حكامة الخدمات السحابية والأمن السيبراني في القانون المغربي:
بين متطلبات السيادة الرقمية وانفتاح الفضاء السيبراني

Governance of Cloud Services and Cybersecurity in Moroccan Law:
Between the Imperatives of Digital Sovereignty and the Openness of Cyberspace

Ali Zahour علي زهور

طالب باحث بسلك الدكتوراه، العلوم القانونية والسياسية

كلية العلوم القانونية والسياسية، جامعة ابن طفيل، المغرب

Ali.zahour@uit.ac.ma

Dr.Abderazak kabouri د. عبد الرزاق كبوري

أستاذ باحث بكلية العلوم القانونية والسياسية، جامعة ابن طفيل، المغرب.

en.abderazak@gmail.com

ملخص:

يقارب البحث إشكالية تأطير الخدمات السحابية ضمن المنظومة القانونية المغربية، مبرزا التوتر القائم بين متطلبات السيادة الرقمية المقررة بموجب القانون 05.20، لاسيما إلزامية الإيواء الوطني للمعطيات الحساسة، وبين الطبيعة العابرة للحدود للحوسبة السحابية، مقيّما مدى انسجام التدابير التنظيمية للمرسوم 2.24.921 مع التزامات المغرب ضمن الاتفاقية العامة للتجارة في الخدمات (GATS) ، وبناء على تحليل المضمون والمقارنة مع التشريعات الأوروبية ، نخلص إلى أن الصرامة التشريعية تعرقل الاستثمارات وتحد من التنافسية الاقتصادية، ونوصي باعتماد تصنيف مرن لحساسية المعطيات، وتعديل المادة 11 لإجازة الإسناد الخارجي المقنن، موازاة مع تعزيز آليات الافتحاص وتطوير أطر التعاون الدولي والقضائي.

الكلمات المفتاحية: الخدمات السحابية، الأمن السيبراني، السيادة الرقمية، القانون 05.20، الإيواء الوطني.

Summary:

This research examines the regulation of cloud services in Morocco, highlighting the tension between Law 05.20's digital sovereignty requirements specifically the mandatory national hosting of sensitive data and the cross-border nature of cloud computing. It assesses the compatibility of Decree 2.24.921 with Morocco's commitments under the General Agreement on Trade in Services (GATS). Using a comparative approach with European legislation, the study concludes that regulatory rigidity hinders investment and economic competitiveness. It recommends adopting a flexible data classification, amending Article 11 to

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

allow regulated outsourcing, and enhancing audit mechanisms alongside international cooperation frameworks.

Keywords: Cloud Services, Cybersecurity, Digital Sovereignty, Law 05.20, National Data Hosting.

مقدمة

يتسم تنظيم الفضاء السيبراني في العصر الرقمي براهنية قصوى، ذلك أن التحول الرقمي تجاوز تطوير الخدمات الرقمية ليعيد تشكيل العلاقات بين الدولة والمواطن، وبين الفاعلين الاقتصاديين بعضهم ببعض، بل وأصبح يعيد تعريف حدود السيادة الوطنية ذاتها في بعدها الرقمي، وإذا كان مفهوم السيادة التقليدية ارتبط بالأرض والماء والجو، فإن امتداد الفضاء السيبراني وما يستتبعه من تدفق للبيانات عبر الحدود، وما يثيره من إشكالات تتعلق بحماية المعطيات الشخصية والحساسة، قد فرض على الدول إعادة النظر في أدواتها القانونية لمواكبة هذه التحولات، وفي ظل التوسع الكبير لاستعمال الخدمات السحابية، التي تمكّن المؤسسات والأفراد من تخزين ومعالجة كميات ضخمة من المعطيات عن طريق بنيات تحتية موزعة جغرافيا، تطرح إشكالية قانونية مركزية تتعلق بمدى قدرة التشريعات الوطنية على استيعاب هذه الخدمات وتنظيمها دون الإخلال بمتطلبات الأمن السيبراني من جهة، ودون إعاقة الابتكار والانفتاح التقني من جهة أخرى.

ولذلك أولى المشرع المغربي هذه الإشكالية عناية خاصة من خلال سلسلة من النصوص التشريعية والتنظيمية، كان في مقدمتها القانون رقم 05.20 الصادر في 4 ذي الحجة 1441 (25 يوليو 2020)[1] المتعلق بالأمن السيبراني، والذي كان نقلة نوعية في المنظومة القانونية الوطنية، بتقنينه لحماية نظم المعلومات، وحدد قواعد ومقتضيات الأمن المطبقة على مؤسسات الدولة والجماعات الترابية والمؤسسات العمومية، فضلا عن البنيات التحتية ذات الأهمية الحيوية، ومستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني والخدمات الرقمية،[2] وقد صيغ هذا القانون في سياق

[1] المملكة المغربية، القانون رقم 05.20 المتعلق بالأمن السيبراني، الرباط، 2020.

[2] المملكة المغربية، المرسوم رقم 2.24.921 المنظم لاستخدام مقدمي الخدمات السحابية من قبل الهيئات والبنيات التحتية الحيوية التي تسير نظم المعلومات الحساسة أو المعطيات الحساسة، الجريدة الرسمية، 2024.

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

دولي اتسم بتصاعد وتيرة الهجمات السيبرانية وتنامي المخاطر المرتبطة بالفضاء الرقمي، وهو ما استدعى تدخلا تشريعيا لتعزيز صمود الأنظمة المعلوماتية الوطنية وتأسيس الآليات الرقابية.

