مداخلة للمشاركة في ملتقى "أثر التوثيق الرقمي في ترقية قطاع المعاملات العقارية في الجزائر"

عنوان المداخلة: "التوثيق الإلكتروني في الجزائر: التحديات العملية لتأمين البيانات وضمان خصوصية المستخدمين"

الدكتورة فاضل عائشة

دكتوراه قانون خاص

جامعة التكوين المتواصل –تبسة

Misaichamsdk12@gmail.com

باحثة الدكتوراه صوار إكرام

دكتوراه قانون عام

جامعة البليدة -2-العفرون على لونيسي

souarikram2022@gmail.com

الملخص

التوثيق الإلكتروني في الجزائر يشكل نقلة نوعية نحو تحديث الإدارة والخدمات القانونية، لكنه يواجه تحديات عملية جوهرية تتمثل في ضعف البنية التحتية للأمن السيبراني، وتشتت الصلاحيات بين الجهات المعنية، ونقص التكوين المتخصص للعاملين، مما يعرقل تأمين البيانات وحماية خصوصية المستخدمين، رغم وجود إطار قانوني متطور نسبياً والسلطة الوطنية لحماية المعطيات الشخصية، إلا أن غياب آليات تنفيذ فعالة وبنية تحتية مؤمنة يعوق بناء ثقة رقمية كاملة، لتعزيز التوثيق الإلكتروني، لا بد من توحيد الجهود المؤسسية، تطوير التشريعات، ورفع كفاءة الكوادر التقنية والقانونية لضمان حماية فعالة ومستدامة للبيانات والحقوق الرقمية.

الكلمات المفتاحية: الأمن السيبراني، حماية البيانات، التوثيق الرقمي، الخصوصية الرقمية، التشريع الإلكتروني

Abstract

Electronic documentation in Algeria represents a qualitative leap towards modernizing administration and legal services, However it faces significant practical challenges, including weak cyber security infrastructure, fragmented responsibilities among relevant authorities, and a lack of specialized training for personnel, These issues hinder data security and the protection of user privacy, Despite the existence of a relatively advanced legal framework and the National Authority for the Protection of Personal Data, the absence of effective

enforcement mechanisms and secure infrastructure obstructs the establishment of full digital trust, To strengthen electronic documentation, institutional efforts must be unified, legislation developed, and the technical and legal workforce's competence enhanced to ensure effective and sustainable protection of data and digital rights.

Keywords: Cyber security, Data Protection, Digital Documentation, Digital Privacy, Electronic Legislation

مقدمة

لم يعد النقاش حول الرقمنة مجرّد ترف معرفي أو خيارًا مؤجّلًا، بل أصبح في صلب أولويات الدول والمؤسسات التي تسعى إلى تحقيق الفعالية، الشفافية، وسرعة الأداء في ظل التحولات العميقة التي فرضتها الثورة الرقمية. وقد امتد هذا التحوّل ليشمل مختلف القطاعات، وعلى رأسها المجال القانوني والإداري، باعتبارهما من أكثر الميادين ارتباطًا بمصالح الأفراد والجماعات، وأكثرها حاجة إلى التحديث ومواكبة العصر، من هنا برز مفهوم التوثيق الإلكتروني كبديل متطوّر للتوثيق الورقي التقليدي، يفتح آفاقًا جديدة في تسيير المعاملات، حفظ الوثائق، وتقديم الخدمات القانونية والإدارية.

