دور الرقمنة في تحقيق الأمن القانوني
الآليات والضمانات والتحديات
دراسة في ضوء التشريع المغربي والمعايير المقارنة

د. احمد شرقي
دكتور في القانون الخاص
المملكة المغربية

الملخص:

تبحث هذه الدراسة في أثر الرقمنة في بناء الأمن القانوني، انطلاقا من أن الانتقال إلى البيئة الرقمية لا يكتمل بمجرد استبدال الحامل الورقي بملف إلكتروني، وإنما يستلزم إعادة تصميم دورة القاعدة والقرار والمعاملة بما يكفل الوضوح، وقابلية التوقع، والمساواة في الولوج، وسلامة البيانات، وإمكان التتبع والمراجعة. واعتمدت الدراسة منهجا تحليليا ووظيفيا ومقارنا، يقوم على قراءة النصوص الدستورية والتشريعية المغربية، وربطها بالأدبيات القانونية والإدارية المتخصصة وبالمعايير الأممية والأوروبية. وتبين أن التشريع المغربي أرسى مرتكزات مهمة في مجالات التبادل الإلكتروني، وخدمات الثقة، وحماية المعطيات، والأمن السيبراني، والحق في المعلومات، وتبسيط المساطر؛ غير أن الأثر العملي لهذه المرتكزات يظل رهينا بتجاوز التجزؤ المؤسسي، وتعميم التشغيل البيني، وضبط الزمن القانوني للوثائق والقرارات الإلكترونية، وتنظيم آثار الأعطال، وإخضاع الأنظمة الخوارزمية والسجلات الرقمية للتدقيق. وتقترح الدراسة تصورا للأمن القانوني الرقمي يجمع بين الشرعية، والحجية، والشفافية، والاستمرارية، والحماية السيبرانية، والإدماج، مع مؤشر عملي وخارطة تنفيذ قابلة للقياس.

الكلمات المفتاحية: الرقمنة؛ الأمن القانوني؛ الإدارة الرقمية؛ التوقيع الإلكتروني؛ حماية المعطيات؛ الأمن السيبراني؛ تبسيط المساطر؛ التشغيل البيني.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

مقدمة

غدت الرقمنة جزءا من البنية التنظيمية التي تعمل من خلالها الدولة المعاصرة؛ فهي لا توفر قناة جديدة للخدمة فحسب، بل تعيد تشكيل إنتاج القرار الإداري، وتداول النص القانوني، وإثبات التصرفات، وترتيب الآثار على أفعال تتم داخل نظم مترابطة. وقد وصفت الأدبيات هذا التطور بانتقال الحكومة الرقمية من مجرد الحضور الإلكتروني إلى التحول ثم إلى التكيف مع السياقات القانونية والمؤسساتية1. لذلك لا يندرج الموضوع في المجال التقني وحده، بل يتصل مباشرة بشروط دولة القانون: فعندما يصبح الترخيص أو الأداء أو التبليغ أو التعاقد أو حفظ الملف عملا رقميا، تنتقل ضمانات الورقة والختم والحضور المادي إلى الهوية الرقمية، والختم الزمني، وسلامة قاعدة البيانات، وسجل الأحداث، وإمكان استرجاع الوثيقة والتحقق من مصدرها.

يقر الدستور المغربي إلزامية نشر القواعد القانونية وعدم رجعيتها، وهو ما يجعل العلم بالنص وضبط نفاذه الزمني من مقومات النظام القانوني. وفي المجال الرقمي، تتجسد هذه الضمانة في تحديد النسخة الرسمية، وإثبات تاريخ إتاحتها، وحفظ التعديلات المتعاقبة، وتمكين المخاطب من الوصول إلى النص الذي كان نافذا وقت الواقعة. ومن ثم، قد تكون القاعدة سليمة من حيث جهة إصدارها، لكنها تظل ضعيفة من زاوية الأمن القانوني إذا تعذر العثور عليها، أو تعددت نسخها، أو تغير محتواها من دون سجل زمني موثوق.2

يرتبط الأمن القانوني، في التصور الفقهي والقضائي، بوضوح القاعدة وإتاحتها واستقرار المراكز وإمكان توقع آثار القانون؛ وهو لا يرادف الجمود، بل يضبط كيفية التغيير وحدوده. فالتعديل المشروع ينبغي أن يصدر في مسار معلوم، وأن يصاغ بعبارات مفهومة، وأن يقترن عند الحاجة بأحكام انتقالية تحمي التوقعات المشروعة. وتؤكد نظرية حكم القانون أن عمومية القاعدة ووضوحها واستقرارها وإمكان الامتثال لها شروط تمنع السلطة من مفاجأة المخاطبين بها3. وتكتسب هذه الفكرة حساسية مضاعفة رقميا، لأن تحديثا برمجيا واحدا قد يغير شروط الإجراء أو طريقة حساب الأجل بالنسبة إلى عدد كبير من المرتفقين في اللحظة نفسها.4

---

1 Tomasz Janowski, "Digital Government Evolution: From Transformation to Contextualization", Government Information Quarterly, vol. 32, no. 3, 2015, pp. 221-236.

2 دستور المملكة المغربية لسنة 2011، الظهير الشريف رقم 1.11.91، الجريدة الرسمية عدد 5964 مكرر، 30 يوليوز 2011، ص. 1905، الفصل 6.

3 Joseph Raz, "The Rule of Law and Its Virtue", in The Authority of Law, Oxford University Press, 1979, pp. 210-229; Lon L. Fuller, The Morality of Law, rev. ed., Yale University Press, 1969, pp. 33-94.

4 Conseil d'État, Sécurité juridique et complexité du droit, Rapport public 2006, La Documentation française, Paris, 2006, p. 229.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

يكشف التحليل المقارن عن بعدين تقليديين للأمن القانوني: بعد موضوعي يتعلق بجودة القاعدة واتساقها، وبعد زمني يحمي استقرار الأوضاع ويجعل الانتقال من حكم إلى آخر قابلاً للتوقع1. وتضيف البيئة الرقمية بعداً معلوماتياً لا يقل أهمية؛ فالقرار لا يكتسب درجة كافية من اليقين إلا إذا أمكن التحقق من سلامة البيانات التي استند إليها، وهوية الجهة التي أصدرته، وثبات محتواه بعد الإصدار، والمسار الذي قطعته المعالجة. وبهذا المعنى يصبح الأمن القانوني نتيجة مشتركة للصياغة القانونية والهندسة المعلوماتية، لا خاصية للنص وحده.2

ويمنح الحق الدستوري في الحصول على المعلومات الرقمنة وظيفة حقوقية تتجاوز تحسين الخدمة. فإتاحة النصوص والقرارات والدلائل بصيغ قابلة للبحث وإعادة الاستخدام تحد من تفاوت المعرفة بين الإدارة والمرتفق، وتضيق مجال التطبيق الانتقائي، وتمكن الأفراد من توقع القرار وإعداد ملفاتهم والطعن داخل الأجل. غير أن النشر لا يؤدي هذه الوظيفة إذا اقتصر على صور ممسوحة ضوئيا، أو مواد غير محينة، أو منصات متفرقة لا تبين مصدر الوثيقة ونسختها النافذة.3

وتتصل الرقمنة كذلك بالمبادئ الدستورية المنظمة للمرافق العمومية، ولا سيما المساواة في الولوج، والتغطية العادلة للتراب، والاستمرارية، والجودة، والشفافية، والمحاسبة. لذلك لا ينبغي أن تتحول القناة الرقمية إلى شرط إقصائي يضر بمن يفتقر إلى اتصال مستقر أو مهارة رقمية أو وسيلة أداء إلكترونية، كما لا يجوز أن يؤدي عطل المنصة إلى فوات أجل أو سقوط حق. فالأمن القانوني الرقمي يجمع بين كفاءة الخدمة واستمرار المركز القانوني للمرتفق متى تعذر استعمالها لأسباب لا يد له فيها.4

أظهرت مراجعة منظمة التعاون والتنمية الاقتصادية للحكومة الرقمية في المغرب أن التحول الفعلي يحتاج إلى التشغيل البيني، والهوية الإلكترونية، والخدمات المشتركة، وسجلات مرجعية موثوقة، وشبكات آمنة لتبادل البيانات، إلى جانب القياس والكفاءات الرقمية. ويتقاطع هذا التشخيص مع التوجهات المعلنة في استراتيجية «المغرب الرقمي 2030»، التي تجعل تحسين الخدمات العمومية الرقمية وتنمية الاقتصاد الرقمي محورين متكاملين5. ويترتب على ذلك أن المنصة المنعزلة قد تسرع إجراءً بعينه، لكنها لا تحقق أمنا قانونيا شاملا ما دام المرتفق يعيد تقديم الوثائق، وتتعارض البيانات بين الجهات، وتضيع المسؤولية عند انتقال الملف من نظام إلى آخر.6

1 Bertrand Mathieu, "France / Constitution et sécurité juridique", Annuaire international de justice constitutionnelle, vol. 15, 2000, pp. 155-192; Dominique J. M. Soûlas de Russel et ,"Philippe Raimbault, "Nature et racines du principe de sécurité juridique : une mise au point .Revue internationale de droit comparé, vol. 55, no. 1, 2003, pp. 85-103

2.Conseil d'État, op. cit., pp. 281-283

3 دستور المملكة المغربية لسنة 2011، مرجع سابق، ص. 1909، الفصل 27.

4 دستور المملكة المغربية لسنة 2011، مرجع سابق، ص. 1935، الفصول 154 إلى 156.

5 وزارة الانتقال الرقمي وإصلاح الإدارة، استراتيجية المغرب الرقمي 2030، الرباط، 2024.

6 - OECD, Digital Government Review of Morocco: Laying the Foundations for the Digital .Transformation of the Public Sector in Morocco, OECD Publishing, Paris, 2018, pp. 22-25

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

تعتمد الدراسة مفهوما وظيفيا للرقمنة يميز بين تحويل الوثيقة إلى صيغة رقمية، ورقمنة المسار بكامل مراحله، والتحول المؤسسي الذي يعيد تصميم الخدمة والاختصاصات. كما تتبنى مفهوما مركبا للأمن القانوني يشمل الوضوح، والإتاحة، والاستقرار، وقابلية التوقع، وسلامة الإثبات، والمساواة الإجرائية. وانطلاقاً من هذا التأطير تطرح الإشكالية الآتية: إلى أي مدى تسهم الرقمنة في تعزيز الأمن القانوني، وما الضمانات القانونية والمؤسساتية والتقنية الكفيلة بمنع تحولها إلى مصدر جديد للغموض وعدم المساواة والمخاطر؟

للإجابة عن هذه الإشكالية، تم الجمع بين المنهج التحليلي في تفكيك النصوص المؤطرة للمعاملات والخدمات الرقمية، والمنهج الوظيفي في قياس أثر الأدوات الرقمية في مكونات الأمن القانوني، والمنهج المقارن باستحضار مبادئ الأونسيترال ومنظمة التعاون والتنمية الاقتصادية والتنظيم الأوروبي لخدمات الثقة والذكاء الاصطناعي. ويعالج المبحث الأول الأساس المفاهيمي والقانوني للعلاقة بين الرقمنة والأمن القانوني، بينما يخصص المبحث الثاني لآليات الإسهام العملي، والتحديات، والضمانات المقترحة.

