلطة الوطنية للأمن السيبراني، باعتبارها هيئة مركزية، صلاحيات واسعة تشمل التنسيق الوطني، التأهيل، الافتحاص، الرصد، إدارة الأزمات، وتعزيز الثقة الرقمية، في ظل التزام صارم بواجب السرية وحماية المعطيات الحساسة[97].

وتعزيزا للنجاعة، رصد القانون إطارا زجريا مشددا، حيث منح السلطة الوطنية ولضباط الشرطة القضائية صلاحية معاينة المخالفات بموجب محاضر رسمية، مع إقرار عقوبات مالية تراوح بين مائة ألف وأربعمائة ألف درهم، بحسب طبيعة المخالفة وتشديد العقوبات في حالة العود[98].

وبذلك، يتجلى أن القانون رقم 05.20 يؤسس، بشكل صارم ودقيق، لمنظومة وطنية للأمن السيبراني، تقوم على مبادئ الوقاية، الرصد، الردع، السيادة الرقمية، والتكامل بين القطاعين العام والخاص، بما ينسجم مع التحولات السيبرانية العالمية، ويضمن الدفاع عن المصالح الحيوية للمملكة المغربية في الفضاء الرقمي[99].

ب – القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي:

قد وضع المشرع تعريفا دقيقا للمعطيات ذات الطابع الشخصي وأنواع المعالجة والمسؤولين عنها، محددا نطاق التطبيق، ومبينا الاستثناءات المرتبطة بالدفاع الوطني والأمن العام والوقاية من الجرائم[100]. أما على مستوى نوعية المعطيات وشروط المعالجة، فقد ألزم المشرع باحترام مبادئ المعالجة النزيهة والمشروعة، وجمع المعطيات لأغراض محددة ومعلنة، وضمان ملاءمتها وتحديثها، وعدم الاحتفاظ بها إلا للمدة الضرورية، مع اشتراط الحصول على رضى صريح للشخص المعني قبل الشروع في أي معالجة، إلا في حالات محددة مثل الالتزامات القانونية أو المصالح الحيوية أو تنفيذ مهام ذات طابع عام[101].

---

[97] م.س من *المادة 38 الى 39* من القانون رقم 05.20 المتعلق بالأمن السيبراني.

[98] م.س من *المادة 48 و 49 و 50 و 52* من القانون رقم 05.20 المتعلق بالأمن السيبراني.

[99] مقال بعنوان *"الأمن السيبراني بالمغرب"*، 2025، تاريخ الاطلاع: 23 أبريل 2025، على الساعة 17:41، متاح على: *www.allnews.ma*.

[100] القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي *من المادة 1 إلى المادة 2*.

[101] م.س القانون رقم 09.08 *من المادة 3 إلى المادة 4*.

كرس الإطار التشريعي حق الإخبار أثناء جمع المعطيات وفرض على المسؤولين عن المعالجة تمكين الشخص المعني من الاطلاع على معلوماته، وتصحيحها عند اللزوم، أو الاعتراض على معالجتها، مع منع الاستقراء المباشر بالوسائل الإلكترونية دون رضاه، وضمان ألا تؤدي المعالجة الآلية إلى اتخاذ قرارات تمس بحقوقه دون تدخله الشخصي[102]، ألزم المشرع المسؤول عن المعالجة بالتصريح المسبق قبل أي معالجة اعتيادية، والحصول على إذن مسبق عند معالجة معطيات حساسة، مع ضرورة اتخاذ جميع التدابير التقنية والتنظيمية اللازمة لضمان سرية وسلامة المعطيات، سواء خلال معالجتها أو أثناء نقلها أو حفظها، وإخضاع المعالجين من الباطن لشروط حماية صارمة لضمان عدم خرق المعطيات[103].

ولتأمين فعالية الإطار القانوني، تم إنشاء اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي بصلاحيات واسعة، منها الإذن بالمعالجة، وتلقي التصاريح والشكايات، والقيام بالتحقيقات، وإصدار التوصيات، وممارسة سلطات المراقبة والزجر الإداري لضمان حماية الحياة الخاصة في مواجهة المخاطر الرقمية[104]. فرض المشرع قيودا صارمة على نقل المعطيات نحو الخارج، حيث اشترط ضمان الدولة المستقبلة لمستوى حماية مكافئ، مع إمكانيات استثنائية محددة تهم المصالح الحيوية أو التعاقدية أو الحالات الخاصة المرتبطة بالدفاع أو التعاون القضائي، وكل ذلك تحت إشراف اللجنة. أحدث القانون سجلا وطنيا لحماية المعطيات الشخصية، يودع فيه كل تصريح أو إذن بمعالجة المعطيات، ويوضع هذا السجل رهن إشارة العموم، بما يعزز مبدأ الشفافية والمراقبة المجتمعية للمعالجات المعلوماتية[105].

لحماية الطابع الحساس للمعطيات، تم تقييد معالجتها، خاصة تلك المرتبطة بالمخالفات والإدانات، محصورا ذلك في السلطات العمومية المختصة ومساعدي القضاء، مما يعزز من حماية هذه الفئة الخاصة من المعلومات ذات الأهمية الكبرى للأمن السيبراني. أقر المشرع منظومة زجرية متدرجة تشمل الغرامات والعقوبات الحبسية، تهم المخالفات المرتبطة بمعالجة

---

102 م.س القانون رقم 09.08 *من المادة 5 إلى المادة 11.*
103 م.س القانون رقم 09.08 *من المادة 12 إلى المادة 26.*
104 م.س القانون رقم 09.08 *من المادة 27 إلى المادة 42.*
105 م.س القانون رقم 09.08 *من المادة 43 إلى المادة 48.*

المعطيات بدون تصريح أو إذن، وخرق حقوق المعنيين أو الالتزامات الأمنية، مع مضاعفة العقوبات في حالات العود أو إذا ارتكبت من قبل أشخاص معنويين[106].

ج – القانون 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية:

تأسس الإطار القانوني للتبادل الإلكتروني للمعطيات القانونية في المغرب مع صدور القانون رقم 53.05 الذي وضع منظومة من القواعد الناظمة للمعادلة بين المحررات الورقية والمحررات الإلكترونية، مما ينبني عليه فهم مكونات الأمن السيبراني في مجال حماية سرية المعلومات وتأمين المعاملات الرقمية.

وقد نص القانون على أن الوثيقة المرقمة تتمتع بنفس قوة الإثبات المخولة للوثيقة المعدة على الورق، شرط توفر القابلية القانونية لتعرف هوية الموقع وسلامة الوثيقة من التعديل أو العبث[107]. كما قرر المشرع معادلة التوقيع الإلكتروني بالتوقيع العرفي والرسمي، شرط استكماله بوسيلة تعريف موثوقة ومطابقته للمتطلبات القانونية من حيث ضمان هوية الموقع وسلامة المحتوى[108].

ومن أجل الضمان المؤسسي لهذه العمليات، أنشأ المشرع سلطة وطنية لاعتماد ومراقبة خدمات المصادقة الإلكترونية، تتولى إسناد الاعتمادات ومراقبة مقدمي خدمات المصادقة والتحقق من التزامهم بالمعايير القانونية والتقنية[109].

وفضلا عن ذلك، حدد المشرع مسؤولية مقدمي خدمات المصادقة ومواليتهم القانونية في حماية معطيات التوقيع وصون سريتها والإبلاغ عن أي خرق للمعايير، مع فرض جملة من العقوبات الجزرية على كل من انتهك هذه المقتضيات[110]. بهذا الإطار، أصبح التوقيع الإلكتروني والمعاملة الرقمية في المغرب ضمن منظومة قانونية آمنة ومنسجمة مع متطلبات الأمن السيبراني الحديثة.

---

106 م.س لقانون رقم 09.08 *من المادة 50 إلى المادة 66.*
107 القانون 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، من *المادة 4 إلى المادة 5.*
108 م.س القانون رقم 53.05، من *المادة 6 الى 11.*
109 م.س القانون رقم 53.05، *من المادة 15 الى 19.*
110 م.س القانون رقم 53.05، *من المادة 20 و 41.*

د – القانون رقم 08-31 القاضي بتحديد تدابير لحماية المستهلك، بما في ذلك حماية المستهلك على الإنترنت:

يتقاطع القانون رقم 08-31 المتعلق بحماية المستهلك في المغرب بشكل واضح مع قضايا الأمن السيبراني، خاصة في ظل تنامي المعاملات الإلكترونية. فبموجب هذا القانون، يُلزم الموردون بتمكين المستهلك من معلومات دقيقة وشفافة، خصوصاً في حالات البيع عن بُعد، مما يعزز الثقة الرقمية ويقلل من المخاطر المرتبطة بالنصب الإلكتروني. كما يحظر الإشهار المضلل، بما يشمل الإعلانات عبر الإنترنت، وهو ما يعد أداة مهمة للحد من الاحتيال السيبراني. يُجرّم القانون أيضاً الشروط التعسفية في العقود، ما يمنح المستهلك حماية إضافية ضد الهيمنة الرقمية لبعض المنصات التجارية. وفي نفس السياق، يُخول لجمعيات حماية المستهلك التدخل واللجوء إلى القضاء باسم المستهلكين، وهو ما يفتح الباب أمام رقابة جماعية على التجاوزات السيبرانية. إلا أن التطبيق العملي لا يزال يعاني من ضعف، خاصة في ما يتعلق بتفعيل الحق في التراجع عن الشراء، أو مواجهة الشركات التي لا توفر بيانات قانونية واضحة، لا سيما تلك التي تنشط عبر شبكات التواصل الاجتماعي. كما يتكامل هذا القانون مع مقتضيات حماية المعطيات الشخصية (القانون 08-09)، من خلال فرضه لإشعار المستهلك بجمع بياناته، ما يساهم في تعزيز الخصوصية الرقمية. ورغم أن القانون يشكل خطوة مهمة نحو تأمين المستهلك رقمياً، إلا أن الخبراء يدعون اليوم إلى مراجعة شاملة له، قصد مواكبة التغيرات السريعة في الفضاء الرقمي وتنظيم المنصات التجارية الافتراضية، بما يضمن بيئة سيبرانية أكثر أماناً وثقة للمستهلك المغربي[111].

ثانيا: المراسيم ذات الصلة

1. مرسوم رقم 673-82-2:

يشكل هذا المرسوم الإطار المؤسسي لتنظيم إدارة الدفاع الوطني، والذي أُحدثت بموجبه المديرية العامة لأمن نظم المعلومات، بوصفها الهيئة العليا المكلفة بتأمين وحماية البنى

[111] الحسان العصري، "قراءة في القانون رقم 31.08 القاضي بتحديد تدابير لحماية المستهلك"، منصة مغرب القانون MarocDroit، 31 غشت 2013، تم الاطلاع عليه بتاريخ 2025/07/10 على الساعة 22.02 على الموقع التالي: https://www.marocdroit.com

التحتية المعلوماتية ذات الأهمية الوطنية. وقد مكن هذا التأسيس من وضع الأسس الإدارية والتنظيمية لمواجهة التهديدات السيبرانية ومواكبة التحولات التكنولوجية العالمية[112].

2. مرسوم رقم 509-11-2:

أتى هذا المرسوم متمما للمرسوم المؤسس لسنة 1983، ليعزز اختصاصات المديرية العامة لأمن نظم المعلومات، ويوسع مهامها لتشمل قيادة السياسة الوطنية للأمن السيبراني، وضمان يقظة مستمرة تجاه المخاطر السيبرانية، وإرساء منظومة وطنية متكاملة لحماية نظم المعلومات الحيوية[113].

3. مرسوم رقم 518-08-2:

صدر هذا المرسوم لتطبيق المواد 13 و14 و15 و21 و23 من القانون رقم 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، مكرسا بذلك قواعد دقيقة لضمان صحة المحررات الإلكترونية، وحماية أمن التبادلات الرقمية، ولا سيما فيما يتعلق بالمصادقة الإلكترونية وحماية البيانات أثناء المعاملات الرقمية[114].

4. مرسوم رقم 165-09-2:

جاء هذا المرسوم لتفعيل مقتضيات القانون رقم 08-09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي. وقد سعى إلى ضمان انسجام الإطار القانوني المغربي مع المعايير الأوروبية، واضعا آليات صارمة لحماية المعطيات الشخصية ضد أي استغلال غير مشروع، ومؤسسا بذلك أحد أعمدة الأمن السيبراني الوطني[115].

5. مرسوم رقم 881-13-2:

عمل هذا المرسوم على تغيير وتتميم مرسوم 2009 الخاص بالتبادل الإلكتروني للمعطيات القانونية، وذلك بتحديث الإجراءات التنظيمية المرتبطة بالمصادقة الإلكترونية، وتقوية

---

[112] مرسوم رقم *673-82-2* الصادر في 28 ربيع الأول 1403 (13 يناير 1983).
[113] مرسوم رقم *509-11-2* الصادر في 22 شوال 1432 (21 شتنبر 2011).
[114] مرسوم رقم *518-08-2* الصادر في 25 جمادى الأولى 1430 (21 ماي 2009).
[115] مرسوم رقم *165-09-2* الصادر في 25 جمادى الأولى 1430 (21 ماي 2009).

الضمانات المتعلقة بموثوقية المعاملات الرقمية وحماية المعطيات المتبادلة عبر الوسائط الإلكترونية، بما يتلاءم مع التطور المتسارع للتهديدات السيبرانية[116].

6. مرسوم رقم 406-21-2:

يُعد هذا المرسوم نصا محوريا لتطبيق مقتضيات القانون رقم 05.20 المتعلق بالأمن السيبراني، إذ وضع الإطار التنظيمي لتنزيل التوجيهات الوطنية في مجال حماية نظم المعلومات الحيوية، وفرض على الهيئات الخاضعة للقانون المذكور اعتماد منهجيات دقيقة لإدارة المخاطر السيبرانية والامتثال للمعايير الأمنية الصادرة عن السلطة الوطنية المختصة[117].

7. مرسوم رقم 2.24.921:

خصص هذا المرسوم لتأطير لجوء الهيئات والبنيات التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة أو معطيات حساسة إلى مقدمي الخدمات الرقمية السحابية. وقد فرض نظاما دقيقا لتأهيل مقدمي هذه الخدمات، مع تمييز بين مستويين من التأهيل لضمان معالجة وتخزين المعطيات الحساسة داخل التراب الوطني، ومنع إخضاعها لأي قوانين أجنبية عابرة للحدود. وجاء ذلك استجابة للتحديات الأمنية المستجدة المرتبطة بالحوسبة السحابية، بما يكرس سيادة المغرب الرقمية ويحمي مصالحه السيبرانية العليا[118].

ثالثا: القرارات والمناشير ذات الصلة

في سياق دينامية التحول الرقمي التي انخرطت فيها المملكة المغربية، وتماشيا مع الرؤية الملكية السامية الرامية إلى جعل الرقمنة رافعة أساسية للتنمية الاقتصادية والاجتماعية[119]، صدر منشور رئيس الحكومة رقم 2023/02، الذي يهدف إلى تفعيل النسخة المحينة من التوجيهات الوطنية لأمن نظم المعلومات. وقد جاء هذا المنشور استجابة للحاجة الملحة إلى تعزيز الثقة الرقمية ومواجهة المخاطر السيبرانية المتزايدة التي تصاحب الانتشار السريع

---

116 *مرسوم رقم 881-13-2* الصادر في 28 ربيع الأول 1436 (20 يناير 2015).

117 *مرسوم رقم 406-21-2* الصادر في 4 ذو الحجة 1442 (15 يوليو 2021).

118 *مرسوم رقم 2.24.921* الصادر في 2024.

119 محمد السادس، خطاب بمناسبة الذكرى الثلاثين لتأسيس الإيسيسكو، سنة 2012، مقتطف: *"وفي نفس السياق، ينبغي اعتماد مقاربات جديدة وفعالة، لمواكبة التطورات المتلاحقة التي يعيشها العالم في مختلف المجالات، وخاصة في ميدان المعلوميات والتكنولوجيات الحديثة، لما لذلك من ارتباط وثيق بالتنمية البشرية والاقتصادية والثقافية".*

للخدمات الرقمية. وتعد النسخة الجديدة من التوجيهات الوطنية التي أعدتها المديرية العامة لأمن نظم المعلومات، تنفيذا للتعليمات الملكية، إطارا معياريا يحدد التدابير الأمنية التنظيمية والتقنية التي يتعين على جميع الإدارات العمومية والجماعات الترابية والمؤسسات والمقاولات العمومية، فضلا عن البنيات التحتية ذات الأهمية الحيوية، احترامها وتنفيذها. وتتجلى أهمية هذه التوجيهات في كونها تضع الأسس الضرورية لحماية نظم المعلومات الحساسة، عبر تحديد القواعد الأمنية الإلزامية وتوفير المتطلبات الدنيا للامتثال لمعايير الأمن السيبراني الوطني. وقد منح المنشور الهيئات المعنية مهلة ستة (6) أشهر ابتداء من تاريخ النشر لإعداد جداول زمنية دقيقة لتطبيق التدابير الواردة ضمن التوجيهات، مع إلزامها باستخدام أداة تقييم الامتثال التي وضعتها المديرية العامة لأمن نظم المعلومات، بهدف قياس مدى التزامها بالمعايير الأمنية الجديدة[120].

رابعا: الإتفاقيات الدولية والإقليمية

وقع المغرب عدة اتفاقيات دولية وإقليمية تهدف إلى مكافحة الجرائم السيبرانية وتعزيز أمن الفضاء الرقمي. أبرز هذه الاتفاقيات هي اتفاقية بودابست لمكافحة الجرائم السيبرانية، التي صادق عليها المغرب سنة 2018، ليكون أول بلد إفريقي وعربي ينضم إليها، ما مكّنه من الاستفادة من إطار قانوني موحّد للتجريم والتعاون القضائي الدولي[121]. كما التحق باتفاقية مالابو التابعة للاتحاد الإفريقي، التي تهدف إلى تعزيز حماية المعطيات الشخصية ومكافحة الجرائم المرتبطة بالتجارة الإلكترونية[122]. وعلى المستوى الثنائي، أبرم المغرب اتفاقيات تعاون مع عدة دول من بينها كوريا الجنوبية، التي ساهمت في إنشاء المركز المغربي للاستجابة للحوادث السيبرانية (maCERT)[123]، وكذلك مع فرنسا وألمانيا والهند، لتعزيز تبادل المعلومات والخبرات التقنية والتدريب. إقليمياً، يشارك المغرب في مشروع Cyber South بالتعاون مع الاتحاد الأوروبي ودول متوسطية، ويقود منصة مراكش كمبادرة إفريقية لمكافحة

---

120 منشور رئيس الحكومة رقم 2023/02 الصادر في 12 يناير 2023 حول *تطبيق التوجيهات الوطنية لأمن نظم المعلومات*.

121 «*المغرب يوقّع على "اتفاقية بودابست" لمحاربة الجريمة الإلكترونية*»، الشرق الأوسط، نُشر في 12 ماي 2022، تم الاطلاع عليه بتاريخ 10 يوليو 2025، على الساعة 17:45، عبر الموقع التالي: *https://aawsat.com*

122 «*Malabo Convention*»، *Wikipedia: The Free Encyclopedia*، آخر تعديل في 23 يونيو 2025، تم الاطلاع عليه بتاريخ 10 يوليو 2025، على الساعة 18:30، عبر الموقع التالي: *https://en.wikipedia.org*

123 Op.Cit. Kezzoute, M. (2025). *Cyber Governance in Morocco: Between the Consolidation of Interne Status and the Enhancement of Global Positioning.*

الإرهاب السيبراني[124]. تعكس هذه الاتفاقيات مجتمعة التزام المغرب بالتصدي للتهديدات السيبرانية في سياق من التعاون الدولي المتكامل، ووضع أرضية صلبة لتحديث تشريعه الرقمي وبنياته الأمنية.

الفقرة الثانية: مدى نجاعة الترسانة القانونية في مواجهة التهديدات

شهد المغرب خلال العقدين الأخيرين اهتماماً متزايداً بالأمن السيبراني على مستويات عليا، انطلاقاً من إدراكه لتنامي التهديدات الإلكترونية على مؤسساته الحيوية ومصالحه الوطنية [125]. وتعكس المؤشرات الدولية هذا الاهتمام، إذ صُنّف المغرب في المرتبة الأولى (الفئة الأولى) عالمياً في مؤشر الأمن السيبراني العالمي 2024 (*Global Cybersecurity Index*) الصادر عن الاتحاد الدولي للاتصالات، بمجموع نقاط 97.5 (من 100). وقد جاء هذا التصنيف بفضل تنوّع شامل للجهود المغربية في بناء الإطار القانوني والتنظيمي الموجه للأمن السيبراني، حيث أكد التقرير الدولي على وجود «إطار قانوني شامل» يتناول مجالات أمن الأنظمة المعلوماتية، ومحاربة الجرائم الإلكترونية، وحماية البيانات الشخصية، والهوية الرقمية، والخدمات الموثوقة[126].

تتكون الترسانة القانونية المغربية للأمن السيبراني من مجموعة من النصوص المنظمة تغطي جوانب عدة، أبرزها: قانون رقم 05.20 بشأن الأمن السيبراني (2020)، وقانون رقم 09.08 المتعلق بحماية الأشخاص فيما يخص معالجة المعطيات ذات الطابع الشخصي (2009)، وقانون رقم 53.05 الخاص بالتبادل الإلكتروني للمعطيات القانونية (2007) ولاحقاً تحديثه بقانون 43.20 (2020) الخاص بخدمات الثقة في المعاملات الإلكترونية. كما تشمل القائمة قوانين وقواعد جزائية، منها القانون رقم 07.03 المتعلق بالجرائم المعلوماتية الذي أُدرج في القانون الجنائي (2003) لمواجهة التعديات التي تطال نظم المعالجة الآليّة للبيانات. وعلاوة

---

[124] Op.Cit. Driss Abbadi, *"Morocco's cybersecurity strategy between challenges and aspirations*,"

[125] Hind Idrissi, *Cybersecurity in Morocco: between achievements and challenges*, MIPA Institute, 2023, (Accessed: 27 April 2025, at 23:00), available at: *www.mipa.institute.*

[126] Directorate General of Information Systems Security (DGSSI), *Morocco has improved its position in the Global Cybersecurity Index recently published by the International Telecommunication Union (ITU)*, DGSSI official website, 2024, (Accessed: April 11, 2025, at 19:00), available at: *www.dgssi.gov.ma.*

على ذلك، اعتمد المغرب استراتيجيات وطنية وخططاً للتشريع، مثل نشر الاستراتيجية الوطنية للأمن السيبراني (مع أفق 2030) وتحديث التوجيه الوطني لأمن نظم المعلومات (*DNSSI*)[127].

- **حداثة القوانين ومواكبتها للتطورات**

تختلف أعمار هذه القوانين اختلافاً كبيراً: فبينما يُعد قانون 05.20 (2020) حديث النشأة، تأتي نصوص مثل قانون 09.08 (2009) وقانون 53.05 (2007) من حقبة قبل الطفرة الراهنة للتكنولوجيا والتهديدات السيبرانية المعاصرة. وقد عمل المغرب على تحديث بعض هذه النصوص، فمثلاً ألغى قانون 43.20 (2020) الفصل التمهيدي والجزء الثاني من قانون 53.05، وحلَّ محله نظام متقدم للخدمات الموثوقة والتواقيع الإلكترونية[128]. كما راعى المغرب تعزيز الإطار القانوني للأمن السيبراني بإصدار مرسوم تطبيقي رقم 2.21.406 (2021) لقانون 05.20، إضافة إلى تحديث التوجيهات الوطنية لأمن النظم المعلوماتية استجابةً للتعليمات الملكية، حيث صدرت نسخة مطوّرة للتوجيه الوطني سنة 2023 تأخذ في الحسبان المستجدات القانونية والتنظيمية والتكنولوجية[129].

بالتالي، يُعد قانون 05.20 مكمِّلاً حديثاً لجهود سابقة، تزامناً مع قانون خدمات الثقة (43.20) المعاصر، بينما تبقى نصوص حماية المعطيات وقانون التبادل الإلكتروني قديمة النشأة نسبياً. وتنبع الحاجة إلى تجديدها من تسارع التهديدات (الحوسبة السحابية، الإنترنت الصناعي، الذكاء الاصطناعي، إلخ)، وهو ما أكدت عليه برامج التعاون الدولية لدعم المغرب، التي تضمنت دعوات صريحة لمراجعة قانون 09-08 ليتماشى مع اللائحة العامة لحماية البيانات الأوروبية (*GDPR*) والبروتوكول المطوّر للمعاهدة الأوروبية 108+[130].

---

[127] (DGSSI), *Directive nationale de la sécurité des systèmes d'information (DNSSI)* ,2023, (Accessed: April 11, 2025, at 23:00), available at: *www.dgssi.gov.ma.*

[128] نصّ القانون رقم 43-20 *المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية على إلغاء كل من الباب التمهيدي والقسم الثاني من القانون رقم 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية*، الصادر بتنفيذه الظهير الشريف رقم 1.07.129 بتاريخ 19 ذي القعدة 1428 (30 نوفمبر 2007).

[129] المديرية العامة لأمن نظم المعلومات، *"التوجيهات الوطنية لأمن نظم المعلومات"، 2023*، (تاريخ الاطلاع: 20 أبريل 2025، على الساعة 20:00)، متاح عبر الرابط: *www.dgssi.gov.ma*.

[130] Council of Europe, *"Support to data protection in Morocco"*, 2024, (Accessed: April 22, 2025, at 03:00), available at: *www.coe.int.*

- **شمولية التغطية القانونية للتهديدات السيبرانية**

يحرص الإطار القانوني المغربي على تغطية العديد من أنواع التهديدات السيبرانية، وإن تفاوتت مساحات التغطية. فمثلاً:

- **الهجمات على البنية التحتية الحيوية:**

يكرّس قانون 05.20 (المُنظَّم للأمن السيبراني) مفهوم "البنى التحتية ذات الأهمية الحيوية"، ويُلزم الهيئات المعنية بتصنيف وتعيين مسؤول أمن المعلومات لديها، واتخاذ التدابير التنظيمية والفنية لحمايتها[131]. كما يستلزم إصدار التوجيه الوطني (*DNSSI*) لعام 2023 تطبيق هذه التدابير خلال ستة أشهر من النشر على جهات الدولة والمؤسسات الحيوية[132].

- **الجرائم السيبرانية:**

جرّد القانون 07-03 الجرائم المعلوماتية وجعلها جزءاً من القانون الجنائي (مباشرةً ضمن المادتين 607 و607-3 وما بعده)، معالجةً عمليات اختراق الحواسيب، والاحتيال الإلكتروني، والتجسس الإلكتروني، ونشر البرمجيات الخبيثة، وغيرها. وقد استُكمِل هذا القانون بالتعاون الدولي بالتصديق على اتفاقية بودابست لمكافحة الجريمة الإلكترونية وبروتوكولها الإضافي لمشاركة الأدلة الرقمية[133].

- **حماية البيانات الشخصية:**

ينص قانون 09.08 على ضمان حماية الأشخاص من سوء استخدام معطياتهم، ويؤسس للهيكل التنظيمي (اللجنة الوطنية لمراقبة حماية المعطيات الشخصية «*CNDP*»). ويحرص القانون على مبدأ وضوح الضمانات وتنقل البيانات بما يتوافق مع الشركاء الدوليين[134]. رغم

---

[131] Yassine Maleh and Youness Maleh, *Cybersecurity in Morocco*, op. cit. p. 46.

[132] م.س المديرية العامة لأمن نظم المعلومات، *"التوجيهات الوطنية لأمن نظم المعلومات 2023".*

[133] Yassine Maleh and Youness Maleh, *Cybersecurity in Morocco*, op. cit. p. 47.

[134] م.س القانون رقم 08-09 *المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.*

ذلك، فإن القانون قد لا يلحظ بشكل صريح التحديات الحديثة مثل تحليل البيانات الضخمة (***Big Data***[135]) أو تقنيات الذكاء الصناعي، مما يُستدعى لإصلاحه قريباً.

- **الحوسبة السحابية والخدمات الرقمية:**

أدرج قانون 05.20 صيغاً تعريفية للخدمات الرقمية والحوسبة السحابية ضمن التعاريف القانونية (مثلاً: «الاستضافة» بما يشمل الحوسبة السحابية)[136]. ويُلزم القانون مزودي الخدمات الرقمية ومزوّدي الاتصالات بتطبيق التوجيهات الوطنية (مثل الاحتفاظ بالبيانات التقنية اللازمة لتتبع الحوادث)، بالتنسيق مع السلطات الوطنية[137]. كما أكدت تقارير دولية أن الإطار القانوني المغربي يغطي "الهوية الرقمية وخدمات الثقة" (أي التوقيع الإلكتروني والتصديق)[138]، بفضل تكملة قانون 53.05 بقانون 43.20.

إلى جانب ما سبق، أشار تقرير التقييم المغربي إلى ضرورة توسيع الإطار التنظيمي ليضم تشريعات خاصة ببعض التهديدات الناشئة أو قطاعات محددة، مثل سلامة الشبكات اللاسلكية والتطبيقات المصرفية، والامتثال للمعايير الدولية الجديدة.

- **فعالية تطبيق القانون على أرض الواقع**

تُظهر المؤشرات الرسمية والدولية أن المغرب عزّز تطبيق نصوصه القانونية، لكن مدى الفاعلية يختلف بين المنظومات والقطاعات. ففي مجال البُنى التحتية والهيئات العمومية، وضعت الدولة إجراءات إلزامية للتصنيف الأمني وتعيين مسؤولين أمنيين، كما أجبرتها اللوائح على إخضاع نظمها للتدقيق والتقييم (بمتابعة *DGSSI*)[139]. وقد قامت *DGSSI* منذ عام 2013 بإشراف الفحص والتفتيش الدورية للأنظمة الحكومية وشبكات الاتصالات، مستفيدةً من شهادة الهيئة العليا (*CNDP*) بخصوص الإجراءات الوقائية لمحاسبة المخالفين. كما

---

[135] يقصد بـ *Big Data* أو "البيانات الضخمة" مجموعات بيانات ضخمة جدًا ومتنوعة ومعقدة، تتجاوز قدرة الأدوات التقليدية لمعالجة البيانات على الالتقاط والإدارة والتحليل خلال زمن معقول. *تُستخدم لاستخلاص رؤى قيمة لدعم اتخاذ القرار*، بالاعتماد على تقنيات متقدمة مثل الذكاء الاصطناعي والتحليل التنبئي.

[136] مرجع سابق، *المادة 2* الفقرة 11 من القانون رقم 05.20 المتعلق بالأمن السيبراني.

[137] مرجع سابق، *المادة 26* من القانون رقم 05.20 المتعلق بالأمن السيبراني.

[138] (DGSSI), *Morocco has improved its position in the Global Cybersecurity Index recently published by the International Telecommunication Union (ITU), 2024.* op. cit.

[139] Yassine Maleh and Youness Maleh, *Cybersecurity in Morocco*, op. cit. p. 46.

يتمتع مزودو خدمات الأمن السيبراني ورقمنة الوثائق بإجراءات تراخيص صارمة وتقييم دوري (حيث نشرت *DGSSI* في 2023 قائمة أولى للمزودين المؤهلين).

هذا الجدول مثال حول قائمة متعهدي افتحاص أمن نظم المعلومات المؤهلين وفقاً للوضعية القانونية كما هي منشورة في الموقع الرسمي للمديرية العامة لأمن نظم المعلومات (DGSSI)، تطبيقاً لمقتضيات المادة 26 من المرسوم رقم 2-21-406 المتخذ لتطبيق القانون 05.20 المتعلق بالأمن السيبراني[140].

مقدمي الخدمة	الجهات أو الشركات المؤهلة لتنفيذ مهام افتحاص (تدقيق) أمن نظم المعلومات.
المراجعة التنظيمية	تقييم مدى التزام المؤسسة بالسياسات والإجراءات التنظيمية الخاصة بالأمن السيبراني.
مراجعة البنى	تحليل البنية التحتية المعلوماتية (شبكات، خوادم، نظم تشغيل) لرصد الثغرات والمخاطر الأمنية.
مراجعة التكوينات	تدقيق إعدادات الأنظمة والتجهيزات التقنية للتحقق من مطابقتها لأفضل ممارسات الأمن المعلوماتي.
اختبارات الاختراق	محاولات محاكية للهجمات الإلكترونية بهدف اكتشاف نقاط الضعف التقنية في الأنظمة.
مراجعة الرموز المصدرية	فحص الشيفرة البرمجية للتطبيقات للتحقق من سلامتها وخلوها من الثغرات الأمنية.
مراجعة النظم الصناعية	تقييم الأنظمة المعلوماتية المستخدمة في البنى التحتية الحيوية (مثل الطاقة والنقل) لضمان حمايتها.
تاريخ انتهاء التأهيل	آخر موعد تكون فيه شهادة التأهيل الممنوحة لمقدم الخدمة صالحة.

[140] المديرية العامة لأمن نظم المعلومات، *"قائمة متعهدي افتحاص أمن نظم المعلومات المؤهلين"*، الموقع الرسمي للمديرية العامة لأمن نظم المعلومات، (تم الاطلاع عليه يوم 21 أبريل 2025، على الساعة 23:00)، متاح على الرابط: *www.dgssi.gov.ma*.

فئة معلومات النظام	تصنيف الأنظمة المعلوماتية وفقًا لحساسيتها وأهميتها (الفئة أ: أكثر حساسية، الفئة ب: أقل حساسية).
قرار التأهيل	الحالة الرسمية لمقدم الخدمة، إما "مصادق عليه"، أو "قيد التنفيذ"، أو "موقوف"، بحسب مدى استيفائه للمعايير المطلوبة.

في إطار تنزيل مقتضيات القانون رقم 05.20 المتعلق بالأمن السيبراني، والمرسوم رقم 2-21-406 الصادر لتطبيقه، تقوم المديرية العامة لأمن نظم المعلومات بإصدار قرارات رسمية لتأهيل متعهدي افتحاص[141] أمن نظم المعلومات. تحدد هذه القرارات نطاق التأهيل، الميادين المشمولة، فئة الأنظمة المعلوماتية المعنية، ومدة صلاحية التأهيل[142].

و في سياق مكافحة الجرائم الإلكترونية، أسست مصالح الأمن والعدل وحدات مختصة (مثل "خدمة مكافحة الجريمة التكنولوجية" تحت *DGSN* ووزارة العدل)، وفتحت ملفات عدة قضايا مهمة (مثلاً اعتقالات بناءً على تعاون دولي، وتشريعات عُزّزت بسنّ عقوبات جديدة للجرائم الإلكترونية). ويشير المدير العام للأمن الوطني إلى تجهيز قوات الأمن الشرطية بستة مختبرات تحليل رقمي على الأقل (واحد مركزي وأربعة جهوية) للاستخبارات الجنائية الرقمية [143]، وكذا تشكيل 29 فرقة أمنية إقليمية متخصصة في مكافحة الجريمة الإلكترونية.

أما في مجال حماية المعطيات الشخصية، فتقوم «*CNDP*» بشكل دوري بمراقبة مدى التزام المؤسسات بأحكام 09-08، وقد أصدرت تقارير سنوية تبرز تأثير القانون والإجراءات المرافقة (مثل إلزامية التصريح بالمعالجات وفرض الجزاءات)[144]. غير أن بعض المؤسسات العامة والخاصة ما زالت غير متوافقة بالكامل مع متطلبات القانون، خصوصاً فيما يتعلق بالإبلاغ عن خروقات الحماية وتوظيف التحليل الشامل للبيانات. وهذا ما أشارت إليه تقارير دولية بوجود **«نواقص تشريعية وتنظيمية»** في بعض جزئيات التنفيذ[145]. بالاعتماد على هذه المتغيرات، فإن تقييم فاعلية التطبيق لا يزال نقدياً: من جهة يرى أصحاب الاختصاص أن

---

[141] افتحاص أمن نظم المعلومات يعني: *"فحص شامل ودقيق للأنظمة المعلوماتية (الخوادم، الشبكات، التطبيقات، قواعد البيانات...) بهدف تقييم مدى قوتها وضعفها أمام التهديدات السيبرانية، ومدى احترامها لمعايير الأمن المعتمدة وطنياً ودولياً."*

[142] ويمكن الاطلاع على هذه *الوثائق* عبر البوابة الرسمية للمديرية العامة لأمن نظم المعلومات التابعة لإدارة الدفاع الوطني.

[143] Maroc Diplomatique, *Cybercriminalité: la DGSN traque les délinquants du web*, 5 octobre 2019, (consulté le 22 avril 2025, à 22h00), disponible sur: *www.maroc-diplomatique.net.*

[144] مرجع سابق، *اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (CNDP)* .

[145] Hind Idrissi, *Cybersecurity in Morocco: between achievements and challenges* op. cit.

المغرب حقق قفزات نوعية في تأسيس البنية الإدارية والقانونية (كما أثبت ذلك تصنيف *ITU*) ، ومن جهة أخرى تثبت دراسات محلية أن تمويلات المنشآت والجهات المعنية في غالب الأحيان أقل من المطلوب مقارنة بتعقيد التهديدات. فمثلاً، الموازنات المخصصة للأمن السيبراني ضمن الميزانيات الحكومية والشركات قد لا توازي حجم المخاطر الحقيقية.

- **القدرات التقنية والبشرية وآليات الاستجابة**

توجد بالمغرب بنية تقنية وبشرية متنامية لدعم جهود الأمن السيبراني، ولكنها لا تزال في طور النضوج. فإلى جانب إنشاء *maCERT* (فريق الطوارئ الحاسوبي الوطني التابع *DGSSI*)، الذي يُعنى بالرصد والاستجابة للانتهاكات السيبرانية[146]، عززت الدولة بناء مراكز للاستخبارات الإلكترونية ورفدها بالمهندسين والخبراء. فقد أصدرت *DGSSI* أدلة فنية وأدوات عملية (مثل «أداة تقييم مطابقة *DNSSI*» ونشرات دورية للحوادث السيبرانية) لترشيد جاهزية الإدارات. كما نجحت الدارسات والمشاريع المشتركة (مع جامعات وشركات دولية) في تخريج كوادر متخصصة، ومنحت الجامعات مهام بحث في الأمن الشبكي.