غير أن خصوصية الخدمات السحابية، التي تقوم أساسا على توزيع المعطيات وتخزينها في مراكز بيانات موزعة غالبا ما تمتد عبر الحدود الوطنية، تطرح تحديا جوهريا أمام تطبيق بعض مقتضيات هذا القانون، وعلى رأسها المادة 11 التي تنص على أن "يجب أن يكون توطين المعطيات الحساسة، حصريا، داخل التراب الوطني"، فهذا الالتزام، الذي يندرج في إطار الحرص على السيادة الرقمية وحماية المعطيات الحيوية من أي تدخل خارجي، يصطدم في واقع الأمر مع النموذج التشغيلي للحوسبة السحابية الذي يعتمد على مبدأ التوزيع الجغرافي المرن للبيانات تحقيقا لمتطلبات الأداء واستمرارية الخدمة، ومن هنا تظهر المعضلة الأساسية التي يسعى هذا البحث إلى مقاربتها، وهي: كيف يمكن التوفيق بين مقتضى السيادة الرقمية المتجسد في إلزامية الإيواء الوطني للمعطيات الحساسة، وبين طبيعة الخدمات السحابية التي تتجاوز بطبيعتها الحدود الجغرافية، في إطار قانوني يحقق الأمن السيبراني دون أن يتحول إلى عائق أمام تنافسية الاقتصاد الرقمي الوطني؟

وإزاء هذه الإشكالية، لم يقف المشرع المغربي موقف المتفرج، بل بادر إلى إصدار المرسوم رقم 2.24.921 بتاريخ 18 ربيع الثاني 1446 (22 أكتوبر 2024)[3] المنظم لاستخدام مقدمي الخدمات السحابية من قبل الهيئات والبنيات التحتية الحيوية التي تسير نظم المعلومات والمعطيات الحساسة،[4] وهي خطوة تنظيمية مهمة حددت شروط وإجراءات اللجوء إلى هذه الخدمات، مع وضع نظام تأهيل لمقدميها يراعي خصوصية المعطيات التي يتعاملون معها، غير أن هذا المرسوم، رغم كونه تطورا إيجابياً على مستوى التدقيق التنظيمي، لم يحسم بعد كل الإشكالات المرتبطة بهذا المجال، بل أثار بدوره تساؤلات جديدة تتعلق بمدى توافق شروط التأهيل التي يتضمنها مع التزامات المغرب الدولية في إطار منظمة التجارة العالمية، خاصة ما يتعلق بمتطلبات الملكية المحلية والإيواء الوطني، مما يستدعي وقفة بحثية ونقدية متأنية.

[3] المملكة المغربية، المرسوم رقم 2.24.921 المنظم لاستخدام مقدمي الخدمات السحابية من قبل الهيئات والبنيات التحتية الحيوية التي تسير نظم المعلومات الحساسة أو المعطيات الحساسة، الرباط، 2024.

[4] نفس المرجع

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

وعليه، فإن هذا البحث يسعى من خلال المقاربة القانونية المقارنة إلى الإجابة عن جملة من التساؤلات الفرعية، تتعلق أولا بمدى ملاءمة المادة 11 من القانون 05.20 لطبيعة الخدمات السحابية المعاصرة في ضوء المرسوم 2.24.921 والإستراتيجية الوطنية للأمن السيبراني 2030 التي أطلقتها المديرية العامة لأمن نظم المعلومات في يوليوز 2024،[5] وثانياً بكيفية تقييم نظام التأهيل المستحدث في ضوء المعايير الدولية والالتزامات التجارية للمغرب، وثالثاً بالدروس المستفادة من التجارب المقارنة، وخاصة التوجيه الأوروبي NIS2 وقانون التضامن السيبراني الأوروبي،[6] التي يمكن توظيفها لتطوير الإطار الوطني، ورابعا النموذج الأمثل لحكامة الخدمات السحابية الذي يوازن بين الأمن والتنافسية، وللإجابة عن هذه التساؤلات، اعتمدنا في المقال على المستوى المنهجي تحليل مضمون النصوص القانونية، والمنهج المقارن للاستفادة من التجارب الأوروبية، ومقاربة تحليل السياسات لتقييم أثر الإطار القانوني على تنافسية القطاع الرقمي المغربي.

أما الدراسات السابقة القريبة والتي قاربت إشكالية حكامة الفضاء الرقمي من مختلف الزوايا، فبعضها أصّل للتحولات العميقة التي أحدثتها تكنولوجيا المعلومات في بنية السيادة التقليدية، ولعل أهمها مقاربة الفيلسوف لوتشيانو فلوريدي في مؤلفه "الثورة الرابعة سنة 2014،[7] والذي فكك فيها تمدد المحيط المعلوماتي وتجاوزه للحدود الجغرافية للدول، وعلى المستوى المغربي، ركزت الأبحاث على تحليل البنية التشريعية المواكبة لهذا التحول، ومنها دراسة فاطمة الزهراء الفضلي (2025) المنشورة في "مجلة منازعات الأعمال"، والتي قوضت الإطار القانوني والتنظيمي للحوسبة السحابية بالمغرب، راصدة تداخل الاختصاصات بين المؤسسات الوطنية في ظل القانون 09-08 والقانون 05.20،[8] غير أن هذه المقاربات المحلية وغيرها، ظلت حبيسة التحليل الوصفي للنصوص، متجنبة الخوض في التناقض التشغيلي بين مطلب الإيواء الوطني المطلق للبيانات والطبيعة البنيوية الموزعة للخدمات السحابية، وعلى الصعيد الدولي المقارن، انصبت الدراسات والتقارير الإستراتيجية الحديثة على هندسة معايير مفهوم "السيادة الرقمية" وتجاوز الطرح الجغرافي الكلاسيكي، وهو ما تجلى بوضوح في الوثائق المرجعية الصادرة عن المفوضية

[5] المديرية العامة لأمن نظم المعلومات DGSSI ، Stratégie nationale de cybersécurité 2030، 2024

[6] European Parliament & Council, Regulation (EU) 2024/2847 establishing the European Cyber Solidarity Act, Official Journal of the European Union, L 2024/2847, 2024, p:) 5

[7] Floridi, The Fourth Revolution: How the infosphere is reshaping human reality, Oxford University Press, 2014,

[8] الفضلي، ف. ز.، الإطار القانوني والتنظيمي للحوسبة السحابية بالمغرب، مجلة منازعات الأعمال، العدد 91، الصفحات 41-62، 2024.