المبحث الأول: التأصيل المفاهيمي والقانوني لدور الرقمنة في تحقيق الأمن القانوني

يقتضي تقويم أثر الرقمنة في الأمن القانوني ضبط المفهومين وتجنب الخلط بين استعمال الحاسوب والتحول المؤسسي، أو بين استقرار القانون ورفض إصلاحه. كما يتطلب بيان الكيفية التي تنتقل بها الحجية والثقة والحماية من المحرر الورقي إلى منظومة رقمية تتوزع فيها المسؤولية بين النص، والجهة الإدارية، ومقدم خدمة الثقة، ومصمم النظام، وحافظ البيانات.

المطلب الأول: الإطار المفاهيمي للعلاقة بين الرقمنة والأمن القانوني

يقتضي بحث العلاقة بين الرقمنة والأمن القانوني الوقوف أولا على الأسس والمفاهيم التي تؤطر هذه العلاقة، باعتبار أن التحول الرقمي لم يعد مجرد وسيلة تقنية لتحديث أساليب العمل، وإنما أصبح عنصرا مؤثرا في مختلف مجالات الحياة القانونية والإدارية والقضائية. فقد أفرزت الرقمنة أنماطا جديدة في إنتاج المعلومة القانونية وتداولها وحفظها، كما ساهمت في تسريع الإجراءات وتيسير الولوج إلى القاعدة القانونية وتعزيز الشفافية، وهو ما ينعكس بصورة مباشرة على متطلبات الأمن القانوني.

وفي المقابل، تطرح البيئة الرقمية جملة من الإشكالات المرتبطة بمدى وضوح القواعد القانونية واستقرارها، وحماية المعطيات والحقوق، وضمان موثوقية المعاملات والوثائق الإلكترونية، الأمر الذي يجعل تحقيق الأمن القانوني في ظل التحول الرقمي رهينا بوجود إطار قانوني واضح ومستقر وقادر على مواكبة التطورات التقنية.

وعليه، يقتضي تناول هذا المطلب تحديد المقصود بكل من الرقمنة وتمييزها عن المفاهيم المرتبطة بها ، قبل الخوض في تحديد مفهوم الأمن القانوني وتمييزه عن المفاهيم المشابهة له.

الفقرة الأولى: مفهوم الرقمنة وتمييزها عن المفاهيم المرتبطة بها

تعني الرقمنة في مستواها التقني الضيق تحويل معلومة أو وثيقة من حامل مادي إلى تمثيل رقمي قابل للتخزين والمعالجة والنقل. وهذا المستوى مفيد للأرشفة والبحث، لكنه لا يغير بالضرورة منطق العمل؛ فقد تمسح الاستمارة ضوئياً فيما يستمر اشتراط

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

الحضور والتوقيع اليدوي والتنقل بين المصالح. أما رقمنة المسار فتعيد تنظيم الإيداع والتحقق والأداء والتبليغ والتتبع داخل نظام مترابط، بينما يعيد التحول الرقمي المؤسسي تصميم الخدمة على أساس حاجات المستخدم والبيانات المشتركة، ويغير توزيع الاختصاصات وآليات الرقابة والقياس1.

يقوم الإطار المرجعي لمنظمة التعاون والتنمية الاقتصادية على ستة أبعاد مترابطة: التصميم الرقمي منذ البداية، والقطاع العام القائم على البيانات، والحكومة كمنصة، والانفتاح الافتراضي، والتوجيه باحتياجات المستخدم، والاستباقية. وتؤكد دراسات الحكومة الرقمية أن القيمة لا تتولد من إدخال التقنية وحدها، بل من قدرتها على خدمة القيم العامة والمساءلة2. ومن ثم، ينبغي أن يسجل النظام، منذ تصميمه، تاريخ الإيداع، وطريقة حساب الأجل، والنسخة المقدمة، والإشعار المرسل، ومسار التظلم؛ فلا تترك هذه الضمانات لإجراءات يدوية لاحقة.3

وتشدد توصية منظمة التعاون والتنمية الاقتصادية بشأن استراتيجيات الحكومة الرقمية على إشراك أصحاب المصلحة، وإدارة المخاطر، وتنسيق الاستثمار، وربط المشاريع بنتائج قابلة للقياس. وبناء عليه، تستوجب رقمنة أي إجراء ذي أثر قانوني تقييما قبليا لأثره الحقوقي والإجرائي؛ إذ إن اختيار بنية النظام، أو مستوى التعرف، أو قواعد تبادل البيانات يحدد عملياً من يستطيع الولوج، وما الوثيقة المقبولة، ومتى يبدأ الأجل، ومن يتحمل تبعة الخطأ.4

عرف المغرب تعدد تطبيقات الرقمنة في الضرائب والجمارك والموانئ والشكايات والوثائق الإدارية والرخص، فضلا عن توظيف المحاكمة عن بعد في ظرفية استثنائية. ويؤكد هذا التنوع امتداد الرقمنة إلى قطاعات تنتج آثارا قانونية مباشرة، إلا أن عدد المنصات لا يصلح وحده لقياس النضج. فالمعيار الأدق هو اكتمال السلسلة: هل ينجز الإجراء من بدايته إلى نهايته؟ هل تقبل الوثيقة الإلكترونية لدى مختلف الجهات؟ هل يمكن معرفة سبب الرفض وتصحيحه؟ وهل تسلم نسخة رسمية قابلة للتحقق؟5

وعليه، يقصد بالرقمنة في هذه الدراسة إعادة تمثيل المعلومات والمساطر والعلاقات القانونية داخل نظم تسمح بالإيداع والمعالجة والتبادل والإثبات والتتبع، وفق قواعد تضمن صحة المصدر، وسلامة المحتوى، واستمرارية الخدمة، وممارسة الحقوق. ويتميز

---

1 :Antonio Cordella and Niccolò Tempini, "E-government and Organizational Change Reappraising the Role of ICT and Bureaucracy in Public Service Delivery", Government .Information Quarterly, vol. 32, no. 3, 2015, pp. 279-286; J. Ramon Gil-Garcia, Sharon S :Dawes and Theresa A. Pardo, "Digital Government and Public Management Research .Finding the Crossroads", Public Management Review, vol. 20, no. 5, 2018, pp. 633-646

2 Frank Bannister and Regina Connolly, "ICT, Public Values and Transformative Government: A Framework and Programme for Research", Government Information .Quarterly, vol. 31, no. 1, 2014, pp. 119-128

3 OECD, The OECD Digital Government Policy Framework: Six Dimensions of a Digital .Government, OECD Public Governance Policy Papers, No. 02, Paris, 2020, pp. 6-8

4 ,OECD, Recommendation of the Council on Digital Government Strategies .OECD/LEGAL/0406, 15 July 2014, pp. 3-5

5 المجلس الاقتصادي والاجتماعي والبيئي، نحو تحول رقمي مسؤول ومدمج، إحالة ذاتية رقم 2021/28، الرباط، 2021، ص. 14.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

هذا التعريف يربط الأداة بأثرها القانوني؛ فرفع ملف أو استعمال البريد الإلكتروني لا يكفي إذا غابت هوية الأطراف، وحجية الوثيقة، وسرية البيانات، وضبط الآجال.

الجدول رقم 1: التمييز الوظيفي بين مستويات الرقمنة

المستوى	موضوع التحول	الأثر المحتمل في الأمن القانوني	الخطر عند الاكتفاء به
التحويل الرقمي للوثيقة	نقل الورق إلى ملف رقمي	سهولة الحفظ والبحث والاستنساخ	غياب الحجية أو النسخة الرسمية وسهولة تعدد النسخ
رقمنة المسطرة	إلكترنة الإيداع والمعالجة والأداء والتبليغ	ضبط المراحل والآجال وتتبع الملف	إعادة إنتاج التعقيد القديم داخل منصة مغلقة
التحول الرقمي المؤسسي	إعادة تصميم الخدمة والاختصاصات وتبادل البيانات	توحيد المعلومة وتقليص الخطأ وتحسين التوقع	توسع القرار الآلي من دون رقابة أو تفسير
الحكومة الرقمية	منظومة مشتركة تتمحور حول المستخدم والبيانات	خدمة متكاملة واستباقية وقابلة للقياس	المركزية المفرطة للبيانات ومخاطر الأمن والخصوصية

المصدر: إعداد الباحث بالاستناد إلى إطار منظمة التعاون والتنمية الاقتصادية للحكومة الرقمية.

الفقرة الثانية: مضمون الأمن القانوني ومتطلباته

يمكن تعريف الأمن القانوني بأنه قدر معقول من الثقة في القاعدة وفي نمط تطبيقها، بما يسمح للأشخاص بتنظيم سلوكهم وتقدير النتائج المحتملة لأفعالهم. وهو ثمرة تفاعل بين شرعية المصدر، ووضوح الصياغة، وإتاحة النص، واستقرار المراكز، وعدم المفاجأة غير المبررة، واتساق التطبيق، وفعالية الطعن. وقد أبرز الفقه المغربي ارتباط الأمن القانوني والقضائي بجاذبية الاستثمار وبالثقة في المؤسسات1. لذلك قد تكون القاعدة منشورة لكنها غير آمنة لغموضها، أو واضحة لكنها متقلبة، أو مستقرة لكنها تطبق بصورة متفاوتة.

تضيف البيئة الرقمية إلى هذه العناصر شروط أصالة الوثيقة، وسلامة البيانات، وتحديد الزمن القانوني، وتوثيق سلسلة المعالجة. ففي المحرر الورقي يستدل على الحجية من التوقيع والختم والتاريخ والنسخة المحفوظة، بينما يتطلب المحرر الإلكتروني التحقق من هوية الموقع، وصلاحية الشهادة، والختم الزمني، وثبات الملف، وسياسة حفظه. وتبين دراسات الإثبات الإلكتروني أن

1 يونس العياشي، الأمن القانوني والقضائي وأثرهما في التنمية الاقتصادية والاجتماعية، الطبعة الأولى، مكتبة دار السلام، الرباط، 2012، انظر عموما.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

الأصالة لا تنفصل عن سلامة السجل وسياق إنشائه وسلسلة حفظه1. فإذا غابت هذه الضمانات، قد يواجه المرتفق قرارا ظاهرا في حسابه من دون أن يعرف لحظة صدوره أو الجهة التي عدلته.

تدل تقارير تقييم الخدمات العمومية على أن قياس النضج ينبغي أن يميز بين نشر معلومات عامة، وإتاحة التفاعل، وإنجاز المعاملة كاملة، وربط الخدمات بأحداث الحياة. ويرتفع الأمن القانوني كلما انتقل النظام من مجرد إعلام المستخدم إلى تمكينه من إتمام المسطرة والحصول على أثر نهائي يمكن إثباته. وفي المقابل، تزداد مسؤولية الإدارة كلما اكتملت المعاملة رقميا، ولا سيما بشأن دقة البيانات، واستمرارية المنصة، ووضوح الإشعارات، وحفظ السجلات.2

يقوم الأمن القانوني الرقمي على سبعة مؤشرات متداخلة: الشرعية، أي وجود سند لكل معالجة وقرار؛ والإتاحة، أي إمكان الوصول إلى القاعدة والخدمة؛ والوضوح، أي فهم الشروط والنتائج؛ والثبات الزمني، أي حفظ النسخ والتواريخ؛ والحجية، أي إثبات الهوية والمحتوى؛ وقابلية التتبع، أي إعادة بناء مسار القرار؛ وقابلية المراجعة، أي وجود تصحيح وطعن وتدخل بشري. ويؤدي اختلال أحد هذه المؤشرات إلى نقل عدم اليقين من النص إلى النظام المعلوماتي.