التوثيق الإلكتروني لا يقتصر فقط على تحويل الوثيقة من صيغة ورقية إلى رقمية، بل هو منظومة متكاملة تقوم على أسس قانونية، تقنية، ومؤسساتية، تضمن سلامة المعاملة، حجية الإثبات، وحماية الحقوق. فالتحول الرقمي في هذا المجال يتيح مزايا نوعية، أهمها: تسريع الإجراءات، تقليص التكاليف، تقليل هامش الخطأ البشري، وإتاحة الوصول السهل إلى البيانات. كما يساهم في دعم الشفافية الإدارية ومحاربة الفساد، من خلال تقليل التماس المباشر بين المواطن والإدارة، غير أن هذا التحول لا يخلو من تعقيدات، أبرزها: التحديات القانونية المتعلقة بحجية الوثائق الإلكترونية، سلامة التوقيع الرقمي، أمن المعلومات، وحماية المعطيات الشخصية، في ظل هذا الواقع تسعى الدول إلى مواءمة تشريعاتها مع التطورات التقنية، ووضع أطر تنظيمية تضمن سلامة المعاملات الرقمية وتحمي الحقوق والحريات. وقد شهدت العديد من الأنظمة القانونية المتقدمة تطورات كبيرة في مجال التوثيق الإلكتروني، عبر إقرار قوانين متخصصة للتوقيع الإلكتروني، وإنشاء هيئات اعتماد رقمية، وتطوير آليات المصادقة والتصديق، في حين ما تزال بعض الدول النامية، ومنها الجزائر، تتلمّس طريقها نحو إنشاء بيئة رقمية آمنة ومتجانسة، رغم المبادرات المتعددة التي أطلقتها ، في الجزائر تنبّه المشرّع منذ سنوات إلى ضرورة إدماج التكنولوجيات الحديثة ضمن البنية القانونية

والإدارية، فصدرت عدة قوانين ذات صلة، مثل القانون رقم 18-05 المتعلق بالتجارة الإلكترونية[1]، والقانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، بالإضافة إلى بعض المراسيم التنفيذية التي تؤطر التوقيع والتصديق الإلكترونيين، كما تم استحداث منصات رقمية لإيداع الملفات الإدارية، وتعميم استخدام البريد الإلكتروني الرسمي، وغيرها من المبادرات التي تهدف إلى تحديث الإدارة وتحسين جودة الخدمات العمومية ، ورغم هذه الجهود، إلا أن الواقع العملي يُظهر أن الجزائر ما تزال تواجه تحديات هيكلية ومعوقات تطبيقية تحول دون تحقيق الانتقال الرقمي الفعلي، وخصوصًا في مجال التوثيق الإلكتروني، من بين هذه التحديات: ضعف البنية التحتية الرقمية، محدودية الوعي القانوني لدى الفاعلين، نقص التكوين في المجالين التقني والقانوني، غياب إطار مؤسساتي واضح لحوكمة البيانات الرقمية، وتردد المواطن في الثقة بالتقنيات الجديدة نتيجة ضعف الضمانات المتعلقة بالأمن السيبراني، كما أن هناك إشكاليات قانونية غير محسومة، مثل مدى حجية المحررات الرقمية أمام القضاء، والمسؤولية القانونية في حالة اختراق أو تسريب البيانات.

أمام هذا الواقع، تُطرح الحاجة الملحة إلى تقييم شامل لمدى نجاعة البيئة القانونية والمؤسساتية في الجزائر فيما يخص التوثيق الإلكتروني، من خلال تحليل التشريعات القائمة، ورصد أوجه النقص والثغرات، والبحث عن السبل الكفيلة بتحقيق التوازن بين التقدّم الرقمي وحماية الحقوق، خصوصًا في ظل التزامات الجزائر الدولية في مجال حماية البيانات، ومعايير الأمن الرقمي التي تفرضها الاتفاقيات والمنظمات العالمية.

انطلاقًا من ذلك، تسعى هذه المداخلة إلى معالجة الإشكالية التالية: **إلى أي مدى تمكنت الجزائر من توفير بيئة رقمية آمنة وموثوقة للتوثيق الإلكتروني، تضمن حماية البيانات الشخصية وخصوصية المستخدمين، وتواكب متطلبات العصر الرقمي؟**

إن البحث في هذا الموضوع يكتسي أهمية بالغة، ليس فقط من حيث راهنيته، بل لما له من أثر مباشر على فعالية المنظومة القانونية والإدارية، وعلى ثقة المواطن في مؤسسات الدولة، وعلى قدرة الجزائر في الانخراط الجاد ضمن المنظومة الرقمية العالمية التي لم تَعُد تعترف إلا بالأنظمة المرنة، المحمية، والمتكيّفة مع متطلبات الأمان القانوني والرقمي.