على صعيد الإجراء العملي، أظهرت أجهزة الأمن الوطني (*DGSN*) قدرات متقدمة: ففي خبر صحفي أنشأت الشرطة المختصة في جرائم التقنية مختبرات بحث جنائي رقمي مجهزة بأدوات تحليل معترف بها دولياً[147]، واستقطبت الكفاءات من حاملي دكتوراه والهندسة في الإعلاميات والأمن المعلوماتي. كما تنظم الدورات التدريبية المستمرة لتحديث مهارات فرق مكافحة الجرائم الإلكترونية بنِظم مراقبة متقدمة (مثل الذكاء الاصطناعي لرصد التهديدات)[148].

تعكس هذه التطورات أن مكوّن الاستجابة السريعة للمغرب يتمتع بآليات فاعلة نسبياً (مراكز وطنية وجهوية للاستجابة للحوادث)، وإن كان حجم الهجمات المرتفع يفرض عليه تحديات

---

[146] المديرية العامة لأمن نظم المعلومات، *"ماسيرت - الفريق المغربي للاستجابة لحالات الطوارئ التي تحدث في الحواسيب"*، (تم الاطلاع عليه بتاريخ 27 أبريل 2025، على الساعة 22:30)، متاح على: *www.dgssi.gov.ma*.

[147] MAP News, *Directorate of National Security, "General Directorate of National Security 2024 Report*," 25 December 2024, (Accessed: 21 April 2025, at 05:00), available at: *www.mapnews.ma*.

[148] مؤتمر *DFIR212* في المغرب للأدلة الرقمية والاستجابة للحوادث، وهو مؤتمر علمي وتقني مجاني، يهدف هذا الحدث إلى جمع الباحثين الأكاديميين، والمهنيين الصناعيين، والخبراء المستقلين في مجال الأدلة الجنائية الرقمية (*Digital Forensics*) والاستجابة للحوادث المعلوماتية (*Incident Response*) .

مستمرة. غير أن القطاع الخاص والشركات الصغيرة والمتوسطة ما زالت تواجه صعوبات في توفير الخبرات الفنية والتجهيزات. إذ يجد العديد من الفاعلين أن الكفاءات المؤهلة في الأمن السيبراني محدودة نسبياً في السوق المحلي، مما يؤدي إلى الاعتماد على خدمات استشارية أو تطوير داخلي ببطء. وقد رصدت تقارير محلية قلة نسبية في الوعي السيبراني وتنظيم أولويات التدريب بين العاملين، وهي عوامل تفاقم أثر نقص الكفاءات[149].

مع ذلك، فإن الإطار القانوني الحالي يُعتبر متيناً نسبياً ويشكل قاعدة صلبة لبقية الجهود. ويتيح إشراك القطاع الخاص في الرقابة (مثل إلزام مقدمي خدمات الاتصالات بالقوانين ومشاركة بيانات الأحداث) تعزيز سرعة الاستجابة. ويعد النشاط الدولي للمغرب (انضمام للاتفاقيات العالمية، شراكات بحثية) فرصة لبقاء القانون حديثاً ومتكامل.

المطلب الثاني: المؤسسات الوطنية المعنية بالأمن السيبراني

يكتسي البعد المؤسساتي أهمية حيوية في تنزيل الاستراتيجيات الوطنية المتعلقة بالأمن السيبراني، إذ يُعهد إلى عدد من الهيئات بأدوار تنظيمية وتقنية ورقابية لضمان حماية الفضاء الرقمي. يتجه هذا المطلب الثاني إلى تفكيك الإطار المؤسساتي المكلف بتدبير الأمن السيبراني بالمغرب، وذلك عبر فقرتين متكاملتين: نتناول في الفقرة الأولى عرضًا تحليليًا لأدوار وصلاحيات الهيئات الوطنية المختصة، وعلى رأسها المديرية العامة لأمن نظم المعلومات، واللجنة الوطنية لحماية المعطيات الشخصية، وأجهزة الأمن الوطني، بينما نخصص الفقرة الثانية لتحليل العلاقة بين هذه المؤسسات والسياسات العمومية الأمنية، مع إبراز مظاهر التنسيق والتكامل في حماية الفضاء الرقمي الوطني.

الفقرة الاولى: الأدوار والصلاحيات : *DGSSI*، *CNDP*، وأجهزة الأمن

تشمل المؤسسات الرسمية المعنية في المغرب بالأمن السيبراني وحماية المعطيات الشخصية كل من المديرية العامة لأمن نظم المعلومات (*DGSSI*)، واللجنة الوطنية لحماية المعطيات ذات الطابع الشخصي (*CNDP*)، وأجهزة الأمن (الشرطة والدرك الملكي وجهاز المخابرات)،

[149] Taieb Debbagh, *15 Ans de Cybersécurité au Maroc*, Édition indépendante, 2023, p. 58.

إضافة إلى لجان تنسيقية مثل اللجنة الاستراتيجية للأمن السيبراني ولجنة إدارة الأزمات السيبرانية.

أولا – المديرية العامة لأمن نظم المعلومات (*DGSSI*)

أنشئت المديرية العامة لأمن نظم المعلومات بمقتضى المرسوم الملكي رقم 2.11.509 في 21 سبتمبر 2011، وهي تابعة لإدارة الدفاع الوطني للمملكة[150]. وتعد *DGSSI* السلطة الوطنية التقنية المعتمدة في رسم وتنفيذ السياسة العامة للأمن السيبراني[151]، **وتتشكل الهيكلة الداخلية للمديرية العامة لأمن نظم المعلومات من التالي:**

- **مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية (*maCERT*):** تضطلع هذه المديرية بمهمة إحداث وتفعيل نظم للرصد والإنذار المبكر ضد التهديدات السيبرانية التي قد تستهدف نظم معلومات الدولة، بالإضافة إلى تنسيق التدخلات الاستباقية وتدبير الاستجابة للحوادث الرقمية الطارئة[152].
- **مديرية الاستراتيجية والتقنين:** تتولى هذه المديرية إعداد وتنفيذ الاستراتيجية الوطنية للأمن السيبراني، بالتشاور مع القطاعات الوزارية المعنية، كما تتكلف باقتراح مشاريع النصوص القانونية والتنظيمية المرتبطة بالأمن السيبراني، ودراسة التصاريح الخاصة بالمنتجات الأمنية، والإشراف على المصادقة على أنظمة التوقيع الإلكتروني[153].
- **مديرية المساعدة والتكوين والمراقبة والخبرة:** تهدف إلى تحسين مستوى أمن المعلومات داخل المؤسسات العمومية من خلال اقتراح توصيات فنية ومعايير مرجعية، وتنظيم برامج

---

[150] مرسوم رقم 2.11.509 صادر في 22 شوال 1432 (21 سبتمبر 2011)، بتتميم المرسوم رقم 2.82.673 الصادر في 28 ربيع الأول 1403 (13 يناير 1983)، المتعلق بتنظيم إدارة الدفاع الوطني *وإحداث المديرية العامة لأمن نظم المعلومات*.

[151] مرسوم رقم 2.15.712 الصادر بتاريخ 12 جمادى الآخرة 1437 (22 مارس 2016) *بتحديد إجراءات حماية نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية، المادة الأولى، الفقرة 5.*

[152] *Le maCERT, puissant bouclier de la DGSSI contre les menaces cybernétiques,* Barlamane, 6 mai 2024, (Accessed: 20 avril 2025, at 23:00), available at: *https://www.barlamane.com/fr.*

[153] إلهام بنعلا، *"الآليات المؤسساتية للسياسة الجنائية في المجال المعلوماتي"*، مجلة المحيط القانوني الأكاديمي للدراسات والبحوث، العدد الثاني، المركز الأكاديمي للدراسات والبحوث - المملكة المغربية، مطبعة جزيرة التكنولوجيا الرباط، 2025، ص. 261.

التكوين والدعم التقني، فضلاً عن إجراء الافتحاصات الأمنية المنتظمة (***Security Audits***[154]) على البنيات المعلوماتية للإدارات[155].

- **مديرية نظم المعلومات المؤمنة:** تختص بتطوير الحلول المعلوماتية المؤمنة لفائدة الإدارات والمؤسسات العمومية، مع إجراء الدراسات البحثية وتحليل النظم لضمان تماشيها مع المعايير الدولية لحماية نظم المعلومات ضد الاختراقات والتهديدات المتطورة[156].

وتغطّي اختصاصاتها عموم الإدارة الحكومية. ومن أبرز مهامها الرسمية[157]:

- **تنسيق الاستراتيجية الوطنية:** تنسق عمل المصالح الوزارية والإدارات المختلفة لوضع وتنفيذ الاستراتيجية الوطنية للأمن السيبراني، وتتابع إحكام تطبيق توجهات اللجنة الاستراتيجية للأمن السيبراني.
- **التكوين والتوعية:** تُنظم الدورات التدريبية وبرامج التوعية للكوادر التقنية في الإدارات والمؤسسات العمومية، بغية رفع مستوى التأهب والوعي بالتهديدات السيبرانية.
- **إدارة التشفير والتوقيع الإلكتروني:** تصدر التراخيص والتصاريح المتعلقة بوسائل التشفير (الوسائل والمنتجات المشفرة)، وتقوم أيضاً بمنح الشهادات واعتماد أجهزة التوقيع الإلكتروني.
- **المراقبة التقنية:** تُكلف بمواكبة التقنيات الناشئة وتقييم المخاطر المرتبطة بها، إذ تقوم بمسح أخطار الأمن السيبراني واقتراح الابتكارات والتحديثات اللازمة لتعزيز الدفاع الإلكتروني.
- **التدقيق الأمني:** تُجري دورياً تدقيقاً أمنياً على نظم المعلومات في الإدارات العمومية والبنيات الحيوية، وفق نطاق تُحدده اللجنة الاستراتيجية، وتضع تقارير التقييم والتوصيات الواجبة لرفع مستوى الأمان.

---

154 مصطلح Security Audits يعني: *التدقيقات الأمنية أو افتحاصات الأمن السيبراني*. بمعنى أدق، هو عبارة عن عملية منهجية يتم فيها فحص وتحليل الأنظمة المعلوماتية (مثل الشبكات، الخوادم، قواعد البيانات، التطبيقات...) بهدف: التأكد من مدى امتثالها للمعايير الأمنية، رصد نقاط الضعف والثغرات، تقييم فعالية السياسات والإجراءات الأمنية المعتمدة، ثم اقتراح حلول أو إجراءات تصحيحية لتعزيز مستوى الأمان.

155 عزالدين بوزلماط، "دور المؤسسات الخاصة للتصدي للجريمة السيبرانية على الصعيدين الدولي والوطني"، مجلة القانون والأعمال، (تم الاطلاع عليه بتاريخ 28 أبريل 2025، على الساعة 03:30)، متاح عبر الرابط: *https://www.droitetentreprise.com*.

156 *مديرية نظم المعلومات المؤمنة* إحدى المديريات الأربع المكونة للمديرية العامة لأمن نظم المعلومات (DGSSI).

157 Op. cit, Taieb Debbagh, *15 Ans de Cybersécurité au Maroc*, p. 24

- **الإرشاد والمساعدة:** تقدم توصيات استشارية وتعاوناً فنياً للهيئات الحكومية والجهات العمومية بشأن حماية نظمهم المعلوماتية وتعزيزها.
- **رصد الحوادث السيبرانية:** تدير مركز الاستجابة الوطنية للحوادث السيبرانية (معروفًا باسم *maCERT*)، والذي يعمل على المراقبة الدائمة للشبكات الحكومية والكشف عن الهجمات الرقمية وتنسيق استجابة عاجلة لها.
- **تطوير الأنظمة الآمنة:** تشرف على وضع المواصفات والأدوات المطلوبة لإنشاء نظم معلومات مؤسساتية آمنة (نظم مشفرة ومحمية)، وتدعم الجهات العمومية في تنفيذها.

تمارس *DGSSI* بهذه المهام صلاحيات تشريعية وتنظيمية (اقتراح مشاريع نصوص قانونية وتنفيذها)، ورقابية وفنية (إصدار تراخيص واعتماد منتجات أمنية وإجراء تفتيشات أمنية)، ومساندة على صعيد التوعية والتأهب في مجال الأمن السيبراني. فعليًا، تعتمد الإدارة المغربية الخطوط التوجيهية الصادرة عن *DGSSI* عند تحصين شبكات الحكومة ومؤسساتها أمام الهجمات الإلكترونية.

ثانيا: اللجنة الوطنية لحماية المعطيات ذات الطابع الشخصي (*CNDP*)

أُحدثت اللجنة الوطنية لحماية المعطيات ذات الطابع الشخصي (*CNDP*) بمقتضى القانون رقم 09-08 الصادر شتنبر 2009، المتعلق بحماية الأشخاص الذاتيين تجاه معالجة معطياتهم الشخصية[158]. وتضطلع هذه اللجنة المستقلة بالمهمة الرئيسة المتمثلة في ضمان تطبيق قانون حماية البيانات الشخصية، بما يحقق حماية خصوصية المواطن وثقته الرقمية. من مهام وصلاحيات اللجنة[159]:

---

[158] مرسوم رقم 2.09.165 صادر في 25 من جمادى الأولى 1430 (21 ماي 2009) لتطبيق القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، المادة الأولى.

[159] اللجنة الوطنية لحماية المعطيات ذات الطابع الشخصي (*CNDP*) ولجنة الحق في الحصول على المعلومات (*CDAI*)، "بلاغ صحفي حول حماية المعطيات ذات الطابع الشخصي والحق في الحصول على المعلومات بالمغرب"، الرباط، 19 أبريل 2024.

- **التوعية والمواكبة:** تقوم *CNDP* بإعلام الأفراد بحقوقهم المنصوص عليها في القانون وتمكينهم من حماية معطياتهم الشخصية، إضافة إلى نشر الوعي العام بين المؤسسات حول كيفية التقيد بمعايير حماية البيانات[160].
- **الاستشارة والمساعدة:** تنصح اللجنة الأشخاص المعنيين ومسؤولي معالجة البيانات بالإجراءات العملية للامتثال للقانون، وتدعم الإدارات والشركات في تنفيذ الإجراءات الأمنية الملائمة والتدابير التقنية والتنظيمية[161].
- **الإشراف والمراقبة:** تشرف *CNDP* على قواعد البيانات الشخصية الكبرى، وتملك سلطة تقييم مدى امتثالها للمعايير القانونية. كما تنظر في الشكاوى المقدمة من متضررين، وتحقق في حالات التسريبات أو الاستخدام غير المشروع للبيانات.
- **الإعتماد وترخيص العمليات الخاصة:** تخضع بعض المعالجات الحساسة (مثل قواعد بيانات الصحة أو الأمن) لإجراءات خاصة، وتمنح اللجنة تراخيص أو تعطي رأيها القانوني حول معالجة تبادل المعطيات مع جهات أجنبية.
- **العقوبات والإنفاذ:** تخول لها صلاحيات إنفاذ القانون، حيث لها سلطة توقيع العقوبات على المخالفين. وينص القانون على غرامات مالية قد تصل إلى عشرات آلاف الدراهم والسجن في بعض الحالات، لضمان رادع فعّال ضد الانتهاكات.

بذلك، تمارس *CNDP* دورًا رقابيًا تنظيميًا (مراجعة ومراقبة عمليات المعالجة)، وكذلك دورًا توجيهيًا تثقيفيًا. ويعكس دورها الرسمي التزام المغرب بمعايير حماية البيانات العالمية[162]، وتشدد على التعاون بين القطاعين العام والخاص لإرساء بيئة رقمية آمنة[163]. على أرض الواقع، توجد مبادرات دورية لـ *CNDP* كإطلاق سجل حماية المعطيات الوطني[164]، وتفعيل برامج للتوعية بالشبكات الرقمية، وتعزيز التنسيق مع المؤسسات الأخرى لضمان الثقة الرقمية.

---

[160] *تقرير حماية المعطيات ذات الطابع الشخصي في إطار قطاع الأمن بالمغرب*، مركز دراسات حقوق الإنسان والديمقراطية ومركز جنيف للرقابة الديمقراطية على القوات المسلحة، الرباط، 19-20 أكتوبر 2015، ص. 24.

[161] *تقرير حماية المعطيات ذات الطابع الشخصي في إطار قطاع الأمن بالمغرب*، ص. 25.

[162] مجلس المستشارين، *مقترح قانون يقضي بإحداث الهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي*، رقم التسجيل 09، 20 يناير 2022، المملكة المغربية، المادة الاولى.

[163] DLA Piper, *Data Protection Laws of the World: Morocco*, 2025 Edition.

[164] *السجل الوطني لحماية المعطيات ذات الطابع الشخصي*، نسخة أولى، (اطلع عليه في: 23 أبريل 2025، على الساعة 06:00)، متوفر على رابط: *https://rn-pdp.cndp.ma*.

ثالثا: أجهزة الأمن (الأمن الوطني، الدرك الملكي، أجهزة الاستخبارات)

يظل الأمن السيبراني من صلب اختصاصات أجهزة الأمن التقليدية في المغرب، إذ يُعد الدفاع عن استقرار الوطن وحماية المواطنين من الجرائم الالكترونية امتدادًا لإطار اختصاصاتها الدستورية والقانونية. فالشرطة القضائية في المديرية العامة للأمن الوطني وجهاز الدرك الملكي[165] لهما وحدات متخصصة في مكافحة الجرائم المعلوماتية؛ حيث تقوم بالتحقيق في القضايا الجنائية الإلكترونية (مثل الاحتيال المالي الإلكتروني والاختراق ونشر المحتوى المحظور) وتقديم مرتكبيها للمحاكمة[166]. كما يشارك جهاز المخابرات الداخلي (المديرية العامة لمراقبة التراب الوطني) وذراع الاستخبارات الخارجية (المديرية العامة للدراسات والمستندات) في مكافحة التهديدات السيبرانية التي تمس الأمن القومي. عمليًا، يتعاون الجميع ضمن إطار تنسيقي؛ فعلى سبيل المثال تشكل هذه الأجهزة أعضاء في لجنة إدارة الأزمات السيبرانية الجسيمة[167] بمجرد حصول هجوم إلكتروني حاد، ما يؤكد الشراكة الأمنية الكاملة بين أجهزة الأمن وقطاع تكنولوجيا المعلومات.

رابعا: اللجنة الاستراتيجية للأمن السيبراني[168]

اللجنة الاستراتيجية للأمن السيبراني هي هيئة عليا تم إحداثها بموجب القانون 05.20 الصادر في يوليوز 2020 (والمنظم لاحقًا بالمرسوم التطبيقي رقم 2.21.406)، لتحل محل ما كان يسمى "اللجنة الإستراتيجية لأمن نظم المعلومات". وتختص هذه اللجنة برئاسة الوزير المنتدب لدى رئيس الحكومة المكلف بإدارة الدفاع الوطني، وتضم في عضويتها وزراء الداخلية والخارجية والاقتصاد والمالية والصناعة والاقتصاد الرقمي، إضافة إلى كبار مسؤولي القوات المسلحة وقائد الدرك الملكي وغيرهم. مهام اللجنة الاستراتيجية الرسمية تشمل:

---

165 مجلة الدرك الملكي، العدد 80، *"حماية الخصوصية أمام التهديدات السيبرانية"*، الرباط، 09 ماي 2024.

166 المديرية العامة للأمن الوطني: فضاء مغرب الثقة السيبرانية، متاح عبر: *www.cyberconfiance.ma* - البوابة الرسمية للوكالة المغربية للتنمية الرقمية، متاح عبر: *www.add.gov.ma* - المنصة الوطنية للتبليغ الإلكتروني، متاح عبر: *www.e-blagh.ma*.

167 م.س المادة 36 من القانون رقم 05.20 المتعلق بالأمن السيبراني.

168 م.س *الفرع الأول الخاص باللجنة الاستراتيجية للأمن السيبراني* - القانون رقم 05.20 المتعلق بالأمن السيبراني.

- **إعداد التوجهات الاستراتيجية:** تضع التوصيات الأساسية والاستراتيجية العامة للدولة في مجال الأمن السيبراني، وتعمل على ضمان استمرارية عمل وحماية نظم المعلومات لدى الهيئات الحكومية والبنيات التحتية الحيوية.
- **التقييم الدوري:** تجري اللجنة تقييمًا سنويًا لفعالية عمل المديرية العامة لأمن نظم المعلومات، وللجنة إدارة الأزمات السيبرانية الجسيمة المنصوص عليها في المادة 36 من القانون المذكور.
- **تحديد نطاق التفتيشات:** تحدد نطاق عمليات التفتيش والفحوص الأمنية (الافتتاحيات) التي تجريها *DGSSI* على نظم المعلومات في الإدارات والمؤسسات العامة.
- **تشجيع البحث والتوعية:** تساهم في دعم البحث والتطوير في مجال الأمن السيبراني، وتشجع برامج التكوين ورفع الوعي بالتهديدات الرقمية لدى الهيئات والمنشآت ذات الأهمية الحيوية.
- **الرأي القانوني:** تعطي اللجنة رأيًا استشاريًا في مشاريع القوانين والتنظيمات ذات الصلة بالأمن السيبراني قبل اعتماده.

يُظهر دور هذه اللجنة أنها تتداخل سياسيًا ورقابيًا مع مهام *DGSSI* و*CNDP* وغيرها، فتنسق الخطط العامة وتضبط أولويات العمل الوطني في الأمن الرقمي. فعلى سبيل المثال، صدرت أول استراتيجية وطنية للأمن السيبراني عام 2012[169] بإقرار اللجنة الاستراتيجية، ثم تحديثها لاحقًا للمرحلة 2023–2030. ويُطبّق دورها على أرض الواقع من خلال اجتماعات دورية لاستشراف المخاطر وبناء خطط وقاية، بالإضافة إلى إحاطة صناع القرار بتنظيم تدريبات مشتركة ومحاكاة لأزمات سيبرانية.

خامسا: لجنة إدارة الأزمات السيبرانية الجسيمة[170]

تستجيب المملكة المغربية أيضًا للطوارئ السيبرانية بهيئة متخصصة، هي لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة، التي أُحدثت وفقًا للمادة 36 من قانون 05.20. وتُعنى هذه

---

[169] Driss Abbadi, *"Morocco's cybersecurity strategy between challenges and aspirations*," International Journal of Information & Digital Security, Vol. 2, Issue 1, 2024, p. 30, Emirates Scholar Center for Research and Studies.

[170] *لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة، استنادًا إلى المادة 36* من القانون رقم 05.20 المتعلق بالأمن السيبراني، والمادة 6 من المرسوم رقم 2.21.406 الصادر بتاريخ 16 يوليو 2021، بشأن تطبيق أحكام القانون المذكور.

اللجنة بتنسيق مواجهة الحوادث الأمنية السيبرانية الكبرى بشكل منظم؛ فهي تضمن تضافر الجهود بين مختلف الأجهزة عند حدوث هجمات على البنى التحتية الحيوية أو مؤسسات الدولة. ووفقًا للمرسوم التطبيقي ذي الصلة، فإن اللجنة يرأسها المدير العام لـ *DGSSI* وتضم ممثلين عن وزارة الداخلية، والمفتشية العامة للقوات المسلحة الملكية، والدرك الملكي، والمديرية العامة للأمن الوطني (الشرطة)، والمديرية العامة لمراقبة التراب الوطني (الأمن المركزي).

وبناءً عليه، يلتقي في هذا التشكيل مسؤولو الأمن والقوات المسلحة والخبراء التقنيون لضمان تدخل استباقي عند وقوع أزمة سيبرانية[171]. في الممارسة العملية، يعقد أعضاء اللجنة اجتماعات طارئة لوضع بروتوكول مواجهة الأزمات – من العزل والتبليغ إلى استعادة الأنظمة المتضررة – بالإضافة إلى التنسيق مع قطاعات اقتصادية حيوية لتخفيف الأضرار. وتجدر الإشارة إلى أن الإطار القانوني لهذه اللجنة رسم بدقة مسؤولياتها وطرق عملها، ما أدى إلى تحسين ملموس في سرعة الاستجابة والتعاون بين الشركاء الأمنيين كلما ظهرت حادثة إلكترونية خطيرة.

الفقرة الثانية: دور القوات المسلحة الملكية في الأمن السيبراني والحروب السيبرانية

تزايدت أهمية الفضاء السيبراني كجزء من الأمن القومي المغربي، مما استدعى انخراط القوات المسلحة الملكية المغربية بشكل مباشر في تأمينه. ويُعد إشرافها على المديرية العامة لأمن نظم المعلومات، وتطوير قدراتها العملياتية والتعاون الدولي، تعبيرًا واضحًا عن تحول نوعي في العقيدة الدفاعية المغربية، التي باتت تعتبر الأمن السيبراني امتدادًا طبيعيًا للدفاع الترابي والسيادي.

أولا: دور القوات المسلحة الملكية المغربية (*FAR*) في الأمن السيبراني:

يشكل الأمن السيبراني ركيزة استراتيجية للأمن القومي المغربي، و القوات المسلحة الملكية المغربية (*FAR*) دورًا محوريًا في بناء وتعزيز هذا المجال الحيوي، لاسيما عبر إشرافها

[171] *لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة*، تاريخ الاطلاع: 28 أبريل 2025.على ساعة 16.30، متاح عبر الرابط: *https://www.dgssi.gov.ma*.

المباشر على المديرية العامة لأمن نظم المعلومات(*DGSSI*) ، وتطوير قدرات دفاعية وهجومية، بالتعاون مع شركاء دوليين مثل الولايات المتحدة الأمريكية والأردن.

يعد إشراف القوات المسلحة الملكية على *DGSSI* واحدًا من أبرز مظاهر التداخل بين الأمن الدفاعي التقليدي والأمن الرقمي. تأسست هذه المديرية سنة 2011 وتخضع إداريًا وتنظيميًا للقيادة العليا للقوات المسلحة الملكية المغربية، مما يرسخ انخراط *FAR* القوات المسلحة الملكية المغربية المباشر في صياغة وتنفيذ الاستراتيجية الوطنية للأمن[172].

القوات المسلحة الملكية المغربية لها دور المشرف الاستراتيجي على حماية البنية التحتية الرقمية الحيوية (*IIV*) وحماية الأنظمة الحساسة (*SIS*)، من خلال المركز الوطني للاستجابة لحوادث الحاسوب (*maCERT*)، إضافةً إلى إنشاء مركز عمليات الأمن السيبراني الوطني (*National SOC*)الذي يعمل على مدار 7/24 لمراقبة التهديدات السيبرانية والرد عليها.

في سنة 2023، أثبتت القوات المسلحة عبر *DGSSI* فاعلية عملياتية ملحوظة، حيث نجحت في صد حوالي 150 هجومًا سيبرانيًا وإصدار أكثر من 400 نشرة أمنية موجهة إلى مختلف القطاعات الحكومية والخاصة[173]. هذا الأداء يعكس تطور قدرات الدفاع الرقمي الوطني تحت إشراف القوات المسلحة الملكية المغربية ، كما يظهر مدى نجاعة منظومة الرصد والتصدي للحوادث.

ضمن سياق تأمين الفضاء الرقمي الوطني، أطلقت القوات المسلحة الملكية المغربية عملية مراجعة شاملة للاستراتيجية الوطنية للأمن السيبراني. تضمنت وضع بروتوكولات لإدارة الأزمات الرقمية الكبرى، وإنشاء لجان مختصة داخل المؤسسات السيادية لإدارة الحوادث عند وقوعها[174].

على المستوى الدولي، لم تقتصر جهود القوات المسلحة الملكية المغربية على النطاق الداخلي، بل سعت إلى تعزيز التعاون السيبراني مع قوى عسكرية كبرى. ضمن هذا الإطار، شارك جنود مغاربة من القوات المسلحة في تدريبات مشتركة مع جنود أمريكيين من الكتيبة الحادية

---

[172] م.س المديرية العامة لأمن نظم المعلومات (*DGSSI*) 2023 ، *"استراتيجية المغرب الوطنية للأمن السيبراني 2030"*.

[173] *" وحدة خاصة في الجيش المغربي تعزز دفاعات المملكة ضد الهجمات السيبرانية"* 2024 ، تم الاطلاع عليه بتاريخ 26 أبريل 2025، على الساعة 01:45 منشور على موقع مغرس. رابط: *https://www.maghress.com*

[174] م.س 2023، *"استراتيجية المغرب الوطنية للأمن السيبراني 2030"*.

عشرة للعمليات السيبرانية خلال تمرين .« *African Lion 2024* » ركز التدريب على أساسيات الحرب السيبرانية، وتقنيات الهجوم والدفاع عبر الفضاء الرقمي[175].

تضمن التدريب تمارين متقدمة حول كيفية استخدام أنظمة مثل *"Beast+"* لرصد الإشارات الإلكترونية وتحديد مواقع مصادرها، مما ساهم في رفع جاهزية القوات المسلحة الملكية المغربية في التعامل مع الهجمات التي تستهدف الطيف الكهرومغناطيسي الحيوي للعمليات السيبرانية والعسكرية[176].

علاوةً على التعاون مع الولايات المتحدة، شهد عام 2023 تعزيز العلاقات المغربية الأردنية في مجال الأمن السيبراني، عبر لقاءات رسمية هدفت إلى تبادل الخبرات وتنسيق السياسات الدفاعية الإلكترونية[177] .

على الصعيد الإقليمي والدولي، احتل المغرب المرتبة 50 عالميًا ضمن المؤشر العالمي للأمن السيبراني لعام 2021، متقدمًا من المرتبة 93 سنة 2018[178].ويعزى هذا التقدم إلى الجهود المتواصلة للقوات المسلحة الملكية في مجال الأمن السيبراني عبر تطوير الموارد البشرية، تحديث البنية التحتية السيبرانية، وتعزيز الوعي المؤسسي.

من الناحية المؤسساتية، تبرز *DGSSI* كجهة وطنية منوط بها تنسيق الجهود الدفاعية السيبرانية، وتضع ضمن أولوياتها حماية المؤسسات السيادية مثل الوزارات، البنوك المركزية، المؤسسات الأمنية، وشبكات الطاقة. إضافة إلى ذلك، تدير القوات المسلحة الملكية المغربية مشاريع تعزيز المرونة السيبرانية من خلال تمارين محاكاة الهجمات *(cyber crisis*

---

[175] Alisha Grezlik, "*U.S. Soldiers train Moroccan partners in cyber operations*," DVIDS – Defense Visual Information Distribution Service, April 19, 2024. Consulted on April 27, 2025, at 02:18 AM. Available at: *https://www.dvidshub.net.*

[176] The United States Army, *"Cyber Soldiers support Moroccans in electronic warfare training"*, April 22, 2024. Consulted on April 22, 2025, at 02:20 AM. Available at: *https://www.army.mil.*

[177] القوات المسلحة الأردنية – الجيش العربي، *"تدريب مشترك في الأمن السيبراني بين القوات المسلحة الأردنية والقوات المسلحة الملكية المغربية"*، الموقع الرسمي للقوات المسلحة الأردنية، تم الاطلاع عليه بتاريخ 29 أبريل 2025، على الساعة 02:30 صباحًا. متاح عبر الرابط: *https://www.jaf.mil.jo*.

[178] الاتحاد الدولي للاتصالات (*ITU*)، *"المؤشر العالمي للأمن السيبراني 2021"*.

exercises) التي تستهدف اختبار قدرات الفاعلين الوطنيين في الاستجابة السريعة والمنظمة[179].

وفي إطار تعزيز بنيتها الدفاعية، توجهت القوات المسلحة الملكية المغربية إلى إرساء نظام إدارة المخاطر السيبرانية لدى القطاعات الحيوية عبر مقاربة معيارية تستند إلى تحليل المخاطر وتحديد أولويات الحماية، بما يتماشى مع أفضل المعايير الدولية مثل NIST و ISO 27001[180].

جدير بالذكر أن القوات المسلحة الملكية المغربية تتعامل مع الأمن السيبراني باعتباره بُعدًا تكامليًا من أبعاد الدفاع الوطني، حيث لم يعد الصراع يقتصر على الميدان التقليدي (البري، البحري، الجوي)، بل أصبح الفضاء السيبراني يشكل ميدانًا مستقلاً يتطلب تحصينات دفاعية وهجومية متطورة[181]).

في إطار تعزيز قدراتها في مجال الأمن السيبراني، تعمل القوات المسلحة الملكية المغربية (FAR) على دمج تقنيات الذكاء الاصطناعي ضمن استراتيجيتها الدفاعية الرقمية. ومع تعاظم التهديدات السيبرانية وظهور فاعلين غير حكوميين يستغلون إمكانات الذكاء الاصطناعي في شن الهجمات، أصبح من الضروري تطوير وسائل مراقبة وتحليل تعتمد على تقنيات ذكية، تُمكّن من كشف الهجمات وإحباطها بفعالية أكبر. وفي هذا السياق، تركز الجهود الوطنية على بناء منظومات دفاع سيبراني قادرة على حماية البنية التحتية الرقمية الحيوية وضمان السيادة المعلوماتية للبلاد، مع اعتماد الذكاء الاصطناعي كعنصر استباقي في منظومة الأمن السيبراني العسكري، كما تم التأكيد عليه خلال فعاليات منتدى الرباط رفيع المستوى حول الذكاء الاصطناعي والأمن الرقمي[182].

---

[179] Revue des Forces Armées Royales (FAR), « *L'intelligence artificielle au service de la défense* », n° 420, février-mars 2024, p. 26.

[180] م.س 2023، *"استراتيجية المغرب الوطنية للأمن السيبراني 2030"*.

[181] *Guerre numérique: les Forces Armées Royales sur tous les fronts*, Le360, 19 janvier 2024, consulté le 24 avril 2025 à 02h15, disponible sur: *https://fr.le360.ma.*

[182] Revue des FAR, "*Rôle de l'IA dans la Défense et la Cybersécurité",* Édition 422, 2024, p. 79.

وفي مجال تطوير الكفاءات، أطلقت *FAR* برامج متخصصة لتكوين الكوادر البشرية في الأمن السيبراني، بالتعاون مع جامعات ومعاهد وطنية وعالمية. هذا التوجه يسعى إلى سد الخصاص في الموارد المؤهلة والذي يمثل أحد أكبر التحديات في المشهد السيبراني الوطني[183].

وفي الجانب التشريعي، أسهمت القوات المسلحة عبر *DGSSI* في بلورة الإطار القانوني الوطني المنظم للأمن السيبراني، خصوصًا عبر دعم إعداد مشاريع القوانين والأنظمة المتعلقة بحماية المعطيات الحساسة، حماية البنية التحتية المعلوماتية، وإلزامية التبليغ عن الحوادث السيبرانية[184].

هكذا، يتجلى بوضوح أن القوات المسلحة الملكية المغربية أصبحت فاعلًا أساسيًا في الأمن السيبراني الوطني، من خلال الإشراف الاستراتيجي، التنفيذ العملياتي، التعاون الدولي، بناء القدرات البشرية والتكنولوجية، والدفع نحو تطوير منظومة الحماية القانونية والمؤسساتية.

ختامًا، فإن دور القوات المسلحة الملكية المغربية في الأمن السيبراني يعكس تحولًا استراتيجيًا عميقًا في العقيدة الدفاعية المغربية، حيث بات الفضاء الرقمي ميدانًا متقدمًا للدفاع عن السيادة الوطنية، ومجالاً تنافسيًا لتعزيز المكانة الإقليمية والدولية للمملكة المغربية في عصر التحولات التكنولوجية السريعة.

ثانيا: دور القوات المسلحة الملكية المغربية في الحروب السيبرانية

أصبحت الحروب السيبرانية جزءًا لا يتجزأ من استراتيجيات الأمن القومي للدول. القوات المسلحة الملكية المغربية (*FAR*)، كجزء من المنظومة العسكرية للمملكة المغربية، تمتلك القدرة النظرية على المشاركة في هذه الحروب، سواء دفاعيًا أو هجوميًا، وفقًا لإطار دليل طالين 2.0[185]. يهدف هذا الجزء من البحث إلى تحليل دور القوات المسلحة الملكية المغربية كفاعل محتمل في الحروب السيبرانية.

---

[183] مرجع سابق، "*وحدة خاصة في الجيش المغربي تعزز دفاعات المملكة ضد الهجمات السيبرانية*" 2024.

[184] م.س 2023، "*استراتيجية المغرب الوطنية للأمن السيبراني 2030*".

[185] دليل تالين 2.0 (*Tallinn Manual 2.0*) هو مرجع أكاديمي غير ملزم قانونيًا، يهدف إلى توضيح كيفية تطبيق القانون الدولي على العمليات السيبرانية، سواء في أوقات السلم أو النزاعات المسلحة. تم تطوير هذا الدليل من قبل مجموعة دولية

أ – دليل طالين للحروب السيبرانية

يوفر دليل طالين 2.0 إطارًا قانونيًا شاملًا لتنظيم العمليات السيبرانية، سواء في أوقات السلم أو النزاعات المسلحة. من أبرز القواعد التي يجب على الدول، بما في ذلك المغرب، مراعاتها[186]:

- **السيادة (القاعدة 4):** العمليات السيبرانية التي تتدخل في السيادة الوطنية لدولة أخرى دون موافقتها تُعتبر انتهاكًا للقانون الدولي. لا يُشترط وجود آثار مادية للانتهاك، ولكن يجب أن تكون العملية قابلة للنسبة إلى دولة.
- **التمييز (القاعدتان 92 و93):** في حالة النزاع المسلح، يجب على الدول التمييز بين الأهداف العسكرية والمدنية في العمليات السيبرانية. الأهداف المدنية، مثل المستشفيات أو المدارس، لا يجوز استهدافها.
- **الضرورة (القاعدتان 69 و100):** يجب أن تكون أي عملية قوة، بما في ذلك السيبرانية، ضرورية لتحقيق هدف عسكري مشروع. في سياق العمليات العسكرية، يجب أن تكون العملية ضرورية لتحقيق مساهمة فعالة في العمل العسكري.
- **التناسب (القاعدتان 71 و113):** يجب ألا تسبب العمليات السيبرانية أضرارًا جانبية مفرطة للمدنيين أو الأهداف المدنية مقارنة بالميزة العسكرية المتوقعة. كما يجب أن يكون الرد متناسبًا مع الهجوم الأصلي، وفقًا للمادة 51 من ميثاق الأمم المتحدة.