لا تفترض قابلية التوقع معرفة نتيجة كل طلب مقدما، لأن السلطة التقديرية قد تظل مشروعة، وإنما تقتضي إعلان معايير القرار وإمكان تفسير كيفية استعمال السلطة ومراقبتها. ويزداد هذا الشرط أهمية في الأنظمة المؤتمتة؛ إذ ينبغي إعلام الشخص بوجود معالجة آلية مؤثرة، وبالبيانات الأساسية المستعملة، وبطريق تصحيح الخطأ وطلب مراجعة بشرية. وقد صاغ الفقه مفهوم «الإجراءات القانونية الواجبة تكنولوجيا» للتنبيه إلى أن الأتمتة لا يجوز أن تحجب التعليل أو تقوض حق الاعتراض3.

الجدول رقم 2: مكونات الأمن القانوني في البيئة الرقمية

دليل التحقق	الأداة الرقمية الملائمة	السؤال القانوني الحاسم	المكوّن
مرجع النص وتاريخ النفاذ	سجل قانوني وربط كل خدمة بسندها	هل توجد قاعدة تجيز الإجراء والمعالجة؟	الشرعية
نسخة رسمية محدثة ودليل خدمة	بوابة موحدة ونص قابل للبحث وشرح إجرائي	هل يستطيع المستخدم فهم القاعدة والشروط؟	الإتاحة والوضوح
سجل التعديل وتاريخ الإتاحة	أرشفة النسخ والختم الزمني	أي نسخة كانت نافذة عند الواقعة؟	الثبات الزمني
التحقق من الشهادة والبصمة الرقمية	توقيع وختم إلكترونيان وشهادة ثقة	من أصدر الوثيقة وهل عدلت؟	الحجية

1 Luciana Duranti and Allison Stanfield, "Authenticating Electronic Evidence", in Stephen ,.Mason and Daniel Seng (eds.), Electronic Evidence and Electronic Signatures, 5th ed .University of London Press, 2021, pp. 236-242

2.iii-iv .المجلس الأعلى للحسابات، تقييم الخدمات العمومية على الخط، الرباط، ماي 2019، ص

3 ,Danielle Keats Citron, "Technological Due Process", Washington University Law Review .vol. 85, no. 6, 2008, pp. 1249-1313

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

دليل التحقق	الأداة الرقمية الملائمة	السؤال القانوني الحاسم	المكوّن
سجل الإيداع والمعالجة والتبليغ	سجل أحداث غير قابل للمحو	كيف عولج الطلب ومن تدخل؟	التتبع
وصل التظلم وأجل الجواب وقرار معلل	واجهة تظلم وتدخل بشري	كيف يصحح الخطأ أو يطعن في القرار؟	المراجعة

المصدر: تركيب الباحث.

المطلب الثاني: الأسس القانونية والمؤسساتية للرقمنة في خدمة الأمن القانوني

الفقرة الأولى: التأطير التشريعي للمعاملات والخدمات الرقمية

مثل القانون رقم 53.05 منعطفاً في الاعتراف بالمعطيات والمحررات المتبادلة إلكترونياً، بإقراره المعادلة بين الكتابة الورقية والكتابة الإلكترونية وتنظيمه للتوقيع الإلكتروني. وتكمن قيمته في نقل النقاش من قبول الوسيلة إلى تحقق شروطها؛ فالحجية لا تثبت للملف لمجرد كونه رقمياً، بل لأن طريقة إنشائه وحفظه تسمح بالتعرف على صاحبه وتضمن سلامة محتواه. وتؤكد الدراسات العربية المقارنة أن وظيفة التوقيع الإلكتروني تجمع بين نسبة المحرر إلى صاحبه وحماية مضمونه من التغيير[1].

كما نظم القانون تكوين العقد الإلكتروني، وأوجب تمكين المتعاقد من مراجعة تفاصيل الطلب وتصحيح الأخطاء قبل تأكيده. ويؤدي هذا المقتضى وظيفتين: حماية الرضا، وإنشاء أثر يمكن الرجوع إليه عند النزاع. وتبين الكتابات المتخصصة أن الإثبات في التعاقد عبر الإنترنت لا يتعلق بواقعة النقر وحدها، بل أيضاً بمضمون العرض الذي ظهر للمستخدم وبزمن قبوله وطريقة التعرف عليه[3]. ولذلك يتعين حفظ النسخة المقبولة، ووقت التأكيد، ووسيلة التعرف، والإشعار المرسل[4].

وأقام القانون رقم 43.20 إطارا أكثر تخصصا لخدمات الثقة، يشمل التوقيعات والأختام والختم الزمني والإرسال الإلكتروني المضمون والتحقق من مواقع الويب. ويعكس ذلك انتقالاً من أداة منفردة إلى سلسلة ثقة متكاملة: فالقرار الإداري قد يحتاج إلى ختم الشخص المعنوي بدل توقيع موظف بعينه، كما يحتاج إلى إثبات زمن الإرسال والتوصل وصلاحية الشهادة عند الإصدار. وتكتمل قيمة هذه الخدمات متى أمكن للقاضي والخبير إعادة التحقق منها عند المنازعة[6].

ويلزم المرسوم التطبيقي السلطة الوطنية بنشر المعايير والمراجع التقنية والتنظيمية ذات الصلة. ويعد هذا النشر جزءا من الأمن القانوني، لأن مقدم الخدمة والإدارة والقاضي والخبير يحتاجون إلى معيار معلوم لتقويم سلامة التوقيع أو الختم. غير أن اليقين

1 –عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، 2005، ص. 128 وما بعدها.
2 –القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، الجريدة الرسمية عدد 5584، 6 دجنبر 2007، ص. 1357، المادة الأولى.
3 –خالد ممدوح إبراهيم، إبرام العقد الإلكتروني: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2006، ص. 50 وما بعدها؛ حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، القاهرة، 2000، ص. 20 وما بعدها.
4 –القانون رقم 53.05، مرجع سابق، ص. 1358، الفصلان 65-4 و65-5 من قانون الالتزامات والعقود كما تم تتميمه.
5– محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، 2010، انظر عموماً.
6 –القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية، الجريدة الرسمية عدد 6970، 18 مارس 2021، ص. 535-536، المواد 1 إلى 4.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

يقتضي أيضا أرشفة النسخ السابقة من هذه المعايير، حتى تقوّم المعاملة القديمة وفق المرجع الذي كان نافذا عند إنجازها لا وفق تحديث لاحق.1

وتتوافق هذه المقاربة مع قانون الأونسيترال النموذجي للتجارة الإلكترونية، المبني على عدم التمييز ضد الوسيلة الإلكترونية، والمعادلة الوظيفية، والحياد التقني. والحياد لا يعني حصر الحجية في منتج قد يتقادم، بل تحديد وظائف التعرف والسلامة وإمكان الرجوع. ومع ذلك ينبغي ألا يتحول إلى غموض تنظيمي؛ إذ يلزم بيان درجات الثقة الملائمة لطبيعة المعاملة وخطورتها.2

أما قانون الأونسيترال النموذجي للتوقيعات الإلكترونية فيربط موثوقية التوقيع بملاءمة الطريقة للغرض، وبسيطرة الموقع على وسيلة الإنشاء، وبإمكان كشف التعديل. ويترتب على ذلك ضرورة اعتماد منهج متدرج: تعريف مبسط للمعاملات اليومية منخفضة المخاطر، وخدمة ثقة أقوى للقرارات والعقود ذات الأثر المالي أو العيني المرتفع، مع ختم زمني وحفظ طويل الأمد. ففرض مستوى واحد على جميع الخدمات إما أن يثقل المساطر أو يضعف الحجية.3

الفقرة الثانية: حماية الحقوق في البيئة الرقمية

لا يستقيم الأمن القانوني الرقمي من دون حماية المعطيات الشخصية، لأن القرار الإلكتروني يعتمد على بيانات الهوية والوضع الاجتماعي والمالي والصحي والمهني. وقد كرس القانون رقم 09.08 مبادئ المشروعية، وتحديد الغرض، والتناسب، والدقة، وتقييد مدة الحفظ. وتوضح الكتابات المقارنة أن حماية البيانات ليست قيدا خارجيا على الإدارة الرقمية، بل إطارا لتوزيع السلطة المعلوماتية وضمان حقوق الشخص4. ومن ثم، يمنع احترام هذه المبادئ ترتيب آثار قانونية على بيانات زائدة أو قديمة أو جمعت لغرض آخر.5

وتتأسس حماية المعطيات على الحق الدستوري في الحياة الخاصة وسرية الاتصالات. لذلك لا يكفي الاستناد إلى التبسيط لتبرير تبادل واسع بين الإدارات. فقاعدة عدم مطالبة المرتفق بوثيقة موجودة لدى جهة عامة أخرى تستلزم، في المقابل، تحديد الغرض، وتقليل البيانات، وضبط صلاحيات الولوج، وتسجيل عمليات الاطلاع، وإتاحة التصحيح والاعتراض في الحدود

1- المرسوم رقم 2.22.687 الصادر في 21 نونبر 2022 بتطبيق القانون رقم 43.20، الجريدة الرسمية عدد 7162، 19 يناير 2023، ص. 148، المادة 32.

2 UNCITRAL, Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, New York, 1999, pp. 17-18.

3 UNCITRAL, Model Law on Electronic Signatures with Guide to Enactment 2001, United Nations, New York, 2002, pp. 23-25.

4 Orla Lynskey, The Foundations of EU Data Protection Law, Oxford University Press, 2015, pp. 89-130; Lee A. Bygrave, Data Privacy Law: An International Perspective, Oxford University Press, 2014, pp. 1-23.

5 القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 5714، 5 مارس 2009، ص. 345-347، المواد 1 إلى 4.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

القانونية. وقد ربطت دراسات مغربية بين تنمية الإدارة الرقمية وضرورة بناء الثقة بواسطة حماية فعلية للمعطيات الشخصية[1].

ويؤطر القانون رقم 05.20 الأمن السيبراني لدى الإدارات والمؤسسات العمومية والبنيات ذات الأهمية الحيوية ومقدمي الخدمات الرقمية. وترتبط أحكامه بالأمن القانوني لأن توافر النظام وسلامته وسريته ليست أهدافا تقنية منعزلة: فتعديل سجل للرخص، أو تعطيل منصة للطعن، أو فساد بيانات الحالة المدنية قد يغير مركزا قانونيا أو يمنع ممارسة حق داخل الأجل[2].

يفرض القانون سياسات أمن وتصنيفاً للمعلومات وتدقيقا وإبلاغا عن الحوادث، كما يؤطر إيواء بعض البيانات الحساسة وتأهيل مقدمي الخدمات. ويعبر هذا البناء عن انتقال من معالجة الحادث بعد وقوعه إلى إدارة المخاطر قبل تحققه. ويقتضي التنزيل العملي ربط شدة الضوابط بقيمة الأثر القانوني؛ فالنظام الذي يصدر قرارا أو يحسب استحقاقا أو يحفظ دليلا يحتاج مستوى ضمان أعلى من موقع يكتفي بنشر معلومات عامة[3].