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

الأوروبية، ولا سيما إطار السيادة السحابية (Commission European) الذي أسس لمستويات لضمان ناجع للسيادة التي تراعي التبعية القانونية والتقنية وتأثيرات الملكية الأجنبية، وتزامنا مع ذلك، قاربت الأبحاث التقنية والقانونية أثر التوجيه الأوروبي المتعلق بأمن الشبكات والمعلومات (NIS2) وقانون التضامن السيبراني، مبينة حدوث انتقال نوعي بتبني آليات تصنيفية لتقييم المخاطر السيبرانية وإدارة سلسلة التوريد، بفرض الضمانات التعاقدية التي تحصن المعطيات الحساسة من الامتداد العابر للحدود للتشريعات الأجنبية ذات الطابع الإلزامي.

تتبلور الإضافة العلمية لهذا البحث في تبني مقاربة نقدية تفكك شروط التأهيل المستحدثة بموجب المرسوم 2.24.921، لاستجلاء التداعيات القانونية والاقتصادية لفرض الملكية المحلية، مقترحة استنبات التجربة التصنيفية الأوروبية ضمن السياق الوطني لإعادة هندسة آليات الإسناد الخارجي تحقيقا للتوازن الاستراتيجي بين الأمن السيادي والتنافسية الرقمية.

وتستهدف الدراسة أساسا تقييم الانعكاسات العملية لتطبيق المادة 11 من القانون 05.20 المتعلقة بإلزامية الإيواء الوطني للمعطيات الحساسة، ومساءلة مدى انسجام قيود التخزين المكرسة في المرسوم 2.24.921 مع الالتزامات التجارية للمغرب داخل منظمة التجارة العالمية؛ وقد تمت صياغة خطة البحث ضمن مبحثين؛ يقارب الأول محددات السيادة الرقمية وإشكالية التوطين في القانون 05.20 ونظام التأهيل المحدث بالمرسوم 2.24.921 وتقاطعاته مع الالتزامات الدولية، بينما يرتكز المبحث الثاني على مأسسة حكامة الخدمات السحابية وبناء النموذج الوطني استلهاماً للمعايير الأوروبية، وتحديداً توجيه NIS2 وقانون التضامن السيبراني.

المبحث الأول: المقاربة التشريعية والتنظيمية للخدمات السحابية في النظام القانوني المغربي: قراءة نقدية

يقارب هذا المبحث الإشكالات التي يفرزها الإطار التشريعي والتنظيمي للخدمات السحابية بالمغرب، راصدا التعارض البنيوي بين حتمية التوطين الجغرافي للمعطيات الحساسة المقررة بموجب القانون 05.20 والطبيعة اللامركزية لهذه التكنولوجيا، مع تقييم مدى انسجام اشتراطات الملكية المحلية المستحدثة في المرسوم 2.24.921 مع الالتزامات التجارية الدولية للمملكة.

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

المطلب الأول: محددات السيادة الرقمية وإشكالية توطين المعطيات في القانون 05.20

في هذا المطلب سنؤصل للسيادة الرقمية من خلال التشريع المغربي وذلك على مستوى المادة 11 من القانون 05.20 التي تفرض توطين المعطيات الحساسة داخل التراب الوطني، ثم ننتقل إلى بيان التعارض بين هذا الإلزام وطبيعة الحوسبة السحابية القائمة على التوزيع الجغرافي للبيانات، مع إبراز الإشكالات العملية التي يطرحها تطبيق هذا المقتضى في ظل غياب تعريف دقيق للمعطيات الحساسة وتعدد الجهات الوصية على القطاع.

الفقرة الأولى: التأصيل المفاهيمي للسيادة الرقمية في ظل التشريع المغربي

إذا كانت فكرة السيادة ارتبطت تقليديا بسلطة الدولة على إقليمها المادي، فإن امتداد الفضاء السيبراني إلى ما وراء الحدود الجغرافية قد فرض على الفقه القانوني إعادة تعريف مفهوم السيادة بما يتلاءم مع متطلبات العصر الرقمي، فظهر ما اصطلح على تسميته بالسيادة الرقمية التي تعني قدرة الدولة على ممارسة سلطتها على المعطيات والبنيات التحتية الرقمية الموجودة في إقليمها، وضمان حمايتها من التدخلات الخارجية،[9] وقد تجلت هذه السيادة في القانون المغربي 05.20 من خلال مجموعة من المقتضيات التي تعكس إرادة المشرع في تأكيد سيطرة الدولة على بياناتها ومعلوماتها الحساسة، ومن أهمها المادة 11 التي نصت على إلزامية توطين المعطيات الحساسة داخل التراب الوطني، والمادة 12 التي قررت أن عقود الإسناد لنظم المعلومات الحساسة يجب أن تخضع للقانون المغربي، فضلاً عن المادة 25 التي ألزمت البنيات التحتية ذات الأهمية الحيوية باللجوء إلى مقدمي خدمات مؤهلين من طرف السلطة الوطنية للأمن السيبراني.

يُجسد التوجه التشريعي المغربي مقاربة سيادية حازمة تروم تحصين المعطيات الوطنية في مواجهة الهيمنة التكنولوجية العالمية والتهديدات السيبرانية المتنامية، غير أن هذا الحرص الأمني يفرز تعقيدات تشغيلية عند تقاطعه مع الطبيعة اللامركزية للخدمات السحابية؛ مما حذا بالمشرع إلى إرساء مبدأ التصنيف المرتكز على مقاربة إدارة المخاطر بموجب المادة الخامسة من القانون، وإلزام الهيئات بهيكلة أصولها ونظمها المعلوماتية استنادا إلى معايير السرية والتمامية والتوافر، ضمانا لتناسب التدابير الحمائية مع

[9] Floridi, The Fourth Revolution op cit,, p: 76

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

التفاوت الفعلي في درجات حساسية المعطيات، وهو المسار الذي تدعم مؤسساتيا بإصدار دليل مرجعي تنظيمي يضبط آليات التنزيل العملي والتطبيقي لهذا الالتزام القانوني.