ب – مثال بارز في الحروب السيبرانية:

في يونيو 2017، شهدت أوكرانيا واحدة من أكثر الهجمات السيبرانية تدميرًا في التاريخ الحديث، والتي تُعرف باسم *NotPetya* ورغم أن الهجوم اتخذ شكل برمجية فدية (*ransomware*)[187]، إلا أن تحليلات أمنية كشفت أنه لم يكن يهدف إلى طلب فدية حقيقية،

من الخبراء القانونيين بدعوة من مركز التميز للتعاون في الدفاع السيبراني التابع لحلف الناتو (*NATO CCDCOE*)، ونُشر في عام 2017 عن طريق دار نشر جامعة كامبريدج.

[186] Tallinn Manual on *the International Law Applicable to Cyber Warfare*, prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, edited by Michael N. Schmitt, Cambridge University Press, 2013, (Rules 6-92-93-69-100-71-113).

[187] Ransomware (برمجيات الفدية) هو *نوع من البرمجيات الخبيثة* (malware) يقوم بتشفير ملفات أو أنظمة الضحية، ويطلب مبلغًا ماليًا (فدية) مقابل استرجاع الوصول إلى البيانات.

بل كان غرضه الوحيد هو **إحداث دمار شامل في البنية التحتية الرقمية للدولة المستهدفة.** هذا الهجوم الذي نُسب لاحقًا إلى جهات مدعومة من الدولة الروسية، استغل ثغرة أمنية تُعرف باسم"*EternalBlue*" ، والتي كانت قد سُرّبت من وكالة الأمن القومي الأمريكية (*NSA*[188]) ما يجعل هذه الحادثة ذات دلالة استراتيجية هو أنها تجاوزت الهجمات التقليدية ذات الطابع التجسسي أو التخريبي المحدود، إلى استخدام الفضاء السيبراني كأداة حربية صريحة تستهدف مؤسسات الدولة والقطاع الخاص معًا، بما في ذلك أنظمة المعاشات، شبكات البنوك، **والبنى التحتية الحيوية**[189].

يشكّل هذا النموذج حالة دراسية مركزية لفهم كيفية توظيف العمليات السيبرانية في الصراعات الجيوسياسية، حيث لا تُعدّ فقط وسيلة لإرباك العدو أو شل قدراته العسكرية، بل تُستخدم لضرب الاستقرار الاقتصادي والاجتماعي. وتُبرز هذه الحالة الحاجة إلى استراتيجيات دفاعية وطنية تقوم على الاستباق، التحليل المستمر للتهديدات، وبناء القدرات المحلية في الأمن السيبراني، **وهي عناصر يُفترض أن تتكامل ضمن العقيدة الدفاعية السيبرانية للقوات المسلحة في أي دولة، بما فيها المغرب.**

خاتمة الفصل:

تناول الفصل الأول الإطار النظري والمؤسساتي للأمن السيبراني وحماية البنية التحتية الرقمية، من خلال تحليل معمق لمفهوم الأمن السيبراني في أبعاده التقنية والقانونية والسيادية، وكذا لمكانته ضمن مكونات الأمن القومي المغربي. وقد أبرز هذا الفصل الأهمية الاستراتيجية للبنية التحتية الرقمية في تفعيل وظائف الدولة الحديثة، ودورها في دعم القطاعات الحيوية من دفاع واقتصاد وخدمات اجتماعية ودبلوماسية وبيئية، مع الوقوف عند المؤشرات الرقمية الدالة على تطور الأداء المؤسساتي في هذا المجال، وفي مقدمتها مؤشر تنمية الحكومة الإلكترونية. كما عالج الفصل المكونات الأساسية للأمن السيبراني، من توافر وسلامة وسرية

---

188 الوكالة الوطنية للأمن (National Security Agency - NSA)، هيئة تابعة لوزارة الدفاع الأمريكية تأسست سنة 1952، وتُعنى بجمع وتحليل المعلومات الاستخباراتية المستندة إلى الإشارات والاتصالات (SIGINT)، كما تُشرف على تأمين شبكات الحكومة الأمريكية ضد التهديدات السيبرانية، *وتُعد من أبرز الجهات الفاعلة في مجال الحرب السيبرانية العالمية.*

189 Nicole Perlroth, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race* (New York: Bloomsbury Publishing, 2021), 18.

وإثبات، مبرزاً التفاعل بين الأبعاد التقنية والتنظيمية في بناء منظومة حماية فعالة. وعلى الصعيد القانوني، تم استعراض وتحليل الترسانة التشريعية المغربية المؤطرة للأمن السيبراني، وفي مقدمتها القانون 05.20، إلى جانب النصوص المكملة له، مع تقييمٍ لنجاعتها ومواكبتها للتحولات الرقمية المتسارعة، بالإضافة إلى تفكيك البنية المؤسساتية القائمة، وأدوار الهيئات الفاعلة في حماية الفضاء السيبراني، لا سيما المديرية العامة لأمن نظم المعلومات واللجنة الوطنية لحماية المعطيات الشخصية وأجهزة الأمن الوطني. ويُمهّد هذا التأسيس النظري والمؤسساتي للانتقال في الفصل الثاني إلى دراسة التحديات السيبرانية الراهنة التي تواجه المغرب، سواء في شكل تهديدات رقمية أو هشاشة بنيوية، مع تحليل استراتيجيات الحماية الوطنية، واستقراء التجارب الدولية الرائدة التي يمكن استلهامها لتعزيز الأمن السيبراني المغربي في أبعاده السيادية والتنموية.

الفصل الثاني: التحديات السيبرانية واستراتيجيات الحماية في المغرب

يشهد المغرب، على غرار العديد من الدول، تصاعدًا لافتًا في التهديدات السيبرانية التي تستهدف بنيته الرقمية ومؤسساته الحيوية، مما يسلّط الضوء على هشاشة البنية التحتية المعلوماتية، وضعف التنسيق المؤسساتي، ومحدودية الإطار القانوني في مجاراة التحديات الرقمية المتسارعة. أمام هذا الواقع، لم يعد من الممكن التعاطي مع الأمن السيبراني بوصفه شأناً تقنياً محضاً، بل غدا مكوّناً أساسياً من مكونات السيادة الوطنية والاستقرار الداخلي. وعليه، يتناول هذا الفصل التحديات السيبرانية واستراتيجيات الحماية في المغرب من خلال مبحثين متكاملين: يُخصص المبحث الأول لتحليل التهديدات ونقاط الضعف في البنية الرقمية الوطنية، سواء من حيث طبيعة الهجمات أو مكامن القصور القانوني والتقني والمؤسساتي، فيما يركّز المبحث الثاني على استشراف آفاق التطوير عبر دراسة التجارب الدولية الرائدة واستلهام عناصر القوة القابلة للتكييف مع الخصوصية المغربية، مع اقتراح آليات وطنية لتعزيز المناعة السيبرانية وتحقيق السيادة الرقمية المستدامة.

المبحث الأول: البنية الرقمية الوطنية، التهديدات ونقاط الضعف

تكشف قراءة الوضع الراهن في المغرب عن مجموعة من التحديات الهيكلية التي تعيق إرساء منظومة سيبرانية متماسكة وقادرة على مواجهة التهديدات الرقمية المتصاعدة. فالهجمات الإلكترونية التي استهدفت مؤسسات استراتيجية خلال السنوات الأخيرة عرّت هشاشة البنية الرقمية الوطنية، وأظهرت اختلالات تقنية وأمنية يصعب التغاضي عنها. وفي موازاة ذلك، يعاني الإطار القانوني والحكامة المؤسساتية من ثغرات بنيوية تؤثر بشكل مباشر على فعالية الاستجابة الوطنية، كما تبرز محدودية في الثقافة الأمنية لدى الأفراد والفاعلين، وضعفًا في التنسيق بين الهيئات المعنية، وغيابًا لمقاربات شمولية قائمة على الاستباق والتحصين المستدام. في هذا السياق، يتناول هذا المبحث تحديات الأمن السيبراني في المغرب من خلال مطلبين مترابطين: يرصد الأول طبيعة التهديدات السيبرانية التي استهدفت البنية التحتية الرقمية، ويُعالج الثاني أبرز أوجه القصور التي تعيق بناء منظومة دفاع سيبراني فعّالة، سواء من الناحية القانونية أو التقنية أو التنسيقية.

المطلب الأول: التهديدات السيبرانية التي تواجه البنية التحتية الرقمية

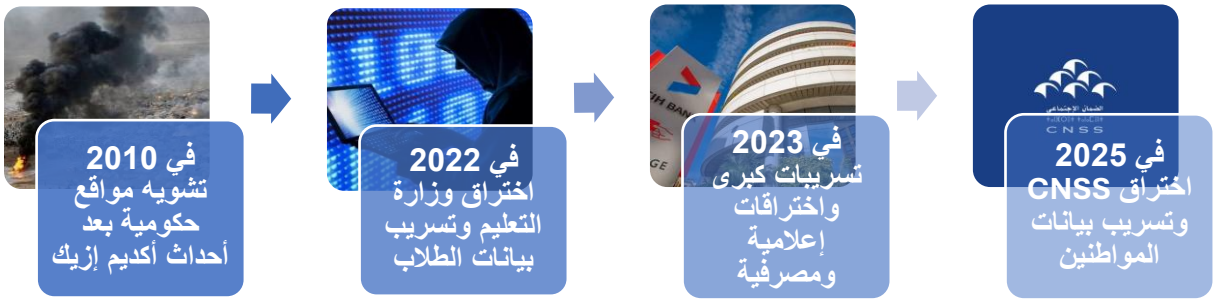
تُظهر التطورات الأخيرة في المشهد السيبراني المغربي أن البنية الرقمية الوطنية باتت هدفًا متكررًا لهجمات إلكترونية متزايدة في الحدة والتعقيد، مما يؤشر على تغير نوعي في طبيعة المخاطر التي تواجه الدولة. فالهجمات لم تعد عشوائية أو فردية، بل اتخذت طابعًا ممنهجًا يرتبط أحيانًا بصراعات إقليمية، وأحيانًا أخرى بدوافع إجرامية ذات طابع مالي أو استخباراتي. وعليه، يعالج سيتم تقسيم هذا المطلب إلى فقرتين: الفقرة الأولى، يتم رصد وتحليل أبرز الهجمات التي استهدفت المغرب، مع التمييز بين الهجمات السياسية، والإجرامية، وتلك التي مست القطاع الخاص والمجتمع المدني؛ وفي الفقرة الثانية، تُناقش الانعكاسات الأمنية والاقتصادية لهذه التهديدات، من خلال إبراز أثرها على الأمن الوطني والسيادة الرقمية، وكذا على الثقة العامة والنمو في الاقتصاد الرقمي الوطني.

الفقرة الأولى: أبرز الهجمات التي استهدفت المغرب

شهدت المملكة المغربية في السنوات الأخيرة تصاعدًا ملحوظًا في وتيرة وخطورة الهجمات السيبرانية التي تستهدف مختلف القطاعات، وبالأخص مؤسسات الدولة والبنية التحتية الرقمية الحيوية. يأتي هذا التصاعد في سياق إقليمي متوتر، حيث تُستغل الهجمات الإلكترونية كواجهة جديدة للصراع الجيوسياسي، لاسيما في ظل التوتر المزمن بين المغرب والجزائر حول قضية الصحراء المغربية[190]. وإلى جانب الدوافع السياسية، يواجه المغرب أيضًا هجمات ذات دوافع إجرامية ومالية تستهدف المصالح الاقتصادية والبيانات الحساسة للمؤسسات والمواطنين. وقد صنّفت تقارير دولية المغرب ضمن البلدان الأفريقية الأكثر تعرضًا للهجمات الإلكترونية؛ فقد

[190] CYFIRMA. *Decoding Cyberattacks on Morocco*. Published on November 28, 2024. Accessed on May 01, 2025 at 22:17. Available at: *https://www.cyfirma.com*.

كشف تقرير حديث **لشركة كاسبرسكي**[191] أن المغرب جاء في طليعة دول أفريقيا المستهدفة بالجرائم السيبرانية إلى جانب كينيا ونيجيريا وجنوب أفريقيا[192].



أولا: الهجمات على مؤسسات الدولة والبنية التحتية الحيوية

تعرّضت مواقع ومنصات حكومية مغربية لهجمات سيبرانية متكررة كان لها صدى واسع نظرًا لطبيعتها الحساسة. كثير من هذه الهجمات ارتبطت بسياقات سياسية وصراعات إقليمية. فمنذ مطلع العقد الماضي، بدأت حرب سيبرانية غير معلنة بين قراصنة مغاربة وجزائريين، تزايدت حدتها مع كل أزمة سياسية بين البلدين. على سبيل المثال، عقب أحداث أكديم إزيك 2010 التي شهدت توترًا أمنيًا في الصحراء المغربية، قام قراصنة مغاربة باختراق مواقع تابعة لوزارة الداخلية الجزائرية ومؤسسات حكومية أخرى انتقامًا. وردّ نظراؤهم الجزائريون بهجمات مضادة شملت تشويه عشرات المواقع المغربية وترك رسائل عدائية. واستمرت هذه المناوشات السيبرانية خلال العقد 2010–2020 بوتيرة متقطعة، حيث استهدف القراصنة المغاربة مواقع حكومية وإعلامية جزائرية للتأكيد على موقف الرباط في قضايا سيادية، في حين رد القراصنة الجزائريون بهجمات على مواقع مغربية بما فيها مواقع مؤسسات والمقاولات العمومية. هذه الهجمات المتبادلة – التي وُصفت بأنها "حرب سيبرانية" بين البلدين – بلغت ذروتها مؤخرًا مع تفجر الخلافات الدبلوماسية، مما أعطى بعدًا جديدًا للتهديدات الرقمية في المغرب[193].

---

[191] كاسبرسكي (*Kaspersky*): شركة روسية عالمية متخصصة في أمن المعلومات والأمن السيبراني، تأسست عام 1997 على يد "يوجين كاسبرسكي". تُعد من أبرز الشركات العالمية في مجال تطوير برامج مكافحة الفيروسات، وأنظمة الحماية من التهديدات الرقمية، وتأمين الشبكات والبنى التحتية الحيوية. توفر حلولها لملايين المستخدمين في أكثر من 200 دولة، وتشمل خدماتها أيضًا الأمن السيبراني الصناعي، ومراكز الاستجابة للحوادث السيبرانية، والتحليل الاستخباراتي للتهديدات.

[192] TELQUEL. *Le Maroc parmi les pays africains les plus ciblés par les cyberattaques, selon Kaspersky*, Instant T, 16 avril 2025, consulté le 02 mai 2025 à 01h32, disponible *sur : https://telquel.ma.*

[193] BABAS, Latifa. *Cyberattacks: The new frontline in the Morocco-Algeria rivalry*, Yabiladi, 9 April 2025, consulted on 02 May 2025 at 02h52, available at: *https://en.yabiladi.com.*

ومن أبرز الهجمات السيبرانية التي استهدفت مؤسسات الدولة مباشرةً الهجوم واسع النطاق الذي تعرض له الصندوق الوطني للضمان الاجتماعي (*CNSS*) في أبريل 2025، والذي اعتبره مراقبون أكبر خرق بيانات في تاريخ المغرب السيبراني[194]. في هذه العملية تمكن قراصنة من اختراق أنظمة *الـ CNSS* وتسريب عشرات آلاف الملفات التي تحوي بيانات شخصية حساسة لملايين المواطنين. ووفق تقارير رسمية، فقد نُشر على قناة تلغرام نحو 54 ألف ملف *PDF* تضم معلومات عن حوالي 2 مليون مواطن ونحو 500 ألف شركة مسجلة في نظام الضمان الاجتماعي. شملت البيانات المسرّبة أسماء وأرقام بطاقات الهوية الوطنية وأرقام التسجيل في الضمان الاجتماعي ورواتب موظفين وتصاريحهم المالية، مما كشف مدى خطورة الاختراق[195]. وقد تبنّت مجموعة تطلق على نفسها "جباروت *JabaROOT*" – مسؤولية الهجوم، معلنةً أنه جاء كرد على ما وصفته بـ"المضايقات الرقمية" الجزائرية المزعومة من طرف المغرب[196]. ونشر القراصنة رسالة تهديد مفادها أنهم سيصعّدون الهجمات ما لم يتوقف المغرب عن استهداف المنصات الجزائرية[197]. تجدر الإشارة إلى أن موقع وزارة العمل المغربية تعرّض أيضًا للتخريب (*Defacement*) في نفس الفترة على يد المجموعة نفسها، حيث تم اختراق واجهة الموقع ونشر شعارات سياسية قبل أن يتم تعطيله. وعلى إثر هذه التطورات، وصفت الحكومة المغربية تلك الهجمات بأنها "عمل إجرامي تقف وراءه جهات معادية" تستهدف أمن المملكة واستقرارها. وأكد مسؤولون مغاربة أن مثل هذه العمليات العدائية تأتي انتقامًا للتقدم الدبلوماسي الذي يحرزه المغرب في قضية الصحراء المغربية، ومحاولةً لعرقلة نجاحاته على الساحتين الإقليمية والدولية[198].

---

[194] ZECURION. *Major Data Breach at Morocco's CNSS: A Deep Dive*, publié le 15 avril 2025, consulté le 02 mai 2025 à 04h10, disponible sur: *https://zecurion.com.*

[195] *K36*، *"اختراق سيبراني ثان وخطير في تاريخ المغرب. قراصنة جزائريون يهاجمون CNSS ويسربون بيانات ملايين المواطنين"*، منشور في 9 أبريل 2025، تم الاطلاع عليه بتاريخ 03 ماي 2025 على الساعة 14:55، متوفر على الرابط: *https://k36.ma.*

[196] Daryna Antoniuk. *"Morocco investigates major data breach allegedly by Algerian hackers"*, The Record by Recorded Future, April 11, 2025. Accessed May 03, 2025, at 18:15. Available at: *https://therecord.media*.

[197] Sam Metz. *"Hackers breach Morocco's social security database in an unprecedented cyberattack,"* The Associated Press (AP), April 10, 2025. Accessed May 03, 2025 at 21:10. Available at: *https://apnews.com.*

[198] مرجع سابق، بوابة المغرب. السيد بايتاس يصف الهجمات السيبرانية التي استهدفت مؤسسات وطنية في هذا التوقيت المشبوه بـ"الفعل الإجرامي".

لم تقتصر الاختراقات على مؤسسة الضمان الاجتماعي؛ فقد طالت الهجمات السيبرانية عدة وزارات وهيئات حكومية أخرى. في أواخر عام 2022، تعرضت قاعدة بيانات وزارة التعليم العالي والبحث العلمي لخرق كبير أدى إلى تسريب معلومات شخصية واسعة النطاق. بدأت الواقعة بقيام مجموعة قراصنة (يُرجح أنها ذات دوافع إجرامية) بنشر ملف يحوي بيانات قرابة مليون طالب مغربي على أحد الأسواق السوداء الإلكترونية. وبعد أيام قليلة فقط، ظهرت مجموعة قراصنة أخرى محسوبة على الجزائر استغلت نفس الثغرة لتخترق المنظومة بشكل أعمق، وتقوم بتسريب قاعدة البيانات الكاملة للوزارة بما في ذلك 23 جدولًا تضم معلومات الطلاب والموظفين[199]. كشفت التحقيقات أن البيانات المكشوفة تشمل الأسماء الكاملة وتواريخ الميلاد وأرقام البطاقات الوطنية ومعرفات الطالب (*Massar*)، بالإضافة إلى معلومات موظفي الجامعات بما فيها البيانات البنكية. وتبيّن أن تلك القاعدة الإلكترونية كانت معروضة للبيع في البداية مقابل مبلغ زهيد (~30 يورو)، قبل أن تُنشر مجانًا للعامة. هذا الاختراق أثار انتقادات لاذعة حول ضعف التأمين السيبراني في المنصات التعليمية الرسمية، لا سيما أن الوزارة المعنية لم تصدر أي بيان توضيحي أو تحذيري بعد الحادثة. وقد اعتبر خبراء أمنيون هذا الحادث دليلًا على "فشل ذريع" في حماية البيانات الأكاديمية، مما يضع مسؤولية معنوية كبيرة على عاتق الجهات الوصية لضمان عدم تكرار مثل هذه الكارثة[200].

وفي سياق متصل، تعرّضت منصات ثقافية وإعلامية رسمية لهجمات سيبرانية كان الهدف منها إحداث اضطراب وإيصال رسائل سياسية. من ذلك ما وقع في يناير 2023 عندما تم اختراق موقع المكتبة الوطنية للمملكة المغربية (*BNRM*) من قبل قراصنة يُعتقد أنهم جزائريون، حيث تركوا رسالة تحدٍّ موجهة إلى المخترقين المغاربة مطالبين إياهم بوقف هجماتهم حتى يتوقف الجانب الآخر بدوره[201]. وأسفرت هذه العملية عن نشر بيانات سرية تتعلق بنحو مليون طالب (يُحتمل أنها مرتبطة بوزارة التعليم) على الإنترنت، تلتها ردود انتقامية تمثلت في

---

[199] AfricaCyberMag. *Le Ministère de l'éducation nationale du Royaume du Maroc touché deux fois par une fuite de données*, 28 décembre 2022. Consulté le 03 mai 2025 à 11h35, disponible sur: *https://cybersecuritymag.africa.*

[200] Kabiri Kettani, Mounia. *Les données du ministère de l'enseignement supérieur auraient-elles fuité ?, L'Observateur du Maroc et d'Afrique*, 21 décembre 2022. Consulté le 03 mai 2025 à 20h07, disponible sur: *https://lobservateur.info.*

[201] يوسف يعكوبي. *"المغرب يحقق في عملية 'قرصنة جزائرية' لموقع المكتبة الوطنية"*. هسبريس، 4 يناير 2023. تم الاطلاع عليه في 03 ماي 2025، على الساعة 12:34، على رابط التالي: *https://www.hespress.com*.

تسريب آلاف السجلات الخاصة بطلاب جزائريين، في تصعيد متبادل خطير[202]. كما استُهدفت مواقع وكالة المغرب العربي للأنباء (*MAP*) الرسمية بهجمات حجب خدمة *DDOS* في 2023، أدت إلى تعطيل منافذها الإعلامية لفترة قصيرة[203]. ويُذكر أن هذه الهجمات جاءت على خلفية توترات إقليمية، حيث تبنّى القراصنة شعارات مرتبطة بالخلافات السياسية في المنطقة[204].

إلى جانب الهجمات ذات الطابع السياسي، شهدت البنية التحتية الرقمية الحيوية في المغرب حوادث اختراق ذات طابع إجرامي وتقني متطور. فقد كشفت تقارير أمنية عن ثغرات خطيرة جرى استغلالها للنفاذ إلى أنظمة بعض المؤسسات الحيوية. في أكتوبر 2024، رُصد نشاط على منتديات الويب المظلم يعرض للبيع صلاحيات دخول إلى إحدى المنصات الحيوية للبنية التحتية المغربية، مع وثائق ومستندات داخلية تم اختراقها. وقد ادعى الفاعل المجهول أن الوصول المعروض يتجاوز جميع أنظمة الحماية (جدران النار وأنظمة كشف التسلل) ويمكِّن المشتري من السيطرة على الشبكة بأكملها. وعلى نحو مشابه، أعلنت مجموعة *ransomware*دولية تُدعى "ستورموس (*STORMOUS*)" عام 2023 أنها حصلت على ولوج غير مصرح به إلى شبكة شركة الاتصالات المغربية إنوي (*Inwi*)، وعرضت للبيع بيانات اعتماد *VPN*[205] تتيح التخطي الكامل لإجراءات الأمان والدخول الحر إلى منظومة إنوي الداخلية[206]. تدّعي هذه المجموعة أنها استخدمت تقنيات تشفير متقدمة لتجنب الرصد، ما يشير إلى مدى تطور أساليب الجريمة السيبرانية العابرة للحدود. وقد أثار هذا الحادث مخاوف بشأن حماية قطاع الاتصالات، نظرًا لما يمثله من عصب أساسي للاقتصاد والأمن الوطني.

---

[202] BABAS, 2025, *Cyberattacks*. op. cit.

[203] وكالة المغرب العربي للأنباء. "المواقع الإلكترونية لوكالة المغرب العربي للأنباء مستهدفة بهجوم إلكتروني لحجب الخدمة من نوع (*DDOS*)". MAP News، 16 فبراير 2023. تم الاطلاع عليه في 04 ماي 2025، على الساعة 10:16، متوفر على الرابط: *https://www.mapnews.ma/ar*.

[204] *IDRISSI*, Hind. op. cit.

[205] يُقصد بـ *VPN* هنا بيانات اعتماد الوصول إلى الشبكات الخاصة الافتراضية (*Virtual Private Networks*) المستخدمة من طرف المؤسسات لتأمين الاتصال الداخلي، وليس خدمات *الـVPN* التجارية العامة المخصصة للتصفح. وتشكل هذه البيانات، عند تسريبها، خطراً بالغاً لأنها تتيح للمهاجمين تجاوز الحماية الخارجية والولوج المباشر إلى الأنظمة الداخلية الحساسة.

[206] *CYFIRMA*. op. cit.

رغم عدم تسجيل هجمات كبرى معلنة استهدفت قطاعي الصحة والطاقة بشكل مباشر في المغرب حتى الآن، إلا أن خبراء الأمن السيبراني يحذرون من احتمال تصاعد الاستهداف ليشمل البنية التحتية الحرجة في هذين القطاعين. ويرى محللون أن السيناريوهات المحتملة في حالة تفاقم "الحرب السيبرانية" قد تطال منشآت حيوية كشبكات الكهرباء وأنظمة الطاقة والمطارات وغيرها. ومما يعزز هذه المخاوف أن عدة دول إقليمية شهدت بالفعل محاولات لاختراق مرافق صحية أو تعطيل أنظمة إمداد الطاقة عبر الإنترنت في إطار صراعات خفية. لذا يشدد المختصون على أن تحصين البنية التحتية الرقمية الوطنية بات أولوية قصوى لتفادي الأسوأ[207].

ثانيا: الهجمات على القطاع الخاص والمجتمع المدني

إلى جانب استهداف مرافق الدولة، تعرض القطاع الخاص المغربي ومكونات المجتمع المدني لسلسلة من الهجمات السيبرانية التي تنوعت دوافعها بين البحث عن الربح المالي والتجسس الإلكتروني. كان القطاع المصرفي والمالي في طليعة المستهدفين، نظرًا لحساسية البيانات المالية وإمكانات الكسب غير المشروع. فقد كشف تقرير للإنتربول عام 2022 أن المغرب جاء الأول أفريقيًا من حيث التعرض لهجمات برمجيات طروادة المصرفية (*Banking Trojans*) بنحو 18,827 هجمة خلال ذلك العام. وتعرّضت عدة بنوك مغربية لهجمات تصيّد واحتيال إلكتروني أوقعت خسائر مادية وسمعة سيئة. فعلى سبيل المثال، تعرض البنك الشعبي المركزي (*BCP*) لهجوم تصيّد في أكتوبر 2021 استغل حيل هندسة اجتماعية للإيقاع بالعملاء. كما شهد بنك *CIH* عدة محاولات اختراق في السنوات الأخيرة، نجح أحدها في 2023 وتسبب في خداع 105 من عملائه وسرقة ما يقارب 3 ملايين درهم من حساباتهم. وسبقت ذلك حوادث مشابهة، منها ما وقع في 2017 عندما فوجئ عدد كبير من عملاء *Société Générale Maroc* بسحب مبالغ من أرصدتهم دون علمهم نتيجة عملية قرصنة لبيانات بطاقاتهم البنكية[208]. وإلى جانب استهداف البنوك مباشرة، كشفت تقارير أمنية عن وجود عشرات آلاف البطاقات المصرفية المغربية معروضة للبيع في منتديات الإنترنت المظلم،

---

[207] BASHIR, Hamdy. *A Cyber Shadow-War between Algeria and Morocco*, The Arab Wall, 24 March 2022, consulted on 04 May 2025 at 01:45. Available at: *https://arabwall.com.*

[208] *IDRISSI*, Hind. Op. cit.

إذ تم رصد بيانات أكثر من 31 ألف بطاقة دفع مغربية ضمن تسريب إلكتروني حديث[209]. هذه المعطيات تؤكد أن البيانات المالية للمواطنين باتت عرضة للاستغلال الإجرامي على نطاق واسع، سواء عبر هجمات تصيّد الاحتيالي أو الاختراقات لقواعد بيانات شركات الخدمات المالية.

قطاع الأعمال والشركات الكبرى في المغرب لم يكن بمنأى عن التهديدات السيبرانية، حيث شهدت السنوات الأخيرة حوادث بارزة طالت شركات في مجالات مختلفة. فقد ضربت هجمات برامج الفديةransomware[210] عددًا من المؤسسات، وقامت عصابات إلكترونية بابتزازها عبر تشفير بياناتها والتهديد بنشرها ما لم يتم دفع فدية مالية. من بين الأمثلة اللافتة، تعرضت شركة ستيريفارما (*Steripharma*) للأدوية لهجوم ببرنامج الفدية "ميدوسا (*Medusa*)" في سبتمبر 2023، مما أدى إلى تعطيل أنظمة الشركة وتسريب جزء من بياناتها الداخلية على موقع التسريبات الخاص بالعصابة. كما استُهدف فرع شركة لوجستية دولية في المغرب (*Ipsen Logistics*)بهجوم من مجموعة *LockBit* 3.0 في منتصف 2023، وطال الهجوم خوادمها وقواعد بياناتها الحساسة. وفي العام السابق 2022، كانت شركة صناعية محلية ضمن ضحايا الإصدار السابق من فيروس *LockBit*، حيث سُربت معلوماتها التجارية على الإنترنت. هذه الحوادث وغيرها تشير إلى أن الشركات بمختلف أحجامها أضحت هدفًا مغريًا لعصابات الجريمة الإلكترونية العالمية، التي وجدت في التحول الرقمي المتسارع للشركات المغربية فرصةً لاستغلال الثغرات وسوء الوعي الأمني لاقتحام الأنظمة المعلوماتية وسرقة البيانات أو ابتزاز المؤسسات[211].

---

[209] IBRIZ, Sara. *Fuite de cartes bancaires marocaines dans le dark web: ce que révèle une analyse de Cypherleak*, Médias24, 18 mars 2025. Consulté le 09 mai 2025 à 22h03. Disponible sur: *https://medias24.com.*

[210] برمجية الفدية هي نوع من البرمجيات الخبيثة (*malware*) التي *تقوم بتشفير ملفات الضحية أو قفل أجهزته*، وتطلب فدية مالية (غالبًا بعملة رقمية مثل بيتكوين) مقابل فك التشفير أو استرجاع الوصول إلى البيانات.

[211] موقع *Ransomware.live* هو منصة مفتوحة تُعنى برصد وتحليل الهجمات السيبرانية التي تتم بواسطة برامج الفدية (*ransomware*) عبر العالم، ويعرض بيانات محدثة عن الضحايا حسب الدول والقطاعات، بما في ذلك المغرب. يقدم الموقع معلومات تقنية مفصلة مثل تاريخ اكتشاف الهجوم، اسم المجموعة المخترقة، وملاحظات الفدية، إلى جانب أدوات تحليلية موجهة للباحثين في الأمن السيبراني. ووفقًا لتحديث 24 ماي 2025، سُجلت 11 حالة مؤكدة لمؤسسات مغربية تعرضت لهجمات فدية، من بينها شركات ومؤسسات حكومية مثل *Inwi*، *Imanor*، وجامعة سيدي محمد بن عبد الله. (*Ransomware.live, consulté le 04 mai 2025 à 20h55, disponible sur: https://www.ransomware.live/map/MA*).

أما على صعيد المجتمع المدني والأفراد، فقد تكاثر استهداف المواطنين عبر الفضاء السيبراني بوسائل متنوعة. تشير الدراسات إلى أن برمجيات سرقة المعطيات الشخصية (مثل برامج الاختراق عبر أجهزة الكمبيوتر والهواتف) أضحت تهديدًا قائمًا، حيث تم الكشف عن إصابة ما يقرب من 10 ملايين جهاز حول العالم خلال 2023 ببرمجيات تجسس وسرقة كلمات المرور. وكان للمغرب نصيب غير هيّن من تلك الهجمات؛ إذ كُشف أن نطاق *.ma*[212] المحلي شهد اختراق حوالي 1.1 مليون حساب لمستخدمين مغاربة في عام 2023، وفق تحليل سجلات التسريب على الشبكة المظلمة[213]. هذا الرقم يعكس اتساع شريحة الضحايا المحتملين من المواطنين الذين تم الاستحواذ على بيانات دخولهم لمواقع وخدمات مختلفة *.ma*)يدل على حسابات بريدية أو منصات محلية .(ويستغل القراصنة هذه البيانات لشن عمليات احتيال مالي أو انتحال هوية، ما يضع الأفراد في مواجهة مخاطر كبيرة كسرقة الأموال أو الابتزاز أو انتهاك الخصوصية. ومما يزيد الوضع تعقيدًا أن مستوى الوعي الأمني الرقمي لدى شريحة واسعة من المستخدمين لا يزال دون المأمول، ما يجعلهم أهدافًا سهلة نسبياً لهجمات التصيّد وانتحال الهوية.

خلاصة القول، أظهرت الهجمات السيبرانية البارزة التي طالت المغرب مدى هشاشة المنظومات الرقمية في مواجهة التهديدات المتنامية، سواء كانت بدوافع سياسية لاستهداف سيادة الدولة وزعزعة الثقة في مؤسساتها، أو بدوافع إجرامية لابتزاز الشركات وسرقة أموال الأفراد. لقد كشفت حوادث اختراق مؤسسات حكومية مهمة (مثل *CNSS* ووزارات حيوية) عن ثغرات أمنية خطيرة[214]، كما بينت الهجمات على البنوك والشركات الخاصة أن القطاع الخاص ليس بمأمن من خطر القرصنة الإلكترونية المنظّمة. ومع تسارع التحول الرقمي في المغرب وازدياد الاعتماد على الخدمات الإلكترونية في الإدارة والاقتصاد، تصبح الحاجة ملحّة إلى تعزيز القدرات الدفاعية السيبرانية على كافة المستويات. لقد أوضحت *Transparency*

---

[212] النطاق *.ma* هو النطاق العلوي الخاص بالمغرب (*Country Code Top-Level Domain – ccTLD*)، ويُستخدم لتمييز مواقع الإنترنت المرتبطة بالمملكة المغربية. يُدار هذا النطاق من قبل الوكالة الوطنية لتقنين المواصلات (*ANRT*)، ويُمنح عادةً للأفراد أو المؤسسات أو الشركات التي تمارس أنشطة داخل المغرب أو لها صلة به. يساعد استخدام هذا النطاق في تعزيز الهوية الرقمية المغربية على الإنترنت، كما يوفر دلالة جغرافية واضحة على محتوى الموقع أو الجهة المالكة له.

[213] AMAOUI, Rachid. *Cyberattaques : 1,1 million de comptes .ma compromis en 2023*, Tic Maroc, 3 avril 2024. Consulté le 05 mai 2025 à 20h50. Disponible sur : *https://www.tic-maroc.com*.

[214] KABIRI *KETTANI*, op. cit.

Maroc (منظمة الشفافية) أن حادثة تسريب *الـCNSS* الأخيرة كشفت قصورًا هيكليًا في حماية البيانات العمومية[215]، مما يستدعي اعتماد إستراتيجية شاملة للأمن السيبراني تتضمن تحديث البنية التقنية وتطوير الموارد البشرية المختصة وتعزيز التعاون الدولي في مواجهة هذا النوع المستجد من التهديدات. على ضوء تلك الهجمات البارزة، بات من الواضح أن الأمن السيبراني في المغرب لم يعد ترفًا تقنيًا، بل ضرورة لحماية أمن الدولة واقتصادها وخصوصية مواطنيها في العصر الرقمي المتشابك.

الفقرة الثانية: انعكاساتها على الأمن الوطني والاقتصاد الرقمي

يشهد العالم المعاصر ترابطًا غير مسبوق بين الفضاء السيبراني ومختلف مناحي الحياة الوطنية والاقتصادية. فقد أصبح الاقتصاد رقميًا على نحوٍ متزايد، مع اعتماد الحكومات والشركات والأفراد على التقنيات الرقمية في إدارة الخدمات والمعاملات. في المقابل، تزايدت التهديدات السيبرانية من هجماتٍ إلكترونية وتجسسٍ رقمي وحروب معلوماتية، مما رفع الأمن السيبراني إلى مقدمة الأولويات ضمن قضايا الأمن الوطني[216]. لم يعد الأمن السيبراني مجرد شأن تقني محدود، بل غدا ركيزة أساسية للحفاظ على الأمن الوطني وحماية الاقتصاد الرقمي على حد سواء. في هذا السياق، يتناول هذا التحليل الأبعاد النظرية والعملية لانعكاسات الأمن السيبراني على أمن الدول وسيادتها من جهة، وعلى ازدهار الاقتصاد الرقمي وثقة المعاملات الإلكترونية من جهة أخرى. سيتطرق التحليل إلى دور الأمن السيبراني في حماية الدولة من التهديدات الحديثة (مثل الهجمات على البنى التحتية الحيوية والحروب السيبرانية) وفي الحفاظ على سيادتها الرقمية، بالإضافة إلى دوره في تعزيز الثقة والابتكار وجذب الاستثمار ضمن الاقتصاد الرقمي. يهدف هذا الطرح إلى تقديم فهم متكامل لكيفية تأثير الأمن السيبراني كعامل مزدوج على الاستقرار الوطني والتنمية الاقتصادية الرقمية، مع الاستناد إلى أدبيات أكاديمية ودراسات محكّمة لتأكيد النقاط الرئيسية.