وتدعو الاستراتيجية الوطنية للأمن السيبراني 2030 إلى مراجعة دورية للترسانة القانونية والمعيارية وتكييفها قطاعيا بحسب المخاطر. وهذه المرونة ضرورية لملاحقة تهديدات سريعة التطور، لكنها يجب أن تراعي بدورها الأمن القانوني: نشر التحديثات، وإقرار فترات انتقال، وضمان استمرار التحقق من الوثائق القديمة قبل سحب الآليات أو الشهادات التي صدرت في ظلها[4].

كما تربط الاستراتيجية التنفيذ بمؤشرات ولوحات قيادة وتقييم دوري لمستوى النضج والتهديدات. وتصلح هذه المقاربة للتعميم على المشاريع ذات الأثر القانوني؛ فلا يكفي إطلاق المنصة، بل يلزم قياس الانقطاعات والأخطاء وطلبات التصحيح ونسب الرفض والفوارق الترابية ومدة حل الشكايات، ثم نشر نتائج مناسبة تسمح بالتقويم والمساءلة[5].

الجدول رقم 3: الإطار القانوني المغربي ووظيفته في الأمن القانوني الرقمي

الفجوة التطبيقية المحتملة	الضمان الأساسي	المجال	النص
تفاوت قبول الوثائق الإلكترونية بين الجهات	المعادلة والحجية وتنظيم التعاقد	المحرر والعقد والتوقيع الإلكتروني	القانون 53.05
كلفة التعميم وضعف الاندماج داخل المساطر	التوقيع والختم والختم الزمني والإرسال المضمون	خدمات الثقة	القانون 43.20

1 أمينة أعتاب، «الإطار القانوني لحماية المعطيات الشخصية كمدخل لتنمية الإدارة الرقمية بالمغرب»، النداء التربوي، العددان 29-30، 2022، ص. 80 وما بعدها.

2 دستور المملكة المغربية لسنة 2011، مرجع سابق، ص. 1909، الفصل 24.

3 -القانون رقم 05.20 المتعلق بالأمن السيبراني، الجريدة الرسمية عدد 6906، 6 غشت 2020، ص. 1294-1295، المواد 1 إلى 3.

4 -القانون رقم 05.20، مرجع سابق، ص. 1296-1297، المواد 8 إلى 20.

5 -المديرية العامة لأمن نظم المعلومات، الاستراتيجية الوطنية للأمن السيبراني 2030، الرباط، 2024، ص. 24.

6 -المديرية العامة لأمن نظم المعلومات، المرجع نفسه، ص. 45.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

الفجوة التطبيقية المحتملة	الضمان الأساسي	المجال	النص
التبادل الواسع وضعف تحديث البيانات	المشروعية والتناسب والدقة وحقوق الشخص	المعطيات الشخصية	القانون 09.08
عدم ربط الحادث التقني مباشرة بأثره على الحقوق والآجال	إدارة المخاطر والتدقيق والإبلاغ عن الحوادث	الأمن السيبراني	القانون 05.20
نشر غير قابل للبحث أو غير محين	الإتاحة والشفافية والنشر الاستباقي	الحق في المعلومات	القانون 31.13
رقمنة مسطرة معقدة دون إعادة تصميمها	توحيد المتطلبات والآجال والمنصة والتبادل	تبسيط المساطر	القانون 55.19
غياب مؤشرات منشورة خاصة بالأمن القانوني الرقمي	الجودة والمساواة والاستمرارية والمحاسبة	ميثاق المرافق العمومية	القانون 54.19

المصدر: إعداد الباحث استناداً إلى النصوص التشريعية المذكورة.

المبحث الثاني: آليات إسهام الرقمنة في تحقيق الأمن القانوني وحدود فعاليتها

تظهر فائدة الرقمنة عندما تقلص عدم اليقين في علاقة الفرد بالقانون والإدارة، فتجعل القاعدة أيسر وصولا، والمسطرة أوضح، والإثبات أقوى، والقرار أكثر قابلية للتتبع. غير أن التقنية ليست محايدة تنظيميا دائما؛ فقد تعيد إنتاج التعقيد البيروقراطي أو توسعه إذا بنيت المنصة على قواعد ناقصة أو بيانات غير صحيحة1. ومن ثم، ينبغي دراسة الإسهام والمخاطر ضمن إطار واحد.

المطلب الأول: مظاهر إسهام الرقمنة في تعزيز الأمن القانوني

أضحى التحول الرقمي أحد أبرز التحولات التي شهدتها المنظومة القانونية والإدارية المعاصرة، لما أتاحه من إمكانات جديدة لتطوير آليات إنتاج القاعدة القانونية وتطبيقها وتيسير الولوج إليها. ولم تعد الرقمنة تقتصر على مجرد استعمال الوسائل التقنية في معالجة المعلومات وحفظها، وإنما أصبحت أداة أساسية لإرساء قدر أكبر من الوضوح والشفافية والسرعة واليقين في المعاملات والإجراءات القانونية.

الفقرة الأولى: الرقمنة كآلية لضمان الولوج إلى القاعدة والمعلومة القانونية

يؤسس القانون رقم 31.13 لحق الأشخاص في الحصول على المعلومات التي تحوزها الجهات الخاضعة له، ويحدد واجبات النشر والطلب والاستثناءات. وتتيح الرقمنة تنفيذ هذا الحق بكلفة أقل وعلى نطاق أوسع، من خلال النشر الاستباقي للقرارات

1.Frank Bannister and Regina Connolly, op. cit., pp. 119-128

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

والدلائل والإحصاءات والميزانيات والمساطر؛ وبذلك ينتقل الحق من طلب فردي ينتظر جواب الإدارة إلى بنية معلوماتية عامة متاحة للجميع.1

غير أن الإتاحة لا تقاس بوجود ملف على موقع إلكتروني، بل بجودة بياناته الوصفية، وإمكان البحث في محتواه، ووضوح تاريخ تحيينه، وإتاحته بصيغة قابلة لإعادة الاستخدام، وبيان النسخة النافذة. وقد نبهت أدبيات الشفافية الرقمية إلى أن نشر كميات كبيرة من المعلومات لا يحقق المساءلة تلقائيا إذا كانت المادة غير قابلة للفهم أو الاستعمال2. فالوثيقة مجهولة المصدر والبوابة التي تجمع نسخا متعارضة قد تزيدان عبء التحقق بدلا من تقليصه.

ومن أهم وظائف النشر الرقمي إنشاء ذاكرة معيارية تحفظ النص الأصلي، وتعديلاته، وتاريخ دخول كل تعديل حيز التنفيذ، والنص المدمج، وقرارات التطبيق، والاجتهادات ذات الصلة. وينبغي أن تسمح هذه الذاكرة بإعادة بناء القانون الذي كان نافذا في تاريخ محدد، لأن معالجة تنازع القواعد في الزمن جزء أصيل من استقرار المراكز القانونية3. وتبرز الحاجة بصفة خاصة في المنازعات الضريبية والعقارية والعقود المستمرة، حيث لا تكفي معرفة النص الحالي.

كرس القضاء الدستوري المقارن هدف إتاحة القانون ووضوحه وقابليته للفهم باعتباره ضمانة في مواجهة التعسف. وتساعد الرقمنة على خدمة هذا الهدف بواسطة البحث والربط الزمني والتنبيه إلى التعديل، لكنها لا تعفي السلطة المعيارية من جودة الصياغة. بل قد تكشف الأدوات الرقمية كثرة الإحالات والتعارضات بصورة أوضح، وهو ما ينبغي استثماره في تنقية النصوص وتبسيطها، لا في إخفاء التعقيد خلف واجهة بحث.4

ويستحسن أن تجمع البوابة القانونية الرسمية بين طبقتين واضحتين: طبقة حجية تعرض النص الرسمي وصورة الجريدة الرسمية وبصمته الرقمية، وطبقة استعمال تقدم نصا مدمجا قابلا للبحث، وروابط بين المواد، وخطا زمنيا للتعديلات، وشرحا غير ملزم للمسطرة. ويمنع الفصل بين الطبقتين الخلط بين النص الملزم والمحتوى التفسيري، من دون التضحية بقابلية القانون للاستخدام.

وتؤدي رقمنة الاجتهاد القضائي وظيفة مماثلة، لأن توقع التطبيق لا يستمد من النص وحده. وينبغي أن يوازن نشر الأحكام بين الشفافية وحماية المعطيات، من خلال إخفاء الهوية وفق قواعد ثابتة، ووصف موضوع الحكم، وإظهار المحكمة والتاريخ والمرجع، وإتاحة البحث في المبادئ. كما يتعين بيان معايير اختيار الأحكام المنشورة، لأن الانتقاء غير المعلن قد يرسم صورة غير دقيقة لاتجاه القضاء.

---

1. القانون رقم 31.13 المتعلق بالحق في الحصول على المعلومات، الجريدة الرسمية عدد 6670، 3 ماي 2018، ص. 1142-1144، المواد 1 إلى 10.

2 Frank Bannister and Regina Connolly, "The Trouble with Transparency: A Critical Review of Openness in E-Government", Policy & Internet, vol. 3, no. 1, 2011, article 8, pp. 1-30.

3 ,Paul Roubier, Le droit transitoire (Conflits des lois dans le temps), 2e éd., Dalloz et Sirey Paris, 1960, pp. 3-9.

4, المجلس الدستوري الفرنسي، القرار رقم DC 421-99 بتاريخ 16 دجنبر 1999، الفقرة 13، بشأن هدف إتاحة القانون ووضوحه وقابليته للفهم.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

الفقرة الثانية: الرقمنة كوسيلة لتبسيط المساطر وتعزيز الثقة القانونية

يربط القانون رقم 55.19 علاقة الإدارة بالمرتفق بمبادئ الثقة والشفافية والتناسب وتحديد الآجال وعدم طلب الوثيقة أكثر من مرة وتحسين الجودة والرقمنة. وتخدم هذه المبادئ الأمن القانوني لأنها تحول المسطرة من معرفة داخلية تحتكرها الإدارة إلى قواعد منشورة يمكن الاحتجاج بها. وقد أبرزت دراسات مغربية أن نجاح التحول الإداري الرقمي يتوقف على وضوح الإسناد المؤسسي وتكامل آليات التنفيذ1. فعندما يحدد الدليل الوثائق والأجل وأثر السكوت وطرق الطعن، تنخفض مساحة المفاجأة والتقدير غير المنضبط.2

ويلزم القانون الإدارات برقمنة المساطر وتبادل الوثائق التي تحوزها وإنشاء بوابة وطنية تنشر الأدلة والمؤشرات. ويكشف الجمع بين الرقمنة والتبادل أن التبسيط لا يتحقق بنقل عبء الوثيقة من الشباك إلى شاشة المستخدم، بل بعدم مطالبته بها متى توفرت لدى جهة عامة، مع احترام حماية البيانات. ولذلك يعد التشغيل البيني وسيلة لتنزيل التناسب ومنع التكرار، لا مجرد تحسين تقني.3

ويقرر ميثاق المرافق العمومية قواعد الحوكمة والجودة والفعالية والشفافية وربط المسؤولية بالمحاسبة. ويتطلب تنزيلها رقميا تعيين مسؤول عن كل خدمة، ومالك للبيانات المرجعية، ومسؤول عن الاستمرارية، ومسار واضح للشكاية والتصحيح. فالغموض المؤسسي عند وقوع خطأ في منصة مشتركة يبدد مكسب السرعة، لأن المرتفق قد يتنقل بين الجهة المالكة للبيانات، والجهة المدبرة للمنصة، والجهة مصدرة القرار من دون مخاطب يتحمل المسؤولية.4

وتسمح الرقمنة بضبط تاريخ الإيداع وتسليم وصل فوري، وهما ضمانتان حاسمتان لحماية الآجال. وينبغي أن يتضمن الوصل معرفاً فريداً، وتاريخا ووقتا موثوقين، وقائمة الملفات المودعة وبصمتها الرقمية، والأجل القانوني المتوقع، وقناة التبليغ. وإذا استكمل المستخدم ملفه، وجب إنشاء حدث جديد في السجل بدل استبدال الوصل الأول، حتى تبقى السلسلة الزمنية قابلة للإثبات.