الفقرة الثانية: التعارض البنيوي بين إلزامية الإيواء الوطني وطبيعة الحوسبة السحابية

تطرح المادة 11 من القانون 05.20، باعتبارها ركيزة للسيادة الرقمية، إشكالية عملية ناجمة عن تعارض فرض الإيواء الوطني الحصري مع الطبيعة التشغيلية الموزعة جغرافيا للحوسبة السحابية، مما يصعب تحقيقه تقنيا ويقيد ولوج المؤسسات الوطنية إلى خدمات الفاعلين العالميين كأمازون ومايكروسوفت وغوغل. وفي مفارقة تشريعية، تبيح المادة 10 من القانون ذاته إسناد نظم المعلومات الحساسة لجهات خارجية شريطة التقيد بالضوابط الأمنية، مدعومة بالمادة 13 التي تخول السلطة الوطنية تحديد القواعد المرجعية التقنية لهذا الإسناد، وهو ما يطرح تساؤلا حول التمييز القانوني بين "الإسناد" و"الإيواء"، ويفرز فجوة تشريعية بين الإباحة المشروطة والحظر القطعي. وتتفاقم هذه التقاطعات المعقدة في ظل تنامي الخدمات السحابية الهجينة، فضلا عن القصور المفاهيمي الذي يعتري المادة 2 من نفس القانون؛ إذ اكتفت بتقديم تعريف دائري يصنف "نظام المعلومات الحساس" استنادا إلى معالجته لمعطيات حساسة، دون إرساء معيار دقيق يحدد ماهية هذه المعطيات، مما يشرع الباب لتأويلات متباينة تعرقل الاستقرار القانوني.

هذا، وقد أشارت الدراسات السابقة إلى أن الإطار القانوني والتنظيمي للحوسبة السحابية في المغرب يعكس تعددا في الجهات المسؤولة عن تنظيم هذا القطاع، حيث تتقاطع اختصاصات اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (CNDP) والوكالة الوطنية لتقنين المواصلات (ANRT) و السلطة الوطنية للأمن السيبراني –المديرية العامة لأمن نظم المعلومات (DGSSI) –، بالإضافة إلى قوانين كالقانون 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، والقانون 05.20،[10] وهذا التعدد، وإن كان يعكس حرص المشرع على تغطية كل جوانب الأمن السيبراني، يؤدي في بعض الأحيان إلى تضارب في الاختصاصات وعدم وضوح في تحديد الجهة المخولة بالبت في بعض الإشكالات التقنية والقانونية، مما يستدعي تنسيقا أكثر وضوحا بين هذه الهيئات.

[10] الفضلي، الإطار القانوني والتنظيمي للحوسبة السحابية بالمغرب، مرجع سابق، ص 41

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

المطلب الثاني: نظام التأهيل المستحدث في المرسوم 2.24.921 وتقاطع متطلبات الملكية مع الالتزامات الدولية

يعالج هذا المطلب نظام التأهيل المستحدث بموجب المرسوم 2.24.921 من خلال تحليل مستوياته ومعاييره التنظيمية والتقنية، ثم نتناول الإشكالية المركزية المتعلقة بمدى توافق متطلبات الملكية المحلية والإيواء الوطني الواردة فيه مع التزامات المغرب الدولية في إطار منظمة التجارة العالمية، وخصوصا اتفاقية GATS[11] التي تحظر القيود التمييزية على الخدمات الأجنبية.

الفقرة الأولى: تحليل نظام التأهيل وآليات الإيواء في المرسوم 2.24.921

لقد كان إصدار المرسوم رقم 2.24.921 بتاريخ 22 أكتوبر 2024 نقلة نوعية في الإطار التنظيمي المغربي للخدمات السحابية، حيث انتقل المشرع من المقاربة العامة التي كان يرسمها القانون 05.20 إلى تنظيم تفصيلي يحدد شروط وإجراءات استعمال مقدمي الخدمات السحابية من قبل الهيئات والبنيات التحتية الحيوية التي تسير نظم المعلومات الحساسة أو المعطيات حساسة،[12] وقد وضع هذا المرسوم نظاما للتأهيل غايته ضمان مستوى عالٍ من الأمن في الخدمات السحابية المقدمة للقطاعات الحيوية، وذلك بتحديد المعايير التنظيمية والفنية والقانونية والإدارية، والتي يتعين على المزودين استيفاؤها للحصول على شهادة التأهيل المطلوبة، ومن أهم ما يميز هذا النظام، التمييز بين مستويين من التأهيل، بحيث يشترط لمقدمي الخدمات من المستوى الأول أن يكونوا شركات يقع مقرها في المغرب مع أنظمتها التشغيلية والتجارية بأكملها موجودة داخل البلاد، في حين يكتفي لمقدمي الخدمات من المستوى الثاني بأن تكون أغلبية مساهميهم مغاربة مع إجراء المعالجة والعمليات والتخزين في المغرب.

يؤسس الإطار المرجعي لمتطلبات التأهيل منظومة شمولية للأمن السيبراني تستوعب الأبعاد التنظيمية والتقنية والتعاقدية وآليات الافتحاص واستمرارية الأنشطة، مستلهمة ضوابطها من المعايير الدولية الرائدة على غرار معيار ISO/IEC 27001 ، غير أن السمة الجوهرية لهذا النظام تتجلى في التشديد الحازم على محددات الملكية المحلية والإيواء التوطيني متجاوزا المقتضيات العامة الواردة في القانون 05.20؛ إذ يفرض على مقدمي الخدمات من المستوى الأول حتمية تأسيس مقرهم الاجتماعي وحصر بنياتهم التشغيلية

11 World Trade Organization. (1994). General Agreement on Trade in Services. Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167

12 المملكة المغربية، المرسوم رقم 2.24.921

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

والتجارية بصفة كلية داخل التراب الوطني، بينما يشترط لمقدمي المستوى الثاني تركزا لملكية أغلبية الأسهم بيد مساهمين مغاربة مع إلزامية توطين عمليات المعالجة والتخزين، مما يجسد توجها إستراتيجيا يروم تحصين السيادة الرقمية ومنع الاختراقات الخارجية، بالتوازي مع هيكلة منظومة سحابية وطنية تسهم في تحفيز الاستثمار وتطوير الاقتصاد الرقمي المحلي.