---

[215] FAOUZI, Adil. *Transparency Maroc: CNSS Data Breach Exposes Critical Flaws in Morocco's Cybersecurity*, Morocco World News, 23 avril 2025. Consulté le 06 mai 2025 à 15h43, disponible sur: *https://www.moroccoworldnews.com*.

[216] د. سلمى عبد الرحيم عبد الحسن داغر الشمري، *"طبيعة العلاقة بين الأمن السيبراني والنمو الاقتصادي الرقمي في دول العالم"*، المجلة الأمريكية الدولية المحكمة للعلوم الإنسانية والاجتماعية، العدد 10، بغداد: مديرية شباب ورياضة بغداد/الرصافة، مايو 2025.

- **الارتباط البنيوي بين الأمن السيبراني والأمن الوطني**

أحدث توسع الفضاء الإلكتروني وتكنولوجيات المعلومات تحولًا عميقًا في مفهوم الأمن الوطني للدول. تقليديًا، كان الأمن الوطني يُحصر في الجوانب العسكرية وحماية الحدود المادية والسيادة الترابية. أما اليوم، فقد برز الأمن السيبراني بوصفه بعدًا أساسيًا من أبعاد الأمن الوطني، حيث تعتمد قطاعات الدولة الحيوية (العسكرية، والاقتصادية، والبنى التحتية) على أنظمة معلوماتية قد تكون هدفًا لهجمات سيبرانية معادية. ويُعرَّف الأمن السيبراني بأنه مجموعة من الوسائل التقنية والإدارية لحماية الفضاء المعلوماتي للبُنى التحتية الرقمية والشبكات والبيانات من الاستخدام غير المصرح به أو من أي ضرر أو تعطيل. وتشمل أهداف الأمن السيبراني ضمان توافر واستمرارية عمل نظم المعلومات، وسلامة البيانات وخصوصيتها، وحماية مصالح المواطنين والدولة في الفضاء الرقمي[217]. إن دخول الإنترنت في صميم الحياة اليومية وتغلغله عبر الحدود الجغرافية التقليدية جعل الأمن الرقمي جزءًا لا يتجزأ من سيادة الدولة الحديثة. وقد ظهر مفهوم السيادة الرقمية ليعبّر عن قدرة الدولة على بسط سلطتها واستقلاليتها في المجال السيبراني غير المادي، من خلال السيطرة على البنى التحتية الرقمية والتحكم بتدفق البيانات والمحتوى داخل فضائها الإلكتروني. هذا التحول نابع من تجاوز الإنترنت للحدود الوطنية التقليدية وما نتج عنه من تحديات تمس سيادة الدول وأمنها؛ فقد أصبح بإمكان أطراف خارجية التأثير في أمن دولة ما عبر الفضاء السيبراني دون الحاجة إلى اختراق حدودها المادية[218]. بناءً على ذلك، اضطرت الدول إلى توسيع عقيدتها الأمنية لتشمل الفضاء الإلكتروني كعنصر استراتيجي. وتشير الدراسات إلى أن الأمن السيبراني غدا في صدارة أجندة الأمن القومي لمعظم البلدان، مما دفعها إلى إعادة صياغة استراتيجياتها الأمنية والدفاعية لتلائم التهديدات السيبرانية المستجدة[219]. وبالفعل، أنشأت عشرات الدول وحدات وقيادات عسكرية متخصصة بالحرب السيبرانية ضمن جيوشها) على غرار قيادة العمليات السيبرانية *Cyber Command*[220] لتعزيز قدراتها على الردع السيبراني وحماية

---

[217] مرجع سابق، الشمري، *"طبيعة العلاقة بين الأمن السيبراني والنمو الاقتصادي الرقمي في دول العالم"*.

[218] محمد فرحان، *"الأمن القومي المغربي: مواجهة التهديدات السيبرانية وتكريس السيادة الرقمية"*، المركز الديمقراطي العربي، قسم الدراسات البحثية المتخصصة، 12 أكتوبر 2024.

[219] مرجع سابق، الشمري، *"طبيعة العلاقة بين الأمن السيبراني والنمو الاقتصادي الرقمي في دول العالم"*.

[220] *قيادة عسكرية أمريكية متخصصة في العمليات السيبرانية*، أُنشئت سنة 2010 وتطورت لتصبح قيادة مقاتلة موحدة *(Unified Combatant Command)* سنة 2018، وهي مسؤولة عن الدفاع السيبراني لشبكات وزارة الدفاع الأمريكية،

الفضاء الإلكتروني الوطني[221]. هذه التطورات على المستوى النظري والمؤسسي تعكس حقيقة أن حماية الفضاء السيبراني أضحت جزءًا لا يتجزأ من مفهوم الأمن الوطني الشامل.

تتجلى انعكاسات الأمن السيبراني على الأمن الوطني بوضوح عند النظر إلى طبيعة التهديدات السيبرانية الحديثة وتأثيرها العملي على استقرار الدول. فالتقدم التكنولوجي رافقه ظهور طيف جديد من التهديدات الأمنية التي توصف بأنها لاتماثلية (أي غير تقليدية يصعب مواجهتها بالوسائل الكلاسيكية)[222]. من أبرز هذه التهديدات:

الهجمات السيبرانية الموجهة ضد البنى التحتية الحيوية: تشمل محاولات اختراق أو تعطيل شبكات الكهرباء والمياه والاتصالات والنقل والمؤسسات المالية وغيرها من المرافق الاستراتيجية. تعتمد الدول الحديثة اعتمادًا كبيرًا على هذه البنى التحتية المُدارة رقميًا، ما يجعل أي اختراق لها ذا تبعات خطيرة على الأمن الوطني. وقد شهد الواقع أمثلة ملموسة تؤكد ذلك؛ فالهجوم السيبراني الذي شنته جهة مرتبطة بروسيا على شبكة الكهرباء الأوكرانية في ديسمبر 2015 أدى إلى انقطاع التيار عن حوالي 200 ألف مواطن بشكل مؤقت، مما قدّم إنذارًا مبكرًا بإمكانية استخدام الهجمات السيبرانية لإحداث شلل في الخدمات الحيوية وتهديد سلامة المدنيين. إن حماية البنى التحتية المعلوماتية الحرجة أصبحت مهمة استراتيجية للدول لمنع ما يُعرف بـ"شلل الدولة الرقمي" في حال وقوع نزاعات سيبرانية. على سبيل المثال، تؤكد سياسات الدفاع في دول كبرى ضرورة حماية أنظمة المعلومات والاتصالات الخاصة بالبنى التحتية الحرجة كجزء من واجب تأمين السكان والاقتصاد والأمن الوطني عمومًا[223].

التجسس الإلكتروني وسرقة المعلومات السيادية: تقوم جهات معادية (دول أو مجموعات قرصنة مدعومة) بمحاولات اختراق شبكات الحكومة أو الجيش لسرقة معلومات حساسة تتعلق بالأمن القومي أو الخطط العسكرية أو أسرار التكنولوجيا المتقدمة. مثل هذه الاختراقات تهدد سيادة الدولة وتفوقها الاستراتيجي، خاصة إذا تمكنت من الحصول على معلومات استخباراتية

وتنفيذ عمليات هجومية ودفاعية في الفضاء السيبراني، إضافة إلى التعاون مع الوكالات الفيدرالية الأخرى والقطاع الخاص لحماية البنية التحتية الحيوية.

[221] Reveron, Derek S., and John E. Savage. *"Cybersecurity Convergence: Digital Human and National Security."* Orbis, vol. 64, no. 4, 2020, pp. 555–570. Elsevier, *https://doi.org/10.1016/j.orbis.2020.08.005.*

[222] مرجع سابق، *"الأمن القومي المغربي: مواجهة التهديدات السيبرانية وتكريس السيادة الرقمية"*.

[223] *Reveron and Savage*. op. cit.

سرية أو أسرار صناعات دفاعية متطورة. لقد تعرضت العديد من الدول لمحاولات اختراق استهدفت قواعد بيانات حكومية أو شبكات وزارات سيادية، وأدركت الأجهزة الأمنية أن حماية سرية المعلومات جزء أساسي من أمن الدولة. ولذلك تبذل الجهود لبناء قدرات دفاعية سيبرانية متقدمة تكتشف محاولات التسلل الإلكتروني مبكرًا وتتصدى لها، بالتعاون أحيانًا مع القطاع الخاص المشغل لمعظم البنية التحتية الرقمية. وتُظهر التقارير الاستخباراتية الدولية أن حملات التجسس الإلكتروني الاقتصادي والعسكري (مثل سرقة براءات الاختراع أو تصميمات الأسلحة) باتت واسعة النطاق وتمثل تهديدًا مباشرًا لمصالح الدول.

حملات التأثير وحروب المعلومات السيبرانية: لم يعد تهديد الأمن الوطني سيبرانيًا محصورًا في الاختراق التقني للبنى التحتية، بل برز أيضًا في شكل حملات تضليل إعلامي وهجمات على الرأي العام عبر الفضاء الإلكتروني. تقوم بعض الأطراف بشن حرب معلومات عبر اختراق حسابات إعلامية أو بث أخبار كاذبة على مواقع التواصل الاجتماعي بهدف زعزعة الاستقرار الداخلي وإثارة الانقسامات المجتمعية أو التأثير في العمليات الديمقراطية (مثل الانتخابات). وقد اعتبرت الأجهزة الأمنية في عدة دول أن هذه الحملات الموجهة عبر الإنترنت تشكل خطرًا أمنيًا حقيقيًا، نظرًا لقدرتها على تقويض الثقة بالمؤسسات وإضعاف التماسك الوطني دون إطلاق رصاصة واحدة[224]. لذلك يعمل صناع القرار على تطوير استراتيجيات للأمن السيبراني تشمل مواجهة التهديدات المعلوماتية، عبر تعزيز الوعي العام وتمكين الوكالات المتخصصة من مراقبة الفضاء الإلكتروني لرصد أنشطة التأثير الأجنبية والتصدي لها ضمن الأطر القانونية التي تحافظ على حرية التعبير.

إن هذه الأنماط المتنوعة من المخاطر السيبرانية تقود إلى نتيجة واضحة: الأمن السيبراني بات شرطًا أساسيًا لصيانة الأمن الوطني في العصر الرقمي. دولةٌ لا تملك القدرة على حماية فضائها الإلكتروني وتأمين شبكاتها وأنظمتها الحيوية هي دولة معرضة لمخاطر تعطيل مفاصلها الحيوية وشل اقتصادها وحتى تهديد أمن مواطنيها. وقد خلص أحد البحوث إلى أن الجرائم والهجمات السيبرانية أضحت تحديًا أمنيًا جديدًا أمام الدول، ليس فقط على الصعيد التقني بل أيضًا كعائق أمام النمو الاقتصادي والاستقرار العام[225]. لذا تتبنى الدول نهجًا شاملًا

---

[224] Ibid.,

[225] مرجع سابق، الشمري، *"طبيعة العلاقة بين الأمن السيبراني والنمو الاقتصادي الرقمي في دول العالم"*.

في الأمن الوطني يدمج الدفاع السيبراني ضمن العقيدة الأمنية، وتعمل على تطوير قدرات الاستجابة الوطنية للطوارئ السيبرانية وبناء مراكز عمليات أمنية متقدمة (*SOC*[226]) وأنظمة إنذار مبكر لرصد الهجمات قبل تفاقم أضرارها. وبموازاة ذلك، تسعى الدول إلى تعزيز التعاون الدولي لوضع أطر قانونية تحد من الجرائم السيبرانية العابرة للحدود، وتشارك المعلومات بشأن التهديدات مع حلفائها للمساعدة في التصدي الفعّال لها. كل هذه الجهود تعكس حقيقة أن الأمن الوطني الرقمي اليوم لا يقل أهمية عن الأمن العسكري أو الاقتصادي، بل أصبح مكملًا لهما وجزءًا حيويًا من مفهوم سيادة الدولة وحماية مصالحها العليا في القرن الواحد والعشرين.

- **الأمن السيبراني والاقتصاد الرقمي**

يشكّل الاقتصاد الرقمي اليوم عصب النمو الاقتصادي في العديد من البلدان، حيث تقوم قطاعات واسعة من التجارة والصناعة والخدمات على التقنيات الرقمية والمنصات الإلكترونية. ويتطلب ازدهار هذا الاقتصاد توافر بيئة رقمية آمنة وموثوقة. هنا يبرز الأمن السيبراني بوصفه عامل تمكين أساسي لتحقيق الثقة والاستقرار في المعاملات الرقمية. إن الثقة في سلامة وأمن العمليات الإلكترونية هي حجر الزاوية لأي نشاط اقتصادي رقمي ناجح؛ فإذا ساورت الشكوكُ المستهلكين أو المستثمرين حيال أمان منصات التجارة الإلكترونية أو المدفوعات عبر الإنترنت، ستتراجع مشاركتهم وتنكمش سوق الاقتصاد الرقمي. ومن هذا المنطلق، تُعتبر الثقة الإلكترونية نتاجًا مباشرًا لمستوى الأمن السيبراني المتحقق. تشير الدراسات الحديثة إلى أن الأمن السيبراني لم يعد مجرد وسيلة لحماية الأصول الرقمية من الخسائر، بل غدا محفزًا للنمو والابتكار في الاقتصاد ككل. فقد وجدت دراسة صادرة عن البنك الدولي سنة 2024 أن تعزيز أمن المعلومات يساهم في بناء ثقة المستخدمين، ويعزز تنافسية الشركات، ويدفع عجلة الابتكار الرقمي مما يؤدي في النهاية إلى رفع الإنتاجية والنمو الاقتصادي. وبصيغة أخرى، الأمن السيبراني القوي يخلق مناخًا آمنًا يشجع الأفراد والمؤسسات على تبنّي التقنيات الرقمية والخدمات الجديدة دون تردد، وبالتالي يوسّع قاعدة الاقتصاد الرقمي. وعلى النقيض، فإن تكرار الحوادث السيبرانية الكبرى (مثل تسريب بيانات ملايين المستخدمين أو تعرض بنوك إلكترونية للاحتيال والاختراق) يُقوِّض ثقة الجمهور ويبطئ وتيرة

[226] مركز عمليات الأمن السيبراني، يُعنى بالمراقبة المستمرة وتحليل الأنشطة الرقمية، ويشكّل *نقطة محورية في إدارة الحوادث السيبرانية* والكشف المبكر عن التهديدات الإلكترونية.

التحول الرقمي. لهذا ترى الحكومات أن الاستثمار في الأمن السيبراني هو استثمار في الاقتصاد نفسه، عبر تجنيب الاقتصاد كلفة الهجمات وتداعياتها وبناء أساس متين للتنمية الرقمية المستدامة. بل إن التقديرات تشير إلى أن تقليص معدل الحوادث السيبرانية يمكن أن ينعكس إيجابًا بشكل ملحوظ على النمو الاقتصادي؛ فقد وجد البحث ذاته للبنك الدولي أن خفض حوادث الاختراق والأضرار السيبرانية في بلد نامٍ قد يرفع نصيب الفرد من الناتج المحلي الإجمالي بنسبة تقارب 1.5% خلال عقد واحد[227]. هذه الزيادة ناتجة عن تراكم الآثار الإيجابية كزيادة ثقة المستهلكين والمستثمرين، وتجنب الخسائر المالية الضخمة التي تنتج عن الهجمات (سواء مباشرة كتعطيل الأنظمة أو بشكل غير مباشر كتراجع سمعة الشركات)، فضلًا عن تحفيز الابتكار في قطاع التقنية الأمنية وخلق فرص عمل جديدة في هذا المجال. ويمكن القول نظريًا إن الأمن السيبراني يؤدي دورًا تمكينيًا (*Enabler*) للاقتصاد الرقمي، يكفل ديمومة العوائد المتحققة من الرقمنة ويحمي مكتسباتها من المخاطر.

تترجم العلاقة بين الأمن السيبراني والاقتصاد الرقمي عمليًا من خلال عدة مجالات جوهرية تؤثر فيها حماية الفضاء الإلكتروني على الأداء الاقتصادي العام للدولة. فيما يلي أبرز تلك المجالات وانعكاسات الأمن السيبراني عليها:

الثقة في المعاملات الإلكترونية والأسواق الرقمية: تُعد الثقة العنصر الحاسم الذي يُمكن الاقتصاد الرقمي من النمو. جميع أطراف السوق – من مستهلكين وشركات ومستثمرين – بحاجة إلى الاطمئنان بأن المنصات الرقمية التي يستخدمونها آمنة من الاختراق والاحتيال. عندما يكون مستوى الأمن السيبراني مرتفعًا، يزداد يقين المستخدمين بأن بياناتهم المالية والشخصية محمية بشكل كافٍ، مما يشجعهم على اعتماد وسائل الدفع الإلكتروني والتسوق عبر الإنترنت والخدمات المصرفية الرقمية دون تردد. أما في حال حدوث اختراقات كبيرة أو تسريبات بيانات واسعة النطاق، فإن ذلك ينعكس فورًا في تراجع ثقة الجمهور. على سبيل المثال، أدت بعض حوادث الاختراق الشهيرة لمنصات تجارة إلكترونية عالمية إلى خسائر مالية فادحة وإلى عزوف مؤقت للمستخدمين عن تلك المنصات حتى استعادة الثقة. من هنا،

[227] Vergara Cobos, Estefania. Cybersecurity Economics for Emerging Markets. Washington, DC: World Bank, 2024. Accessed on April 5, 2025, at 11:00, at: https://hdl.handle.net/10986/42130.

فإن تعزيز الأمن السيبراني هو تعزيز للثقة في البيئة الرقمية. وقد أكدت الأدبيات أن الأمن السيبراني الجيد يبني الثقة ويمثل "الغراء الذي يربط العملاء بالشركات" في العصر الرقمي[228]. باختصار، لا يمكن للاقتصاد الرقمي أن ينمو بشكل مستدام دون ثقة المستخدمين، والأخيرة مرهونة بمدى ما توفره الحكومات والشركات من أمن سيبراني فعال.

دعم الابتكار والتحول الرقمي: إن وجود بيئة رقمية آمنة يشجّع روّاد الأعمال والشركات على الاستثمار في ابتكار خدمات رقمية جديدة وتقنيات ناشئة (مثل الحوسبة السحابية، وإنترنت الأشياء، والذكاء الاصطناعي) من دون الخوف المفرط من المخاطر السيبرانية. فحين يثق المطوّرون بأن منصاتهم محمية، يندفعون نحو إطلاق تطبيقات وخدمات مبتكرة تدفع عجلة التحول الرقمي. كما أن الشركات القائمة تكون أكثر استعدادًا لاعتماد تقنيات حديثة – كالحوسبة السحابية أو إنترنت الأشياء في التصنيع – إذا توفرت حلول أمنية تضمن سلامة تلك التقنيات من الاختراق. في المقابل، قد يؤدي ضعف الأمن السيبراني إلى إحجام بعض القطاعات عن تبنّي التحول الرقمي الكامل خوفًا من التعرض لهجمات مُكلفة. مثلًا، قد تتردد المؤسسات الصحية في رقمنة كامل بيانات المرضى أو ربط أجهزة المستشفيات بالإنترنت إذا كانت الهجمات الإلكترونية (كفيروسات الفدية وغيرها) شائعة وتسبب تعطيلًا لأنظمتها. من جهة أخرى، شكّل الطلب المتنامي على الأمن السيبراني ذاته فرصة لقطاع اقتصادي جديد نسبيًا، يتمثل في صناعة أمن المعلومات وتطوير البرمجيات والحلول الأمنية، مما أوجد مجالات ابتكار وفرص عمل متقدمة. وتدعم الحكومات البحث والتطوير في هذا القطاع إدراكًا منها لدوره المزدوج: فهو يعزز حماية الاقتصاد الرقمي من المخاطر، وفي الوقت نفسه يمثل قطاعًا إنتاجيًا معرفيًا يُسهم في الناتج المحلي[229].

جذب الاستثمار الأجنبي المباشر وتعزيز المناخ الاستثماري: أصبح مستوى الأمن السيبراني في أي دولة عاملًا مؤثرًا في قرارات المستثمرين الدوليين حول توجيه استثماراتهم. فالمستثمر الأجنبي حين ينوي إنشاء مشروع أو مقر لشركته في بلد ما، يأخذ بعين الاعتبار عوامل عديدة

---

[228] Bhalla, Ajay. "Securing the Digital Economy Requires Trust." Bloomberg, Sponsored Content by Mastercard. Last accessed on May 25, 2025, at 09:30, at: https://sponsored.bloomberg.com.

[229] World Economic Forum. *Global Cybersecurity Outlook 2024*. In collaboration with Accenture. Published January 11, 2024.

من بينها مدى سلامة البيئة الرقمية في ذلك البلد. إن حدوث اختراقات أمنية متكررة للبنوك أو تعطل للبنية التحتية الإلكترونية الحكومية مثلًا قد يبعث إشارات سلبية حول استقرار مناخ الاستثمار في الدولة. في المقابل، يُنظر إلى الدول التي تمتلك أطرًا تنظيمية قوية في مجال الأمن السيبراني وتطبّق معايير حماية صارمة على أنها وجهات أكثر أمانًا لاستثمارات الشركات التقنية والمالية وغيرها. ولقد أظهرت دراسة اقتصادية قياسية نُشرت عام 2021 وجود ارتباط وثيق بين بيئة الإنترنت الآمنة وجاذبية الدولة للاستثمارات الأجنبية المباشرة. فبحسب هذه الدراسة، يؤدي ارتفاع مستوى الأمن السيبراني في دولة ما إلى تشجيع الشركات الأجنبية (لا سيما تلك الرقمية أو المعتمدة على التقنيات) على الاستثمار فيها بشكل ملحوظ. ويرجع ذلك إلى عدة عوامل أهمها أن الأمن السيبراني القوي يخفّض تكاليف التشغيل على المستثمرين عبر تقليل حوادث الانقطاع والأعطال التقنية، كما يقلّل تكلفة المعاملات من خلال تعزيز موثوقية الأنظمة الإلكترونية المستخدمة في إدارة الأعمال. إضافة إلى ذلك، توفر البيئة الآمنة حماية للملكية الفكرية والبيانات السرية للمستثمرين، وتحدّ من مشكلة عدم تماثل المعلومات بين المستثمر والبيئة الجديدة[230]. ونتيجة لهذه القنوات مجتمعة، خلصت الدراسة إلى توصية صريحة مفادها أن على الدول الساعية إلى جذب الاستثمارات الأجنبية أن تولي اهتمامًا كبيرًا لرفع جودة أمنها السيبراني واعتباره جزءًا من البنية التحتية الجاذبة للاستثمار. ويؤكد هذا المنحى دراسات أخرى أشارت إلى أن وجود سياسات فعالة لحماية الفضاء السيبراني يجعل الموقع الاستثماري أكثر جاذبية، لا سيما في القطاعات عالية التقنية والخدمات الرقمية التي تشكّل اليوم نسبة متزايدة من تدفقات الاستثمار العالمي.

تجنب الخسائر المالية وحماية استقرار الأسواق: إضافة إلى ما سبق، يساهم الأمن السيبراني في وقاية الاقتصاد من خسائر مباشرة وغير مباشرة يمكن أن تكون جسيمة. فالهجمات الإلكترونية الكبيرة (مثل هجمات فيروسات الفدية واسعة الانتشار أو الاختراقات التي تستهدف أنظمة الدفع الإلكتروني) قد تُلحق خسائر مالية بملايين أو مليارات الدولارات بالشركات وحتى بالاقتصاد الوطني ككل. وتشير التقديرات العالمية إلى أن كلفة الجرائم السيبرانية ترتفع سنويًا

[230] Youxing Huang, Na Jiang, and Yan Zhang, *Does Internet Security Matter for Foreign Direct Investment? A Spatial Econometric Analysis,* Telematics and Informatics 59 (2021): 101559, *https://doi.org/10.1016/j.tele.2020.101559.*

وتنعكس في خسائر إنتاجية وفي كلف إصلاح أنظمة واستعادة بيانات وفي تعويضات قانونية قد تضطر الشركات لدفعها جراء خروقات البيانات. كما قد تقود حادثة اختراق كبرى إلى اهتزاز ثقة المساهمين في شركة ما وانخفاض سهمها في الأسواق المالية، محدثةً تأثيرات سلبية على سوق الأوراق المالية المحلية وعلى قطاع الأعمال عامةً. لذا فإن الاستثمار الاستباقي في وسائل الحماية السيبرانية يمثل توفيرًا للتكاليف على المدى البعيد، عبر تفادي حوادث مُدمّرة والتقليل من اضطراب الأسواق. وتبيّن الأدبيات أن الدول التي تبدي التزامًا قويًا بالأمن السيبراني وتسارع إلى سد الثغرات، تحقق قطاعاتها الرقمية أداءً أفضل وتكون أقل عرضة للاضطرابات. ولعل في المقولة الحديثة "الأمن السيبراني ليس كلفةً إضافية، بل هو استثمار في اقتصاد أقوى وأكثر مرونة" تلخيصًا بليغًا لهذا الواقع؛ فبقدر ما تصون الدولة فضاءها الإلكتروني وتحصّنه، فإنها تحمي عجلة اقتصادها من التعطل وتضمن استمرار النمو بثبات واستقرار[231].

أضحى الأمن السيبراني عاملًا حاسمًا يتقاطع مع كلٍ من أمن الدولة القومي وتنميتها الاقتصادية الرقمية. فعلى صعيد الأمن الوطني، توفر القدرات السيبرانية للدولة حصنًا ضد تهديدات جديدة ومتطورة قادرة على تجاوز الحدود وإلحاق الضرر بالبنى التحتية والمؤسسات، مما يجعل التحصين الرقمي جزءًا لا يتجزأ من سيادة الدولة وحماية مواطنيها. إن الحفاظ على سيادة الدولة في الفضاء الإلكتروني وتأمين مقدراتها الرقمية بات ضرورة استراتيجية توازي في أهميتها حماية الحدود الترابية. وقد رأينا كيف أن كثيرًا من الدول أعادت صياغة عقيدتها الدفاعية وأولت الأمن السيبراني موقع الصدارة ضمن أولوياتها الأمنية، وكيف أن بناء منظومات فعالة للدفاع والرصد السيبراني أصبح معيارًا لمدى جاهزية الدولة لمواجهة تحديات القرن الحالي.

وفي الاقتصاد الرقمي، يتجلى تأثير الأمن السيبراني بصورة مزدوجة: فهو من جهة يوفر بيئة آمنة تعزّز ثقة المشاركين في الاقتصاد الرقمي – من مستهلكين ومستثمرين – مما يسمح بازدهار المعاملات الإلكترونية والتوسع في الخدمات الرقمية. ومن جهة أخرى، يحمي الأمن السيبراني ذلك الاقتصاد من الانتكاسات والخسائر الفادحة التي قد تنجم عن الهجمات

[231] World Economic Forum, *Global Cybersecurity Outlook 2024*. op. cit.

الإلكترونية الكبرى؛ فكلما ارتفعت قدرة الدولة على تأمين فضائها السيبراني، انعكس ذلك ازدهارًا في قطاعات الاقتصاد الرقمي وتطورًا في خدماته[232]. وبالعكس، فإن أي خلل جسيم في أمن المعلومات قد يؤدي إلى تقويض ثقة المستخدمين والمستثمرين، وبالتالي ينعكس سلبًا على مسار النمو الاقتصادي. لذا ليس غريبًا أن نرى دولًا تجعل من تحسين جاهزيتها السيبرانية محورًا أساسيًا في استراتيجيات التحول الرقمي وتضع معايير صارمة للأمن ضمن مشاريع البنية التحتية التقنية.

في المحصلة، يُمكن القول إن الأمن السيبراني يملك انعكاسات عميقة على استقرار الدولة وازدهارها الاقتصادي في العصر الرقمي. فهو درع حماية للأمن الوطني يصد التهديدات ويصون السيادة، وفي الوقت نفسه يُعدّ ممكنًا أساسيًا للنمو الاقتصادي من خلال بناء الثقة وتمكين الابتكار. وعليه، فإن تبنّي منظور شامل للأمن السيبراني – يدمج بين البعد السيادي والبعد التنموي – أصبح ضرورة حتمية لصنّاع القرار. ذلك أن تحقيق التنمية الاقتصادية الرقمية المستدامة يتطلب فضاءً سيبرانيًا آمنًا ومحصنًا، تمامًا كما يتطلب تحقيق الأمن الوطني إدماج الدفاع السيبراني ضمن منظومة الحماية الشاملة للدولة. باختصار، **الأمن السيبراني هو شرط لازدهار الاقتصاد الرقمي وضمان لأمن الوطن في آنٍ واحد؛ وإهماله أو التقليل من شأنه قد يعرّض كِلا الجانبين لمخاطر جسيمة.** من هنا تبرز الحاجة المستمرة للاستثمار في التقنيات الأمنية المتقدمة، وتطوير الكفاءات البشرية القادرة على إدارتها، ووضع سياسات وطنية ودولية تكفل فضاءً رقميًا أكثر أمنًا واستقرارًا.

المطلب الثاني: نقاط الضعف البنيوية والتقنية في المنظومة الرقمية

رغم الخطوات التشريعية والمؤسساتية التي اتخذها المغرب لتعزيز أمنه السيبراني، إلا أنّ الواقع العملي يكشف عن ثغرات بنيوية لا تزال تُضعف نجاعة المنظومة الرقمية الوطنية. فالهجمات المتكررة التي طالت مؤسسات حيوية، إلى جانب التفاوت في درجات الجاهزية والوعي الرقمي، تُبرز هشاشة البنية القانونية والتقنية، وتعكس قصورًا في التنسيق بين الجهات المعنية، وغياب ثقافة أمنية مجتمعية راسخة. لذلك، يتوزع هذا المطلب على فقرتين تحليليتين: في الفقرة الأولى، سيتم التطرق الثغرات القانونية والتقنية التي حدّت من فعالية الردع والاستجابة السيبرانية؛ وفي

[232] مرجع سابق، الشمري، *"طبيعة العلاقة بين الأمن السيبراني والنمو الاقتصادي الرقمي في دول العالم"*.

الفقرة الثانية، يُعالج الإشكال من زاوية سوسيومؤسساتية، عبر إبراز أثر ضعف الثقافة الأمنية الرقمية، وتفكك آليات التنسيق الوطني، والنقص الحاد في الموارد والكفاءات المتخصصة، بوصفها عوائق هيكلية أمام بناء منظومة سيبرانية فعّالة ومتكاملة.

الفقرة الاولى: الثغرات القانونية والتقنية

لقد أبرزت التجربة المغربية في تدبير منظومة الأمن السيبراني، سواء على مستوى الهياكل القانونية أو التقنيات الرقمية، اختلالات متجذّرة أثرت بشكل مباشر على قدرة الدولة في احتواء التهديدات المتزايدة التي تطال الفضاء السيبراني الوطني. فمن جهة أولى، عانت المنظومة التشريعية من تأخر واضح في بلورة إطار قانوني منسجم وشامل، ما جعل السلطات القضائية تلجأ إلى تكييف مقتضيات مشتتة لمحاصرة أفعال معقدة مثل الاختراقات، أو تسريب البيانات، أو الاعتداء على الخصوصية الرقمية، مما يُؤشّر على قصور في التكييف المعياري والإجرائي لمقتضيات العدالة الرقمية. ومن جهة ثانية، لم تواكب البنية التحتية المعلوماتية متطلبات المعايير الدولية لحكامة الأمن السيبراني، فظلت عرضة لهجمات متطورة تستغل ثغرات تقنية مكشوفة في أنظمة التشفير والمراقبة والاستجابة. ويكفي التذكير بتوالي الهجمات في العقدين الأخيرين، سواء تلك التي استهدفت الوزارات التعليمية، أو تلك التي طالت مؤسسات ذات طابع اجتماعي ومالي، لتؤكد حجم التحديات البنيوية التي تواجهها الدولة في بناء فضاء سيبراني آمن وموثوق. أمام هذا الوضع، تبرز ضرورة التشخيص الدقيق لمجمل الاختلالات القانونية والتقنية القائمة، سواء قبل صدور القانون 05.20 أو بعد دخوله حيز النفاذ، من أجل تطوير سياسات عمومية أكثر نجاعة واستباقية في الدفاع الرقمي الوطني.

أولا: الثغرات القانونية:

في سياق بناء الأمن السيبراني، تمثل الإطار القانوني أحد أهم مرتكزات التحصين الرقمي. غير أن التجربة المغربية تكشف عن مواطن خلل واضحة في التنظيم التشريعي، سواء في فترة ما قبل القانون 05.20 أو حتى بعد صدوره، مما جعل البنية الرقمية عرضة لاختراقات متكررة، وأضعف من فعالية الردع والوقاية القانونية.

1. قبل صدور القانون 05.20:

عرف المغرب، قبل دخول القانون 05.20 حيز التنفيذ، حالة فراغ تشريعي بنيوي جعل منظومته الرقمية مكشوفة لتهديدات متزايدة. فقد ظل التجريم يعتمد أساسا على الباب العاشر من القانون الجنائي كما عدل بمقتضى 07-03، الأمر الذي حصر المقاربة في «المساس بنظم المعالجة الآلية» دون التطرق إلى قضايا أكثر تعقيدا كحماية البريد الإلكتروني، قرصنة أسماء النطاقات، أو مسؤولية مقدمي الخدمات السحابية[233]. هذا التجزيء التشريعي أفضى إلى لجوء المحاكم إلى تكييف نصوص تقليدية كلما تعلق الأمر باختراق مواقع حكومية أو تسريب قواعد بيانات، وهو ما أكده الخبراء حين أبرزوا اضطرار القضاء إلى استعمال «قانون الإرهاب» لملاحقة الإشادة الإلكترونية بالأفعال المتطرفة. كما انحصرت الرؤية الإستراتيجية للدولة في بعدها الاقتصادي المرتبط بجذب استثمارات التعهيد، ما جعل الوثيقة الأهم--*DNSSI*--تركّز على حماية المنظمات ذات الأهمية الحيوية وتغفل مئات المقاولات الصغيرة، بينما ظل القطاع المالي والتعليمي الهدف الأسهل للقرصنة[234]. ومن دلائل القصور أن موجة الهجمات بين 2010 و2013، التي شملت مواقع وزارات التربية والطاقة وأزيد من عشر جامعات، كشفت هشاشة البنى الحكومية وأكدت اعتراف «الجيش الإلكتروني المجهول» بأن الحماية سطحية ويمكن تخطيها دون عناء.[235] كذلك، ورغم سنّ قوانين متفرقة مثل القانون رقم 24.96 المتعلق بالبريد والمواصلات[236] و القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية[237] و 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي[238]، فإنها افتقرت إلى آليات إنفاذ منسجمة؛ فلا عقود أمن

---

[233] أمين أعزان، خبير في الجرائم الإلكترونية وأستاذ القانون العام. المغرب يلجأ إلى القانون الجنائي ضد القراصنة لأنه لا يتوفر على قانون الأنترنت. جريدة المساء، منشور في موقع مغرس، بتاريخ 31 ماي 2013. تم الاطلاع عليه بتاريخ 25 أبريل 2025، على الساعة 16:00، على الرابط: https://www.maghress.com.

[234] وزارة الصناعة والاستثمار والتجارة والاقتصاد الرقمي (تسمية سابقة). المغرب بين تنمية الثقة الرقمية وتطوير الأمن السيبراني. المملكة المغربية، بدون تاريخ نشر. تم الاطلاع عليه بتاريخ 24 ماي 2025، على الساعة 12:00، على موقع اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا): https://www.unescwa.org.

[235] بهية مستغفر. قراصنة يخترقون الموقع الرسمي لوزارة التربية. جريدة هسبريس، 22 شتنبر 2010. تم الاطلاع عليه بتاريخ 15 ماي 2025، على الساعة 14:42، على الرابط: https://www.hespress.com.

[236] القانون رقم 24.09 المتعلق بالبريد والمواصلات الصادر بتنفيذه الظهير الشريف رقم 1-97-162 المؤرخ في 2 ربيع الآخر 1418 الموافق ل 7 غشت 1997، كما وقع تغييره وتتميمه بمقتضى القانون رقم 29-06 الصادر بتنفيذه الظهير الشريف رقم 1-07-43 المؤرخ في 28 ربيع الأول 1428 الموافق ل 17 أبريل 2007.

[237] مرجع سابق، القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية كما تم تعديله: القانون رقم 43.20.

[238] القانون رقم 09.08 ظهير شريف رقم 1.09.15 صادر في 22 من صفر 1430 (18) فبراير (2009) بتنفيذ القانون رقم المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

إلزامية مع مستضيفي البيانات، ولا جزاءات واضحة لعدم التبليغ عن الخروقات، وظلت المسطرة الجنائية عاجزة عن استيعاب الدليل الرقمي العابر للحدود[239].