تساعد الأتمتة على توحيد الفحص الأولي ومنع طلب وثائق غير مقررة، لكنها تصبح مصدرا لعدم اليقين إذا تحولت قواعد التحقق التقنية إلى شروط قانونية غير منشورة. وقد بين فقه الإدارة الرقمية أن انتقال القرار من موظف الواجهة إلى النظام يجعل هندسة المعلومات نفسها حاملة لقواعد البيروقراطية5. لذلك يجب إعلان قيود الصيغة والحجم والحقول، وتعليل الرفض التقني، وإتاحة التصحيح، وألا تتحول رسالة خطأ غامضة إلى قرار نهائي غير قابل للمراجعة البشرية.

---

1 .محمد ختام، «التحول الرقمي بالإدارة المغربية: بحث في آليات الإسناد»، مجلة الباحث للدراسات والأبحاث القانونية والقضائية، العدد 40، 2022، ص. 85 وما بعدها.

2. القانون رقم 55.19 المتعلق بتبسيط المساطر والإجراءات الإدارية، نسخة وزارة العدل، 2021، ص. 3-4، المادتان 3 و4.

3. القانون رقم 55.19، المرجع نفسه، ص. 12-13، المادتان 25 و26.

4. القانون رقم 54.19 بمثابة ميثاق المرافق العمومية، الجريدة الرسمية عدد 7106، 7 يوليوز 2022، ص. 785-787، المواد 1 إلى 8.

5 :Mark Bovens and Stavros Zouridis, "From Street-Level to System-Level Bureaucracies How Information and Communication Technology Is Transforming Administrative Discretion

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

وتقوي قابلية التتبع الرقابة على التأخير والتدخل غير المشروع؛ إذ يبين السجل من فتح الملف، ومتى طلب الاستكمال، ومن غير حالته، ومتى صدر القرار. غير أن هذا السجل لا يؤدي وظيفة الثقة إلا إذا حُمي من التعديل، وخضع لسياسة حفظ معلنة، وأتيح لأجهزة الرقابة. كما ينبغي تمكين المرتفق من الجزء اللازم للدفاع عن حقوقه من دون كشف معلومات أمنية أو معطيات تخص الغير.

تربط خدمات الثقة الإجراء بصاحبه وتثبت سلامة المحتوى وزمنه. ويقدم تنظيم الاتحاد الأوروبي نموذجا متدرجا للتعريف الإلكتروني والتوقيع والختم والإرسال المضمون، وقد عُدّل سنة 2024 لإقامة إطار للهوية الرقمية الأوروبية ومحفظة هوية قابلة للاستعمال عبر الحدود1. ولا يتعلق الاستئناس بهذا النموذج بنسخه، بل بإبراز قيمة قابلية التحقق المتبادل: فالوثيقة الصادرة عن إدارة ينبغي أن تقبلها إدارة أخرى، وأن يظل القاضي والخبير قادرين على التحقق من صلاحيتها بعد سنوات.2

وتقيس مسوح الأمم المتحدة نضج الحكومة الإلكترونية من خلال تكامل الخدمات والبنية والموارد البشرية والمشاركة، لا بعدد المواقع وحده. ويقترح، في السياق المغربي، استكمال مؤشرات النضج بمؤشر للأمن القانوني يرصد نسبة الخدمات التي تسلم وصولات موثوقة، ونسبة القرارات المعللة رقمياً، وقابلية التحقق من الوثائق، وعدد الحقوق المتأثرة بالأعطال، ومدة تصحيح البيانات.3

الجدول رقم 4: قراءة تطبيقية في مستوى اكتمال الخدمات الرقمية

الاستنتاج	الدلالة القانونية	المعطى المرصود	المؤشر
ينبغي قياس اكتمال المسار لا عدد الواجهات	انقطاع السلسلة يجبر المستخدم على العودة إلى الورق والحضور	رصد تقرير المجلس الأعلى للحسابات 74 خدمة، لم يكن متاحاً منها على الخط سوى 33 خدمة تقريباً	الخدمات المرتبطة بأحداث الحياة
الأولوية للخدمات ذات الأثر المباشر في الحقوق	الخدمة الناقصة لا تنتج أثرا قانونيا نهائيا	كان المتاح على الخط أقل من نصف الخدمات الأساسية محل التقييم	الخدمات الأساسية

and Constitutional Control", Public Administration Review, vol. 62, no. 2, 2002, pp. 174-184.

1 . Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 30 April 2024.

2 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services, OJ L 257, 28 August 2014, pp. 73-114, especially pp. 84-87.

3 United Nations, E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development, New York, 2024, pp. 30-35.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

الاستنتاج	الدلالة القانونية	المعطى المرصود	المؤشر
يلزم تحديد النسخة المرجعية وقواعد الانتقال	استمرار ازدواج الورق والرقمي يخلق نسخا وآجالا متعارضة	أشار المجلس الاقتصادي والاجتماعي والبيئي إلى أن 23% فقط من الخدمات كانت منزوعة الطابع المادي بالكامل	الرقمنة الكاملة
التبسيط مؤشر للأمن القانوني وليس للكفاءة فقط	الكلفة الزمنية تحد من الولوج الفعلي للحق	تقدير متوسط 50 ساعة سنوياً للمواطن و200 ساعة للمقاولة	كلفة التعامل الإداري

المصدر: المجلس الأعلى للحسابات، 2019، ص. 30-31؛ والمجلس الاقتصادي والاجتماعي والبيئي، 2021، ص. 18 و21.24

تؤكد المعطيات السابقة أن كثرة الخدمات الرقمية لا تعني اكتمالها. فإذا بدأ الإجراء إلكترونيا ثم استلزم إيداع أصل ورقي أو أداء حضوريا أو سحب قرار غير قابل للتحقق، نشأت ازدواجية معيارية: تاريخ رقمي في مقابل تاريخ ورقي، وملف مرفوع في مقابل ملف مادي، وإشعار إلكتروني في مقابل وصل تقليدي. وهذه الازدواجية تفتح منازعات حول الآجال والنسخة المرجعية، مما يفرض قواعد انتقال صريحة تعالج التعارض.

قدر المجلس الاقتصادي والاجتماعي والبيئي وفورات التحول الرقمي للإدارة بأكثر من عشرة ملايير درهم، أي نحو 0.9% من الناتج الداخلي وفق الفرضيات المعتمدة. بيد أن القيمة القانونية للتحول لا تختزل في الوفر المالي؛ فالوقت الذي يستعيده المرتفق يقلص كلفة ممارسة الحق، والحد من التنقل يضيق فرص المعاملة غير المتكافئة، والتتبع يقلل ضياع الطلبات. لذلك ينبغي إدماج مؤشرات العدالة واليقين ضمن دراسات الجدوى الرقمية.3

ويبرز مؤشر نضج GovTech أهمية المنصات المشتركة، والهوية، والمدفوعات، والمشاركة، والبيانات الحكومية. وتفيد هذه المقاربة أن الحاجة لا تتجه إلى حلول منفصلة لكل قطاع، بل إلى هندسة مرجعية تربط الخدمات بمكونات موحدة. فالمكون المشترك يحقق اقتصاد الحجم، ويضمن قبل ذلك اتساق مستوى الثقة، وحساب الزمن، وقواعد الإثبات بين الإدارات.4

المطلب الثاني: تحديات الرقمنة وضمانات تحقيق الأمن القانوني

على الرغم من المزايا التي أتاحتها الرقمنة في تعزيز الأمن القانوني، فإن اعتماد التقنيات الرقمية داخل المنظومة القانونية لا يخلو من تحديات قد تؤثر في استقرار المراكز القانونية وثقة المتعاملين. فالتوسع في رقمنة الإجراءات وتبادل البيانات يثير إشكالات

1. المجلس الاقتصادي والاجتماعي والبيئي، نحو تحول رقمي مسؤول ومدمج، مرجع سابق، ص. 18-19.
2. المجلس الأعلى للحسابات، تقييم الخدمات العمومية على الخط، مرجع سابق، ص. 30-31.
3. المجلس الاقتصادي والاجتماعي والبيئي، نحو تحول رقمي مسؤول ومدمج، مرجع سابق، ص. 24.
4. البنك الدولي، GovTech Maturity Index 2022 Update: Trends in Public Sector Digital Transformation, Washington, 2023, pp. 10-15.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

تتعلق بحماية المعطيات ذات الطابع الشخصي، والأمن السيبراني، وحجية المحررات الإلكترونية، إضافة إلى الفجوة الرقمية التي قد تحد من مبدأ المساواة في الولوج إلى الخدمات القانونية والعدالة.

ومن ثم، فإن تحقيق الأمن القانوني في البيئة الرقمية لا يتوقف على توظيف التكنولوجيا فحسب، بل يقتضي إرساء ضمانات تشريعية ومؤسساتية وتقنية تكفل حماية الحقوق والحريات، وتضمن سلامة المعاملات الإلكترونية وموثوقيتها، بما يحقق التوازن بين متطلبات الابتكار الرقمي ومقتضيات اليقين والاستقرار القانونيين.

وعليه، سيتم تناول هذا المطلب من خلال بيان أبرز تحديات الرقمنة التي تواجه الأمن القانوني، ثم الوقوف على الضمانات الكفيلة بتحقيق الأمن القانوني في ظل التحول الرقمي.

الفقرة الأولى: التحديات القانونية والتقنية المرتبطة بالرقمنة

يتمثل التحدي الأول في التجزؤ التشريعي والمؤسسي. فالمعاملة الرقمية الواحدة قد تخضع في آن واحد لقواعد الإثبات وخدمات الثقة وحماية المعطيات والأمن السيبراني والحق في المعلومات وتبسيط المساطر، مع تدخل جهات رقابية متعددة. ولا يعد هذا التعدد عيبا بذاته، لأن كل نظام يحمي مصلحة مختلفة، لكن الخطر يظهر عندما تغيب قواعد الأولوية والمسؤولية والإبلاغ. ومن ثم، تحتاج كل خدمة إلى خريطة امتثال تجمع السند والالتزامات والجهات المختصة ومسارات الطعن.