<u>تم تقسيم المداخلة الى محورين:</u>

- ✓ **المحور الأول: الإطار القانوني والمؤسساتي للتوثيق الإلكتروني في الجزائر**
- ➢ **المحور الثاني: التحديات التقنية والعملية لتأمين البيانات وضمان خصوصية المستخدمين في منظومات التوثيق الرقمي**

[1]قانون رقم 18-05 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 ، يتعلق بالتجارة الإلكترونية ، ج ر عدد28

✓ المحور الأول: الإطار القانوني والمؤسساتي للتوثيق الإلكتروني في الجزائر

يُعتبر وجود إطار قانوني ومؤسساتي متكامل شرطًا أساسيًا لنجاح أي سياسة رقمية، خصوصًا عندما يتعلق الأمر بالتوثيق الإلكتروني، الذي يلامس الجوانب الحساسة للمعاملات القانونية والإدارية فالتحول من التوثيق الورقي إلى الرقمي يتطلب قواعد واضحة تضمن الشرعية، المصداقية، والحجية القانونية للمحررات الإلكترونية، إلى جانب مؤسسات قادرة على تنفيذ هذه القواعد وضمان احترامها.

في الجزائر حاول المشرّع مواكبة هذا التحول من خلال إصدار عدد من القوانين والتنظيمات ذات الصلة، على غرار قانون التجارة الإلكترونية (18-05) والقانون المتعلق بحماية المعطيات ذات الطابع الشخصي (18-07)[2]، بالإضافة إلى مراسيم تنفيذية تنظّم التوقيع والتصديق الإلكترونيين، كما تم استحداث هيئات ومؤسسات تُعنى بتنظيم ومراقبة هذا المجال، غير أن هذه المنظومة ما تزال في طور البناء، وتواجه تحديات في التطبيق والتنسيق.

أولًا: الأساس التشريعي للتوثيق الإلكتروني في الجزائر

سعت الجزائر، منذ مطلع الألفية الثالثة، إلى مواكبة التحول الرقمي من خلال وضع إطار قانوني ينظّم المعاملات الإلكترونية ويضفي عليها الشرعية القانونية. وقد تم ذلك عبر مجموعة من النصوص القانونية والتنظيمية التي تشكل اليوم مرجعية مهمة في مجال التوثيق الإلكتروني.

1. قانون 15-04: الاعتراف القانوني بالتوقيع الإلكتروني[3]

يُعد القانون رقم 15-04 المؤرخ في 1 فبراير 2015، والمتعلق بالتوقيع والتصديق الإلكترونيين، حجر الأساس في تنظيم المعاملات الإلكترونية، إذ كرّس مبدأ المساواة في الحجية القانونية بين التوقيع الإلكتروني والتوقيع الخطي، شريطة احترام الشروط التقنية والأمنية المحددة قانونًا ، نص القانون صراحة على أن "كل توقيع إلكتروني يتم إنشاؤه وتوثيقه وفقًا للأحكام القانونية، له القيمة القانونية نفسها للتوقيع اليدوي"، ما يشكل خطوة متقدمة نحو الاعتراف بالوثائق الرقمية كأدلة قانونية كاملة في المعاملات المدنية والإدارية. غير أن فعالية هذا النص تبقى مرتبطة بوجود بنية تحتية تكنولوجية ومؤسساتية تسمح بالتنفيذ السليم، وهو ما لا يزال محدودًا في الممارسة الفعلية.

2. قانون 18-07: حماية المعطيات الشخصية في البيئة الرقمية

---

[2] القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي.
[3] القانون رقم 15-04 المؤرخ في 1 فبراير 2015، المتعلق بالتوقيع والتصديق الإلكترونيين.

في سياق موازٍ، أقرّ المشرع القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، والذي يمثل الإطار المرجعي لحماية الخصوصية الرقمية وضبط طرق جمع وتخزين واستعمال البيانات. وقد جاء هذا النص تماشيًا مع المعايير الدولية، خصوصًا تلك الواردة في اللائحة الأوروبية لحماية البيانات(GDPR) ، ينص القانون على مبادئ أساسية، من بينها: شرط الموافقة المسبقة، الغرض المشروع للمعالجة، وضمان أمن البيانات، وهي شروط جوهرية لضمان توثيق إلكتروني يحترم حقوق الأفراد ويمنع أي انتهاك لخصوصيتهم.