2. بعد صدور القانون 05.20:

يُسجَّل، بعد التطبيق العملي للقانون رقم 05.20 المتعلِّق بالأمن السيبراني، أنّ الحاجة باتت ملحّة إلى إدخال تعديلات مُوجَّهة نحو ثلاث ثغرات جوهرية. أولاها أنّ المادة 8، وما يقابلها في المادتين 30 و 33، تقف عند عبارة «يجب على كل هيئة فور علمها[240]» من غير أن تُحدِّد أجلاً مقيداً للتبليغ عن الحوادث؛ وهي صياغة فضفاضة تُبطِّئ نظم الاستجابة ويصعب مساءلة المخالفين على أساسها، بينما توصي الأطر المعيارية الدولية[241] بآجال محدّدة (24 أو 48 أو 72 ساعة) مع إلزام المُصرّح بتبرير كل تجاوز لهذه المهلة درءاً لتفاقم الأضرار. ثانيها أنّ سقف الغرامات المنصوص عليه في المادتين 49 و 50 والذي لا يتجاوز 400 ألف درهم[242] يبقى أدنى بكثير من الخسائر المحتملة الناجمة عن اختراقٍ متوسط لقواعد بيانات عمومية أو مالية؛ بل يستطيع الفاعل الاقتصادي الكبير احتسابها ضمن «تكلفة مقبولة للمخاطر». وعليه، يقتضي منطق الحكامة الرشيدة تحويل العقوبة إلى نِسَبٍ من رقم المعاملات، أو ربطها بعدد السجلات المُسرَّبة، بما يُولِّد ردعاً حقيقياً ويُوازن بين الفاعلين الكبار والمقاولات الصغرى والمتوسطة. أما المأخذ الثالث فيكمن في غياب آلية دينامية لتحديث النص: فلا تُلزم أيّ مادة الحكومة بإجراء تقييم دوري ولا بعرض تعديلات تشريعية منتظمة، على الرغم من أنّ ميدان الأمن السيبراني يتسم بتطوّر تكنولوجي سريع (هجمات الثغرات صفرية، وتطبيقات الذكاء الاصطناعي). إدراج بند يفرض مراجعة كل خمس سنوات مثلا كفيل بضمان مواكبة التشريع للتحديات المستجدة، وترسيخ مقاربة استباقية تؤمِّن حماية أكثر نجاعة للبيئة الرقمية الوطنية.

---

[239] مرجع سابق، وزارة الصناعة والاستثمار والتجارة والاقتصاد الرقمي (تسمية سابقة). *المغرب بين تنمية الثقة الرقمية وتطوير الأمن السيبراني*.

[240] المادة 8 من القانون رقم 05.20 المتعلق بالأمن السيبراني.

[241] اللائحة العامة لحماية البيانات رقم 679/2016 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية، وبشأن حرية تداول هذه البيانات، وإلغاء التوجيه EC/46/95، *المادة 33*، الجريدة الرسمية للاتحاد الأوروبي، L 119، 4 ماي 2016، الصفحات 1–88.

[242] المادة 49 من القانون رقم 05.20 المتعلق بالأمن السيبراني.

ثانيا: الثغرات التقنية:

تُعاني البنية التحتية السيبرانية المغربية من ثغرات تقنية حرجة، كشفت عنها سلسلة من الهجمات الأخيرة التي استهدفت مؤسسات حيوية مثل الصندوق الوطني للضمان الاجتماعي (*CNSS*) ووزارة الإدماج الاقتصادي والتشغيل في أواخر عام 2024 وأوائل 2025. هذه الهجمات، التي نُسبت بشكل رئيسي إلى كيان إجرامي سيبراني[243]، أظهرت ضعفًا في تطبيق المعايير الأمنية الدولية؛ حيث افتقرت المنصات المتضررة إلى "الضمانات الحيوية المنصوص عليها بموجب معيار *ISO/IEC 27001*[244]"[245]. هذا الفشل في تطبيق ضوابط الأمن أوجد "ثغرات قابلة للاستغلال في البنية الخلفية للمواقع"، مما جعلها عرضة لـ "هجمات متقدمة مثل حقن *SQL* وتصعيد الامتيازات"[246]. علاوة على ذلك، كشفت التحقيقات عن استغلال "ثغرة يوم-صفر (*zero-day vulnerability*[247]) في نظام قائم على *Oracle* لطرف ثالث"، مما سمح لمرتكبي هذه الأفعال باختراق الشبكة دون اكتشاف وتجاوز "بروتوكولات الأمان الداخلية" للوصول إلى "كميات كبيرة من البيانات غير المشفرة". هذا التسريب تضمن معلومات حساسة للغاية مثل أرقام الهوية الوطنية، التفاصيل المالية، ومعلومات الرواتب. مما يؤكد الافتقار إلى التشفير الفعال والرقابة الدقيقة على أنظمة الطرف الثالث. لم تكن هذه الحوادث مفاجئة؛ ففي عام 2020، تعرضت بيانات 3.5 مليون مستخدم للاختراق بسبب "نقطة وصول غير مؤمنة"[248]. مما يشير إلى استمرارية الثغرات وتجاهل التحذيرات السابقة. وإلى جانب ثغرات اختراق البيانات، شهد المغرب تصاعدًا كبيرًا في هجمات حجب الخدمة الموزعة (*DDoS*[249])،

---

[243] EL HAMDI, Soufiane. Opinion: *The CNSS attack and the road to justice*, Hespress English, 25 avril 2025. Consulté le 06 mai 2025 à 17h00, available at: *https://en.hespress.com.*

[244] معيار *ISO/IEC 27001* هو معيار دولي معتمد لنظام إدارة أمن المعلومات، يُحدّد إطارًا منهجيًا لتأسيس وتطبيق ومراجعة وتحسين سياسات وإجراءات *تهدف إلى حماية سرية وسلامة وتوافر المعلومات*. يركّز هذا المعيار على تقييم المخاطر الأمنية ومعالجتها، ويُلزم المؤسسات بوضع ضوابط تقنية وتنظيمية للحد من التهديدات وضمان الامتثال للمتطلبات القانونية والتنظيمية ذات الصلة.

[245] EL HAMDI, Soufiane. Opinion: *The CNSS attack and the road to justice*. Op. cit.

[246] STAFF WRITER. *Digital Onslaught in Morocco: Govt Hacked, 30K+ Bank Cards Leaked in Escalating Cyberwar,* Launchbase Africa, 10 avril 2025. Consulté le 07 mai 2025 à 15h00, available at : *https://launchbaseafrica.com.*

[247] الثغرة "*Zero-day*": هي نقطة ضعف أو خلل في أحد الأنظمة أو البرمجيات لم يُكشف عنها بعد من قِبل المطوّرين أو الشركات المسؤولة، وبالتالي لا يتوفر لها أي تحديث أمني عند استغلالها. تُعد من *أخطر أنواع الثغرات الأمنية لأنها تُستغل من قبل المهاجمين دون سابق إنذار أو حماية، مما يسمح بتنفيذ هجمات مفاجئة وفعّالة*.

[248] BABAS, 2025, *Cyberattacks*. op. cit.

[249] هجوم حجب الخدمة الموزّع (*DDoS*): هو نوع من الهجمات السيبرانية يُنفّذ من خلال إغراق خادم أو شبكة بحجم هائل من الطلبات الزائفة من مصادر متعددة، بهدف إنهاك موارد النظام وجعله غير قادر على الاستجابة للطلبات الشرعية، مما

مسجلًا "أعلى عدد من هجمات *DDoS* في المنطقة"[250]. هذه الهجمات استهدفت وزارات حيوية مثل الفلاحة والضرائب، وكشفت عن "عدم كفاية استعداد البنية التحتية المغربية للتعامل مع هجمات تشبع حركة المرور واسعة النطاق" و"نقص في موازنة التحميل، ومراقبة حركة المرور، وحماية جدار الحماية المتقدمة"[251]. ولم يقتصر الأمر على الثغرات التقنية في الأنظمة، بل امتد ليشمل نقص الوعي والتدريب الأمني للموظفين؛ فـ"الهندسة الاجتماعية وهجمات التصيد الاحتيالي" لا تزال "نقاط الدخول الأكثر شيوعًا للمهاجمين"، مما يستدعي "تحديثًا كبيرًا لوعي الأمن السيبراني لجميع موظفي تكنولوجيا المعلومات الحكوميين". أخيرًا، سلطت هذه الحوادث الضوء على مشكلة "المركزية" في البنية الأمنية، حيث أن الاعتماد على "نقطة فشل واحدة" يجعل "البنية التحتية بأكملها هشة"، مما يؤكد الحاجة الملحة للانتقال نحو "بنى الأمن السيبراني اللامركزية" وتعزيز "مرونة السيادة الرقمية"[252].

الفقرة الثانية: ضعف الثقافة الأمنية الرقمية وضعف التنسيق الوطني

رغم التقدّم في بعض جوانب البنية الرقمية بالمغرب، تظلّ الثقافة الأمنية الرقمية والتنسيق الوطني من أبرز نقاط الضعف التي تُقوّض فاعلية الاستجابة للتهديدات السيبرانية. وتكشف هذه الفقرة عن التحديات المرتبطة بضعف الوعي، وتشتت المسؤوليات، ونقص الموارد البشرية والتقنية، مما يضعف الجبهة الوطنية في مواجهة الهجمات المتزايدة.

أولاً: مكامن الضعف في ثقافة الأمن الرقمي بالمغرب

تُعد ثقافة الأمن الرقمي حجر الزاوية في أي منظومة دفاع سيبراني فعالة. فمهما بلغت التقنيات والتشريعات من تطور، يبقى الوعي والسلوك البشري عاملين حاسمين. يكشف التحليل نقاط

يؤدي إلى توقف الخدمة جزئيًا أو كليًا. تُستخدم شبكات ضخمة من الأجهزة المخترقة (*botnets*) لتنفيذ هذا النوع من الهجمات، *ويُعد من أكثر الوسائل شيوعًا لتعطيل الأنظمة الرقمية الحساسة.*

[250] MEATECH WATCH, *DDoS Attacks Surge Across North Africa, With Morocco Leading the Region in Cyber Threat Activity*, May 12, 2025. Accessed May 11, 2025, at 20:11, *available at: https://meatechwatch.com*.

[251] RIAHI, Raouf. *Comprehensive Analysis of the April 2025 Cyberattacks on Morocco,* LinkedIn, April 14, 2025. Accessed May 13, 2025, available at: *https://www.linkedin.com.* op. cit.

[252] BABAS, 2025, Cyberattacks.

الضعف المتجذرة في هذا الجانب، والتي تساهم بشكل مباشر في زيادة سطح الهجوم وتسهيل مهمة المهاجمين.

أ – تحليل نقدي لأسباب ضعف الوعي الرقمي

إن ضعف الوعي بمخاطر الفضاء الرقمي وأفضل الممارسات لتأمينه يمثل تحديًا هيكليًا في المغرب، وتتعدد العوامل المساهمة في هذا الضعف.

- **نقص الوعي العام والمؤسسي بمخاطر الأمن السيبراني:**

يشكل نقص الوعي والتثقيف بمخاطر الأمن السيبراني وأفضل ممارساته أحد أبرز التحديات التي تواجه المغرب[253]. هذا النقص لا يقتصر على المواطنين العاديين، بل يمتد ليشمل المؤسسات، ويؤدي إلى ما يمكن تسميته بضعف "النظافة الرقمية" العامة، وبالتالي ارتفاع قابلية الأفراد والأنظمة للتعرض للهجمات. يشير المعهد المغربي لتحليل السياسات في تقريره إلى أن "نقص الوعي بمخاطر الأمن السيبراني" هو تحدٍ رئيسي[254]. هذا النقص في الوعي ليس مجرد غياب للمعلومات، بل يترجم إلى سلوكيات وممارسات رقمية خاطئة تزيد من المخاطر[255]، مما يجعله التربة الخصبة التي تنمو فيها بقية المخاطر السيبرانية.

- **محدودية حملات التوعية الفعالة وتقييمها:**

على الرغم من إطلاق مبادرات توعوية، مثل تلك التي نظمتها وكالة التنمية الرقمية (*ADD*) بالتعاون مع شركائها، والتي استهدفت الجمهور العام والمهنيين والشباب وغطت مواضيع حيوية كمكافحة برامج الفدية وأمن إنترنت الأشياء[256]، إلا أنه لا توجد معلومات واضحة حول مدى فعالية هذه الحملات على المدى الطويل أو تحديدًا دقيقًا لأوجه القصور فيها. إن غياب التقييم المنهجي والمستمر لفعالية حملات التوعية يمثل نقطة ضعف جوهرية في حد ذاته.

---

[253] مليح، يونس. *الهجمات السيبرانية على المؤسسات العمومية المغربية: بين التحديات ومتطلبات الوقاية المؤسسية*، منصة مغرب القانون، 16 أبريل 2025. تم الاطلاع عليه بتاريخ 22 ماي 2025، على الساعة 14:00، متاح على: *https://www.marocdroit.com*.

[254] Hind Idrissi, *Cybersecurity in Morocco: between achievements and challenges*. op. cit.

[255] Tachfine, Khadija. *Report warns Morocco is becoming fertile ground for cyberattacks amid geopolitical tensions.* HESPRESS English – Morocco News, 19 April 2025. Consulted on 20 May 2025 at 15:15. Available at: *https://en.hespress.com*.

[256] الأكاديمية الرقمية. الإطلاق الرسمي لحملة التوعية بالأمن السيبراني. الأكاديمية الرقمية، 1 يوليوز 2022. تم الاطلاع عليه بتاريخ 06 ماي 2025، على الساعة 16:20، على الرابط: https://academiaraqmya.gov.ma.

فبدون آليات تقييم واضحة ومؤشرات أداء محددة، يصبح من الصعب معرفة ما إذا كانت هذه الحملات تحقق أهدافها بالفعل في ترسيخ ثقافة أمنية مستدامة، أم أنها تظل مجرد أنشطة متفرقة لا تحدث التأثير العميق المطلوب. هذا الغياب يعيق عملية التحسين المستمر ويجعل من الصعب توجيه الموارد نحو المبادرات الأكثر نجاعة.

- **العوامل الثقافية: "ثقافة حجب المعلومات" وتأثيرها المحتمل:**

يسلط تقرير صادر عن مؤسسة فريدريش ناومان على ما وصفه بـ "ثقافة حجب المعلومات" في المغرب، حيث تُعتبر المعرفة في كثير من الأحيان ملكية فردية يُحتفظ بها، بدلاً من اعتبارها مورداً مشتركاً يجب تقاسمه[257]. وإن كان هذا لم يرتبط بشكل مباشر وصريح بين "ثقافة حجب المعلومات" وضعف الأمن السيبراني، إلا أنه يمكن استنباط تداعيات سلبية غير مباشرة على هذا الأخير. فالأمن السيبراني الفعال، خاصة في مواجهة التهديدات المتطورة والمعقدة، يعتمد بشكل كبير على التعاون وتبادل المعلومات والخبرات، سواء كان ذلك بين المؤسسات أو حتى بين الأفراد. إذا كانت هناك نزعة عامة نحو التحفظ في مشاركة المعلومات، فمن المحتمل أن يمتد هذا السلوك ليشمل المعلومات المتعلقة بالحوادث الأمنية، أو الثغرات المكتشفة، أو حتى أفضل الممارسات الدفاعية. هذا التردد في الشفافية والمشاركة يمكن أن يعيق بناء فهم مشترك للمخاطر ويضعف القدرة الجماعية على التصدي لها، مما يؤدي إلى إبطاء الابتكار في الحلول الأمنية وتعميق انعدام الثقة بين مختلف الفاعلين.

- **انخفاض مستوى الثقافة الرقمية في بعض المناطق:**

تشير بعض التحليلات النقدية الموجهة لاستراتيجية "المغرب الرقمي 2030" إلى أن التركيز المعلن على الإدماج الرقمي قد لا يستجيب بشكل كامل للتحديات القائمة في المناطق القروية أو المهمشة. ففي هذه المناطق، قد تظل خدمات الاتصالات غير كافية، والبنية التحتية الرقمية غير متطورة بالقدر اللازم، وينخفض مستوى الثقافة الرقمية الأساسية لدى السكان[258]. هذا

---

[257] Zayakh, Yasmine. *The Culture of Withholding Information in Morocco: A Barrier to Progress?* Friedrich Naumann Foundation for Freedom, 22 April 2025. Accessed on 06 May 2025 at 16:40. Available at: *https://www.freiheit.org*.

[258] بوجبير، فؤاد. نقد استراتيجية المغرب الرقمي 2030 مصحوبًا بتوصيات (مع إدماج عنصر الذكاء الاصطناعي). موقع أشطاري 24، 15 ماي 2025. تم الاطلاع عليه بتاريخ 13 ماي 2025، على الساعة 17:10، على الرابط: https://achtari24.com.

الانخفاض في الأبجديات الرقمية يجعل الأفراد في هذه المناطق أكثر عرضة للمخاطر السيبرانية الأساسية، مثل الوقوع ضحية لعمليات احتيال بسيطة أو عدم القدرة على تمييز الرسائل الخبيثة.

ب – تأثير ضعف الوعي على الأفراد والمؤسسات

إن ضعف الوعي بالأمن الرقمي ليس مجرد مفهوم نظري، بل له تداعيات ملموسة وخطيرة على الأفراد والمؤسسات على حد سواء، ويظهر ذلك جليًا في طبيعة الحوادث السيبرانية السائدة.

- **العامل البشري كسبب رئيسي للحوادث:**

تؤكد العديد من الدراسات العالمية أن الخطأ البشري يشكل سببًا رئيسيًا في نسبة كبيرة جدًا من انتهاكات الأمن السيبراني، حيث تشير إحدى الدراسات التي أجرتها شركة *IBM* إلى أن هذه النسبة قد تصل إلى 95% من الحوادث[259]. وفي السياق المغربي، يشير بارومتر الأمن السيبراني المغربي لعام 2025، الصادر عن جمعية مستخدمي نظم المعلومات بالمغرب (*AUSIM*) بالتعاون مع شركة *PwC*، إلى أن رأس المال البشري لا يزال يمثل نقطة ضعف حرجة، حيث يُعتبر الخطأ البشري ناقلًا أساسيًا وممرًا رئيسيًا للهجمات السيبرانية. وتعتبر 52% من الشركات المغربية التي شملها الاستطلاع أن توعية الموظفين تمثل تحديًا كبيرًا، خاصة فيما يتعلق بمحاولات التصيد الاحتيالي (*phishing*)، وتقنيات التزييف العميق (*deepfakes*)، ونقاط الضعف المتعلقة بإدارة كلمات المرور[260].

ويأتي حادث اختراق أنظمة الصندوق الوطني للضمان الاجتماعي (*CNSS*) كدليل إضافي، حيث تشير التحليلات إلى أنه نتج على الأرجح عن مزيج من الخطأ البشري والثغرات التقنية[261]. هذا التركيز المتواتر على "الخطأ البشري" كسبب جوهري للحوادث يؤكد حقيقة أن

---

[259] IBM Global Technology Services. *"IBM Security Services 2014 Cyber Security Intelligence Index: Analysis of Cyber Attack and Incident Data from IBM's Worldwide Security Operations."* Somers, NY: IBM Corporation, June 2014.

[260] PwC et AUSIM, *Ausimètre 2025 – Baromètre de la cybersécurité au Maroc : Livre blanc présentant la synthèse des résultats de l'enquête (2e édition)*, Casablanca, PwC & AUSIM, 2025, PP.12.

[261] FAOUZI, Adil. *Transparency Maroc: CNSS Data Breach Exposes Critical Flaws in Morocco's Cybersecurity.* op. cit.

الاستثمار في الحلول التكنولوجية وحدها، مهما بلغت تطورًا، يظل غير كافٍ لضمان حماية شاملة. فالحلقة الأضعف في سلسلة الدفاع غالبًا ما تكون المستخدم غير الواعي أو غير المدرب بشكل كافٍ، مما يجعل برامج التوعية والتدريب المستمر ليست مجرد إضافة شكلية، بل ضرورة استراتيجية لا غنى عنها لحماية الأصول الرقمية والمعلومات الحساسة.

- **انتشار التصيد الاحتيالي (*Phishing*) وبرامج الفدية (*Ransomware*) نتيجة ضعف الوعي:**

تعتبر هجمات التصيد الاحتيالي من أبرز الأمثلة على كيفية استغلال ضعف الوعي الأمني لدى المستخدمين[262]. كما أشار تقرير للمعهد المغربي لتحليل السياسات إلى تنامي هجمات برامج الفدية، والهندسة الاجتماعية، والاحتيال المالي، والتي تستهدف بشكل مباشر نقاط الضعف البشرية. وقد شهد المغرب ارتفاعًا في هذه الأنواع من الهجمات، فبين أبريل ويونيو 2020 وحدها، سجل تقرير لشركة كاسبرسكي أكثر من 13.4 مليون هجوم سيبراني في المغرب، مع تصاعد ملحوظ في محاولات التصيد وهجمات الفدية.[263]

وتشير دراسة استقصائية أجرتها شركة *KnowBe4* حول تجارب الجرائم السيبرانية في أفريقيا إلى ارتفاع نسبة ضحايا التصيد الاحتيالي من 26% في عام 2023 إلى 32% في عام 2025، بينما ظلت نسبة الإصابة بالفيروسات مستقرة عند حوالي 51%، مع زيادة طفيفة في الخسائر المالية الناجمة عن عمليات الاحتيال. ومما يثير القلق بشكل خاص هو تصنيف المغرب، وفقًا لتقرير تقييم التهديدات السيبرانية في أفريقيا لعام 2022 الصادر عن الإنتربول، كأكثر دولة أفريقية تضررًا من برمجيات "حصان طروادة" المصرفية (*banking trojans*) وبرمجيات سرقة البيانات (*stealer malware*)، حيث تم تسجيل 18,827 هجومًا في عام 2022.[264]

---

[262] مرجع سابق، مليح، يونس. *الهجمات السيبرانية على المؤسسات العمومية المغربية: بين التحديات ومتطلبات الوقاية المؤسسية*.

[263] Hind Idrissi, *Cybersecurity in Morocco: between achievements and challenges*. op. cit.

[264] KnowBe4, *African Cybersecurity & Awareness Report 2025*, Clearwater, FL, KnowBe4, Inc., 2025. pp.9.

- **تأثير ضعف الوعي على المؤسسات (خاصة الصغيرة والمتوسطة):**

تواجه المؤسسات الصغيرة والمتوسطة في المغرب تحديات مالية وتقنية كبيرة تجعلها أكثر عرضة للمخاطر السيبرانية. فالقيود المالية تحد من قدرتها على الاستثمار في حلول حماية متقدمة أو توظيف خبراء متخصصين. وتشير دراسة حول التحول الرقمي لهذه الشركات إلى أنها تواجه تحديات تشمل نقص المهارات والخبرات الرقمية، والقيود المالية، والمخاوف المتعلقة بالأمن السيبراني وخصوصية البيانات[265].

ويؤكد تقرير لشركة *Orange Cyberdefense* أن الشركات المغربية يبدو أنها "تستثمر أقل في الأمن السيبراني" مقارنة بالمعايير الأوروبية، حيث يخصص في المتوسط حوالي 15% من ميزانية تكنولوجيا المعلومات للأمن في أوروبا[266]. وعلى الرغم من أن وعي الأمن السيبراني لا يزال في مراحله الأولى لدى العديد من المؤسسات المغربية، إلا أن هناك بوادر إدراك متزايد لضرورة مراقبة مشهد التهديدات الخارجية، كما تلاحظ بعض الشركات الناشئة العاملة في هذا المجال[267].

إن ضعف الشركات الصغيرة والمتوسطة ماليًا وتقنيًا في مواجهة التهديدات السيبرانية يكتسب أهمية خاصة عند الأخذ في الاعتبار أنها تشكل حوالي 93% من إجمالي الشركات في المغرب وتساهم بنسبة كبيرة (46%) في التوظيف[268]. هذا الواقع يجعل هذه الشريحة الواسعة من النسيج الاقتصادي بمثابة "كعب أخيل" للاقتصاد الرقمي المغربي. فاستهداف هذه الشركات بهجمات منخفضة التكلفة نسبيًا ولكنها عالية التأثير، مثل برامج الفدية، يمكن أن يكون له تداعيات اقتصادية واجتماعية واسعة النطاق، تتجاوز الخسائر الفردية لهذه الشركات لتؤثر على الاستقرار الاقتصادي العام.

---

[265] Hind Idrissi, *Cybersecurity in Morocco: between achievements and challenges.* op. cit.
[266] Orange Cyberdefense Maroc. (2025, 30 avril). *Multiplication des cyberattaques en Afrique : Orange Cyberdefense Maroc est là pour renforcer la cybersécurité des entreprises*. Orange Cyberdefense. Consulté le 26 mai 2025, à l'adresse : *https://www.orangecyberdefense.com.*
[267] Toutate, I. (2025, 12 avril). *Defendis: The Cybersecurity Startup Shielding Africa's Digital Transformation. Morocco World News.* Consulté le 16 mai 2025, depuis *https://www.moroccoworldnews.com.*
[268] Bennacer, M. K., El Mahdi, E. M., & Lahmouchi, M. (2025). *Digital Transformation in Moroccan SMEs: Overcoming Barriers and Achieving Growth. TEM Journal,* 14(2), pp. 1269. *https://doi.org/10.18421/TEM142-28.*

ج – ضعف تأهيل الموارد البشرية في القطاعين العام والخاص:

تتكامل إشكالية ضعف الوعي مع قصور ملحوظ في برامج تدريب الموظفين، سواء في القطاع العام أو الخاص، مما يفاقم من الهشاشة الرقمية. تشير العديد من التحليلات إلى الحاجة الماسة إلى "موظفين ملمين بالوضع وفرق مدربة" كأحد التحديات الرئيسية التي يجب معالجتها. وفي القطاع العام تحديدًا، هناك توصيات متكررة بضرورة "تنظيم برامج تكوينية دورية في مجال الأمن السيبراني". كما أن تعزيز ثقافة الأمن السيبراني يتطلب جهودًا مكثفة في "التدريب والتوعية والدعم، خاصة للهياكل الصغيرة" التي غالبًا ما تفتقر إلى الموارد والخبرات الداخلية[269].

إن هذه الدعوات المتكررة للتدريب والتأهيل تشير بوضوح إلى أن برامج التدريب الحالية، إن كانت موجودة بشكل ممنهج ومنتظم، لا ترقى إلى مستوى التحديات القائمة. هذا النقص لا يقتصر على المهارات التقنية المتقدمة التي قد يحتاجها متخصصو الأمن السيبراني، بل يشمل أيضًا الوعي الأمني الأساسي الذي يجب أن يتمتع به جميع الموظفين. فالموظف العادي الذي لا يمتلك الأدوات المعرفية والسلوكية للتعرف على رسالة تصيد بسيطة أو لتطبيق ممارسات آمنة في التعامل مع البيانات وكلمات المرور، يشكل خط الدفاع الأول الذي يسهل اختراقه، وبالتالي يجعل الاستثمارات في الحلول التقنية أقل جدوى.

ثانيا: مكامن الضعف في التنسيق الوطني للأمن السيبراني بالمغرب:

لا يقتصر الأمر على ثقافة الأمن الرقمي، بل يمتد ليشمل آليات التنسيق الوطني التي تُعتبر حاسمة في بناء جبهة موحدة وفعالة ضد التهديدات السيبرانية. يكشف هذا الجزء عن مجموعة من نقاط الضعف.

- **نقد تشتت المسؤوليات المؤسسية وغياب آليات تنسيق عملياتي فعالة**

تعتبر الحكامة الرشيدة والتنسيق الفعال بين مختلف الفاعلين المؤسسيين شرطًا أساسيًا لنجاح أي استراتيجية وطنية للأمن السيبراني. إلا أن الواقع في المغرب يشير إلى تحديات كبيرة في

[269] Bennani, A.-E. (2025, 13 avril). *Cybersécurité, IA et gouvernance numérique : construire une stratégie marocaine dans un monde connecté.* L'Opinion. Consulté le 23 mai 2025 à 19h47, depuis : *https://www.lopinion.ma.*

هذا الصدد. ويُلاحظ وجود "تفتيت للمهارات المؤسسية بين المديرية العامة لأمن نظم المعلومات (*DGSSI*) التابعة لإدارة الدفاع الوطني، واللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (*CNDP*)، ووزارة الانتقال الرقمي وإصلاح الإدارة، وهيئات أخرى" معنية بشكل أو بآخر بالأمن السيبراني[270]. هذا التشتت في المسؤوليات يمكن أن يؤدي حتمًا إلى تداخل في الصلاحيات بين هذه الجهات، وبطء في عملية اتخاذ القرارات الحاسمة، خاصة في أوقات الأزمات السيبرانية التي تتطلب استجابة سريعة ومنسقة. كما أنه قد يجعل من الصعب تحديد المسؤولية بشكل واضح عند وقوع حوادث أو إخفاقات، مما يضعف من فعالية الاستجابة الوطنية الشاملة ويؤدي إلى ضياع الجهود والموارد.

- **محدودية التنسيق العملياتي وتبادل البيانات الفوري:**

أشارت دراسة تحليلية إلى "محدودية التنسيق بين الفاعلين. فكل مؤسسة تعمل ضمن اختصاصها دون آلية فعالة للتنسيق العملياتي وتبادل البيانات في الوقت الحقيقي؛ مما يقلص فعالية الاستجابة للطوارئ السيبرانية"[271]. وتتفق مع هذا الطرح دعوات أخرى تؤكد على الحاجة إلى تعزيز التعاون بين الحكومة والصناعة والأوساط الأكاديمية[272]، وضرورة وجود قيادة مشتركة بين الوزارات وتنسيق فعال بين القطاعين العام والخاص والمجتمع المدني، خاصة في إطار تنفيذ استراتيجيات وطنية كبرى مثل "استراتيجية المغرب الرقمي 2030"[273].

إن غياب التنسيق العملياتي الفعال وتبادل المعلومات الاستخباراتية حول التهديدات في الوقت الحقيقي يعني أن كل مؤسسة قد تجد نفسها تقاتل بمفردها في مواجهة هجمات متطورة ومنظمة. هذا الوضع يسهل على المهاجمين استهداف المؤسسات واحدة تلو الأخرى، مستغلين

---

[270] Yasser Elkouri. « *Cyberattaque contre la CNSS marocaine : une atteinte grave aux systèmes de traitement automatisé de données (STAD)* », Village de la Justice, 14 avril 2025. Consulté le 22 mai 2025 à 21:30, depuis : *https://www.village-justice.com.*

[271] Hind Idrissi, *Cybersecurity in Morocco: between achievements and challenges*. Op. cit.

[272] The Trade Adviser. (2024, March 24). *Securing the Digital Realm: Cybersecurity Developments in Morocco. The Trade Adviser*. Retrieved on May 25, 2025 at 21:45 from: *https://www.thetradeadviser.com.*

[273] مرجع سابق، بوجبير، فؤاد. *نقد استراتيجية المغرب الرقمي 2030 مصحوبًا بتوصيات (مع إدماج عنصر الذكاء الاصطناعي.*

غياب رؤية شاملة وموحدة للتهديدات على المستوى الوطني، مما يعيق بدوره اتخاذ قرارات استباقية فعالة ومبنية على معلومات دقيقة وحديثة.

- **غياب تقاسم الموارد التقنية بين الإدارات:**

يُضاف إلى ما سبق، نقص في تقاسم الموارد التقنية بين الإدارات العمومية[274]. هذا النقص في التشاركية يؤدي إلى هدر واضح للموارد، حيث قد تجد إدارات متعددة نفسها تقوم بشراء نفس الحلول التقنية باهظة الثمن أو تطوير أدوات متشابهة بشكل منفصل ومستقل، بدلاً من الاستفادة من الخبرات والموارد المجمعة على المستوى الوطني. هذا الوضع لا يزيد فقط من التكاليف المالية على الدولة، بل يقلل أيضًا من الكفاءة العامة ويحول دون بناء قدرات تقنية وطنية قوية وموحدة.

ثالثا: تحليل إشكالية نقص الموارد (المالية، البشرية المتخصصة)

يمثل نقص الموارد، بشقيها المالي والبشري المتخصص، عائقًا كبيرًا أمام تعزيز قدرات الأمن السيبراني في المغرب، ويؤثر بشكل مباشر على فعالية آليات التنسيق الوطني.

- **غياب ميزانيات معلنة وواضحة مخصصة للأمن السيبراني:**

يصعب تحديد حجم التمويل المخصَّص لتطوير القدرات السيبرانية في المغرب لعدم توفّر ميزانية معلَنة بهذا الشأن. كما تنتقد بعض التحليلات "استراتيجية المغرب الرقمي 2030" بسبب غياب خريطة طريق مالية واضحة، خاصة لتمويل الطموحات الكبيرة في مجالي الذكاء الاصطناعي والأمن السيبراني[275].

إن عدم وجود ميزانيات معلنة وشفافة ومخصصة بشكل واضح للأمن السيبراني يجعل من الصعب تقييم مدى جدية الالتزام الحكومي بهذا المجال الحيوي. كما أنه يعيق عمليات التخطيط الاستراتيجي طويل الأجل من قبل مختلف المؤسسات المعنية، وقد يشير ضمنيًا إلى

---

[274] Yasser Elkouri. « *Cyberattaque contre la CNSS marocaine : une atteinte grave aux systèmes de traitement automatisé de données (STAD)* ». Op. cit.

[275] مرجع سابق، بوجبير، فؤاد. *نقد استراتيجية المغرب الرقمي 2030 مصحوبًا بتوصيات (مع إدماج عنصر الذكاء الاصطناعي.*

أن الأمن السيبراني لا يحظى بالأولوية الكافية عند توزيع الموارد المالية المتاحة، مما ينعكس سلبًا على قدرات التنسيق والاستجابة.

- **نقص الكفاءات المتخصصة في القطاع العام والفجوة في المهارات:**

تعتبر ندرة الكفاءات المؤهلة لمواجهة التهديدات المتطورة تحديًا رئيسيًا آخر. ويُشار إلى نقص الكفاءات المتخصصة في الأمن السيبراني كأحد الأسباب الرئيسية للفجوة في الاستثمار في هذا المجال. ويؤكد تقرير آخر وجود "شح في الكفاءات المتخصصة في القطاع العام"[276]. هذا النقص في الكفاءات الوطنية يجعل العديد من المؤسسات المغربية، بما فيها الحكومية، تعتمد على حلول وخدمات أجنبية جاهزة، مما يثير تساؤلات مشروعة حول السيادة الرقمية وإمكانية تعرض البيانات الحساسة لمخاطر إضافية[277].

وكذلك هناك وجود نقص فعلي في محترفي الأمن السيبراني في المغرب، وفجوة واضحة في المهارات المطلوبة، مع ملاحظة عدم تطابق أحيانًا بين مخرجات النظام التعليمي والتكويني واحتياجات سوق العمل الفعلية في هذا المجال الدقيق والمتطور. إن نقص الكفاءات لا يؤثر فقط على القدرة التقنية المباشرة على مواجهة الهجمات، بل يمتد ليشمل القدرة على وضع استراتيجيات وطنية فعالة، وتقييم الحلول التقنية المعروضة، وتدريب الكوادر الأخرى، مما يخلق حلقة مفرغة من الضعف. الاعتماد على الخبرات الأجنبية قد يكون حلاً مؤقتًا لبعض المشاكل، ولكنه لا يساهم في بناء قدرة وطنية مستدامة، بل وقد يزيد من التبعية ويثير مخاوف سيادية مشروعة.

- **ضعف ثقافة المخاطر الرقمية لدى صناع القرار:**

يضاف إلى ذلك نقص الموارد المالية والبشرية، مما يعني ضعف ثقافة المخاطر الرقمية لدى كبار صناع القرار[278]. إذا كان صناع القرار على أعلى المستويات لا يقدرون حجم المخاطر الرقمية وتداعياتها المحتملة على الأمن والاقتصاد والمجتمع بشكل كامل ودقيق، فمن غير

---

[276] Yasser Elkouri. « *Cyberattaque contre la CNSS marocaine : une atteinte grave aux systèmes de traitement automatisé de données (STAD)* ». Op. cit.

[277] بشرى الردادي. سيادة رقمية مؤجلة.. متى نؤسس أمننا السيبراني بأيدينا؟ تيل كيل عربي، الخميس 8 ماي 2025، على الساعة 13:15. تم الاطلاع عليه بتاريخ 18 ماي 2025، على الساعة 22:07، على الرابط: https://ar.telquel.ma.

[278] Yasser Elkouri. « *Cyberattaque contre la CNSS marocaine : une atteinte grave aux systèmes de traitement automatisé de données (STAD)* ». Op. cit.

المرجح أن يتم تخصيص الموارد الكافية لهذا المجال، أو إعطاؤه الأولوية اللازمة في السياسات والاستراتيجيات الوطنية. هذا الضعف في تقدير المخاطر على مستوى القمة يؤثر بشكل مباشر على جميع جوانب منظومة الأمن السيبراني، بما في ذلك فعالية التنسيق الوطني وتخصيص الموارد اللازمة.

- **غياب خطط استجابة مُحكمة لدى كثير من المؤسسات:**

علاوة الى ما سبق، هناك غياب خطط استجابة مُحكمة لدى كثير من المؤسسات، بما فيها تلك الموجودة في المغرب. هذا النقص في الاستعداد المسبق يمكن أن يؤدي إلى عواقب وخيمة عند وقوع هجوم سيبراني، مثل "التأخر في الاستجابة الذي يؤدي إلى تفاقم الأضرار، والخسائر المالية والسمعة، وعدم الامتثال للتنظيمات، مما يؤدي إلى فرض عقوبات، بالإضافة إلى الارتباك والذعر بين الموظفين وأصحاب المصلحة"[279].

إن غياب خطط استجابة واضحة ومختبرة مسبقًا يعني أن المؤسسات غالبًا ما تتفاعل مع الحوادث السيبرانية بشكل عشوائي وغير منظم، بدلاً من اتباع إجراءات مدروسة ومحددة سلفًا. هذا الوضع لا يزيد فقط من حجم الأضرار المحتملة، بل يطيل أيضًا من أمد التعافي واستعادة الخدمات. ويعكس هذا النقص في الاستعداد غيابًا للتخطيط الاستباقي، وهو جزء لا يتجزأ من ضعف آليات التنسيق والحكامة على المستويين المؤسسي والوطني.