ويتمثل التحدي الثاني في ضعف التشغيل البيني. فقد عدت مراجعة منظمة التعاون والتنمية الاقتصادية الهوية الإلكترونية والخدمات المشتركة والسجلات المرجعية من ممكنات الحكومة الرقمية في المغرب. ومن دونها تتكرر البيانات وتتعارض، ويضطر المستخدم إلى تصحيح الخطأ في أكثر من سجل، وقد يصدر قرار استناداً إلى معلومة قديمة من دون أن يعرف الشخص مصدرها أو طريق تعديلها.1

أما التحدي الثالث فيتعلق باستمرارية الخدمة. فلا يجوز أن يؤدي تعطل المنصة في اليوم الأخير من أجل الطعن أو الترشيح أو الأداء إلى سقوط الحق. ويستلزم ذلك سجلا علنيا للأعطال، وتمديدا تلقائيا أو قناة بديلة عند العطل العام، وإثبات محاولات المستخدم، ومركز مساعدة مؤهلا، مع تحديد القيمة الإثباتية للرسائل والصور التي يحتفظ بها عند فشل النظام.

ويرتبط التحدي الرابع بالأمن السيبراني؛ فالاختراق قد يسرب البيانات، أو يغير ملفا، أو ينتحل هوية، أو يعطل خدمة، أو يشفر أرشيفا. ولا يتساوى الأثر القانوني للحوادث: فتسريب المراسلات يمس الخصوصية، بينما تعديل سجل ملكية أو رخصة يمس مركزا قانونيا مباشرا. وتؤكد أدبيات هندسة الأمن أن الضمان ليس منتجا نهائيا ثابتا، بل عملية مستمرة تشمل الاختبار والتدقيق والاستدامة2. لذلك ينبغي أن تتضمن الاستجابة للحادث جرد القرارات والآجال والوثائق المتأثرة وكيفية إخطار أصحابها وتصحيحها.

1.OECD, Digital Government Review of Morocco, op. cit., p. 22

2 ,Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems .3rd ed., Wiley, 2020, pp. 1015-1018

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

ويتصل التحدي الخامس بالاعتماد على الحوسبة السحابية ومقدمي الخدمات الخارجيين. وقد أبرز المجلس الاقتصادي والاجتماعي والبيئي إمكانات السحابة للتحول الرقمي، إلى جانب قضايا السيادة والثقة وحماية البيانات. ويقتضي الأمن القانوني تضمين العقود قواعد واضحة بشأن مكان البيانات، وقابلية نقلها، وحقوق التدقيق، والإخطار بالحوادث، واسترجاع السجلات، واستمرارية الخدمة عند انتهاء العقد أو تعثر المزود.1

أما التحدي السادس فهو الفجوة الرقمية. فالإلزام الحصري بالقناة الإلكترونية قد يخل بالمساواة إذا لم يراع ضعف الاتصال أو الإعاقة أو الأمية الرقمية أو عدم تملك وسائل الأداء والتعريف. وقد وصفت دراسات الإدارة الرقمية كيف يمكن لهندسة المعلومات أن تنتج إقصاء إداريا حتى من دون قرار صريح2. لذلك لا يكفي فتح المنصة؛ بل يلزم اختبار قدرة الفئات المختلفة على إتمام الإجراء وفهم أثره والحصول على مساعدة مكافئة.

ويتمثل التحدي السابع في القرار الخوارزمي، سواء تعلق بترتيب الملفات أو كشف المخاطر أو الاحتساب أو المطابقة. فإذا كانت القواعد غير موثقة أو غير قابلة للتفسير، تحولت السلطة التقديرية إلى صندوق مغلق. وقد بينت الأدبيات أن التنظيم الخوارزمي يثير قضايا المشروعية والتناسب والتعليل والمساءلة3. ولذلك يلزم توثيق الغرض والبيانات والمعايير، واختبار الانحياز والخطأ، وحفظ نسخة النظام المستعمل وقت القرار، وتمكين المسؤول من المراجعة، وإعلام الشخص بوجود معالجة آلية مؤثرة.

ويتعلق التحدي الثامن بالحفظ طويل الأمد. فقد تنتهي الشهادة، وتتقادم الصيغة، وتتوقف البرمجية، بينما يبقى الحق أو العقد قائما لعقود. وتوضح دراسات أصالة الأدلة الرقمية أن استمرارية الحجية تتطلب حفظ بيانات التحقق وسلسلة الحيازة وتوثيق عمليات الترحيل4. لذلك ينبغي أن تشمل سياسة الأرشفة تجديد الختم الزمني، وتحويل الصيغ بطريقة موثقة، وحفظ النسخ اللازمة للتحقق؛ فقابلية فتح الملف اليوم لا تضمن حجّيته مستقبلا.

وينشأ التحدي التاسع من تعدد النسخ والمنصات. فقد ينشر القرار في موقع القطاع ثم في بوابة وطنية ويرسل إلى حساب المستخدم، مع احتمال اختلاف الصيغة أو التاريخ. ويقتضي اليقين تحديد القناة التي يبدأ منها النفاذ أو الأجل، وتمييز النسخة الرسمية من النسخ الإعلامية، وربط جميع النسخ بمعرف ثابت؛ وإلا تحولت وفرة النشر إلى سبب للتنازع.

---

1. المجلس الاقتصادي والاجتماعي والبيئي، الحوسبة السحابية: رافعة أساسية للتحول الرقمي، الرباط، 2023، ص. 17-22.

2 Rik Peeters and Arjan Widlak, "The Digital Cage: Administrative Exclusion through Information Architecture – The Case of the Dutch Civil Registry's Master Data Management System", Government Information Quarterly, vol. 35, no. 2, 2018, pp. 175-183; Virginia .Eubanks, Automating Inequality, St. Martin's Press, New York, 2018, passim

3 & Karen Yeung, "Algorithmic Regulation: A Critical Interrogation", Regulation Governance, vol. 12, no. 4, 2018, pp. 505-523; Cary Coglianese and David Lehr, "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era", Georgetown Law .Journal, vol. 105, 2017, pp. 1147-1223; Danielle Keats Citron, op. cit., pp. 1249-1313

4.Luciana Duranti and Allison Stanfield, op. cit., pp. 271-278

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

ويظل العنصر البشري تحديا عابرا لباقي المخاطر. فقد أبرزت منظمة التعاون والتنمية الاقتصادية الحاجة إلى قيادة رقمية وكفاءات مشتركة ومناهج موحدة لإدارة المشاريع وقياسها. فالخطأ في إدخال البيانات أو تصميم الحقول أو تفسير القاعدة قد يتكرر آليا على نطاق واسع. ومن ثم، لا يلغي النظام الحاجة إلى الموظف، بل يفرض تكوينا رقميا للقانوني وتكوينا قانونيا للمهندس وفريقا متعدد التخصصات.1

الجدول رقم 5: مصفوفة مخاطر الأمن القانوني الرقمي

إجراء المعالجة	الضابط الوقائي	درجة الخطورة	الأثر على المركز القانوني	الخطر
تمديد تلقائي وقناة بديلة وسجل عطل	تكرار البنية ومراقبة التوفر	مرتفعة	فوات أجل أو تعذر إيداع الطلب	انقطاع المنصة
حق تصحيح سريع وتعليق الأثر الضار	تحقق من المصدر وتحديث دوري	مرتفعة	رفض أو احتساب أو ترتيب خاطئ	بيانات غير صحيحة
نسخة احتياطية وتحقيق وإخطار الأطراف	بصمة رقمية وختم زمني وسجل غير قابل للمحو	حرجة	نزاع في الحجية والمضمون	تعديل وثيقة أو سجل
تجميد الإجراء وإعادة التحقق	تعريف متناسب ومصادقة متعددة العوامل	حرجة	تصرف أو طلب غير منسوب لصاحبه	انتحال الهوية
مراجعة بشرية وحق الاعتراض	توثيق واختبار وتقييم أثر	مرتفعة	تمييز أو رفض غير معلل	قاعدة خوارزمية غامضة
دعم مباشر وعدم ترتيب جزاء	تصميم شامل ومساعدة وقناة حضورية	متوسطة/مرتفعة	حرمان فعلي من الخدمة	فجوة رقمية
ترحيل موثق وحفظ بيانات التحقق	أرشفة موثوقة وتجديد الأختام	مرتفعة	تعذر التحقق من وثيقة قديمة	تقادم الصيغة أو الشهادة

المصدر: إعداد الباحث وفق منهج إدارة المخاطر القانونية والسيبرانية.

الفقرة الثانية: متطلبات تعزيز الأمن القانوني في البيئة الرقمية

يبدأ الإصلاح بإقرار مبدأ «الشرعية الرقمية بالتصميم»، ومضمونه عدم إطلاق خدمة ذات أثر قانوني قبل تحديد سندها، والجهة المسؤولة عنها، والبيانات الضرورية، وقواعد الآجال، وقيمة الوصل، ومستوى التوقيع، ومسار التصحيح والطعن،

1 OECD, Digital Government Review of Morocco, op. cit., pp. 23-25.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

وخطة الاستمرارية. ويترجم هذا المبدأ إلى بطاقة امتثال قانونية وتقنية ترافق المشروع منذ تحديد المتطلبات إلى التشغيل والتحديث.

ويتطلب الأمن القانوني بوابة معيارية موحدة للنصوص والمساطر. وفي السياق المغربي، ينبغي ربط الجريدة الرسمية بقاعدة تشريعات مدمجة تحفظ تاريخ كل نص، وربط المسطرة بالسند النافذ والدليل المعتمد، مع تنبيه الجهة المدبرة عند تغيير النص الذي تعتمد عليه المنصة. وتسمح هذه البنية بفهم الحكم الحالي وإعادة بناء الحكم الذي كان نافذاً وقت الواقعة.1

كما يتعين اعتماد معرفات موحدة للوثيقة والطلب والقرار تسمح بالتبادل والتحقق من دون كشف بيانات أكثر مما يلزم. فلا يكون المعرف رقما محليا داخل نظام واحد، بل مفتاحا يربط النسخة بالمصدر والحالة والتاريخ. وينبغي أن ترافق الوثيقة بيانات وصفية قانونية تتضمن جهة الإصدار، والاختصاص، والتاريخ، ونوع التوقيع، ومدة الصلاحية، ومرجع المسطرة.

ويلزم إطار وطني للتشغيل البيني لا يقتصر على الصيغ والبروتوكولات، بل يحدد دلالة البيانات، ومسؤولية جودتها، وقواعد تصحيحها. فإذا حمل العنوان أو الصفة أو رقم العقار معنى مختلفا بين سجلين، نقل الربط التقني الخطأ بدلاً من معالجته. لذلك ينبغي تعيين مالك لكل بيان مرجعي، يكون مسؤولا عن تحديثه وإشعار الأنظمة التي تعتمد عليه.

ويقتضي الأمن القانوني تدرجا في وسائل الهوية والتوقيع بحسب المخاطر. فالوصول إلى معلومة عامة لا يستلزم تعريفا، وقد يكفي حساب موثق لطلب بسيط، بينما يحتاج نقل حق أو إصدار قرار حساس إلى خدمة ثقة أقوى. ويمنع هذا التناسب الإفراط في جمع البيانات وارتفاع الكلفة في المعاملات اليومية، ويحمي في الوقت نفسه التصرفات عالية الأثر.

ومن الضروري تنظيم الأثر القانوني للأعطال والحوادث بقواعد عامة أو مقتضيات قطاعية متسقة. وتشمل الحلول وقف الآجال أثناء العطل العام المثبت، وعدم تحميل المرتفق تبعة خلل من جانب الإدارة، وقبول دليل معقول على محاولة الإيداع، ونشر بداية العطل ونهايته، وإخطار المتضررين عند احتمال فساد البيانات. فالمعالجة الصامتة للعطل تقوض الثقة أكثر من وقوعه.