الفقرة الثانية: إشكالية التوافق مع الالتزامات الدولية في إطار منظمة التجارة العالمية

على الرغم من مشروعية الأهداف الأمنية والسيادية التي يتغياها المرسوم رقم 2.24.921، فإن التنزيل الصارم لمتطلبات الملكية المحلية والإيواء الجغرافي يفرز إشكالات قانونية مركبة ترتبط بمدى التزام المملكة المغربية بمقتضيات القانون الدولي الاقتصادي، وتحديداً ضمن إطار منظمة التجارة العالمية (WTO). وتتجلى هذه الإشكالية بوضوح عند استحضار أحكام الاتفاقية العامة للتجارة في الخدمات (GATS)، حيث يصطدم اشتراط حيازة المستثمرين المغاربة لأغلبية أسهم شركات المستوى الثاني، واشتراط تأسيس المقر الاجتماعي محلياً لشركات المستوى الأول، مع مبدأ 'النفاذ إلى الأسواق (Market Access) ' المنصوص عليه في المادة السادسة عشرة، والذي يحظر فرض قيود كيفية أو كمية على مشاركة رأس المال الأجنبي. وعلاوة على ذلك، يتقاطع هذا التوجه التنظيمي مع مبدأ 'المعاملة الوطنية (National Treatment)' المؤطر بالمادة السابعة عشرة من ذات الاتفاقية، والذي يفرض على الدول الأعضاء منح الخدمات ومقدميها الأجانب معاملة لا تقل تفضيلاً عن تلك الممنوحة للفاعلين المحليين، مما يجعل من الشروط التفضيلية المستندة إلى الجنسية أو منشأ رأس المال عائقاً أمام التنافسية العادلة.

وإذا كان الفقه القانوني يقر بإمكانية تحصن الدول بالاستثناءات الأمنية لتبرير هذه القيود، استناداً إلى المادة الرابعة عشرة (الاستثناءات العامة) والمادة الرابعة عشرة مكرر (الاستثناءات الأمنية Article XIV bis) من اتفاقية(GATS) ، والتي تجيز اتخاذ تدابير ضرورية لحماية المصالح الأمنية الأساسية، فإن اجتهادات جهاز تسوية المنازعات التابع لمنظمة التجارة العالمية تخضع هذا الدفع لاختبار دقيق يُعرف بـ"اختبار التناسب" (Proportionality Test) ويقتضي هذا الاختبار إثبات أن التدابير المقيدة للتجارة تمثل الوسيلة الأقل تقييداً (Least Trade-Restrictive) لتحقيق الهدف الأمني المنشود. وفي هذا السياق، يبدو التطبيق الشامل لإلزامية التوطين واشتراطات الملكية على كافة البنيات التحتية الحيوية، دون إرساء معايير

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

دقيقة تميز بين مستويات حساسية المعطيات، تجاوزاً لحدود الضرورة الأمنية، وتوسيعاً قد يُكيّف ضمن خانة القيود الاستثمارية المحظورة بموجب اتفاقية التدابير الاستثمارية المتصلة بالتجارة (TRIMs)[13]

تتفاقم التعقيدات الإشكالية للإطار التنظيمي في ظل غياب محددات معيارية دقيقة تضبط آليات الإعفاء من متطلبات الملكية، مما يوسع نطاق السلطة التقديرية للإدارة ويُنذر بممارسات تفتقر للشفافية، وهو وضع يزداد حدة مع انتفاء التمييز المنهجي بين مستويات حساسية المعطيات، حيث يؤدي فرض اشتراطات صارمة وموحدة على كافة البنيات التحتية الحيوية إلى إثقال كاهل القطاعات بأعباء تنظيمية غير متناسبة تتجاوز الأهداف الأمنية المبررة وتكبح قدرتها التنافسية في استغلال الخدمات السحابية العالمية؛ ولئن كانت المقاربة المغربية تتسم بانفتاح محمود على آليات التعاون الدولي والإقليمي، المتجسد في المصادقة على البروتوكول الإضافي الثاني لاتفاقية بودابست والانخراط في مجلس وزراء الأمن السيبراني العرب، فإن هذا التوجه الخارجي يستوجب بالضرورة إرساء مرونة تشريعية داخلية موازية تكفل استقطاب الاستثمارات الأجنبية، وتضمن تحقيق التوازن الإستراتيجي الدقيق بين متطلبات السيادة الرقمية الصارمة والالتزامات التجارية الدولية، استنادا إلى النماذج المقارنة المرتكزة على مبدأي التصنيف الوظيفي للمعطيات والتناسب التدبيري.

المبحث الثاني: آليات مأسسة حكامة الخدمات السحابية، استلهام التجارب المقارنة وبناء النموذج الوطني

يستوجب القصور التشريعي في تأطير الخدمات السحابية استلهام النماذج الأوروبية (كتوجيه NIS2 وقانون التضامن السيبراني) لمأسسة حكامة وطنية مرنة تصنف البيانات حسب درجة حساسيتها، ويستهدف هذا النموذج إرساء ضوابط للإسناد الخارجي وتطوير آليات التعاون الدولي، بما يكفل التوازن الاستراتيجي بين مقتضيات السيادة الرقمية والانفتاح الاقتصادي التقني.

---

[13] اتفاقية التدابير الاستثمارية المتصلة بالتجارة (TRIMs) هي إطار تشريعي دولي مُقيد للسياسات الاستثمارية الوطنية ذات الأثر المشوه لتجارة السلع، وتحظر الإجراءات المتعارضة مع مبادئ الاتفاقية العامة للتعريفات والتجارة (GATT) ، ولاسيما مبدأي المعاملة الوطنية وإلغاء القيود الكمية. وتُقنن الاتفاقية، بموجب قائمتها التمثيلية، المنع القطعي للممارسات الحمائية كاشتراطات المحتوى المحلي، والتوازن التجاري، والقيود المفروضة على النقد الأجنبي، مع إلزام الدول الأطراف بآليات الإخطار المؤسساتي والتفكيك التدريجي لتلك التدابير وفق مدد انتقالية تراعي التفاوت الاقتصادي والتنموي، تأسيساً لبيئة استثمارية عالمية تنافسية وحرة.