- **الاعتماد المفرط على الحلول الأجنبية وتأثيره على السيادة الرقمية:**

يمثل الاعتماد الكبير على الحلول والخبرات الأجنبية في مجال الأمن السيبراني نقطة ضعف أخرى ذات أبعاد استراتيجية. فنقص الكفاءات الوطنية المتخصصة، كما ذُكر سابقًا، يجعل العديد من المؤسسات المغربية، بما فيها الحكومية، تعتمد بشكل كبير على حلول تكنولوجية وخدمات استشارية أجنبية جاهزة. هذا الاعتماد، وإن كان قد يوفر حلولاً سريعة لبعض المشاكل، فإنه "يطرح أسئلة خطيرة حول السيادة الرقمية وإمكانية الوصول غير المشروع للبيانات الحساسة" من قبل جهات خارجية. كما أن الرغبة المعلنة في الحفاظ على السيادة الرقمية الوطنية تصطدم بالواقع المتمثل في الاعتماد المستمر على مزودي خدمات الحوسبة السحابية

[279] Hind Idrissi, *Cybersecurity in Morocco: between achievements and challenges*. Op. cit.

الدوليين، وهو ما "قد يؤثر سلبًا في المستقبل على السيطرة الوطنية على البيانات الاستراتيجية". إن الاعتماد على الحلول الأجنبية ليس مجرد مسألة تجارية أو تقنية، بل له أبعاد استراتيجية عميقة تتعلق بالسيادة الرقمية والأمن القومي[280]. ففهم هذه الحلول بشكل كامل والتحكم فيها قد يكون محدودًا بالنسبة للكوادر المحلية، وقد تكون هناك مخاطر غير معلنة أو تبعيات غير مرغوب فيها مرتبطة باستخدام هذه الحلول. ويتطلب تحقيق توازن دقيق بين الاستفادة من الخبرات والتكنولوجيات العالمية المتقدمة، وبين بناء قدرات وطنية ذاتية قادرة على ضمان درجة معقولة من الاستقلالية والتحكم في الفضاء الرقمي الوطني.

المبحث الثاني: استراتيجيات التطوير واستلهام التجارب الدولية

في ظل إدراك المغرب لحجم التهديدات الرقمية وتنامي رهانات الأمن السيبراني، يطرح هذا المبحث مقاربة عملية تستند إلى استلهام التجارب الدولية الرائدة واستشراف سبل التطوير الوطني. تمثّل النماذج المتقدّمة مثل الولايات المتحدة، إستونيا، وسنغافورة مختبرات فعلية لصياغة سياسات مرنة وفعّالة في مواجهة الهجمات السيبرانية المعقّدة، وهي تجارب تسمح بفهم عميق لبنية الأمن الرقمي الناجح، سواء على مستوى التشريع أو الحكامة أو رأس المال البشري. لذلك، ينقسم هذا المبحث إلى مطلبين مترابطين: المطلب الأول يركّز على تحليل نقاط القوة في النماذج الثلاثة المذكورة، مع الوقوف عند آليات التكييف الممكنة مع الخصوصية المغربية. أما بخصوص المطلب الثاني ينتقل إلى المستوى الاستشرافي، ويعالج آفاق تعزيز الأمن السيبراني في المغرب، تحديدًا من خلال تأهيل الكفاءات وبناء الوعي السيبراني، ثم بلورة مفهوم السيادة الرقمية كأداة لمناعة وطنية ذكية وقادرة على الصمود.

المطلب الأول: الاستفادة من التجارب الدولية الرائدة في الأمن السيبراني

في سياق تنامي التحديات الرقمية وتعقّد البيئة السيبرانية العالمية، تبرز الحاجة إلى تحليل تجارب الدول التي راكمت خبرة مؤسساتية وتشريعية وتقنية في مجال الأمن السيبراني. فالفهم العميق لهذه النماذج يسمح باستكشاف الآليات الكفيلة بترسيخ مناعة رقمية فعّالة، دون إغفال

[280] Kezzoute, M. (2025). *Cyber Governance in Morocco: Between the Consolidation of Interne Status and the Enhancement of Global Positioning. Cyberspace Studies*, 9(1), pp260. University of Tehran. *https://doi.org/10.22059/jcss.2025.385012.1114.*

اختلاف السياقات الوطنية. وعليه، سيتم في هذا المطلب معالجة الموضوع على مستويين متكاملين: في الفقرة الاولى، تحليل نقاط القوة في النماذج الرائدة (الولايات المتحدة، إستونيا، وسنغافورة)؛ وفي الفقرة الثانية، تكييف الدروس المستخلصة عبر مقارنة معيارية مع الحالة المغربية، واستثمار عناصر النجاح في بناء مقاربة وطنية أكثر صلابة ومرونة.

الفقرة الأولى: تحليل النماذج الرائدة: الولايات المتحدة، إستونيا، وسنغافورة

في ظل تصاعد التهديدات السيبرانية وتزايد الاعتماد على البنية التحتية الرقمية، أصبحت دراسة النماذج الدولية الناجحة في الأمن السيبراني ضرورة لفهم أفضل الممارسات التي يمكن أن تُعزز الحماية الرقمية. تُعد الولايات المتحدة الأمريكية، إستونيا، وسنغافورة من بين الدول الرائدة في هذا المجال، حيث طورت كل منها استراتيجيات شاملة تجمع بين التشريعات القوية، الشراكات بين القطاعين العام والخاص، الاستثمار في البحث والتطوير، والتعليم السيبراني.

أولا: تحليل نقاط القوة في نموذج الأمن السيبراني الأمريكي

يتميز نموذج الأمن السيبراني في الولايات المتحدة بمجموعة متعددة الأوجه من نقاط القوة التي تعزز بشكل جماعي دفاعاتها ضد التهديدات السيبرانية. في صميم هذا النموذج يوجد نهج شامل لإدارة المخاطر، كما هو مفصل في استراتيجية الأمن السيبراني لوزارة الأمن الداخلي (*DHS*). يشمل هذا النهج خمسة أعمدة: تحديد المخاطر، وتقليل الثغرات، وتقليل التهديدات، والتخفيف من العواقب، وتمكين نتائج الأمن السيبراني، مما يوفر إطارًا شاملاً لإدارة مخاطر الأمن السيبراني الوطنية. تتولى وزارة الأمن الداخلي دورًا قياديًا محوريًا، حيث تنسق الجهود عبر الكيانات الفيدرالية وغير الفيدرالية، مما يضمن استجابة موحدة وفعالة لحوادث الإنترنت، علاوة على ذلك، تضع وزارة الأمن الداخلي تركيزًا قويًا على تطوير القوى العاملة، معالجة النقص الحاد في المتخصصين في الأمن السيبراني من خلال برامج التوظيف والتدريب والاحتفاظ المستهدفة، كما هو موضح في دعم برامج التعليم السيبراني[281]. كما تعزز الوزارة حماية البنية التحتية الحيوية، مثل قطاعات الطاقة والمالية والرعاية الصحية، من خلال الشراكات مع الوكالات الخاصة بالقطاعات وتوفير الأدوات وأفضل. وتدعم آليات تبادل

[281] U.S. Department of Homeland Security. 2018. *Cybersecurity Strategy. Washington, DC: U.S. Department of Homeland Security,* pp. 3-10.

المعلومات القوية، مثل مركز التكامل الوطني للأمن السيبراني والاتصالات (*NCCIC*)، تبادل مؤشرات التهديدات السيبرانية، مما يعزز الوعي الظرفي[282].

تكمن إحدى نقاط القوة الرئيسية في الطبيعة الطوعية والمرنة لإطار عمل الأمن السيبراني التابع للمعهد الوطني للمعايير والتكنولوجيا (*NIST*)، والذي يمكّن المنظمات من تخصيص ممارسات الأمن السيبراني لتناسب سياقاتها الخاصة مع الالتزام بالمعايير وأفضل الممارسات المعمول بها، مثل *ISO/IEC 27001*. يتبنى هذا الإطار منهجية قائمة على المخاطر، مما يسمح للمنظمات بتحديد أولويات جهودها في مجال الأمن السيبراني بناءً على تقييمات المخاطر الفردية، وبالتالي تحسين تخصيص الموارد. يوفر الإطار نهجًا منظمًا يدعم اتخاذ القرارات على جميع مستويات المنظمة، من المديرين التنفيذيين إلى الموظفين العملياتيين، مما يضمن استراتيجية أمن سيبراني متماسكة، كما يظهر في تدفقات المعلومات والقرارات داخل المنظمات. علاوة على ذلك، ينشئ الإطار لغة مشتركة تسهل تحسين التواصل بشأن مخاطر الأمن السيبراني سواء داخل المنظمات أو بين أصحاب المصلحة الخارجيين، مما يعزز التعاون[283].

من وجهة نظر عسكرية، تؤكد استراتيجية وزارة الدفاع (*DOD*) للأمن السيبراني على موقف استباقي من خلال استراتيجية "الدفاع إلى الأمام". يتضمن هذا النهج المشاركة الفعالة والتعطيل للجهات الفاعلة السيبرانية الخبيثة قبل أن تتمكن من إلحاق الضرر بمصالح الولايات المتحدة، كما هو موضح في العمليات لحماية الانتخابات الأمريكية منذ عام 2018. تبرز الاستراتيجية أهمية دمج جهود الأمن السيبراني مع الحلفاء والشركاء، وتعزيز الدفاع الجماعي من خلال التدريب المشترك وتبادل المعلومات والعمليات التعاونية مثل مهام "البحث إلى الأمام"، التي عززت العلاقات مع دول مثل أوكرانيا. بالإضافة إلى ذلك، تستثمر وزارة الدفاع في التقنيات الناشئة، بما في ذلك هياكل *Zero Trust* وأدوات الأمن السيبراني المعتمدة على الذكاء الاصطناعي، للحفاظ على التفوق التكنولوجي في الفضاء. كما تدعم حماية البنية التحتية الحيوية وقاعدة الصناعة الدفاعية من خلال الشراكات العامة والخاصة، وبرامج مثل برنامج

---

[282] *U.S. Department of Homeland Security*, op. cit., pp. 11–13.

[283] National Institute of Standards and Technology. 2013. *Preliminary Cybersecurity Framework*. Gaithersburg, MD: National Institute of Standards and Technology.

شهادة نضج الأمن السيبراني، وتوفير خدمات الأمن السيبراني بدون تكلفة للشركات الصغيرة والمتوسطة[284].

تستفيد الولايات المتحدة أيضًا من موقعها كموطن لبعض أكثر شركات التكنولوجيا ابتكارًا في العالم، والتي تقف في طليعة تطوير حلول متقدمة للأمن السيبراني والبنية التحتية الرقمية، كما هو موضح في دعمها لأوكرانيا خلال الغزو الروسي. تحافظ الولايات المتحدة على بيئة سياسية شفافة وشاملة وتمكينية تدعم تدابير الأمن السيبراني الفعالة وتشجع على المشاركة الواسعة من الحكومة والقطاع الخاص والمجتمع المدني والمجتمعات التقنية، كما هو موضح في نهجها متعدد أصحاب المصلحة للحكامة الرقمية .يُعد المشاركة القوية للمجتمع المدني والمجتمعات التقنية أمرًا جديرًا بالملاحظة بشكل خاص، حيث تساهم في الكشف المبكر عن التهديدات وتطوير الحلول والدعوة إلى سياسات رقمية تحترم الحقوق، كما رأينا في دعم ألبانيا وأوكرانيا ضد الهجمات السيبرانية[285].

على الصعيد الدبلوماسي، تشارك الولايات المتحدة بشكل استباقي في تشكيل المعايير الدولية والاستجابة لحوادث الإنترنت، مما يعزز قيادتها في مجال الأمن السيبراني العالمي. يشمل ذلك بناء التحالفات، وتعزيز سلوك الدول المسؤول في الفضاء السيبراني، وتقديم الدعم السريع للحلفاء الذين يتعرضون لهجمات سيبرانية، كما رأينا في الاستجابات لحوادث في أوكرانيا وألبانيا وكوستاريكا. من خلال المشاركة في المنتديات الدولية مثل الأمم المتحدة والمجموعة السبعة، تؤثر الولايات المتحدة على تطوير معايير ومعايير الأمن السيبراني، مثل عملية *G7 Hiroshima AI*. تُظهر هذه الجهود قدرة الولايات المتحدة على تعبئة الموارد والخبرات بسرعة، مما يعزز مكانتها كقائد عالمي في الأمن السيبراني[286].

في الختام، تكمن نقاط القوة في نموذج الأمن السيبراني الأمريكي في استراتيجيات إدارة المخاطر الشاملة، والقيادة والتنسيق القويين، والأطر المرنة والتكيفية، ومواقف الدفاع

---

[284] U.S. Department of Defense. 2023. *2023 Cyber Strategy Summary*. Washington, DC: U.S. Department of Defense.

[285] U.S. Department of State. 2024. *United States International Cyberspace and Digital Policy Strategy.* Washington, DC: U.S. Department of State. Pp. 1-20.

[286] U.S. Department of State. 2024. *United States International Cyberspace and Digital Policy Strategy. op. cit., pp. 32.*

الاستباقية، والنظام البيئي التكنولوجي المبتكر، وأطر السياسات الشاملة، والمشاركة الدبلوماسية العالمية النشطة، والتركيز على تطوير القوى العاملة. تساهم هذه العناصر بشكل تآزري في وضع أمن سيبراني مرن ومتطلع إلى المستقبل قادر على مواجهة الطبيعة الديناميكية والمعقدة للتهديدات السيبرانية. يعكس هذا النموذج نهجًا نقديًا يوازن بين الابتكار والتعاون والمسؤولية، مما يضمن استجابة فعالة للتحديات السيبرانية المعاصرة.

ثانيا: تحليل نقاط القوة في نموذج الأمن السيبراني الإستوني

تنهض قوة استونيا السيبرانية اللافتة على اسس متينة تبدأ من بنيتها الرقمية الامنة والنضج المختبر الذي اكتسبته عبر تجارب حاسمة، فالهوية الالكترونية الامنة الصادرة عن الحكومة وطبقة تبادل البيانات "اكس-رود[287]" (*X-road*) لم تمكن فقط الابتكار الرقمي السريع بل ضمنت تنظيم الامن بأسلوب يرتكز على المواطن ويعزز ثقته، وهي ثقة تترجم اقتصاديا بقيمة تقدر بما يتراوح بين 800 مليون الى 1.5 مليار يورو سنويا لنظام الهوية الالكترونية وحده، اي ما يعادل 4-7% من الناتج المحلي الاجمالي. ان هذا التصميم ليس مجرد انجاز تقني، بل هو تجسيد لفلسفة حكم تعتبر الشفافية والثقة ركائز اساسية، وهو ما تجلى بوضوح خلال ازمتي 2007 و2017 (ثغرة بطاقة الهوية[288])، حيث لم تختبر القدرات التقنية فحسب، بل مرونة النظام بأكمله، بما في ذلك الحكامة والتواصل مع الجمهور، فاستمر المواطنون في استخدام النظام بمعدلات شبه طبيعية حتى في ذروة الازمات، مما اكد صواب الخيارات الاستراتيجية الاربعة الموجهة: حماية الحقوق الاساسية في الفضاء السيبراني، واعتبار الامن ممكنا للتنمية الرقمية، والاقرار بالأهمية الفريدة للحلول التشفيرية، والالتزام بالشفافية والثقة العامة[289].

---

[287] X-Road هو طبقة برمجية وسيطة (middleware) تتيح للأنظمة والمصادر المختلفة (مثل قواعد بيانات الوزارات، البلديات، البنوك، المستشفيات...) أن تتبادل المعلومات بطريقة مؤتمتة وآمنة وموثوقة، دون أن تحتاج إلى دمج فعلي بينها. *مثلا إذا أرادت وزارة الصحة في إستونيا التحقق من دخل شخص معيّن لأغراض التأمين الصحي، فإنها ترسل طلبًا مشفّرًا عبر X-Road إلى مصلحة الضرائب، التي ترد آليًا بالمعلومة المطلوبة، دون تدخل بشري أو نقل يدوي.*

[288] تعرضت إستونيا في *2007* لهجمات *DDoS* عطلت مواقع حساسة ودعَت لتبني أول استراتيجية وطنية للأمن السيبراني، *وفي 2017 واجهت ثغرة ROCA ببطاقات الهوية الإلكترونية* شملت 750,000 بطاقة، وتمت معالجتها سريعًا بالتحديث عن بُعد وبشفافية، مما عزز الثقة ومرونة النظام.

[289] Republic of Estonia, Ministry of Economic Affairs and Communications, *Cybersecurity Strategy 2019-2022* (Tallinn: Ministry of Economic Affairs and Communications, 2019), pp. 10, 18, 24, 25.

لم تكتف استونيا بالاستجابة للازمات، بل حولتها الى محفزات للابتكار المؤسسي والتطور الاستراتيجي؛ فهجمات 2007، التي كانت بمثابة "جرس انذار قوي"، دفعتها لتصبح اول دولة اوروبية تتبنى نهجا شاملا لسياسة الامن السيبراني من خلال استراتيجية وطنية صدرت في مايو 2008، واسفرت عن انشاء هيئات متخصصة مثل وحدة الدفاع السيبراني التابعة لرابطة الدفاع الاستونية (*EDL Cyber Unit*)، واستضافة مركز التميز التعاوني للدفاع السيبراني التابع لحلف الناتو (*CCDCOE*) في تالين، والذي كان توصية استونية مبكرة اكتسبت زخما بعد تلك الهجمات. وتوج هذا المسار بتأسيس قيادة سيبرانية ضمن قوات الدفاع الاستونية في 2018، والتي ستصل الى قدرتها التشغيلية الكاملة بحلول عام 2023 بنحو 300 فرد، مما يمثل حوالي 5% من اجمالي افراد قوات الدفاع. ان تبني مبادئ استباقية مثل "لا للتركة القديمة" (*no-legacy principle*)، والذي تأكدت اهميته بعد هجمات *WannaCry* و*NotPetya* العالمية، وانشاء "سفارات البيانات" كاستجابة لضم القرم لضمان استمرارية الدولة الرقمية حتى في ظل سيناريوهات قاسية، يعكسان تفكيرا يتجاوز تامين الانظمة الحالية الى بناء مرونة بنيوية للمستقبل. حتى حادثة ثغرة *ROCA* في بطاقات الهوية الالكترونية عام 2017، تمت ادارتها بسلاسة بفضل القدرة على التحديث عن بعد ووجود مكتبات تشفير متعددة مدمجة مسبقا، مما اتاح تحويل "الصدمة" الى "ابتكار مؤسسي" يمكن الاستفادة منه بتوسيع مفهوم "سفارات البيانات" لتشمل منصات تشغيلية دولية للخدمات الحيوية[290].

ويستند هذا الصرح المؤسساتي والتقني الى قاعدة مجتمعية رقمية واسعة تعد بحد ذاتها نقطة قوة محورية؛ فنسبة 83% من الاسر لديها اتصال بالأنترنت، و82% من السكان هم مستخدمون منتظمون للأنترنت، وتصل تغطية شبكات الجيل الثالث المتقدم (G3) الى 100%، مع استخدام كثيف للنطاق العريض المتنقل. كما ان اكثر من 90% من السكان يستخدمون بطاقة الهوية الالكترونية للمصادقة الرقمية، وتنجز نسب عالية جدا من المعاملات عبر الانترنت، مثل 94% من الاقرارات الضريبية و98% من المعاملات المصرفية، فضلا عن تجربة التصويت الالكتروني التي تمت بنجاح ثماني مرات منذ عام 2005، مما يدل

[290] Kevin Kohler, *Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations* (Zürich: Center for Security Studies (CSS), ETH Zürich, 2020), pp. 4, 5, 6, 7, 8, 15.

على ترسخ ثقافة رقمية عميقة تتجاوز مجرد التبني التكنولوجي الى تحول ثقافي واجتماعي يجعل المواطنين شركاء فاعلين في الامن ويوفر الشرعية والدعم الشعبي للاستثمارات الحكومية في هذا المجال، وان كانت استونيا لا تزال بحاجة الى "خيارات حكيمة" للمنافسة مع مؤشرات مجتمع المعلومات للدول الاوروبية الاكثر تقدما في بعض الجوانب كسرعة النطاق العريض الثابت. هذا "القبول المجتمعي" للرقمنة يمكن استثماره مستقبلا في برامج توعية متقدمة حول التهديدات السيبرانية الناشئة لجعل المواطنين خط الدفاع الاول[291].

ان هذا التحول الرقمي الشامل لم يكن عبئا امنيا بقدر ما كان قاطرة اقتصادية ودرعا سيبرانيا في ان واحد؛ فقد ارتفعت مساهمة قطاع تكنولوجيا المعلومات والاتصالات في الناتج المحلي الاجمالي من 3.5% عام 2002 الى ما يقرب من 8% عام 2020. وتحتل استونيا المرتبة الاولى اوروبيا في مؤشر اقتصاد ومجتمع رقمي (*DESI*) للخدمات العامة الرقمية والمرتبة الثامنة عالميا في مؤشر الامم المتحدة للحكومة الالكترونية لعام 2022. وعلى الرغم من تصنيفها كقوة سيبرانية من "الدرجة الثالثة" نظرا لحجم مواردها المحدود واعتمادها المدروس على الشركاء في مجالات كالاستخبارات والعمليات الهجومية، فان هذا لا يقلل من تأثيرها، بل قد يكون جزءا من استراتيجيتها الذكية كدولة صغيرة تركز مواردها على مجالات التميز كالحكومة الالكترونية والدفاع السيبراني المرن وتستفيد من التحالفات لتعويض النقص في القدرات الاخرى. وتعد مبادرات مثل "سفارات البيانات"، التي افتتحت اولاها في لوكسمبورغ عام 2019 لضمان استمرارية الدولة الرقمية حتى في حالة فقدان السيطرة على الاقليم، مثالا على هذا التفكير الاستراتيجي الذي يمكن تطويره لتقديم "سفارات البيانات" كخدمة دولية مشتركة للدول الحليفة في الازمات[292].

وتتجسد "رشاقة الدولة الصغيرة" في استونيا ليس فقط في حجمها، بل في ثقافة حكامة تعتمد على شبكات غير رسمية وثقة متبادلة وقنوات اتصال قصيرة، مما يسمح بتعبئة سريعة وفعالة للموارد والخبرات من مختلف القطاعات. ان اشراك القطاع الخاص ومزودي الخدمات الحيوية في هيئات كـ"مجلس الامن السيبراني"، وتفعيل دور المتطوعين ذوي المهارات العالية من خلال

---

[291] Anna-Maria Osula, *National Cyber Security Organisation: Estonia (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015*), pp.5.

[292] International Institute for Strategic Studies (IISS), *"Estonia," in Cyber Capabilities and National Power*, Vol. 2 (London: IISS, 2023), pp. 29, 30, 33.

"وحدة الدفاع السيبراني التابعة لرابطة الدفاع الوطنية" (*EDL CDU*)، وانشاء "لجنة حماية البنية التحتية الحيوية" التي تضم خبراء من القطاعين، واستخدام "ميدان الاختبار السيبراني" (*Cyber Range Project*) كمنصة للتدريب والابتكار، كلها شواهد على نهج "المجتمع بأكمله" الذي يعزز نظاما امنيا شاملا ومرنا، ويمكن تعزيزه مستقبلا بتطوير نماذج شراكة اكثر رسمية واستدامة مع الحفاظ على مرونة النموذج الحالي، وتوسيع نطاق مشاركة المتطوعين، واستخدام "ميدان الاختبار السيبراني" كمنصة وطنية للبحث والتطوير[293].

وفي نهاية المطاف، تتبلور قوة النموذج الاستوني في "ردع سيبراني متعدد الطبقات" لا يعتمد بالضرورة على القدرات الهجومية بقدر ما يعتمد على مزيج ذكي من المرونة الدفاعية العالية (الردع بالرفض)، والقدرة على التأثير في بناء نظام دولي قائم على القواعد في الفضاء السيبراني (الردع بالتشابك والمعايير)، والاستعداد لمساءلة المعتدين من خلال اليات جماعية (الردع بالعقاب). ان استضافة مركز التميز التعاوني للدفاع السيبراني التابع لحلف الناتو (*CCDCOE*) واصدار "كتيبات تالين" (*Tallinn Manuals*) حول القانون الدولي المطبق على الفضاء السيبراني، والتي تعد اداة استراتيجية تعزز قوة استونيا الناعمة، بالإضافة الى مبادرات مثل "سفارات البيانات" ومعيار امن المعلومات الوطني (*E-ITS*[294])، والاسناد العلني للهجمات بالتعاون مع الحلفاء وتطبيق نظام عقوبات سيبرانية، كلها تشكل عناصر هذا الردع المتطور. ان مشاركة معلومات الامن السيبراني وأفضل الممارسات مع الحلفاء لا تزيد من الثقة المتبادلة والاستقرار فحسب، بل تعزز الردع والدفاع بشكل ملموس، مما يفتح افاقا لتطوير اليات "اسناد علني جماعي" أكثر فعالية، وريادة تطوير المعايير الدولية للتحديات الناشئة[295].

ثالثا: تحليل نقاط القوة في نموذج الأمن السيبراني السنغافوري

يعكس صعود سنغافورة الى مصاف القوى السيبرانية الرائدة عملا منهجيا يقوم على خمسة محاور مترابطة: حكامة استباقية، تشريع صارم، دفاع عملياتي متعدد المستويات، منظومة

---

[293] Piret Pernik with Emmet Tuohy, Cyber Space in Estonia: Greater Security, Greater Challenges (Tallinn: International Centre for Defence and Security, 2013), p.1.

[294] معيار أمن المعلومات الإستوني إطارًا مرجعيًا لإدارة أمن المعلومات في إستونيا، وقد تم تطويره باللغة الإستونية بما يتماشى مع البنية القانونية الوطنية. *ويتوافق هذا المعيار بشكل مباشر مع المعيار الدولي ISO/IEC 27001 الخاص بإدارة أمن المعلومات.*

[295] Piret Pernik, *Cyber deterrence: A case study on Estonia's policies and practice*, Hybrid CoE Paper 8 (Helsinki: Hybrid CoE, 2021), pp. 10, 13, 15, 16.

ابتكار وبحث متقدمة، وتنمية رأس مال بشري متخصص. الحكامة تبدأ بالخطة الوطنية لمكافحة الجرائم السيبرانية التي حولت مفهوم الوقاية من توعية نظرية الى برنامج عمل يرتب مسؤوليات الدولة والقطاع الخاص والمجتمع، ويضع اطارا للتبادل المعلوماتي السريع والاستجابة المشتركة لحوادث الفدية[296]. تتبنى الخطة المسح الافقي الدائم للتهديدات، وتربط نجاحها بقياس أثر التدريب العام على السلوك الرقمي للمواطنين، في خطوة تعكس قناعة مبكرة بان الامن يبدأ من المستخدم. يتعزز هذا الاتجاه باستراتيجية الامن السيبراني لعام 2016 التي انشأت وكالة الامن السيبراني سنغافورة ككيان مركزي يحدد الاولويات وينسق الموارد عبر الحكومة وشبكات الاعمال، وأضعت الامن ركيزة للنمو الاقتصادي لا مجرد وظيفة دعم تقني[297].

وتدل المركزية التنظيمية على فهم واضح لضرورة اتساق السياسات والانشطة؛ فالوكالة تراقب امتثال القطاعات الحيوية وترفع تقارير دورية الى مجلس الوزراء لتحديث التمويل والاهداف. ارساء القواعد الصلبة استلزم بنية قانونية حاسمة، فجاء قانون الامن السيبراني 2018 الذي فرض التبليغ الالزامي بالحوادث، ومكن السلطات من اجراء تدقيقات اجبارية، وجرم التقاعس عن تنفيذ توصيات الحماية، محولا الامن من خيار تشغيلي الى التزام قانوني يحمل غرامات وحجز تراخيص[298]، بعد ستة اعوام اثبت مشروع تعديل 2024 قدرة المنظومة على التكيف؛ اذ وسع الرقابة لتشمل مقدمي خدمات السحابة ومراكز البيانات وسلاسل الامداد الرقمية، واضاف فئة «الكيان ذي الاهمية السيبرانية الخاصة»، وعرف الحدود الافتراضية لحماية الموارد حتى اذا كان الخادم خارج البلاد[299].

هذه المواكبة التشريعية تغلق الفراغات التي يستغلها المهاجمون. على المستوى العملياتي يطبق برنامج حماية البنية التحتية المعلوماتية الحيوية منهجية تقييم مخاطر متدرجة، ويلزم الشركات باختبارات اختراق سنوية ومراجعات تصميم قبل تحديث الانظمة، فيما يختبر تمرين «سايبر

---

[296] Ministry of Home Affairs, *National Cybercrime Action Plan (Singapore: Ministry of Home Affairs, 2016)*, p. 1.
[297] *Cybersecurity (Amendment) Bill*, Bill No. 15/2024 (Singapore: Parliament of Singapore, 2024), p. 2.
[298] *Cybersecurity Act 2018*, 2020 Revised Edition (Singapore: Law Revision Commission, 2021), p. 3.
[299] *Cybersecurity (Amendment) Bill, Op. cit. p.3.*

ستار» قدرة الوكالات والموردين على العمل كجسم واحد اثناء هجوم واسع النطاق[300]. واللافت ان السيناريوهات تشمل فشل متزامن في الطاقة والنقل والمياه، ما يرفع وعي القيادات بطبيعة المخاطر النظامية. بموازاة ذلك ركزت النسخة الثانية من مدونة ممارسات الامن السيبراني على التكنولوجيا التشغيلية، وقدمت اطارا من ستة مستويات نضج، بينما أنشأ منتدى خبراء *OT* منصة لتبادل دروس حوادث المصانع ونظم التحكم الصناعي، فساعد قطاعات النفط والكيماويات على سد ثغرات عمرها عقود[301]. ويكتمل الدفاع الوقائي بمبادرة مرونة سلسلة الامداد التي تطلب من الموردين الافصاح عن ضوابطهم وحوادثهم، وفرقة العمل الوطنية لمكافحة الفدية التي طورت بروتوكول استرداد بيانات يقلص زمن العودة الى الخدمة بنسبة اربعين في المئة[302].

هذا الانتقال من رد الفعل الى ادارة مخاطر شاملة يقلص الكلفة ويعزز ثقة المستثمرين. في محور الابتكار يمول برنامج البحث والتطوير الوطني مشروعات لاكتشاف الثغرات والمسح الالي ودفاتر الاستاذ الموزعة، ويمنح الجامعات ميزانيات تنافسية لتأسيس مختبرات مرتبطة بالصناعة، فحولت ادوات مثل *AFLFast* الى منتجات تجارية مستخدمة عالميا. كما توفر منصة *CyberSG* في جامعة نانيانغ حاضنا للنماذج الاولية بالتعاون مع القوات المسلحة وشركات الطيران، ما يختصر دورة الابتكار من بحث أكاديمي الى خدمة سوقية. وتخلق مبادرة *CyberCall* وحاضنة *ICE71* بيئة تمويل وتسريع جعلت سنغافورة مركزا اقليميا لشركات ناشئة استقطبت استثمارات تجاوزت مئة مليون دولار خلال ثلاث سنوات[303].

ويعزز البعد المجتمعي حملة «العدو الخفي»، ونظام توسيم الاجهزة بخمس نجوم، ومعيار التطبيقات الامنة، وبوابة النظافة الرقمية المجانية التي تفحص المواقع والبريد بضغطة زر، فتصل الرسالة الى اصحاب الاعمال الصغيرة والمواطنين. دوليا تقود سنغافورة مبادرة مكافحة الفدية، وتستضيف مركز التميز بين آسيان والامم المتحدة، وتؤهل مئات المسؤولين من الدول

---

[300] Cyber Security Agency of Singapore (CSA), *Singapore's Cybersecurity Strategy (Singapore: CSA, 2016), p.* 12.
[301] Ibid. *(Singapore: CSA, 2022),* p. 47.
[302] Ibid. *(Singapore: CSA, 2021).*
[303] Ibid. *(Singapore: CSA, 2021), p. 4.*

النامية عبر زمالة *UNSCF*[304]، ما يمنحها ثقلا تفاوضيا ويحولها من مستهلك للأمن الى مزود معرفة اقليمي. وعلى صعيد البنية التحتية الرقمية اعتمدت الحكومة منصة موحدة لتبادل البيانات الاستخبارية تسمح بالتحقق اللحظي من مؤشرات الاختراق، كما طبقت خوارزميات تعلم آلي في مركز العمليات الوطني لاكتشاف الشذوذ السلوكي ووفرت لوحات قيادة تنبؤية لصناع القرار تعتمد تحليلات، وابتكرت الحكومة نموذجا معياريا لتبادل السجلات الرقمية بين الوزارات. بذلك تتكامل الحكامة والتشريع والدفاع والابتكار والموهبة في بيئة مرنة تثبت ان الامن محرك خفي للنمو، وتبرر وصف سنغافورة بالقوة السيبرانية القادرة على حماية جولاتها الرقمية المقبلة بثقة واستباق.

يتّضح من تحليل النماذج الثلاثة ـ الأمريكية، الإستونية، والسنغافورية ـ أن تحقيق أمن سيبراني فعّال لا يقتصر على امتلاك التكنولوجيا، بل يتطلب رؤية استراتيجية متكاملة تُجسَّد من خلال حكامة مؤسساتية صلبة، تشريعات مواكِبة، تعاون متعدد المستويات، واستثمار طويل الأمد في البنية التحتية الرقمية ورأس المال البشري. تختلف هذه النماذج في السياقات والموارد والقدرات، لكنها تتقاطع جميعًا في إدراكها العميق بأن الفضاء السيبراني ليس مجرد امتداد تقني، بل مجال سيادي يتطلب دفاعًا مرنًا، ومقاربات استباقية، وأطرًا تنظيمية قابلة للتكيف مع تهديدات متغيرة باستمرار. من خلال هذه المقارنات، تتبيّن ملامح السياسات السيبرانية الناجحة التي يمكن الاستفادة منها لبناء منظومة وطنية قادرة على مواجهة التحديات الرقمية المعاصرة دون أن تغفل خصوصيات السياق المحلي.

الفقرة الثانية: مقارنة وتكييف الدروس مع النموذج المغربي

في سياق السعي إلى فهم موقع المغرب في خريطة الأمن السيبراني العالمي، وتحديد الهوامش الممكنة للتطوير، تندرج هذه المرحلة من التحليل التي تجمع بين البعد المقارن والبعد الاستراتيجي. فمن خلال المقارنة بين أداء المغرب وثلاث دول رائدة هي الولايات المتحدة، سنغافورة، وإستونيا، يمكن الوقوف على الفوارق والتقاطعات فيما يتعلق بمكونات المنظومة السيبرانية، كما تم قياسها وفقًا لمؤشر الأمن السيبراني العالمي لسنة 2024 الصادر عن

---

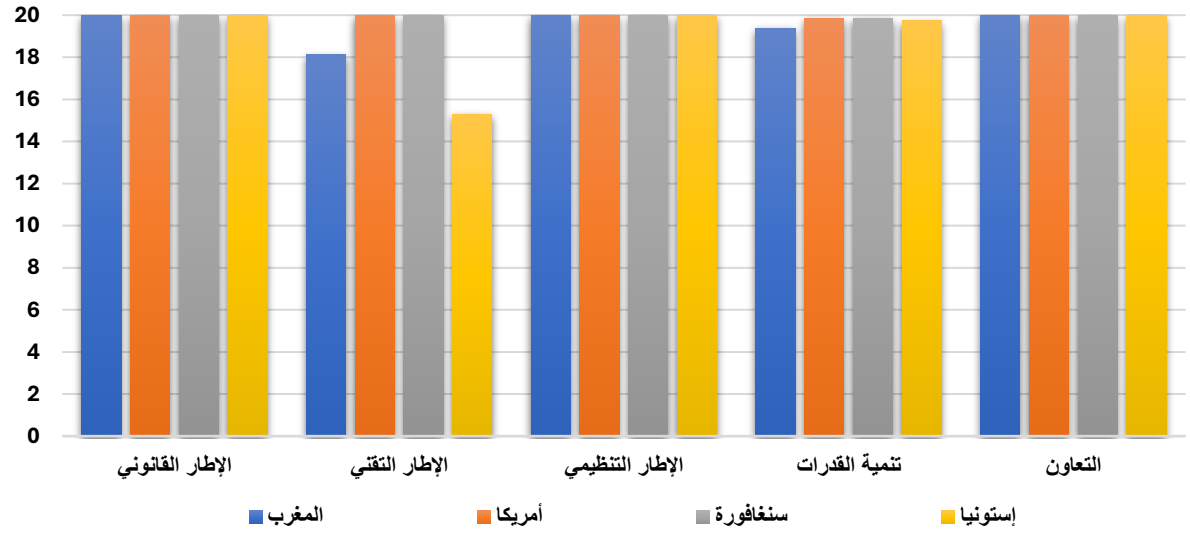
[304] *CII Protection and Cybersecurity Strategy Implementation Progress Report (Singapore: CSA, 2022),* Op. cit. p 59.

الاتحاد الدولي للاتصالات[305]. وتهدف هذه المقارنة إلى إضاءة مستوى التقدم الوطني في محاور محددة، من دون تحميل المؤشرات الرقمية أكثر مما تحتمل، خصوصًا وأن بعض الفجوات قد تكون مرتبطة بطبيعة منهجية التصنيف أكثر من كونها انعكاسًا دقيقًا للواقع النوعي. وعليه، تأتي الخطوة التالية لتجاوز البعد الوصفي، من خلال تكييف الدروس المستخلصة من التجارب الرائدة بما يتلاءم مع السياق المغربي، في أفق بناء منظومة متماسكة وفعّالة ترتكز على التدرج، والتنسيق المؤسسي، والاستثمار الذكي في الموارد التقنية والبشرية.