ويحتاج القرار الآلي إلى نظام حوكمة مستقل يقوم على جرد الأنظمة وتصنيفها بحسب الأثر، وتقييم المخاطر قبل الاستعمال، واختبار الدقة والانحياز دوريا، وحفظ النسخة التي أنتجت القرار، وتقديم تفسير ذي معنى، وضمان المراجعة البشرية. وقد كرس التنظيم الأوروبي للذكاء الاصطناعي نهجا قائما على المخاطر، في حين تربط اتفاقية مجلس أوروبا الإطارية بين دورة حياة

1.Conseil d'État, Sécurité juridique et complexité du droit, op. cit., pp. 327-330

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

الأنظمة وحقوق الإنسان والديمقراطية وسيادة القانون1. وتمثل هذه المعايير مرجعا مقارنا لصياغة ضمانات وطنية متناسبة، لا بديلا عن الاختيارات التشريعية المغربية.2

وتستوجب الشفافية نشر مؤشرات تتجاوز عدد المعاملات، فتشمل نسبة الإجراءات المكتملة رقميا، ومتوسط المعالجة، ونسبة القرارات المصححة بسبب خطأ في البيانات، وعدد الأعطال ومدتها، ونسبة الوثائق القابلة للتحقق، ومدة الاستجابة لطلبات التصحيح، والفوارق بين الجهات والفئات. ويجب تفسير المؤشر على ضوء الحق محل القياس، لأن تقليص المدة مع ارتفاع الرفض غير المعلل لا يمثل تقدما.

كما ينبغي تعزيز الرقابة بتدقيق مشترك قانوني وتقني: فالتدقيق الأمني يختبر الثغرات والاستمرارية، بينما يفحص التدقيق القانوني مشروعية البيانات، والاختصاص، والتعليل، والآجال، والتناسب. ويمكن للمجلس الأعلى للحسابات وهيئات التفتيش والسلطات التنظيمية اعتماد أدلة موحدة للتدقيق الرقمي، مع تمكينها من السجلات الضرورية من دون مساس غير متناسب بالسرية.

وتظل حماية المعطيات التزاما مستمرا لا إجراء شكليا عند إطلاق المشروع. ويجب تحويل قواعد الجمع والاستعمال والحفظ وحقوق الشخص إلى وظائف تقنية محددة: تقليل الحقول، وانتهاء صلاحيات الولوج، وتسجيل النفاذ، والتشفير، والحذف أو الإخفاء بعد انقضاء المدة، ومسار سريع للتصحيح. ويتقاطع ذلك مع الضمانات المقارنة المتعلقة بالقرار الآلي وحق الشخص في الاعتراض وطلب تدخل بشري3. ولا تغني سياسة خصوصية طويلة عن تصميم يحمي الحقوق فعليا.4

ويلزم تطوير التكوين المشترك، وقد جعلت استراتيجية الأمن السيبراني التوعية وبناء القدرات محورا مستقلا. ويقترح إدراج وحدات للمسؤولين القانونيين حول الهوية والتوقيع والسجلات والخوارزميات، ووحدات للمهندسين حول الاختصاص والتعليل والآجال وحماية الحقوق، إلى جانب تمارين محاكاة تجمع بين الحادث السيبراني والنزاع القانوني الناتج عنه.5

ويتحقق الإدماج الرقمي بواسطة مبدأ «المساعدة المكافئة»: أي تمكين من لا يستطيع استعمال المنصة من دعم داخل فضاء عمومي أو عبر وسيط معتمد، من دون رسوم إضافية أو فقدان للأجل. وتبقى القناة الحضورية أو الورقية ضمانة انتقالية حيث

---

1 Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, OJ L, 12 July 2024, especially arts. 6, 9 and 14; Council of Europe, Framework Convention on Artificial ;Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225, 2024 .UNESCO, Recommendation on the Ethics of Artificial Intelligence, Paris, 2021

2 OECD, The E-Leaders Handbook on the Governance of Digital Government, OECD .Publishing, Paris, 2021, pp. 15-18

3 ,Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4 May 2016 .art. 22

4.12 القانون رقم 09.08، مرجع سابق، ص. 348-350، المواد 7 إلى

5.36-34 المديرية العامة لأمن نظم المعلومات، الاستراتيجية الوطنية للأمن السيبراني 2030، مرجع سابق، ص.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

لا تتوافر شـروط الإتاحة، على أن يدخل الموظف الطلب إلى النظام ويسـلم وصـلا رقميا قابلا للتحقق، تجنبا لقيام منظومتين متعارضتين.

وتستدعي الحجية سياسة أرشفة رقمية تحدد مدد الحفظ، والصيغ المقبولة، والتوقيع والختم الزمني، وعمليات الترحيل، والنسخ الاحتياطية، وشـروط الوصـول القضـائي. وتراعي السـياسـة دورة حياة الوثيقة منذ إنشـائها واسـتعمالها إلى حفظها النهائي أو إتلافها، مع توثيق كل انتقال يطرأ عليها. وتظهر أهميتها بوجه خاص في العقود والسـجلات والقرارات التي يتجاوز عمرها الافتراضي للبرمجية.

وأخيرا، يتعين ربط استراتيجية الرقمنة بهدف استعادة الثقة الذي وضعه النموذج التنموي الجديد في صلب الإصلاح، مع اعتبار التقنية أداة لتبسيط العلاقة بين المواطن والمؤسسة. ولا تقاس الثقة بالانطباع، بل بنتائج ملموسة: أن يعرف الشخص القاعدة، ويتم الإجراء، ويحصل على دليل، ويصحح الخطأ، ويطعن أمام جهة مستقلة. وبذلك تصبح مؤشرات الأمن القانوني جزءا من تقويم التحول الرقمي لا ملحقا به.1

الجدول رقم 6: نموذج مقترح لمؤشر الأمن القانوني الرقمي

الهدف	طريقة القياس	المؤشر المقترح	البعد
%100	مراجعة بطاقات الخدمات والنصوص	نسبة الخدمات المرتبطة بسند قانوني محين	الشرعية
ارتفاع سنوي	اختبار أحداث الحياة	نسبة الإجراءات المنجزة من البداية إلى الأثر النهائي رقمياً	الاكتمال
%100 للوثائق ذات الأثر	اختبار التوقيع والختم والبصمة	نسبة القرارات والوثائق القابلة للتحقق إلكترونياً	الحجية
%100	تدقيق عينات وسجلات	نسبة الطلبات التي تتوفر على وصل وحساب أجل آلي صحيح	الآجال
أقل مدة قانونية ممكنة	قياس من الطلب إلى التنفيذ	متوسط مدة تصحيح البيانات المؤثرة	التصحيح
قرب الصفر وخطة تعويض	سجل الأعطال والحوادث	مدة توقف الخدمات الحرجة وعدد الحقوق المتأثرة	الاستمرارية
%100	تدقيق القرارات وواجهات التظلم	نسبة القرارات الرقمية المعللة والقابلة للطعن	الشفافية

1 اللجنة الخاصة بالنموذج التنموي، النموذج التنموي الجديد: تحرير الطاقات واستعادة الثقة لتسريع وتيرة التقدم وتحقيق الرفاه للجميع، الرباط، أبريل 2021، ص. 107-111.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

الهدف	طريقة القياس	المؤشر المقترح	البعد
تقليص الفجوة سنويا	بيانات مجهولة ومسوحات مستخدمين	الفارق في نسبة النجاح حسب المجال والفئة	الإدماج

المصدر: اقتراح الباحث.

الجدول رقم 7: خارطة تنفيذ مرحلية لتعزيز الأمن القانوني الرقمي

المخرجات القابلة للتحقق	الجهات المحورية	الإجراءات ذات الأولوية	المرحلة
سجل وطني للخدمات وبطاقات امتثال ومؤشرات أولية	رئاسة الحكومة والقطاعات والسلطات التنظيمية	جرد الخدمات ذات الأثر، توحيد الوصولات، سجل الأعطال، نشر السند القانوني، قناة تصحيح	قصيرة المدى: 0–12 شهراً
منصة تحقق موحدة وسجلات مترابطة وتقارير تدقيق	الوزارة المكلفة بالانتقال الرقمي، DGSSI، CNDP، ADD	تشغيل بيني للبيانات المرجعية، تعميم خدمات الثقة، أرشفة موثوقة، تدقيق قانوني تقني	متوسطة المدى: 1–3 سنوات
مؤشر وطني للأمن القانوني الرقمي وتقييم مستقل دوري	السلطة التشريعية والقضائية والتنفيذية وأجهزة الرقابة	حكومة استباقية، حوكمة الخوارزميات، نصوص مدمجة زمنياً، قياس الثقة والعدالة الرقمية	بعيدة المدى: 3–5 سنوات

المصدر: تركيب الباحث في ضوء القوانين والاستراتيجيات والتقارير محل الدراسة.

خاتمة

خلصت الدراسة إلى أن الرقمنة تعزز الأمن القانوني من خلال أربع وظائف مترابطة: توسيع الوصول إلى القاعدة والمعلومة، وتوحيد المسطرة والآجال، وتقوية حجية الوثيقة والمعاملة، وإنشاء أثر يسمح بتتبع القرار ومراجعته. وقد أرسى المشرع المغربي أساسا مهما لهذه الوظائف عبر منظومة التبادل الإلكتروني وخدمات الثقة وحماية المعطيات والأمن السيبراني والحق في المعلومات وتبسيط المساطر وميثاق المرافق العمومية.

غير أن النصوص لا تنتج أثرها تلقائيا؛ إذ قد ينتقل الخلل من غياب القاعدة إلى تشتتها، ومن ضياع الورقة إلى تعارض قواعد البيانات، ومن غموض القرار إلى غموض الخوارزمية، ومن انقطاع الشباك إلى انقطاع المنصة. لذلك لا يقاس التحول

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

بعدد المواقع والحسابات، بل باكتمال الإجراء، وصحة البيانات، وثبات الزمن القانوني، وقابلية التحقق من الوثيقة، وفعالية التصحيح والطعن.

ويتأكد أن الأمن القانوني الرقمي مفهوم متعدد الأبعاد يجمع الشرعية والإتاحة والوضوح والثبات والحجية والتتبع والمراجعة والإدماج. وهو يلزم المصمم التقني بفهم الاختصاص والأجل والتعليل، كما يلزم القانوني بفهم الهوية الرقمية والتوقيع والختم والسجلات والأمن السيبراني. ومن دون هذا التكامل قد تعمل المنصة بكفاءة تقنية بينما تنتج قرارا هشا من الناحية القانونية.

وبناء على ذلك، توصي الدراسة بتقييم أثر قانوني رقمي قبل إطلاق الخدمات ذات الأثر، وتوحيد بطاقة الامتثال، وإنشاء سجل رسمي للنسخ القانونية والمساطر، واعتماد معرفات ووصولات قابلة للتحقق، وتنظيم آثار الأعطال، وتعميم التشغيل البيني وخدمات الثقة، وتدقيق الأنظمة الخوارزمية، وحماية حق التصحيح والمراجعة البشرية، ونشر مؤشرات للأمن القانوني لا للاستخدام وحده.