World Trade Organization. (1994). Agreement on Trade-Related Investment Measures. Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1868 U.N.T.S. 186

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

المطلب الأول: تقاطع التشريع المغربي مع المعايير الأوروبية: قراءة في توجيه NIS2 وقانون التضامن السيبراني

يتناول هذا المطلب تقاطع التشريع المغربي مع المعايير الأوروبية من خلال قراءة التوجيه NIS2 كمرجع لسياسات الإيواء والتأهيل، ثم ننتقل إلى استعراض إسهام قانون التضامن السيبراني الأوروبي في بناء قدرات الصمود والاستجابة للهجمات السيبرانية واسعة النطاق، مع رصد الدروس المستفادة من هذه التجارب التي يمكن توظيفها لتطوير الإطار الوطني للخدمات السحابية.

الفقرة الأولى: تقييم التوجيه NIS2 كمرجع لسياسات الإيواء والتأهيل

تكتسب التجربة الأوروبية في تنظيم الأمن السيبراني أهمية خاصة كمرجع للمقارنة، ذلك أن الاتحاد الأوروبي هو من أكثر المناطق تقدما في مجال سن التشريعات الرامية إلى حماية الفضاء السيبراني، وقد توجت هذه الجهود بإصدار التوجيه الثاني لأمن الشبكات والمعلومات NIS2 في ديسمبر 2022 ليحل محل التوجيه الأول الصادر عام 2016، حيث وسع نطاق الالتزامات الأمنية ليشمل قطاعات جديدة وشركات أصغر حجما، وفرض متطلبات أكثر صرامة للإبلاغ عن الحوادث، ورفع مستوى العقوبات المالية لتصل إلى 10 ملايين يورو أو 2 % من المبيعات العالمية للشركة المخالف،[14] وتتمثل أهم نقاط قوة هذا التوجيه في أنه يعتمد مقاربة قائمة على المخاطر، إذ يلزم الدول الأعضاء ومقدمي الخدمات الرقمية بتقييم المخاطر التي تهدد أمن شبكاتهم وأنظمة المعلومات، واتخاذ التدابير التقنية والتنظيمية المناسبة لإدارتها، مع ترك هامش من المرونة للدول الأعضاء في تحديد الكيفيات التي سيتم بها تطبيق هذه المتطلبات، مما يسمح بالتكيف مع الظروف الوطنية الخاصة.

ويمكن للمغرب أن يستلهم من التوجيه NIS2 العديد من العناصر في تطوير إطاره القانوني للخدمات السحابية، وعلى رأسها اعتماد مقاربة تصنيفية مرنة في تحديد مستوى التدخل التنظيمي، بحيث يتم تمييز الخدمات السحابية ومقدميها حسب درجة الأهمية والمخاطر المرتبطة بهم، فالتوجيه الأوروبي لا يطبق ذات المتطلبات على كل القطاعات، بل يصنفها في فئتين: القطاعات الأساسية والقطاعات الهامة، مع تخصيص متطلبات أمنية وإبلاغية أكثر دقيقة وصارمة للفئة الأولى[15] وهذا التصنيف يسمح بتحقيق التناسب بين

[14] European Parliament & Council, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Official Journal of the European Union, L 333/80, 2022,
[15] European Parliament & Council, Directive (EU) 2022/2555 (NIS2), Annexes I & II

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

مستوى الحماية المطلوب ودرجة الأهمية الإستراتيجية للقطاع المعني، ويجنب فرض أعباء تنظيمية غير متناسبة على القطاعات الأقل حساسية، ويمكن تطبيق هذا المنطق في السياق المغربي بتصنيف المعطيات والخدمات السحابية إلى مستويات مختلفة من الحساسية، وتخصيص متطلبات إيواء وتأهيل تتناسب مع كل مستوى، بدلا من فرض ذات الشروط الصارمة على جميع البنيات التحتية الحيوية دون تمييز.

كما أن التوجيه NIS2 أعطى أهمية خاصة لآليات الإبلاغ عن الحوادث والتعاون بين الدول الأعضاء، حيث يُلزم مقدمي الخدمات بالإبلاغ عن الحوادث الجسيمة التي تؤثر على تقديم خدماتهم خلال فترة زمنية قصيرة (24 ساعة للإبلاغ المبكر، و72 ساعة للإبلاغ المفصل)، وينشئ شبكة من فرق الاستجابة للحوادث تتعاون فيما بينها لتبادل المعلومات والتنسيق في التصدي للتهديدات السيبرانية[16] وهو ما يعزز من التعاون الإقليمي والدولي في مجال الأمن السيبراني، ويوفر آلية لتبادل المعلومات حول التهديدات الناشئة والحوادث السيبرانية، ويساهم في رفع مستوى الجاهزية والاستجابة على المستوى الوطني، ويمكن للمغرب أن يستفيد من هذا النموذج في تطوير آليات التعاون الوطني والدولي المنصوص عليها في المادة 47 من القانون 05.20، من خلال إنشاء منصة وطنية لتبادل المعلومات السيبرانية مع الدول الشريكة، وتطوير بروتوكولات التعاون مع الدول الصديقة، خاصة في منطقة الشرق الأوسط وإفريقيا، بما يعزز الموقف السيبراني للمنطقة ككل.

الفقرة الثانية: إسهام قانون التضامن السيبراني في بناء قدرات الصمود والاستجابة

يعتبر قانون التضامن السيبراني الأوروبي (Regulation (EU) 2024/2847) الصادر في ديسمبر 2024 إضافة نوعية للإطار الأوروبي للأمن السيبراني، حيث عزز القدرات المشتركة للكشف عن التهديدات والاستجابة للحوادث واسعة النطاق، من خلال إنشاء شبكة من مراكز العمليات الأمنية تعمل على مستوى الاتحاد الأوروبي،[17] وارتكز هذا القانون على ثلاث ركائز أساسية: الأولى نظام الإنذار الأوروبي في مجال الأمن السيبراني، الذي يهدف إلى تحسين الوعي الظرفي والكشف المبكر عن التهديدات عبر المراكز السيبرانية الوطنية والعابرة للحدود، والثانية آلية الطوارئ السيبرانية التي تشمل تدابير الاستعداد واحتياطي الأمن السيبراني للاتحاد الأوروبي والمساعدة المتبادلة بين الدول الأعضاء في حال وقوع حوادث واسعة النطاق، والثالثة آلية مراجعة الحوادث السيبرانية الأوروبية لإجراء مراجعات منظمة بعد الحوادث الكبرى