أولًا: المقارنة المعيارية بين المغرب والدول الرائدة في الأمن السيبراني

يعرض الشكل البياني التالي مقارنة بين أداء المغرب وثلاث دول مرجعية في مجال الأمن السيبراني، وهي الولايات المتحدة الأمريكية، سنغافورة، وإستونيا، وذلك استنادًا إلى النسخة الخامسة من مؤشر الأمن السيبراني العالمي لسنة 2024 الصادر عن الاتحاد الدولي للاتصالات.

مقارنة حسب معايير مؤشر الأمن السيبراني العالمي 2024 وفق الاتحاد الدولي للاتصالات



يعكس الرسم البياني تباينًا ملموسًا في مستويات الأداء السيبراني للدول الأربع، وفق المحاور الخمسة المعتمدة من طرف مؤشر الأمن السيبراني العالمي (*GCI* 2024). فعلى مستوى

[305] International Telecommunication Union, *Global Cybersecurity Index 2024, 5th ed.* (Geneva: ITU, 2024).

الإطار القانوني، تحقق جميع الدول – المغرب، الولايات المتحدة، سنغافورة، وإستونيا – النقطة الكاملة (20/20)[306]، ما يشير إلى نضج تشريعي في سنّ القوانين المنظمة للأمن الرقمي، إلا أن هذا التساوي لا يُخفي تباينًا محتملًا في جودة التفعيل، والذي لا يلتقطه المؤشر بشكل مباشر.

أما على مستوى الإطار التقني، فتُظهر البيانات تفوق الولايات المتحدة (20/20) وسنغافورة (20/20)[307]، يليهما المغرب (20/18.12)[308]، في حين تتراجع إستونيا إلى (20/15.3)[309]، رغم مكانتها المتقدمة في الرقمنة. يوضح هذا المؤشر أن المغرب استطاع تحقيق تطور واضح على المستوى التقني، يتجاوز حتى دولة أوروبية متقدمة كالإستونية، وهو ما يعكس توفر بنى تحتية وأدوات تدخل تقنية، دون أن يعني بالضرورة تفوقًا نوعيًا في عمق الأداء أو فعالية النظم المستخدمة.

فيما يخص الإطار التنظيمي، نالت جميع الدول العلامة الكاملة (20/20)[310]، مما يعكس نضجًا مؤسساتيًا نسبيًا، لا سيما فيما يتعلق بوضوح الأدوار وتعدد المتدخلين ضمن هندسة الأمن السيبراني. أما في محور تنمية القدرات، فقد تقاربت النسب: الولايات المتحدة وسنغافورة (20/19.86)[311]، المغرب (20/19.38)[312]، إستونيا (20/19.74)[313]، وهو ما يُظهر اهتمامًا جماعيًا ببناء الكفاءات، وإن بدرجات متفاوتة، تظل جميعها قريبة من المستوى الأقصى.

أخيرًا، في محور التعاون، أحرزت كل الدول النقطة الكاملة (20/20)[314]، ما يدل على انخراطها في الشبكات الدولية للردع والتنسيق، ويُعزز موقع المغرب إقليميًا كشريك في برامج ومنتديات الأمن السيبراني.

---

306 *Global Cybersecurity Index 2024* .Op. cit., pp. 68, 75, 95, 110.
307 Ibid., pp. 68, 95.
308 Ibid., p. 75.
309 Ibid., p. 110.
310 Ibid., pp. 68, 75, 95, 110.
311 Ibid., pp. 68, 95.
312 Ibid., p. 75.
313 Ibid., p. 110.
314 Ibid., pp. 68, 75, 95, 110.

من خلال هذا التباين الكمي، يتضح أن المغرب يُحقق أداءً محترمًا في جميع المحاور، مع نقاط قوة واضحة في التشريع والتنظيم، ومجال للتحسين في القدرات التقنية والبشرية. وهو ما يُشكل أساسًا موضوعيًا لتكييف أفضل الممارسات الرائدة وفق الواقع المؤسساتي الوطني.

ثانيًا: تكييف الدروس مع الخصوصية المغربية

استنادًا إلى نموذج نقل السياسات لدولويتز ومارش *(Dolowitz & Marsh Policy Transfer Model, 2000)*[315]، يمكن للمغرب أن يُكيّف أفضل الممارسات الدولية مع خصوصياته عبر مقاربة انتقائية تُحوّل مكامن الضعف إلى عناصر قوة. يتطلّب الانتقال من التشخيص إلى بناء أمن سيبراني فعّال اعتمادَ إطار حكامة مؤسسي جديد قائم على وحدة قيادة مركزية تُنسِّق بين المديرية العامة لأمن نظم المعلومات، واللجنة الوطنية لحماية المعطيات الشخصية، ووزارة الانتقال الرقمي، على غرار وكالة الأمن السيبراني السنغافورية التي قلَّصت زمن اتخاذ القرار في الأزمات[316]. ولتلاؤم هذا الهيكل مع البنية الإدارية المغربية المقسَّمة، يُقترَح إنشاء لجنة مشتركة للأمن السيبراني ترفع تقارير فصلية إلى البرلمان وتملك صلاحية إصدار أوامر مُلزِمة لجميع القطاعات.

في المحور التقني، يُبرز النموذج الأمريكي[317] أهمية الأُطر المرِنة القائمة على المخاطر؛ وعليه يصبح تبنّي نسخةٍ مبسَّطةٍ من إطار *NIST* وتخصيصها للمقاولات الصغيرة والمتوسطة أمرًا ضروريًا، مع ربط الامتثال بحوافز ضريبية وآليات تمويل تصاعدية. تشريعيًا، يمكن سد ثغرات القانون 05.20 باعتماد نظام غرامات نسبيّة مستندٍ إلى نسبةٍ من رقم معاملات الجهة المخالِفة أو حدٍّ أقصى محدَّد، بدل الاكتفاء بمبلغ ثابت، مع التنصيص صراحةً على إجراء تقييم دوري يُقترَح أن يكون كل خمس سنوات لمواكبة تطور الهجمات المتقدّمة.

---

[315] Dolowitz, D. P., & Marsh, D. (2000). Learning from abroad: *The role of policy transfer in contemporary policy-making*. Governance, 13(1), 5–23. *https://doi.org/10.1111/0952-1895.00121*.

[316] *(Singapore: Parliament of Singapore, 2024)*, Op. Cit, p. 2.

[317] *U.S. Department of Homeland Security*, pp. Op. cit 11–13.

أما التجربة الإستونية فتؤكّد أنّ اللامركزيّة وتوزيع البيانات يوفران حصانةً للدول الصغيرة؛ لذلك يُمكن استنساخ مفهوم «سفارات البيانات[318]» عبر اتفاقيات مع مراكزٍ أوروبية موثوقة، مشترِطةً تشفيرًا مزدوجًا وإدارة مفاتيح داخليّة لضمان استمرارية الخدمات الحيويّة. ولمواجهة الارتفاع المستمر للأخطاء البشريّة، يُستحسن اعتماد نهج «الأمن الشامل للمجتمع» بأسلوب إستونيا عبر برنامج وطني للتثقيف السيبراني يمنح شهاداتٍ رقمية قابلة للتحقق ويُدمَج في المناهج المدرسية، إضافةً إلى تنظيم تمارين محاكاة متعدِّدة القطاعات شبيهة بتمرين *Cyber Star*[319] السنغافوري، مع تكييف السيناريوهات لقطاعَي الطاقة والزراعة.

لمعالجة نقص الموارد، يجب إطلاق شراكات ثلاثية بين الدولة والقطاع الخاص والجامعات، مستلهَمة من نموذج الحاضنة *ICE71*[320]، وتحويل المراكز الجامعية إلى منصّات ابتكار مفتوحة تربط تمويل المشاريع بتحقّق مؤشرات نضج أمني محدَّدة. كذلك، يتطلّب سد فجوات الامتثال في سلاسل الإمداد تكييفَ مدونة ممارسات التكنولوجيا التشغيلية السنغافورية لتصبح مرجعيةً صناعيةً مغربية مُلزِمة لمورّدي المياه والفوسفات والطيران، مع شرط الإفصاح السنوي عن اختبارات الاختراق. وأخيرًا، لمعالجة ضعف ثقافة المخاطر الرقمية لدى صنّاع القرار، يُقترَح عقد جلسة استماع سيبرانية برلمانية سنوية بحضور كبار مسؤولي الأمن وخبراء القطاع الخاص، تُرفق بتقرير وطني علني يبيّن المؤشرات والفجوات التمويلية، لترسيخ الأمن السيبراني كأولوية سيادية تضاهي الدفاع التقليدي.

بدمج هذه الإجراءات التي تجمع المركزية بالحكامة التشاركية، والصرامة التشريعية بالابتكار المرن سيتمكّن المغرب من إرساء فضاءٍ رقمي آمن ومرن يُعزّز مكانته الإقليمية ويدعم أهدافه التنموية.

المطلب الثاني: الآفاق المستقبلية لتعزيز الأمن السيبراني بالمغرب

أمام تصاعد التهديدات السيبرانية وتعاظم رهانات السيادة الرقمية، يبرز تحدي الانتقال من منطق الاستجابة إلى منطق الاستباق وبناء مناعة ذاتية مستدامة. فلا يكفي تعزيز أدوات

---

[318] *Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations* (Zürich: Center for Security Studies (CSS), ETH Zürich, 2020), Op. cit. pp. 4, 5, 6, 7, 8, 15.
[319] *Singapore's Cybersecurity Strategy (Singapore: CSA, 2016),* Op. Cit. p. 12.
[320] *Cybersecurity Awareness and Outreach Strategy (Singapore: CSA, 2021)*, Op. Cit. p. 4.

الدفاع التقني، بل يتطلب الأمر تطوير بنية استراتيجية ترتكز على الابتكار والتصنيع وتوظيف التقنيات المتقدمة بشكل سيادي. في هذا السياق، يتناول هذا المطلب مسارين متكاملين يمثلان أبرز آفاق تعزيز الأمن السيبراني بالمغرب: أولًا، استثمار الذكاء الاصطناعي في منظومة الأمن السيبراني عبر إعادة هيكلة القرار، والتحليل الاستباقي، وتعويض نقص الكفاءات؛ وثانيًا، التصنيع والابتكار كدعامة لبناء المناعة السيبرانية، من خلال توطين إنتاج التقنيات الحساسة وتشجيع البحث العلمي وتبني نماذج رائدة في السيادة الرقمية.

الفقرة الأولى: استثمار الذكاء الاصطناعي في منظومة الأمن السيبراني

مع تعقّد التهديدات السيبرانية وتزايد الحاجة إلى استجابة سريعة وفعالة، يبرز الذكاء الاصطناعي كأداة محورية في إعادة تشكيل منظومة الأمن السيبراني. وتستعرض هذه الفقرة كيف يمكن لتقنيات الذكاء الاصطناعي أن تعزز اتخاذ القرار، وتبني قدرات تحليل استباقي، وتسد فجوة الموارد البشرية، وتُفعَّل ضمن إطار وطني متكامل، بما يجعلها ركيزة استراتيجية لمناعة رقمية مستدامة.

أولا: إعادة تشكيل القرار السيبراني داخل الإدارة العمومية

يؤدي توظيف الذكاء الاصطناعي في دوائر القرار السيبراني الى تحول نوعي في منطق الحكامة؛ فالمنظومة تنزاح من معالجة حوادث مشتتة الى يقظة مؤسساتية تتعقب تدفقات البيانات الحكومية آنيًا وتقارنها بنموذج سلوك معياري، فتكشف الانحراف لحظة حدوثه[321]. وهكذا تُطوى حلقات الموافقة البيروقراطية التي كانت تطيل زمن الاستجابة، إذ تنتج الخوارزمية "مشهد تهديد" فوريًا وتعرضه على المسؤول مع قائمة اجراءات مرتبة بحسب الخطورة، مثل عزل خادم حيوي او تقييد امتيازات حساب مشبوه. وتظهر البيانات الحديثة ان المؤسسات التي اعتمدت هذا النهج خفضت عدد التوقيعات البشرية المطلوبة لتفعيل بروتوكول الطوارئ الى النصف تقريبًا، ما يحول القرار من تسلسل هرمي طويل الى عملية مؤتمتة تستند الى

[321] Lizzy Ofusori, Tebogo Bokaba, and Siyabonga Mhlongo, *"Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction,"* Applied Artificial Intelligence 38, no. 1 (2024).

عتبات خطر محددة سلفًا[322]. كذلك تعيد الخوارزميات صياغة مخرجاتها بلغة مفهومة للفني والاداري معًا فتختفي فجوة التواصل التي كانت تعرقل الاجراءات الحاسمة، ويصبح المدير قادرًا في دقائق لا ايام على قراءة لوحة قيادة تلخص مؤشرات الخطر ومعدل التعافي والتأثير المتوقع على المرفق العمومي. وبدل الاكتفاء بتقارير ما بعد الحادث يتابع المخططون المشهد الرقمي لحظة بلحظة ويعيدون ضبط السياسات استنادًا الى بيانات حيّة، فتتبلور حكامة قائمة على الادلة تقيس الاداء الوقائي لا حصيلة الخسائر[323]. هذا التكامل بين الرصد والتحليل والقرار يرفع الشفافية الداخلية بتسجيل كل خطوة في سجل لا يقبل العبث ويمنح هيئات الرقابة صلاحية التحقق الفوري، كما يسمح للمالية العمومية بتقدير تكلفة التهديد مسبقًا وتخصيص الموارد بصورة استشرافية لا ترميمية، لتغدو الخوارزمية محركًا لإعادة هندسة القرار السيبراني بعيدا عن البطء البشري والتخمين الحدسي.

ثانيا: بناء آليات التحليل الاستباقي للتهديدات السيبرانية

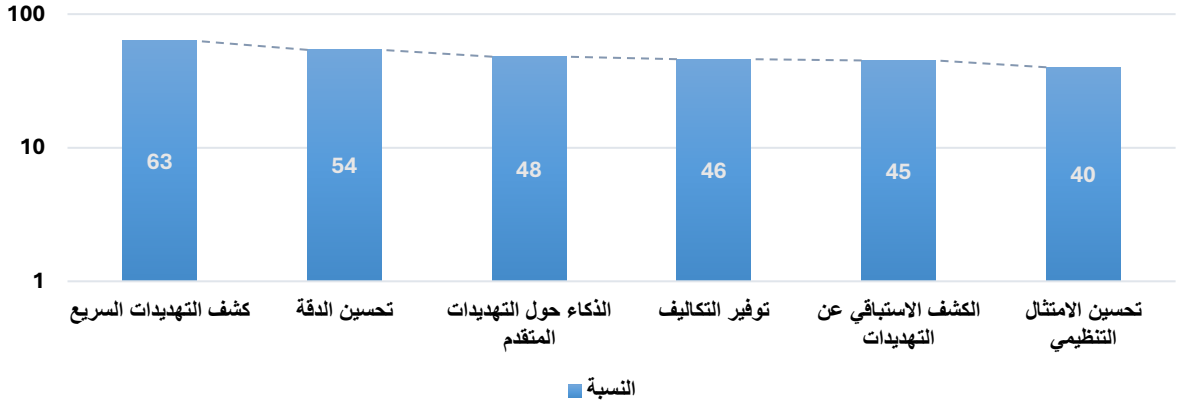
الذكاء الاصطناعي يُحدث ثورة في رصد التهديدات السيبرانية من خلال تطوير آليات تحليل استباقية تعزز الحماية الوقائية. يعتمد هذا النهج على جمع البيانات من مصادر متنوعة مثل الشبكات والأجهزة الذكية، حيث تُدمج تقنيات التعلم الآلي لتحديد الأنماط غير الطبيعية في حركة البيانات[324]. تستخدم النماذج غير الخاضعة للإشراف لمراقبة الإيقاع اليومي للتدفقات الرقمية، مما يتيح كشف انحرافات دقيقة مثل تأخر استجابة الخوادم أو محاولات تسجيل دخول غير مكتملة[325]. هذه الآليات تتجاوز الاعتماد على التهديدات المعروفة، حيث تركز على تحليل السلوك الخفي للهجمات الطويلة البطيئة التي تتجنب التقنيات التقليدية بتقليل بصمة المهاجم[326]. ويتيح التحليل الاستباقي إنتاج "مشهد تهديد" فوري يُقدم للمسؤولين قائمة أولويات مرتبة بناءً على الخطورة، مثل عزل الخوادم الحيوية أو تقييد الصلاحيات[327]. تُساعد هذه التقنيات في تقليل الاعتماد على التدخلات البشرية المتكررة، حيث تُعيد صياغة المخرجات

---

[322] Philippe Funk, *"Artificial Intelligence and Cybersecurity Implications for Business Management,"* Economy & Business 16 (2022).
[323] World Economic Forum, *Global Cybersecurity Outlook 2024* (Geneva: World Economic Forum, 2024).
[324] Capgemini Research Institute, *AI and Gen AI in cybersecurity*, May 2024, pp. 5-6.
[325] ENISA, *Threat Landscape 2024*, September 2024, p. 11.
[326] *AI and Gen AI in cybersecurity*, Op. cit. p. 19.
[327] *Threat Landscape 2024*, Op. cit. p. 7.

بلغة موحدة تُسهل التواصل بين الفرق التقنية والإدارية. كما تُمكّن من تتبع التغيرات اللحظية في البيئات الهجينة والسحابية، مما يقلل مخاطر تسرب البيانات عبر المنصات بمراقبة العلاقات المنطقية بدلاً من قواعد المنافذ الثابتة[328]. وتبرز الدراسات أن هذا النهج يعزز الشفافية من خلال تسجيل كل خطوة في سجل لا يقبل التلاعب، مما يدعم هيئات الرقابة في التحقق الفوري[329] بالإضافة إلى ذلك، يساهم في تقدير تكلفة التهديدات مسبقًا، مما يتيح تخصيص الموارد بطريقة استشرافية تُركز على الوقاية بدلاً من الترميم. هذا التكامل بين الرصد والتحليل يُحوّل القرار السيبراني إلى نظام ديناميكي يعتمد على البيانات الحية، مما يضمن استجابة سريعة وفعالة أمام التهديدات المتطورة.

الفوائد المتوقعة من استخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني



330

يُبيّن المبيان أنّ أكثر المنافع المتوقَّعة من إدماج الذكاء الاصطناعي في الأمن السيبراني تتركّز، بالترتيب التنازلي، في:

- ✓ **التعجيل بكشف التهديدات (أعلى قيمة في الرسم)**، ما يدلّ على إيمان الممارسين بأنّ السرعة تظلّ الرافعة الأولى للحدّ من الأضرار.
- ✓ **تعزيز الثقة لدى المستخدمين والشركاء**، وهو مكسب مؤسّسي يفوق نصف العيّنة تقريبًا.

---

[328] Ibid., p. 16.
[329] Ibid., p. 2.
[330] *AI and Gen AI in cybersecurity*, May 2024, Op. cit. pp. 39.

- ✓ **الإنذار المبكّر بالهجمات المتقدّمة**، ممّا يعكس رهانات متنامية على الرصد السلوكي الذكي.
- ✓ **خفض التكاليف عبر أتمتة الإجراءات الوقائية**، وهو منفعة مالية تأتي مباشرة بعد الحماية التقنية.
- ✓ **الكشف الاستباقي قبل وقوع الضرر**، وهي قيمة قريبة من وفورات التكاليف في الوزن النسبي.
- ✓ **تحسين الامتثال التنظيمي**، وإنْ جاء في المرتبة الأخيرة، فإنّه يبقى ضمن نطاق الاهتمامات الكمية الواضحة.

ثالثا: تعويض نقص الكفاءات وتعزيز الاداء الوظيفي

يساهم الذكاء الاصطناعي في تعزيز الأداء الوظيفي للعاملين في هذا المجال. بحيث يقوم بتحمل المهام اليومية الروتينية التي كانت تثقل كاهل المحللين، مما يتيح لهم التفرغ للتحليلات الاستراتيجية التي تتطلب تفكيرًا عميقًا وخبرة متميزة. من خلال هذا الدور، يساعد في تقليل الفجوة الناتجة عن نقص المتخصصين، خاصة في ظل الضغوط الاقتصادية التي تؤثر على التوظيف. كما يدعم الذكاء الاصطناعي تحسين استجابة فرق الأمن للتهديدات السيبرانية من خلال معالجة كميات كبيرة من البيانات بفعالية، مما يعزز قدرة العاملين على حماية البنية التحتية الرقمية. هذا النهج يساهم في تطوير استراتيجيات دفاعية أكثر دقة، حيث يوفر بيئة عمل أقل ضغطًا تسمح بتحسين الأداء الشامل. بالإضافة إلى ذلك، يعمل كأداة مساعدة تتيح للعاملين الاستفادة من الوقت المحرر لتطوير مهاراتهم ومواجهة التحديات الجديدة في العالم الرقمي. وبهذه الطريقة، يدعم الذكاء الاصطناعي استدامة العمليات الأمنية حتى في ظروف محدودة الموارد، مما يجعله شريكًا استراتيجيًا في تعزيز كفاءة القوى العاملة السيبرانية[331].

رابعا: التفعيل الوطني للذكاء الاصطناعي في السيبراني

لتفعيل وطني شامل للذكاء الاصطناعي السيبراني، يجب تجاوز مرحلة التطبيقات التشغيلية نحو بناء منظومة سيادية متكاملة، وذلك عبر إرساء حكامة استراتيجية وتشريعية متخصصة، وتطوير قدرات وبنية تحتية سيادية، وتحفيز بيئة ابتكار متقدمة. يتطلب ذلك أولاً صياغة

[331] ISC2 *Cybersecurity Workforce Study*, 2024, p. 40

استراتيجية وطنية مخصصة للذكاء الاصطناعي السيبراني، تتكامل مع رؤية "المغرب الرقمي 2030"[332] والاستراتيجية الوطنية للأمن السيبراني 2030[333]، لمعالجة التحديات الفريدة لهذا المجال وضمان تنسيق الجهود بين الفاعلين الرئيسيين كالمديرية العامة لأمن نظم المعلومات ووكالة التنمية الرقمية. ويستدعي هذا التوجه تحديث الإطار القانوني والأخلاقي الحالي، بما يتجاوز القانون 05.20، ليشمل تنظيم أخلاقيات الخوارزميات وتحديد المسؤوليات الناجمة عن أنظمة الذكاء الاصطناعي في السياقات الأمنية، مما يعزز الثقة ويشجع الاستثمار المسؤول[334]. ثانياً، يجب الاستثمار الموجه في بنية تحتية تكنولوجية سيادية، عبر تخصيص جزء من قدرات الحاسوب العملاق الوطني لدعم البحث والتطوير في الذكاء الاصطناعي السيبراني، وإنشاء منصات سحابية سيادية لضمان أمن البيانات وتقليل التبعية الخارجية[335]. ويترافق ذلك مع إطلاق برامج وطنية لتكوين كفاءات متخصصة وعالية المستوى في هذا التقاطع الدقيق، مثل تلك المتوفرة بجامعة محمد السادس متعددة التخصصات[336] وشبكة معاهد الجزري[337]، مع وضع آليات فعالة للاحتفاظ بهذه المواهب النادرة لمواجهة هجرة الأدمغة. ثالثاً، يستلزم الأمر تحفيز منظومة ابتكار متقدمة عبر إنشاء مراكز تميز وبرامج تمويل مخصصة للبحث والتطوير في الذكاء الاصطناعي السيبراني، على غرار مركز الابتكار في

---

[332] المملكة المغربية، وزارة الانتقال الرقمي وإصلاح الإدارة، *«استراتيجية المغرب الرقمي 2030»*، استنادًا إلى التوجيهات الملكية السامية وخطاب جلالة الملك محمد السادس بتاريخ 5 يوليوز 2022، الرؤية الرسمية تروم جعل الرقمنة رافعة للتنمية وتقليص الفجوة الرقمية مع الدول المتقدمة، من خلال تعبئة الكفاءات وبناء حلول تكنولوجية ملائمة للخصوصيات الوطنية والقارية.

[333] المملكة المغربية، *«الاستراتيجية الوطنية للأمن السيبراني 2030»*، إصدار رسمي تحت إشراف وزارة الانتقال الرقمي وإصلاح الإدارة، الرباط، 2023، ص 9–47. تُبرز الوثيقة الرؤية الاستراتيجية للدولة في تأمين الفضاء السيبراني الوطني من خلال أربعة محاور رئيسية تشمل تعزيز الحكامة والتشريع، دعم قدرات الكشف والاستجابة، تطوير الرأسمال البشري، وتعزيز التعاون الدولي، مع تأكيد دور الذكاء الاصطناعي في رصد المخاطر ودعم اتخاذ القرار.

[334] عائشة بوزرار، *"نحو استراتيجية وطنية للذكاء الاصطناعي"*، الأسبوع الصحفي، 4 يونيو 2024، تم الاطلاع عليه في 08 يونيو 2025 على ساعة 14:21، على الرابط: *https://www.alousboue.ma*.

[335] توفيق الناصري. المغرب يطلق أضخم حاسوب في إفريقيا. سكاي نيوز عربية، 14 أبريل 2021. تم الاطلاع عليه بتاريخ 10 يونيو 2025، على الساعة 03:12، على الرابط: https://www.skynewsarabia.com.

[336] UM6P – *Mohammed VI Polytechnic University. Master in Applied Data Science and Artificial Intelligence*. Accessed June 10, 2025, at 03:24 a.m. *https://cc.um6p.ma*.

[337] وزارة الانتقال الرقمي وإصلاح الإدارة. توقيع السيدة الوزيرة لمذكرة تفاهم لإنشاء معهد الجزري المخصص لتعزيز البحث التطبيقي والتكوين المتقدم والابتكار التكنولوجي في جهة كلميم واد نون. 14 أبريل 2025. تم الاطلاع عليه بتاريخ 10 يونيو 2025، على الساعة 03:37، على الرابط: https://www.mmsp.gov.ma.

الأمن السيبراني *CIC* [338] ومركز *DXC.CDG*[339]، وتشجيع الشراكات بين القطاعين العام والخاص والمقاولات الناشئة. كما يجب تفعيل تعاون دولي نوعي، يتجاوز تبادل المعلومات العام، ويركز على جلب الخبرات وتوطين التقنيات المتقدمة في الذكاء الاصطناعي السيبراني، لضمان بناء قدرة ذاتية مستدامة ومواكبة للتطورات العالمية المتسارعة.

يتبيّن من خلال ما سبق أن إدماج الذكاء الاصطناعي في منظومة الأمن السيبراني لا يقتصر على التطوير التقني، بل يمثل تحوّلاً بنيوياً في منطق الحكامة السيبرانية، حيث تُستبدل القرارات البيروقراطية بقرارات مؤتمتة قائمة على تحليل لحظي للبيانات، مما يرفع من فعالية الاستجابة ويعزز الشفافية والمراقبة. كما يتيح الذكاء الاصطناعي تطوير آليات استباقية لرصد التهديدات المعقدة، ويخفف من ضغط نقص الكفاءات المتخصصة. وتُظهر المعطيات الإحصائية أن كشف التهديدات بسرعة وتعزيز الثقة المؤسسية يأتيان في مقدمة الفوائد المتوقعة، تليها مزايا تنظيمية ومالية واضحة. وعليه، فإن تفعيل الذكاء الاصطناعي السيبراني يمثل رافعة استراتيجية لبناء منظومة دفاعية أكثر ذكاءً ومرونة واستدامة.

الفقرة الثانية: التصنيع والابتكار كدعامة لبناء المناعة السيبرانية

تواجه الدول الحديثة تحديًا استراتيجيًا يتمثل في بناء مناعة سيبرانية قادرة على حماية فضائها الرقمي وسيادتها التقنية. بالنسبة للمغرب، يتطلب تعزيز الأمن السيبراني الوطني نظرة بعيدة المدى تركز على ما يجب القيام به مستقبلًا بدلًا من الاكتفاء بالإجراءات التقليدية الآنية. في هذا السياق، يبرز التصنيع التكنولوجي المحلي والابتكار البحثي والمؤسساتي كدعائم أساسية لبناء السيادة الرقمية وتعزيز مناعة الدولة ضد التهديدات السيبرانية. إن تطوير صناعة رقمية وطنية قوية يعني امتلاك القدرة على تصميم وإنتاج التقنيات الحساسة محليًا، مما يقلّص الاعتماد على الخارج ويحدّ من نقاط الضعف في سلاسل التوريد العالمية. تؤكد دراسات أكاديمية أن التركيز على التصنيع المحلي يرفع من مستويات المرونة الأمنية للدولة؛ فعلى سبيل المثال، يشير تقرير للاكاديمية الوطنية الأمريكية إلى أن توطين التصنيع يعزز القدرة

[338] قرار مشترك لوزير التعليم العالي والبحث العلمي والابتكار ووزيرة الاقتصاد والمالية رقم 1148.25 صادر في 6 ماي 2025 (8 ذي القعدة 1446) بالمصادقة على الاتفاقية المؤسسة للمجموعة ذات النفع العام المسماة *"مركز الابتكار في الأمن السيبراني"*، الجريدة الرسمية عدد 7407 بتاريخ 28 ماي 2025، ص. 2864.

[339] MAP, *« IA : DXC CDG inaugure son Centre d'excellence en Intelligence Artificielle »*, Le Desk, publié le 13 février 2025 à 18h21, consulté le 10 juin 2025 à 04h01, *https://ledesk.ma.*

على الصمود الأمني بشكل ملحوظ[340]. بناءً على ذلك، يصبح توطين صناعة المعدات والبرمجيات الرقمية – من رقاقات ومعالجات إلى حلول وبرامج أمنية – عاملًا حاسمًا في حماية البنية التحتية المعلوماتية من الاختراق والتلاعب الخارجي.

أولا: دور التصنيع المحلي في تحقيق المناعة السيبرانية

يمثّل التصنيع التقني المحلي خط الدفاع الأول عن السيادة السيبرانية لأي دولة. فمن خلال بناء قاعدة تصنيع وطنية للمكونات الرقمية الحيوية (مثل المعدات الشبكية وأجهزة الاتصالات والحواسيب)، يكتسب المغرب تحكمًا أكبر في أمن موارده التكنولوجية. إن الاعتماد المفرط على تقنيات مستوردة يفتح ثغرات خطيرة؛ إذ قد تتضمن المنتجات الأجنبية بوابات خفية أو مواطن ضعف مقصودة تستغلها جهات خارجية. لذلك، يعد تطوير القدرة على تصميم وتصنيع التقنيات محليًا ضرورة لحماية الأمن القومي على المدى البعيد. وتجارب الدول الصناعية الرائدة تدعم هذا التوجه: فقد حققت كوريا الجنوبية طفرة تقنية عبر إستراتيجية تصنيع مدعومة حكوميًا مكّنتها من امتلاك شركات رائدة عالميًا في الإلكترونيات والاتصالات. ووفقًا لكتاب «الابتكار والتكنولوجيا في كوريا – تحديات اقتصاد متقدم جديد» فإن كوريا بذلت جهودًا ضخمة في البحث والتطوير حتى أصبحت شركاتها من الرواد العالميين في صناعات التقنية العالية القادرة على منافسة نظرائها الدوليين[341]. هذه القيادة التقنية المحلية منحت كوريا الجنوبية قدرًا من الاستقلالية الرقمية وجعلتها أقل انكشافًا للمخاطر الخارجية. على المنوال نفسه، يتعين على المغرب أن يستثمر في إنشاء مصانع ومراكز تطوير تكنولوجي محلية لإنتاج ما يلزمه من عتاد وبرمجيات، خاصة في المجالات الحساسة كمعدات الاتصالات وأنظمة التحكم الصناعي. إن وجود صناعة وطنية قوية في هذه القطاعات يضمن توفر بدائل محلية موثوقة ويقلل الحاجة إلى استيراد تقنيات قد تشكل تهديدًا أمنيًا مستترًا.

علاوة على ذلك، يسهم التصنيع المحلي في بناء الخبرات الوطنية وتعزيز الاكتفاء الذاتي الرقمي. فامتلاك الدولة لقدرات تصنيع يوفر لها مرونة أكبر في مواجهة الأزمات السيبرانية؛

---

[340] National Academies of Sciences, Engineering, and Medicine, *Convergent Manufacturing: A Future of Additive, Subtractive, and Transformative Manufacturing: Proceedings of a Workshop*, The National Academies Press, Washington, 2022, p. 48.

[341] Jörg Mahlich and Werner Pascha (eds.), *Innovation and Technology in Korea: Challenges of a Newly Advanced Economy*, Heidelberg – New York: Physica-Verlag, 2007, p. 14.

فهي تستطيع تعديل منتجاتها بسرعة وفق احتياجات الأمن القومي دون انتظار حلول خارجية. كما يُمكّن ذلك من تطبيق معايير أمان سيبراني صارمة أثناء مراحل التصميم والإنتاج.

وعلى صعيد آخر، فإن ازدهار الصناعة التقنية المحلية سيكون له أثر إيجابي مزدوج: فمن جهة يخلق ذلك اقتصادًا رقميًا منتجًا يوفر فرص عمل لأفضل المهندسين والعقول المحلية، ومن جهة أخرى يعزز المناعة السيبرانية عبر وجود مورد وطني موثوق للتقنيات الحيوية. لقد بينت خبرات دولية أن سلاسل التوريد المحلية أقل عرضة للاستهداف والتعطيل من قبل الخصوم مقارنةً بالسلاسل العالمية الطويلة[342]، وبالتالي فإن تطوير قدرات تصنيع وطنية يقلّل المخاطر المرتبطة بالاعتماد على مزوّدين أجانب قد يتأثرون بالضغوط السياسية أو الهجمات السيبرانية.

ثانيا: الابتكار السيادي وبناء السيادة الرقمية

إلى جانب التصنيع، يشكّل الابتكار البحثي والمؤسساتي الركيزة الثانية لتعزيز المناعة السيبرانية المغربية على المدى البعيد. إن الابتكار السيادي يعني قدرة الدولة على إيجاد حلول وتقنيات أمنية ذاتية تلبي احتياجاتها الاستراتيجية دون الارتهان لما يُنتج في الخارج. ومن هنا تنبع أهمية الاستثمار المكثف في البحث العلمي والتطوير (*R&D*[343]) في مجالات التكنولوجيا الرقمية والأمن السيبراني. الدول التي نجحت في تحقيق سيادة رقمية هي التي سخرت منظوماتها التعليمية والعلمية لإنتاج المعرفة التقنية محليًا وتحويلها إلى منتجات وشركات منافسة. على سبيل المثال، فنلندا – التي تُعد من الدول المتقدمة رقميًا – تتبنى مقاربة شاملة لتعزيز الابتكار السيبراني تشمل الحكومة والقطاع الخاص والأكاديميات والمجتمع المدني معًا. يقوم نموذج الأمن الشامل الفنلندي على تعاون وثيق بين السلطات والشركات والمواطنين لحماية الوظائف الحيوية للمجتمع[344]. هذا التكامل المؤسساتي يعكس ابتكارًا على مستوى

---

[342] *Convergent Manufacturing: A Future of Additive, Subtractive, and Transformative Manufacturing: Proceedings of a Workshop. Op.cit.*

[343] يُقصد بـ*R&D* (البحث والتطوير) في السياق أنه *مجموع الجهود العلمية والتقنية التي تُبذل من أجل إنتاج حلول رقمية محلية*، وتطوير أدوات أمن سيبراني وطنية. ويُعد *R&D* عنصرًا حاسمًا في تحقيق السيادة الرقمية، لأنه يُمكّن الدول من تقليص الاعتماد على التكنولوجيا الأجنبية، وتطوير أنظمة تشفير ومعالجة وتحليل بيانات خاصة بها، مما يرفع قدرتها على الصمود أمام التهديدات الخارجية.

[344] Astri Edvardsen, *"Finland Strengthens Cybersecurity in the North With Extensive Exercising,"* High North News, February 12, 2025, accessed June 10, 2025, at 14:47, *https://www.highnorthnews.com.*

السياسات، حيث أوجدت فنلندا هيكلاً تنظيميًا يربط الأمن السيبراني بكافة قطاعات الدولة ضمن إطار استراتيجية أمن قومي شاملة. النتيجة هي بيئة محلية حاضنة للتطوير والتأهب: فالبحث العلمي والتقني الموجه نحو الأمن يتكامل مع سياسات التعليم والتوعية السيبرانية، ومع برامج الدعم الحكومي للشركات الناشئة في المجال الرقمي. من هذا المنطلق، ينبغي على المغرب بلورة رؤية وطنية للابتكار السيبراني السيادي، تعتمد على إنشاء مراكز أبحاث متخصصة وشراكات بين الجامعات وشركات التكنولوجيا والأجهزة الأمنية. إن تشجيع الابتكار المحلي في أمن المعلومات سيؤدي إلى حلول مصممة وفق السياق المغربي وبلغة احتياجاته الخاصة، بدلًا من استيراد حلول جاهزة قد لا تراعي الخصوصيات المحلية.