كما توصي بإدماج الاستمرارية الرقمية في تنظيم المرافق العمومية حتى لا يؤدي العطل أو الحادث إلى سقوط الحق، وباعتماد سياسة أرشفة طويلة الأمد، وبإبقاء قنوات مساعدة مكافئة للفئات التي يتعذر عليها الولوج الذاتي. ويجد هذا التوجه سنده في ميثاق المرافق العمومية الذي يربط الأداء بالجودة والشفافية والاستمرارية والمساءلة.1

وفي المجال السيبراني، ينبغي أن تتجاوز الاستجابة للحادث احتواء الاختراق إلى تحديد الآثار القانونية، وإخطار المتضررين، وتصحيح السجلات، وحماية الآجال والوثائق. وقد نظم القانون رقم 05.20 التدقيق والتكوين والتوعية والعقوبات والتعاون؛ ويبقى المطلوب وصل هذه الضوابط بخطط عملية لاستمرار الحقوق والخدمات.2

وخلاصة الأمر أن الرقمنة المحققة للأمن القانوني ليست الأسرع فحسب، بل الأكثر وضوحا وقابلية للتحقق والمراجعة. فهي لا تحل محل القانون، وإنما تعيد تجسيده داخل بنية معلوماتية. وكلما كان السند واضحا، والبيان صحيحا، والسجل سليما، والقرار معللا، والبديل متاحا، تحولت التقنية من مصدر محتمل للغموض إلى بنية مؤسسية للثقة وسيادة القانون.

1 .القانون رقم 54.19 بمثابة ميثاق المرافق العمومية، مرجع سابق، ص. 789-790، المواد 21 إلى 27.
2 .القانون رقم 05.20 المتعلق بالأمن السيبراني، مرجع سابق، ص. 1299-1300، المواد 43 إلى 52.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

المراجع والمصادر

أولا: النصوص الدستورية والتشريعية والتنظيمية

1. دستور المملكة المغربية لسنة 2011، الظهير الشريف رقم 1.11.91، الجريدة الرسمية عدد 5964 مكرر، 30 يوليوز 2011.

2. القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، الجريدة الرسمية عدد 5584، 6 دجنبر 2007.

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

4. القانون رقم 31.13 المتعلق بالحق في الحصول على المعلومات، الجريدة الرسمية عدد 6670، 3 ماي 2018.

5. القانون رقم 55.19 المتعلق بتبسيط المساطر والإجراءات الإدارية، الجريدة الرسمية عدد 6866، 19 مارس 2020.

6. القانون رقم 05.20 المتعلق بالأمن السيبراني، الجريدة الرسمية عدد 6906، 6 غشت 2020.

7. القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية، الجريدة الرسمية عدد 6970، 18 مارس 2021.

8. القانون رقم 54.19 بمثابة ميثاق المرافق العمومية، الجريدة الرسمية عدد 7106، 7 يوليوز 2022.

9. المرسوم رقم 2.21.406 الصادر في 15 شتنبر 2021 بتطبيق القانون رقم 05.20 المتعلق بالأمن السيبراني.

10. المرسوم رقم 2.22.687 الصادر في 21 نونبر 2022 بتطبيق القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية.

ثانيا : الكتب والمراجع العامة

11. العياشي، يونس، الأمن القانوني والقضائي وأثرهما في التنمية الاقتصادية والاجتماعية، الطبعة الأولى، مكتبة دار السلام، الرباط، 2012.

12. Fuller, Lon L., The Morality of Law, revised edition, Yale University Press, New Haven, 1969.

13. Raz, Joseph, The Authority of Law: Essays on Law and Morality, Oxford University Press, Oxford, 1979.

14. Roubier, Paul, Le droit transitoire (Conflits des lois dans le temps), 2e éd., Dalloz et Sirey, Paris, 1960.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

15. Eubanks, Virginia, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, St. Martin's Press, New York, 2018.

ثالثا : الكتب والمراجع المتخصصة

16. إبراهيم، خالد ممدوح، إبرام العقد الإلكتروني: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2006.

17. جميعي، حسن عبد الباسط، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، القاهرة، 2000.

18. حجازي، عبد الفتاح بيومي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، 2005.

19. منصور، محمد حسين، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، 2010.

20. Anderson, Ross, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed., Wiley, Indianapolis, 2020.

21. Bygrave, Lee A., Data Privacy Law: An International Perspective, Oxford University Press, Oxford, 2014.

22. Lynskey, Orla, The Foundations of EU Data Protection Law, Oxford University Press, Oxford, 2015.

23. Mason, Stephen, and Daniel Seng (eds.), Electronic Evidence and Electronic Signatures, 5th ed., University of London Press, London, 2021.

رابعا : المقالات والدراسات المحكمة

24. أعتاب، أمينة، «الإطار القانوني لحماية المعطيات الشخصية كمدخل لتنمية الإدارة الرقمية بالمغرب»، النداء التربوي، العددان 29-30، 2022، ص. 80 وما بعدها.

25. ختام، محمد، «التحول الرقمي بالإدارة المغربية: بحث في آليات الإسناد»، مجلة الباحث للدراسات والأبحاث القانونية والقضائية، العدد 40، 2022، ص. 85 وما بعدها.

26. رزوق، وفاء، «التحول الرقمي والتوقيع الإلكتروني في الإدارة العمومية المغربية: دور القاضي الإداري في حل النزاعات»، مجلة جامعة فزان العلمية، عدد خاص بالمؤتمر، 2025، ص. 747-768.

27. Bannister, Frank, and Regina Connolly, "ICT, Public Values and Transformative Government: A Framework and Programme for Research,"

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

,Government Information Quarterly, vol. 31, no. 1, 2014, pp. 119-128 .doi:10.1016/j.giq.2013.06.002

Bannister, Frank, and Regina Connolly, "The Trouble with Transparency: A .28 ,Critical Review of Openness in E-Government", Policy & Internet, vol. 3, no. 1 .article 8, pp. 1-30, doi:10.2202/1944-2866.1076 ,2011

Bovens, Mark, and Stavros Zouridis, "From Street-Level to System-Level .29 ,Bureaucracies", Public Administration Review, vol. 62, no. 2, 2002, pp. 174-184 .doi:10.1111/0033-3352.00168

Citron, Danielle Keats, "Technological Due Process", Washington University .30 .Law Review, vol. 85, no. 6, 2008, pp. 1249-1313

Coglianese, Cary, and David Lehr, "Regulating by Robot: Administrative .31 .Decision Making in the Machine-Learning Era", Georgetown Law Journal, vol .pp. 1147-1223 ,2017 ,105

Cordella, Antonio, and Niccolò Tempini, "E-government and Organizational .32 ,Change", Government Information Quarterly, vol. 32, no. 3, 2015, pp. 279-286 .doi:10.1016/j.giq.2015.03.005

Duranti, Luciana, and Allison Stanfield, "Authenticating Electronic .33 Evidence", in Stephen Mason and Daniel Seng (eds.), Electronic Evidence and .Electronic Signatures, 5th ed., University of London Press, 2021, pp. 236-278

Gil-Garcia, J. Ramon, Sharon S. Dawes and Theresa A. Pardo, "Digital .34 Government and Public Management Research: Finding the Crossroads", Public ,Management Review, vol. 20, no. 5, 2018, pp. 633-646 .doi:10.1080/14719037.2017.1327181

Janowski, Tomasz, "Digital Government Evolution: From Transformation to .35 .Contextualization", Government Information Quarterly, vol. 32, no. 3, 2015, pp .doi:10.1016/j.giq.2015.07.001 ,236-221

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

36. Mathieu, Bertrand, "France / Constitution et sécurité juridique", Annuaire international de justice constitutionnelle, vol. 15, 2000, pp. 155-192, doi:10.3406/aijc.2000.1551.

37. Peeters, Rik, and Arjan Widlak, "The Digital Cage: Administrative Exclusion through Information Architecture", Government Information Quarterly, vol. 35, no. 2, 2018, pp. 175-183, doi:10.1016/j.giq.2018.02.003.

38. Soûlas de Russel, Dominique J. M., et Philippe Raimbault, "Nature et racines du principe de sécurité juridique : une mise au point", Revue internationale de droit comparé, vol. 55, no. 1, 2003, pp. 85-103, doi:10.3406/ridc.2003.5561.

39. Yeung, Karen, "Algorithmic Regulation: A Critical Interrogation", Regulation & Governance, vol. 12, no. 4, 2018, pp. 505-523, doi:10.1111/rego.12158.

خامساً: التقارير والدراسات الوطنية

40. المجلس الاقتصادي والاجتماعي والبيئي، نحو تحول رقمي مسؤول ومدمج، الرباط، 2021.

41. المجلس الاقتصادي والاجتماعي والبيئي، الحوسبة السحابية: رافعة أساسية للتحول الرقمي، الرباط، 2023.

42. المجلس الأعلى للحسابات، تقييم الخدمات العمومية على الخط، الرباط، ماي 2019.

43. المجلس الأعلى للحسابات، التقرير السنوي برسم 2023-2024، الرباط، 2025.

44. المديرية العامة لأمن نظم المعلومات، الاستراتيجية الوطنية للأمن السيبراني 2030، الرباط، 2024.

45. اللجنة الخاصة بالنموذج التنموي، النموذج التنموي الجديد، الرباط، أبريل 2021.

46. وزارة الانتقال الرقمي وإصلاح الإدارة، استراتيجية المغرب الرقمي 2030، الرباط، 2024.

سادساً: التقارير والمعايير والوثائق الدولية والمقارنة

47. Conseil d'État, Sécurité juridique et complexité du droit, Rapport public 2006, La Documentation française, Paris, 2006.

48. Conseil constitutionnel français, Décision n° 99-421 DC du 16 décembre 1999.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

Council of Europe, Framework Convention on Artificial Intelligence and .49
,Human Rights, Democracy and the Rule of Law, CETS No. 225, Strasbourg
.2024

,OECD, Recommendation of the Council on Digital Government Strategies .50
.OECD/LEGAL/0406, Paris, 2014

,OECD, Digital Government Review of Morocco, OECD Publishing, Paris .51
.2018

OECD, The OECD Digital Government Policy Framework, OECD Public .52
.Governance Policy Papers, no. 02, Paris, 2020

OECD, The E-Leaders Handbook on the Governance of Digital .53
.Government, OECD Publishing, Paris, 2021

,OECD, Open Government Review of Morocco 2024, OECD Publishing .54
.Paris, 2024

,Regulation (EU) No 910/2014 on electronic identification and trust services .55
.OJ L 257, 28 August 2014

Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4 .56
.May 2016

Regulation (EU) 2024/1183 establishing the European Digital Identity .57
.Framework, OJ L, 30 April 2024

Regulation (EU) 2024/1689 laying down harmonised rules on artificial .58
.intelligence, OJ L, 12 July 2024

UNCITRAL, Model Law on Electronic Commerce with Guide to Enactment .59
.United Nations, New York, 1999 ,1996

UNCITRAL, Model Law on Electronic Signatures with Guide to Enactment .60
.United Nations, New York, 2002 ,2001

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/

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

62. United Nations, E-Government Survey 2024, New York, 2024.

63. World Bank, GovTech Maturity Index 2022 Update, Washington, D.C., 2023.

© المؤلفون. مرخص بموجب Creative Commons Attribution-Non Commercial 4.0 (CC BY-NC 4.0) — يُسمح بإعادة الاستخدام غير التجاري مع نسبة المصدر
https://creativecommons.org/licenses/by-nc/4.0/