[16] European Parliament & Council, Directive (EU) 2022/2555 (NIS2), art. 9-12)
[17] European Parliament & Council, Regulation (EU) 2024/2847, art. 7

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

واستخلاص الدروس المستفادة،[18] وتكمن أهمية هذا القانون في كونه ينتقل من المقاربة الوقائية البحتة إلى مقاربة شاملة تجمع بين الوقاية والاستعداد والاستجابة والتعافي، مما يعزز مناعة البنى التحتية الحيوية الأوروبية في مواجهة التهديدات السيبرانية المتطورة، ولدى يتيح استلهام مقتضيات قانون التضامن السيبراني الأوروبي إمكانية هيكلة منظومة وطنية متكاملة لإدارة الأزمات السيبرانية في المغرب، ارتكازا على توسيع صلاحيات اللجنة الوطنية المنصوص عليها في المادة 36 من القانون 05.20، وتأسيس شبكة مترابطة من مراكز العمليات الأمنية المخصصة للرصد والإنذار المبكر، إلى جانب بلورة آلية طوارئ استباقية تضمن تعبئة الاحتياطات التقنية والخبرات البشرية لدعم البنيات التحتية الحيوية وقت الأزمات؛ غير أن نجاعة استنبات هذه النماذج المقارنة القائمة على تقييم المخاطر تظل مشروطة بتكييفها العقلاني مع البنية التشريعية والبيئة الرقمية المغربية، وفق مقاربة تضمن تحقيق توازن استراتيجي دقيق بين فرض ضمانات السيادة الرقمية ومقتضيات الانفتاح الاقتصادي، وتؤمن متطلبات الحماية الأمنية القصوى دون إعاقة دينامية الاستثمار والابتكار التقني.

المطلب الثاني: هندسة إطار تصنيفي مرن يوازن بين الأمن السيبراني والانفتاح التقني

في هذا المطلب الأخير سنقف عند إمكانية وضع إطار تصنيفي مرن يوازن بين الأمن السيبراني والانفتاح التقني، ونقترح ضوابط للإسناد الخارجي وفق مستويات حساسية المعطيات، ثم نعرض آليات الرقابة والتعاون الدولي في النموذج الوطني المقترح، والتي تضمن نجاعة نظام الحكامة وتكفل الالتزام بالضوابط والمعايير المحددة مع الحفاظ على تنافسية القطاع الرقمي المغربي.

الفقرة الأولى: ضوابط الإسناد الخارجي وفق مستويات حساسية المعطيات

إن بناء النموذج الوطني لحكامة الخدمات السحابية يتطلب التوفيق بين متطلبات السيادة الرقمية التي نص عليها القانون 05.20، وبين ضرورة الانفتاح على الخدمات السحابية العالمية والاستفادة من مزاياها التقنية والاقتصادية، وهو ما يستدعي تجاوز المقاربة الثنائية الصارمة (الإيواء الوطني الحصري في مقابل الإسناد الخارجي المطلق)، واعتماد مقاربة تصنيفية مرنة تقوم على تمييز المعطيات والخدمات حسب مستوى حساسيتها، وتخصيص متطلبات إيواء وإسناد تتناسب مع كل مستوى، ويمكن اقتراح تصنيف الخدمات السحابية إلى أربعة مستويات رئيسية: المستوى الأول للبيانات غير الحساسة والعامة التي لا

[18] European Parliament & Council, Regulation (EU) 2024/2847, art. 12-19

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

يشترط الإيواء الوطني لها، والمستوى الثاني للبيانات الإدارية غير الحساسة حيث يُفضل الإيواء الوطني ويُجاز الإسناد الخارجي بضوابط، والمستوى الثالث للبيانات الشخصية والمالية التي يتطلب الإيواء الوطني مع إمكانية الاستثناء بترخيص من السلطة الوطنية، والمستوى الرابع للبيانات السيادية والأمنية والدفاعية التي تستوجب الإيواء الوطني الحصري مع حظر الإسناد الخارجي. ويتمثل الابتكار في هذا النموذج في السماح بالإسناد الخارجي للمستويين الثاني والثالث مع وضع ضوابط وشروط تعاقدية وتقنية صارمة تضمن مستوى الحماية المطلوب، بدلا من الحظر المطلق الذي تفرضه المادة 11 على كافة المعطيات الحساسة دون تمييز[19].

الفقرة الثانية: آليات الرقابة والتعاون الدولي في النموذج الوطني المقترح

لا يمكن لنظام الحكامة المقترح أن يحقق أهدافه دون آليات رقابية فعالة تضمن الالتزام بالضوابط والمعايير المحددة، وتكفل اكتشاف المخالفات ومعالجتها في وقت مبكر قبل أن تتحول إلى أزمات سيبرانية خطيرة، وفي هذا السياق، تقترح الدراسة اعتماد مقاربة رقابية متعددة المستويات منها أولاً الافتحاص الدوري لمقدمي الخدمات السحابية والمؤسسات المستخدمة لها، وذلك إما من قبل السلطة الوطنية مباشرة، أو من قبل متعهدي افتحاص مؤهلين من قبلها، وفقاً للمادة 20 من القانون 05.20 التي تتيح للسلطة الوطنية إجراء افتحاصات لنظم المعلومات الحساسة للبنيات التحتية الحيوية[20] ويمكن تطبيق ذات الآلية على مقدمي الخدمات السحابية، خاصة أولئك الذين يقدمون خدمات للمستويين الثالث والرابع من التصنيف، وذلك للتأكد من التزامهم بالضوابط الأمنية والتعاقدية. ويُقترح أن تكون هذه الافتحاصات دورية (مرة على الأقل سنوياً) وأن تتضمن جوانب تقنية وتنظيمية وقانونية، مع إلزام المزود بإصلاح الثغرات التي يتم رصدها في آجال محددة، وفي حال عدم الامتثال، يُمكن للسلطة الوطنية سحب الترخيص أو التأهيل.