ولا يقتصر الابتكار المطلوب على الجانب التقني فحسب، بل يمتد إلى الابتكار المؤسساتي وبناء الأطر التنظيمية الداعمة. يتعين تطوير مؤسسات وطنية قادرة على قيادة جهود الأمن السيبراني بفعالية، مثل هيئة سيبرانية سيادية تتولى وضع المعايير التقنية الوطنية والتنسيق بين مختلف الفاعلين. كما تشمل جوانب الابتكار المؤسساتي تحديث الأطر القانونية والتشريعية لمواكبة تطور الفضاء السيبراني، وإطلاق مبادرات لتعزيز ثقافة الأمن الرقمي لدى المؤسسات والأفراد. إن وجود بيئة سيبرانية داخلية تتمتع بالثقة (*Trustworthy Cyber Environment*) سيساهم في ازدهار الاقتصاد الرقمي وفي الوقت نفسه يقلل قابلية البلاد للابتزاز الإلكتروني أو الاختراقات واسعة النطاق. ولضمان الاستقلالية الاستراتيجية في هذا المجال، لا بد من تقليص الفجوة التقنية مع الدول المتقدمة عبر توجيه الاستثمارات نحو المجالات التي تشكل عصب السيادة الرقمية (مثل التشفير المتقدّم، والحوسبة السحابية الآمنة، وأمن أنظمة التحكم الصناعي، إلخ). وتشير الدراسات الحديثة إلى أن تحقيق الاستقلالية السيبرانية بات شرطًا لضمان السيادة الرقمية الشاملة؛ إذ إن أي قصور في القدرات السيبرانية الوطنية يشكل خطرًا مباشرًا على سيادة الدولة[345]. لذلك فإن تعزيز الابتكار السيادي، خاصة في أمن المعلومات، يقلّص التبعية للخارج ويزوّد الدولة بهامش مناورة أوسع في الدفاع عن مصالحها الرقمية.

[345] Paul Timmers, Matthijs Punter, and Claire Stolwijk, *Cybersecurity and Digital Sovereignty – Bridging the Gaps* (TNO, 2024), 3.

ثالثا: نماذج دولية رائدة في السيادة السيبرانية من خلال التصنيع

يمكن للمغرب استلهام الدروس من تجارب دول نجحت في المزج بين التصنيع المحلي والابتكار لتعزيز مناعتها السيبرانية:

كوريا الجنوبية: انتهجت كوريا استراتيجية صناعية طموحة بُعَيد الحرب الكورية جعلت من تطوير التكنولوجيا المحلية أولوية قومية. أسست الحكومة منظومة قوية للبحث والتطوير وربطتها بالقطاع الصناعي، مما أثمر نشأة شركات تقنية عملاقة (مثل سامسونغ وإل جي) قادت الابتكار في الإلكترونيات والاتصالات. يذكر كتاب «الابتكار والتكنولوجيا في كوريا» أن هذه الجهود المنسقة مكّنت البلاد من الانتقال من مرحلة اللحاق التكنولوجي إلى مرحلة الريادة التقنية خلال عقود قليلة[346]. فإلى حدود عام 2007 كانت كوريا قد تحولت إلى ثقل اقتصادي بفضل سياستها العلمية؛ إذ استثمرت بكثافة في البحث العلمي حتى باتت العديد من شركاتها في طليعة المنافسة العالمية. النموذج الكوري يؤكد أن الاستثمار الحكومي في التصنيع التقني المحلي وتوجيهه عبر حكامة رشيدة (ICT Governance) شكل مفتاح النجاح. هذه السيادة التقنية مكّنت كوريا من حماية بنيتها التحتية الرقمية بمنتجات محلية موثوقة، كما ساعدتها على بناء نظم سيبرانية متقدمة تخدم حكومتها الإلكترونية وتجعلها أقل تعرضًا للابتزاز التكنولوجي الخارجي.

فنلندا: اتبعت فنلندا نهجًا متميزًا يركز على المقاربة المجتمعية الشاملة للأمن السيبراني. فعلى الرغم من صغر حجمها السكاني، استفادت فنلندا من قوة نظمها التعليمية وثقافة الابتكار لديها لتطوير قدرات دفاع سيبراني رائدة. ينصب نموذجها على تكوين تعاون وثيق بين الهيئات الحكومية والشركات الخاصة والمؤسسات البحثية والمواطنين لتأمين الفضاء الإلكتروني الوطني. وقد حدث تحول نوعي في سياسة فنلندا الأمنية بإدماج الأمن السيبراني ضمن إطار مفهوم الأمن الشامل للمجتمع. تفيد وثائق استراتيجية حديثة بأن مفهوم الأمن الشامل الفنلندي يقوم على عمل مشترك بين السلطات والأعمال والمجتمع المدني والأفراد لحماية الوظائف المجتمعية الحيوية[347]. هذا النموذج يضمن تعبئة كافة الخبرات الوطنية عند التصدي

---

[346] *Jörg Mahlich and Werner Pascha*, Op. cit.
[347] *Finland Strengthens Cybersecurity in the North With Extensive Exercising, Op. cit.*

للتهديدات السيبرانية، كما يخلق بيئة حاضنة للابتكار: فالشركات الفنلندية الناشئة في الأمن السيبراني تلقى دعمًا حكوميًا ومنظومة قوانين مشجعة، ما جعل فنلندا منطلقًا لحلول أمنية متقدمة (مثل برمجيات مكافحة الفيروسات الشهيرة القادمة من خبرات شركة F-Secure الفنلندية[348]). الدرس المستفاد من فنلندا هو أن بناء صناعة رقمية وطنية لابد أن يترافق مع تكامل مؤسسي وتثقيف مجتمعي يرفع الوعي الأمني لدى الجميع، لأن الجبهة السيبرانية لا تقل شمولًا عن الدفاع التقليدي.

وعليه يتضح انه على المغرب أن يركز منذ الآن على ما يجب فعله للغد: بناء صناعة رقمية وطنية قوية، وإطلاق نهضة ابتكارية سيبرانية، وتحقيق تكامل مؤسسي ومجتمعي في مواجهة الأخطار الرقمية. هكذا فقط يمكن إرساء دعائم المناعة السيبرانية المستدامة وجعلها جزءًا لا يتجزأ من مناعة الدولة الشاملة، وبذلك يُضمن أمن المغرب واستقلاله في العصر الرقمي.

خاتمة الفصل:

في ضوء ما سبق من تحليلٍ شاملٍ للتحديات السيبرانية التي يواجهها المغرب، يتبيّن أن البلاد باتت تقف أمام مفترق طرق حاسم: فإما أن تواصل التعامل مع الأمن السيبراني بمنطق التجزئة ورد الفعل، أو أن تتبنى رؤية استراتيجية شاملة تجعل من هذا المجال رافعة للسيادة الرقمية والتنمية المستدامة. لقد كشف هذا الفصل، من خلال رصد دقيق للهجمات التي استهدفت البنية التحتية الرقمية الوطنية، وبيان الثغرات القانونية والتقنية والثقافية التي تعتري المنظومة، عن هشاشة بنيوية تتجاوز الجانب التقني لتطال عمق الحكامة المؤسسية والمقاربة المجتمعية للأمن الرقمي. كما أظهر أن التصدي الفعال للتهديدات السيبرانية لا يمكن أن يتم عبر حلول ظرفية أو استنساخ نماذج جاهزة، بل يتطلب تكييفًا ذكيًا للتجارب الدولية الرائدة، وتطويرًا تدريجيًا لبنية وطنية مرنة قادرة على الصمود في وجه الهجمات المعقدة والمتحوّلة. ومن هنا، فإن تعزيز المناعة السيبرانية في المغرب يقتضي مقاربة متكاملة تجمع بين إصلاح الإطار التشريعي، وتحديث البنية التقنية، وبناء ثقافة أمنية شاملة، وتطوير الكفاءات الوطنية، إضافة إلى الاستثمار في الذكاء الاصطناعي والتصنيع المحلي بوصفهما أداتين حاسمتين

348 شركة *F-Secure*، وهي شركة فنلندية رائدة في مجال الأمن السيبراني، تُعرف بتطويرها لبرمجيات مكافحة الفيروسات، وقد أسهمت في وضع فنلندا على خارطة الصناعات الرقمية الآمنة.

لضمان السيادة الرقمية والاستقلالية الاستراتيجية. وعليه، فإن الأمن السيبراني لم يعد مجرد قطاع تقني داعم، بل غدا رهانًا وجوديًا للدولة الحديثة، يُملي إعادة ترتيب الأولويات وتوجيه السياسات العمومية نحو بناء فضاء رقمي آمن، سيادي، وشامل.

الخاتمة

لقد أضحى الفضاء السيبراني، في خضم التحولات الرقمية المتسارعة التي يشهدها العالم، ركيزة لا غنى عنها لأمن الدول واستقرارها وسيادتها الوطنية. وفي هذا السياق، كشف هذا البحث عن أن المملكة المغربية قد خطت خطوات واسعة ومقدرة في بناء منظومة تشريعية ومؤسساتية متكاملة للأمن السيبراني، وهو ما تجلى في تبوئها مراتب متقدمة عالمياً في مؤشرات الجاهزية الرقمية .بيد أن هذا التقدم، وإن عكس إرادة استراتيجية قوية ووعياً متنامياً بأهمية الفضاء الرقمي، لا يخفي تحديات بنيوية عميقة ونقاط ضعف مستمرة، تتطلب مقاربة متجددة تتجاوز مجرد وجود الأطر إلى تحقيق فعالية عملياتية ومناعة سيبرانية مستدامة. إن هذه المفارقة بين الاعتراف الدولي بالجهود المبذولة وواقع الهجمات الناجحة على البنى التحتية الحيوية، تشير إلى أن وجود الأطر لا يضمن بالضرورة التنفيذ الفعال أو المرونة الكاملة في مواجهة التهديدات المتطورة.

لقد تركزت إشكالية هذا البحث في تقييم مدى فعالية المنظومة التشريعية والمؤسساتية التي اعتمدها المغرب لتأمين فضائه السيبراني وحماية بنيته التحتية الرقمية، بما يكرس السيادة الرقمية للدولة ويصونها من التهديدات المتنامية .وعليه، يؤكد البحث أن فعالية هذه المنظومة هي جزئية ومتطورة باستمرار، وليست حالة ثابتة. ففي حين نجحت المملكة في إرساء دعائم قانونية ومؤسساتية متينة، تمثلت في القانون 05.20 والهيئات المتخصصة كالمديرية العامة لأمن نظم المعلومات واللجنة الوطنية لحماية المعطيات الشخصية ، وحققت تقديراً دولياً يعكس جهودها التأسيسية، إلا أنها لا تزال تواجه فجوات كبيرة في التنفيذ، وهشاشة تقنية، وثقافة سيبرانية ناشئة تعيق تحقيق الفعالية التشغيلية الكاملة والمرونة المستدامة أمام التهديدات المعقدة والسريعة التطور. هذا الواقع يوضح أن الفعالية في الأمن السيبراني هي مسار مستمر من التكيف والتحسين، يتأثر بعوامل متعددة تتجاوز مجرد سن القوانين، لتشمل القدرات المؤسساتية والتقنية والبشرية على حد سواء.

لم يكن مسار إنجاز هذا البحث خالياً من التحديات، فقد واجه الباحث صعوبات جمة، كان أبرزها ندرة المادة العلمية المتخصصة باللغة العربية التي تجمع بين الأمن السيبراني والدراسات السياسية في السياق المغربي .هذا النقص في الأدبيات يعكس حداثة هذا المجال البيني في المشهد الأكاديمي العربي والمغربي، وربما قصوراً في البنى التحتية البحثية والنشرية المحلية لمواكبة التطورات التكنولوجية والقانونية المتسارعة في الأمن السيبراني. وقد اضطر هذا الواقع الباحث إلى الاعتماد على المصادر الأجنبية باللغتين الفرنسية والإنجليزية بالموازاة، مما استلزم جهداً ذاتياً كبيراً في الترجمة الدقيقة للمفاهيم التقنية والقانونية المعقدة إلى اللغة العربية الأكاديمية، لضمان نقل المعنى بوضوح ودون تحريف .كما شكلت محدودية البيانات العلنية حول الحوادث السيبرانية في المغرب، نظراً لحساسيتها الأمنية، عائقاً أمام التحليل الكمي الشامل .هذا النقص في الشفافية، وإن كان مبرراً من منظور الأمن القومي، إلا أنه يؤثر سلباً على قدرة الأوساط الأكاديمية والقطاع الخاص والمجتمع المدني على التعلم من التجارب السابقة وتعزيز الدفاعات بشكل استباقي، مما قد يساهم في ضعف الثقافة السيبرانية العامة. وقد تم التغلب على هذه العراقيل من خلال تنويع مصادر البحث، والاستعانة بالخبرة العملية للباحث في المجال التقني، وتوظيف الاستدلال المنطقي والتحليل المقارن لاستخلاص النتائج حتى مع محدودية البيانات الصريحة.

وفي ضوء ما تقدم، فإن الفرضية الأولى التي انطلق منها البحث، والقائمة على كفاية الإطار المغربي الحالي (القانون 05.20 والهيئات التابعة له) لتحقيق حماية شاملة للبنية التحتية الرقمية دون الحاجة لتعديلات جوهرية ، قد دُحضت بوضوح. فقد أظهر البحث أن الهجمات السيبرانية المتكررة والناجحة على مؤسسات وطنية حيوية، مثل الصندوق الوطني للضمان الاجتماعي ووزارة التعليم العالي ، تؤكد وجود ثغرات بنيوية وتقنية وبشرية عميقة. كما أن الفجوات في إلزامية التبليغ عن الحوادث، وضعف العقوبات، وغياب آلية مراجعة تشريعية دورية ، جميعها عوامل تبرز عدم كفاية الإطار الحالي بمفرده لمواجهة التهديدات المتجددة. وعلى النقيض، فإن الفرضية الثانية التي افترضت أن المنظومة الراهنة، رغم أهميتها، تتطلب تطويرًا تشريعياً وتنظيمياً وتقنياً متواصلاً، بالإضافة إلى تعميق التنسيق وبناء القدرات البشرية المتخصصة وتوطين التكنولوجيا ، قد تأكدت بشكل قاطع. فالتحليل المفصل لنقاط الضعف في الثقافة الأمنية الرقمية، ونقص الكفاءات، والاعتماد المفرط على الحلول الأجنبية ، يؤكد

الحاجة الملحة إلى مقاربة شاملة ومتعددة الأبعاد لتعزيز المناعة السيبرانية وضمان السيادة الرقمية.

من الملاحظات الأساسية المستخلصة أن المغرب، رغم إظهاره نية استراتيجية قوية وتطويره أطر قانونية ومؤسساتية شاملة للأمن السيبراني، وهو ما انعكس في تصنيفه المتقدم دولياً ، إلا أن هناك فجوة واضحة بين صياغة السياسات ونضجها العملياتي. هذا التفاوت أدى إلى استمرار الهشاشة ونجاح الهجمات السيبرانية. كما تبين أن العامل البشري يمثل الحلقة الأضعف في سلسلة الدفاع السيبراني، حيث يستغل المهاجمون ضعف الوعي الرقمي وثقافة الأمن الناقصة لدى الأفراد والمؤسسات .إضافة إلى ذلك، يعيق تشتت المسؤوليات المؤسساتية ومحدودية تبادل المعلومات الفوري ونقص الموارد المالية والبشرية المخصصة، التنسيق الوطني الفعال والاستجابة السريعة للأزمات السيبرانية .وأخيراً، تؤكد الهجمات السيبرانية ذات الدوافع السياسية، والاعتماد الكبير على الحلول التكنولوجية الأجنبية، على الضرورة الملحة للمغرب لبناء قدرات ذاتية في التصنيع والابتكار السيبراني، وذلك لتحصين سيادته الرقمية واستقلاله الاستراتيجي.

وفي سبيل تعزيز المناعة السيبرانية الوطنية، يقترح هذا البحث مجموعة من الحلول المبتكرة:

1. **مركز وطني للدمج السيبراني بالذكاء الاصطناعي** :يُقترح إنشاء مركز وطني متطور تحت إشراف المديرية العامة لأمن نظم المعلومات، يستفيد من خوارزميات الذكاء الاصطناعي المتقدمة لتحليل التهديدات في الوقت الحقيقي، والكشف الاستباقي عن الشذوذ السلوكي في الشبكات الوطنية، وأتمتة مهام الاستجابة الروتينية. هذا المركز سيعيد هيكلة عملية اتخاذ القرار السيبراني داخل الإدارة العمومية، محولاً إياها من عمليات بيروقراطية بطيئة إلى حوكمة استباقية قائمة على البيانات، مما يقلص زمن الاستجابة ويعزز الشفافية.
2. **مبادرة "صنع في المغرب" للتقنيات السيبرانية** :يتوجب إطلاق مبادرة وطنية طموحة لدعم التصنيع المحلي للمكونات السيبرانية الحيوية، مثل الأجهزة الشبكية الآمنة، والوحدات التشفيرية، والبرمجيات الأمنية الوطنية. يجب أن تتضمن هذه المبادرة حوافز حكومية موجهة (كالإعفاءات الضريبية ومنح البحث والتطوير) لشركات التكنولوجيا

المحلية، بهدف بناء قاعدة صناعية رقمية سيادية تقلل من الاعتماد على التقنيات المستوردة التي قد تحمل ثغرات خفية.

3. **فيلق الدبلوماسية السيبرانية ومنصة "المواطن السيبراني الآمن"**: يُقترح إنشاء فيلق متخصص للدبلوماسية السيبرانية ضمن وزارة الشؤون الخارجية، يضم دبلوماسيين مدربين على قواعد السلوك السيبراني الدولي وعمليات التأثير الرقمي، للمساهمة بفاعلية في صياغة المعايير الدولية ومواجهة حملات التضليل التي تستهدف مصالح المغرب . بالتوازي، يجب إطلاق منصة وطنية تفاعلية ومحفزة لتعليم الأمن السيبراني، تستهدف جميع الفئات العمرية، خاصة الشباب، وتدمج مفاهيم النظافة الرقمية في المناهج التعليمية.

4. **منصة وطنية للاختبار السيبراني الآمن وغرامات تناسبية**: يجب تطوير منصة مدعومة حكومياً، تتيح للمقاولات الصغيرة والمتوسطة اختبار أنظمتها الرقمية للكشف عن الثغرات في بيئة آمنة ومراقبة بتكلفة رمزية، مما يعالج ضعفها المالي والتقني . وفي موازاة ذلك، يجب إصلاح نظام الغرامات في القانون 05.20، لتصبح تناسبية مع حجم الخسائر الاقتصادية أو نسبة من رقم معاملات الجهة المخالفة، بدلاً من المبالغ الثابتة، لضمان ردع حقيقي للكيانات الكبرى.

تفتح هذه الدراسة آفاقاً بحثية جديدة وتساؤلات جوهرية تستدعي المزيد من التعمق:

- **قياس العائد على الاستثمار في الأمن السيبراني للدول النامية**: ما هو العائد الحقيقي على الاستثمار في الأمن السيبراني بالنسبة للدول النامية مثل المغرب، وكيف يمكن تطوير نماذج اقتصادية لقياس فعالية الإنفاق الأمني في تعزيز النمو الاقتصادي وتقليل الخسائر غير المباشرة؟
- **الذكاء الاصطناعي الأخلاقي في الأمن السيبراني والسيادة على البيانات**: ما هي التحديات الأخلاقية والقانونية الناشئة عن توظيف الذكاء الاصطناعي في الأمن السيبراني بالمغرب، وكيف يمكن صياغة إطار تشريعي يوازن بين فعالية الدفاع السيبراني وحماية حقوق الأفراد والسيادة على البيانات؟

- **دور المرونة السيبرانية في الاستقرار الإقليمي والجغرافيا السياسية** :كيف يمكن للمغرب، بصفته قوة إقليمية صاعدة، أن يسهم في بناء منظومة أمن سيبراني إقليمية متكاملة في شمال إفريقيا والساحل، وما هي التحديات الجيوسياسية التي تواجه هذا التعاون؟

إن الأمن السيبراني، في جوهره، لم يعد مجرد مسألة تقنية أو قانونية، بل هو رهان وجودي للدولة الحديثة، يملي عليها إعادة ترتيب أولوياتها وتوجيه سياساتها العمومية نحو بناء فضاء رقمي آمن و سيادي وشامل. إن تحقيق هذه الرؤية يتطلب التزاماً مستمراً بالابتكار، وتوطيناً للتقنيات، وتنمية للقدرات البشرية، وتنسيقاً وطنياً وإقليمياً ودولياً، لضمان مستقبل رقمي مزدهر ومحصن للمملكة المغربية.

لائحة المراجع

❖ كتب

- الأصفهاني، الحسين بن علي. المفردات في غريب القرآن. دار المعرفة، بيروت، 2005.
- الأشقر جبور، منى. السيبرانية هاجس العصر. بيروت: المركز العربي للبحوث القانونية والقضائية، 2017.
- البحري، حسن مصطفى. القانون الدستوري: النظرية العامة. الطبعة الأولى. دمشق: الجامعة الافتراضية السورية، 2009.
- هلالي، عبداللاه أحمد. اتفاقية بودابست لمكافحة جرائم المعلوماتية: معلقًا عليها. الطبعة الأولى. القاهرة: دار النهضة العربية، 2011.
- DEBBAGH, Taieb. 15 Ans de Cybersécurité au Maroc. Édition indépendante, 2023.
- EL AZZOUZI, Ali. La Cybercriminalité au Maroc. Casablanca: Bishops Solutions, 2010.
- KEMPF, Olivier. Introduction à la Cyberstratégie. Paris: Economica, 2012.
- MAHLICH, Jörg, and WERNER PASCHA (eds.). Innovation and Technology in Korea: Challenges of a Newly Advanced Economy. Heidelberg – New York: Physica-Verlag, 2007.
- MALEH, Yassine, and Youness Maleh. Cybersecurity in Morocco. 1st ed. Cham, Switzerland: Springer Nature, 2022.
- National Academies of Sciences, Engineering, and Medicine. Convergent Manufacturing: A Future of Additive, Subtractive, and Transformative Manufacturing: Proceedings of a Workshop. Washington, DC: The National Academies Press, 2022.
- OPPLIGER, Rolf. SSL and TLS: Theory and Practice. 3rd ed. Norwood, MA: Artech House, 2023.

- SINGER, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. 1st ed. New York: Oxford University Press, 2014.
- STALLINGS, William, and Lawrie Brown. Computer Security: Principles and Practice. 2nd ed. Boston: Pearson, 2012.

❖ رسائل جامعية

- البراشي، بكيل بن محمد. دور الأمن الفكري في الوقاية من الإرهاب. رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.
- ساعد، طيايبة. مستقبل الممارسة الدبلوماسية في ظل العصر الرقمي. أطروحة دكتوراه في تخصص الدبلوماسية، جامعة الجزائر 3، كلية العلوم السياسية والعلاقات الدولية، 2018.
- عطية، إدريس. مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. رسالة ماجستير، جامعة العربي التبسي – الجزائر، 2019.

❖ دساتير

- دستور المملكة المغربية لسنة 2011 (توطئة الدستور – الفصول: 27 – 31 – 154 – 156).

❖ ظهائر

- الظهير الشريف رقم 1.03.197 الصادر في 16 رمضان 1424 (11 نوفمبر 2003) القاضي بتنفيذ القانون رقم 07.03 المُتمِّم لمجموعة القانون الجنائي فيما يخص الجرائم المرتبطة بنظم المعالجة الآلية للمعطيات.
- الظهير الشريف رقم 1.17.27 الصادر في 8 ذي الحجة 1438 (14 سبتمبر 2017) المتعلق بإحداث وكالة التنمية الرقمية (القانون رقم 61.16).

❖ **قوانين**

- القانون رقم 05.20 المتعلق بالأمن السيبراني. الجريدة الرسمية عدد 6904 (30 يوليوز 2020): ص. 4160. الظهير الشريف رقم 1.20.69 بتاريخ 25 يوليوز 2020.
- القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذه الظهير الشريف رقم 1.09.15 بتاريخ 18 فبراير 2009.
- القانون رقم 24.09 المتعلق بالبريد والمواصلات (الظهير الشريف رقم 1-97-162 بتاريخ 7 غشت 1997)، كما وقع تغييره وتتميمه بمقتضى القانون رقم 29.06 (الظهير الشريف رقم 1-07-43 بتاريخ 17 أبريل 2007).
- القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية كما تم تعديله بالقانون رقم 43.20. الصادر بتنفيذه الظهير الشريف رقم 1.20.100 بتاريخ 31 ديسمبر 2020؛ الجريدة الرسمية عدد 6951 (11 يناير 2021) ص. 271.

❖ **مراسيم**

- مرسوم رقم 2.82.673 صادر في 28 ربيع الأول 1403 (13 يناير 1983) بتنظيم إدارة الدفاع الوطني وإحداث المديرية العامة لأمن نظم المعلومات.
- مرسوم رقم 2.08.518 صادر في 25 جمادى الأولى 1430 (21 ماي 2009).
- مرسوم رقم 2.09.165 صادر في 25 جمادى الأولى 1430 (21 ماي 2009).
- مرسوم رقم 2.11.509 صادر في 22 شوال 1432 (21 سبتمبر 2011) بتتميم المرسوم رقم 2.82.673 الصادر في 13 يناير 1983.
- مرسوم رقم 2.13.881 صادر في 28 ربيع الأول 1436 (20 يناير 2015).

- مرسوم رقم 2.15.712 صادر في 12 جمادى الآخرة 1437 (22 مارس 2016) بتحديد إجراءات حماية نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية.
- مرسوم رقم 2.21.406 صادر في 4 ذو الحجة 1442 (15 يوليو 2021).
- مرسوم رقم 2.24.921 صادر في سنة 2024.
- قرار مشترك لوزير التعليم العالي والبحث العلمي والابتكار ووزيرة الاقتصاد والمالية رقم 1148.25 صادر في 6 ماي 2025 بالمصادقة على الاتفاقية المؤسسة لمركز الابتكار في الأمن السيبراني (مجموعة ذات نفع عام)، الجريدة الرسمية عدد 7407 بتاريخ 28 ماي 2025.

❖ مجلات علمية

- بنعلا، إلهام. "الآليات المؤسساتية للسياسة الجنائية في المجال المعلوماتي." مجلة المحيط القانوني الأكاديمي للدراسات والبحوث، العدد 2، 2025.
- الحسان العصري، "قراءة في القانون رقم 31.08 القاضي بتحديد تدابير لحماية المستهلك"، منصة مغرب القانون MarocDroit، 31 غشت 2013.
- السمحان، منى عبد الله. "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية." مجلة كلية التربية، جامعة المنصورة، المجلد 111، العدد 1، 2020.
- الشمري، سلمى عبد الرحيم عبد الحسن داغر. "طبيعة العلاقة بين الأمن السيبراني والنمو الاقتصادي الرقمي في دول العالم." المجلة الأمريكية الدولية المحكمة للعلوم الإنسانية والاجتماعية، العدد 10، بغداد، مايو 2025.
- العربي، العربي. "الدبلوماسية الرقمية وتأثيراتها في العلاقات الدولية." لباب للدراسات الاستراتيجية والإعلامية، العدد 10، 2021.
- وساك، إسماعيل. "الدبلوماسية المغربية في زمن فيروس كورونا." مجلة المنارة للدراسات القانونية والإدارية، دار المنظومة، أكتوبر 2020.

- BENNACER, M. K., E. M. EL MAHDI, & M. LAHMOUCHI. "Digital Transformation in Moroccan SMEs: Overcoming Barriers and Achieving Growth." TEM Journal 14, no. 2 (2025).
- DOLOWITZ, David P., & David MARSH. "Learning from abroad: The role of policy transfer in contemporary policy-making." Governance 13, no. 1 (2000).
- FUNK, Philippe. "Artificial Intelligence and Cybersecurity: Implications for Business Management." Economy & Business 16 (2022).
- HUANG, Youxing, Na Jiang, & Yan Zhang. "Does Internet Security Matter for Foreign Direct Investment? A Spatial Econometric Analysis." Telematics and Informatics 59 (2021): 101559.
- KEZZOUTE, M. "Cyber Governance in Morocco: Between the Consolidation of Internal Status and the Enhancement of Global Positioning." Journal of Cyberspace Studies 9, no. 1 (2025).
- NYE Jr., Joseph S. "Deterrence and Dissuasion in Cyberspace." International Security 41, no. 3 (2017).
- OFUSORI, Lizzy, Tebogo BOKABA, & Siyabonga MHLONGO. "Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction." Applied Artificial Intelligence 38, no. 1 (2024).
- REVERON, Derek S., & John E. SAVAGE. "Cybersecurity Convergence: Digital Human and National Security." Orbis 64, no. 4 (2020).

❖ تقارير رسمية

- المجلس الاقتصادي والاجتماعي والبيئي. نحو تحول رقمي مسؤول ومدمج. رأي ذاتي الإحالة، 29 أبريل 2021.
- المملكة المغربية – وزارة الانتقال الرقمي وإصلاح الإدارة. "الاستراتيجية الوطنية للأمن السيبراني 2030." إصدار رسمي، الرباط، 2023.

- المديرية العامة لأمن نظم المعلومات. مذكرة تقديمية للقانون 05.20 بشأن الأمن السيبراني. الرباط: المديرية العامة لأمن نظم المعلومات، 2020.
- Capgemini Research Institute. AI and Gen AI in Cybersecurity. May 2024.
- Council of Europe. "Support to data protection in Morocco." 2024.
- Cyber Security Agency of Singapore (CSA). Singapore's Cybersecurity Strategy. 2016 – 21 – 22.
- Cybersecurity (Amendment) Bill No. 15/2024. Singapore Parliament, 2024.
- Cybersecurity Act 2018 (2020 Revised Edition). Singapore: Law Revision Commission, 2021.
- ENISA. Threat Landscape 2024. September 2024.
- International Energy Agency (IEA). Power Systems in Transition – Cyber Resilience. 2021.
- International Institute for Strategic Studies (IISS). Cyber Capabilities and National Power, Vol. 2 – "Estonia". London: IISS, 2023.
- International Renewable Energy Agency (IRENA). Digitalisation and the Energy Transition. 2023.
- International Telecommunication Union (ITU). Global Cybersecurity Index 2024 (5th edition). Geneva: ITU, 2024.
- ISC². Cybersecurity Workforce Study. 2024.
- KnowBe4, Inc. African Cybersecurity & Awareness Report 2025. Clearwater, FL: KnowBe4, 2025.
- Kohler, Kevin. Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations. Zürich: Center for Security Studies (CSS), ETH Zürich, 2020.
- Ministry of Home Affairs (Singapore). National Cybercrime Action Plan. Singapore, 2016.

- National Institute of Standards and Technology (NIST). Preliminary Cybersecurity Framework. Gaithersburg, MD: NIST, 2013.
- Osula, Anna-Maria. National Cyber Security Organisation: Estonia. Tallinn: NATO CCDCOE, 2015.
- Pernik, Piret (with Emmet Tuohy). Cyber Space in Estonia: Greater Security, Greater Challenges. Tallinn: ICDS, 2013.
- Pernik, Piret. Cyber Deterrence: A Case Study on Estonia's Policies and Practice. Helsinki: Hybrid CoE, 2021.
- PwC & AUSIM. Ausimètre 2025 – Baromètre de la cybersécurité au Maroc (2e édition). Casablanca: PwC/AUSIM, 2025.
- Republic of Estonia – Ministry of Economic Affairs and Communications. Cybersecurity Strategy 2019–2022. Tallinn, 2019.
- Timmers, Paul; Matthijs Punter; & Claire Stolwijk. Cybersecurity and Digital Sovereignty – Bridging the Gaps. Den Haag: TNO, 2024.
- U.S. Department of Defense. 2023 Cyber Strategy Summary. Washington, DC: DoD, 2023.
- U.S. Department of Homeland Security. Cybersecurity Strategy. Washington, DC: DHS, 2018.
- U.S. Department of State. United States International Cyberspace and Digital Policy Strategy. Washington, DC: U.S. Department of State, 2024.
- Vergara Cobos, Estefania. Cybersecurity Economics for Emerging Markets. Washington, DC: World Bank, 2024.
- World Bank. New World Bank Program in Morocco Supports Efforts to Boost Water Security and Resilience for All. 24 July 2023.
- World Economic Forum. Global Cybersecurity Outlook 2024. Geneva: World Economic Forum, 2024.

- Hind IDRISSI. Cybersecurity in Morocco: between achievements and challenges. MIPA Institute, 2023. (Accessed: 27 April 2025). Available at: www.mipa.institute.

❖ مقالات صحفية

- أمين أعزان. "المغرب يلجأ إلى القانون الجنائي ضد القراصنة لأنه لا يتوفر على قانون الأنترنت." جريدة المساء (منشور على موقع مغرس)، 31 ماي 2013.
- بهية مستغفر. "قراصنة يخترقون الموقع الرسمي لوزارة التربية." جريدة هسبريس، 22 شتنبر 2010.
- وكالة المغرب العربي للأنباء. "المواقع الإلكترونية لوكالة المغرب العربي للأنباء مستهدفة بهجوم إلكتروني لحجب الخدمة 16 ."(DDOS) فبراير 2023.
- بشرى الردادي. "سيادة رقمية مؤجلة.. متى نؤسس أمننا السيبراني بأيدينا؟" تيل كيل عربي، 8 ماي 2025.
- MAP. « IA : DXC CDG inaugure son Centre d'excellence en Intelligence Artificielle ». Le Desk13 ، février 2025.
- ASTRI EDVARDSEN. "Finland Strengthens Cybersecurity in the North With Extensive Exercising." High North News, 12 February 2025.
- BASHIR, Hamdy. "A Cyber Shadow-War between Algeria and Morocco." The Arab Wall, 24 March 2022.
- BENNANI, Abdel-Ilah. "Cybersécurité, IA et gouvernance numérique : construire une stratégie marocaine dans un monde connecté." L'Opinion, 13 avril 2025.
- BABAS, Latifa. "Cyberattacks: The new frontline in the Morocco-Algeria rivalry." Yabiladi, 9 April 2025.
- EL HAMDI, Soufiane. "Opinion: The CNSS attack and the road to justice." Hespress English, 25 April 2025.

- IBRIZ, Sara. "Fuite de cartes bancaires marocaines dans le dark web : ce que révèle une analyse de Cypherleak." Médias24, 18 mars 2025.
- KABIRI KETTANI, Mounia. "Les données du ministère de l'enseignement supérieur auraient-elles fuité ?" L'Observateur du Maroc et d'Afrique, 21 décembre 2022.
- MAROC DIPLOMATIQUE. "Cybercriminalité : la DGSN traque les délinquants du web." 5 octobre 2019.
- MEATECH WATCH. "DDoS Attacks Surge Across North Africa, With Morocco Leading the Region in Cyber Threat Activity." 12 May 2025.
- BARLAMANE. « Le maCERT, puissant bouclier de la DGSSI contre les menaces cybernétiques ». 6 mai 2024.
- FAOUZI, Adil. "Transparency Maroc: CNSS Data Breach Exposes Critical Flaws in Morocco's Cybersecurity." Morocco World News, 23 April 2025.
- SAOUDI, Oussama. "Morocco adopts smart irrigation amid drought challenges." Hespress English, 23 July 2024.
- STAFF WRITER. "Digital Onslaught in Morocco: Govt Hacked, 30K+ Bank Cards Leaked in Escalating Cyberwar." Launchbase Africa, 10 April 2025.
- TACHFINE, Khadija. "Report warns Morocco is becoming fertile ground for cyberattacks amid geopolitical tensions." Hespress English – Morocco News, 19 April 2025.
- TOUTATE, Ismail. "Defendis: The Cybersecurity Startup Shielding Africa's Digital Transformation." Morocco World News, 12 April 2025.

❖ مواقع إلكترونية

- الموقع الرسمي لحملة Moroccan Investment and Export Agency. "Morocco Now". متاح على الرابط: www.morocconow.com.

- وزارة الأوقاف والشؤون الإسلامية. "بطاقة حول بوابة الصحراء المغربية". الموقع الرسمي للوزارة، الرابط: www.habous.gov.ma.
- المديرية العامة لأمن نظم المعلومات. "قائمة متعهدي افتحاص أمن نظم المعلومات المؤهلين": www.dgssi.gov.ma.
- المديرية العامة لأمن نظم المعلومات. "ماسيرت – الفريق المغربي للاستجابة لحالات الطوارئ التي تحدث في الحواسيب". متاح على : www.dgssi.gov.ma.
- البوابة الوطنية للمملكة المغربية. متاح على الرابط: www.maroc.ma.
- وزارة الانتقال الرقمي وإصلاح الإدارة. "توقيع السيدة الوزيرة لمذكرة تفاهم لإنشاء معهد الجزري..." 14 أبريل 2025. متاح على: www.mmsp.gov.ma.
- وزارة الصناعة والاستثمار والتجارة والاقتصاد الرقمي (تسمية سابقة). المغرب بين تنمية الثقة الرقمية وتطوير الأمن السيبراني. المملكة المغربية، (بدون تاريخ نشر) : www.unescwa.org.
- الأكاديمية الرقمية. الإطلاق الرسمي لحملة التوعية بالأمن السيبراني. الأكاديمية الرقمية، 1 يوليوز 2022. متاح على: academiaraqmya.gov.ma.
- «*Malabo Convention*، *Wikipedia: The Free Encyclopedia*»، آخر تعديل في 23 يونيو 2025، تم الاطلاع عليه بتاريخ 10 يوليو 2025، على الساعة 18:30، عبر الموقع التالي: *https://en.wikipedia.org*

- Centre National de Documentation. Maroc Numeric Cluster. Rabat: Haut-Commissariat au Plan. Disponible à: https://cnd.hcp.ma.
- Orange Cyberdefense Maroc. (30 avril 2025). Multiplication des cyberattaques en Afrique : Orange Cyberdefense Maroc est là pour renforcer la cybersécurité des entreprises. Disponible à : www.orangecyberdefense.com.
- Yasmine ZAYAKH. The Culture of Withholding Information in Morocco: A Barrier to Progress? Friedrich Naumann Foundation for Freedom, 22 April 2025. Available at: www.freiheit.org.

- Raouf RIAHI. Comprehensive Analysis of the April 2025 Cyberattacks on Morocco. LinkedIn, 14 April 2025.
- CYFIRMA. Decoding Cyberattacks on Morocco. 28 November 2024. Available at: www.cyfirma.com.
- Université Mohammed VI Polytechnique (UM6P). Master in Applied Data Science and Artificial Intelligence. Disponible sur: cc.um6p.ma.
- Kobetitsch, Katarina. Information Security vs. Cyber Security: Are They the Same? St. John's University, March 25, 2024.

الفهرس