كما نقترح اعتماد آلية للإبلاغ الإلزامي عن الحوادث الجسيمة، تستلهم من التوجيه NIS2 الذي يلزم مقدمي الخدمات بالإبلاغ عن الحوادث خلال 24 ساعة[21] ويمكن للمغرب أن يستفيد من هذه التجربة في تطوير أحكام المادة 8 من القانون 05.20 التي تلزم الهيئات بالإبلاغ الفوري عن أي حادث يؤثر على

---

[19] المملكة المغربية، القانون رقم 05.20، المادتان 10 و12

[20] المملكة المغربية، القانون رقم 05.20، المادة 20.

[21] European Parliament & Council, Directive (EU) 2022/2555 (NIS2), art. 20–21)

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

أمن نظم المعلومات، وذلك بتحديد آجال زمنية واضحة (مثلا: الإبلاغ الأولي خلال 24 ساعة، والتقرير المفصل خلال 72 ساعة)، وتحديد المعلومات الواجب تضمينها في الإبلاغ (طبيعة الحادث، الأنظمة المتأثرة، المعطيات المتأثرة، الإجراءات المتخذة)، وإنشاء منصة إلكترونية موحدة لتلقي الإبلاغات وتتبعها، كما يُقترح إنشاء آلية وطنية لمراجعة الحوادث السيبرانية الكبرى، على غرار ما نص عليه قانون التضامن السيبراني الأوروبي.[22]

وتفعيلا لمقتضيات المادة 47 من القانون 05.20، يستوجب الارتقاء بآليات التعاون الدولي تأسيس منصة وطنية لتبادل المعلومات السيبرانية، وإرساء إطار متين للتعاون القضائي لتيسير الولوج العابر للحدود إلى المعطيات استناداً للبروتوكول الإضافي الثاني لاتفاقية بودابست؛ وذلك بالموازاة مع ضرورة توحيد المعايير الأمنية السحابية إقليمياً لتسهيل تدفق البيانات، وإبرام اتفاقيات دولية مع الدول المستضيفة لتأطير شروط الإسناد الخارجي وتنسيق جهود الاستجابة للأزمات ضمن بيئة قانونية مستقرة.

خاتمة

يتجسد الإطار القانوني والتنظيمي للخدمات السحابية في المغرب، أساسا في أحكام المادة 11 من القانون رقم 05.20 والتوجه التقييدي للمرسوم رقم 2.24.921، ويفرز تعارضا بنيويا عميقا بين متطلبات السيادة الرقمية المطلقة القائمة على حتمية التوطين الجغرافي للمعطيات واشتراطات الملكية المحلية، وبين الطبيعة التشغيلية اللامركزية والعابرة للحدود للحوسبة السحابية؛ وهو ما ينتج عنه تداعيات سلبية تحد من التنافسية الاقتصادية الوطنية وتعرقل استقطاب الاستثمارات التكنولوجية الأجنبية، فضلا عن إثارته لإشكالات قانونية جوهرية تتعلق بمدى توافق هذا التشدد التشريعي مع التزامات المملكة ضمن منظمة التجارة العالمية، ولا سيما اتفاقية(GATS) ، حيث إن التطبيق الموحد لهذه القيود الصارمة على كافة البنيات التحتية الحيوية، في غياب أي تصنيف معياري يميز بين مستويات حساسية المعطيات، يشكل حواجز حمائية غير مبررة تعيق الانفتاح التجاري وتكبح مسار التحول الرقمي.

واستيعابا لهذه التحديات، تبرز الضرورة الملحة لتبني المشرع المغربي تحولا منهجيا يستلهم المكتسبات المعيارية للتجارب المقارنة، وتحديدا التوجيه الأوروبي (NIS2) وقانون التضامن السيبراني،

[22] European Parliament & Council, Regulation (EU) 2024/2847, art. 19

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

قصد تجاوز المقاربة الثنائية الجامدة وتأسيس هندسة قانونية مرنة ترتكز على تصنيف المعطيات والخدمات وفق درجات التفاوت في الحساسية والمخاطر، بما يتيح إقرار متطلبات أمنية متناسبة تبيح الإسناد الخارجي المقنن للبيانات متوسطة الحساسية ضمن ضوابط تعاقدية وتقنية دقيقة؛ وذلك بالتوازي مع مأسسة آليات الرقابة الاستباقية عبر الافتحاص الدوري والإبلاغ الإلزامي عن الحوادث السيبرانية، وتطوير أطر التعاون الدولي والقضائي، لتشكيل منظومة متكاملة تضمن التوفيق الإستراتيجي بين تحصين الأمن القومي السيادي ومتطلبات الانفتاح الاقتصادي والتكنولوجي.

المصادر والمراجع:

العربية:

- الفضلي، فاطمة الزهراء، الإطار القانوني والتنظيمي للحوسبة السحابية بالمغرب، مجلة منازعات الأعمال، العدد 91، الصفحات 41-62، 2024.
- المملكة المغربية، القانون رقم 05.20 المتعلق بالأمن السيبراني (الجريدة الرسمية عدد 6904)، الرباط، 2020.
- المملكة المغربية، القانون رقم 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي (الجريدة الرسمية عدد 5714)، الرباط، 2009.
- المملكة المغربية، المرسوم رقم 2.24.921 المنظم لاستخدام مقدمي الخدمات السحابية من قبل الهيئات والبنيات التحتية الحيوية التي تسير نظم المعلومات الحساسة أو المعطيات الحساسة (الجريدة الرسمية)، الرباط، 2024.

Anglais:

- DGSSI, *Présentation de la loi n° 05.20 relative à la cybersécurité,* Rabat, 2020.
- DGSSI, *Stratégie nationale de cybersécurité 2030,* Rabat, 2024.
- European Parliament & Council, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive),* Brussels, 2022.
- European Parliament & Council, *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR),* Brussels, 2016.
- European Parliament & Council, *Regulation (EU) 2024/2847 establishing the European Cyber Solidarity Act*, Brussels, 2024.
- Floridi, L., *The Fourth Revolution: How the infosphere is reshaping human reality,* Oxford University Press, 2014.

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013

– World Trade Organization. *General Agreement on Trade in Services. Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167.* Marrakesh 1994
– World Trade Organization. *Agreement on Trade-Related Investment Measures. Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1868 U.N.T.S. 186* Marrakesh 199

ISSN: 3119-6837 - E-ISSN: 3119-6845
DÉPÔT LÉGAL: 2026PE0013