3. المرسوم التنفيذي 20-331: تعزيز الأمن السيبراني[4]

لمواكبة التهديدات الرقمية المتزايدة، أُنشئت الهيئة الوطنية للأمن السيبراني بموجب المرسوم التنفيذي رقم 20-331 المؤرخ في 22 نوفمبر 2020، لتكون الجهة الرسمية المختصة بالسهر على أمن الفضاء السيبراني الوطني، وحماية الأنظمة والمعلومات الحساسة، رغم أهمية هذه الهيئة في خلق بيئة رقمية مؤمّنة، إلا أن فعالية تدخلها في ميدان التوثيق الإلكتروني تبقى مرتبطة بمدى التنسيق بينها وبين باقي المتدخلين، خصوصًا الهيئات القضائية والإدارية، وهو ما لا يزال يفتقر إلى التجانس المطلوب.

ثانيًا: إشكالات التنسيق المؤسساتي وتحديات التطبيق

رغم تعدد النصوص القانونية وتنوع الهيئات المعنية، إلا أن الواقع يكشف عن فجوة مؤسساتية واضحة، تتجلى في:

1. تشتت الصلاحيات وتضارب المهام

يعاني المشهد المؤسساتي في الجزائر من تداخل في الصلاحيات بين مختلف الجهات، مثل وزارة العدل، سلطة الضبط للبريد والمواصلات، والهيئة الوطنية للأمن السيبراني. هذا التشتت يؤدي إلى غياب استراتيجية وطنية موحدة للتوثيق الإلكتروني، ويحول دون تحقيق الانسجام بين الجوانب القانونية والتقنية.

2. محدودية التحقق الرقمي والتصديق الإلكتروني

لا تزال عمليات التحقق من الهوية الرقمية والتصديق على الوثائق الإلكترونية محدودة الانتشار في الجزائر، ويُعزى ذلك إلى غياب بنية تحتية رقمية موثوقة، وعدم توفر شهادات إلكترونية معترف بها بصفة رسمية وواسعة النطاق، ما يجعل من الصعب تعميم التوثيق الإلكتروني على المعاملات الإدارية والقضائية.

---

[4] المرسوم التنفيذي رقم 20-331 المؤرخ في 22 نوفمبر 2020، المتعلق بإنشاء الهيئة الوطنية للأمن السيبراني وتحديد صلاحياتها.

3. غياب نظم موحدة لإدارة الوثائق الإلكترونية

إضافة إلى ما سبق، فإن العديد من الإدارات والمؤسسات العمومية لم تعتمد بعد نظم إدارة الوثائق الإلكترونية (GED) بشكل كامل، نتيجة لذلك تُترك مهمة تأمين الوثائق والبيانات لاجتهادات داخلية قد تفتقر إلى المعايير الأمنية اللازمة، ما يعرض المعطيات للضياع أو الاختراق، ويُضعف ثقة المواطن في المنظومة الرقمية برمّتها.

يتّضح من خلال هذا التحليل أن الإطار القانوني في الجزائر يشكل خطوة إيجابية نحو تنظيم التوثيق الإلكتروني، من خلال الاعتراف بالتوقيع الرقمي، وتوفير الحماية القانونية للبيانات الشخصية، وتأسيس مؤسسات تُعنى بالأمن الرقمي، إلا أن ضعف التنسيق المؤسساتي، محدودية البنية التحتية، ونقص التفعيل العملي لهذه القوانين، يشكّل عائقًا حقيقيًا أمام تحقيق توثيق إلكتروني فعّال وآمن في السياق الجزائري.

المحور الثاني: التحديات التقنية والعملية لتأمين البيانات وضمان خصوصية المستخدمين في منظومات التوثيق الرقمي

مع تزايد الاعتماد على التوثيق الرقمي في المعاملات الإدارية والقانونية، برزت الحاجة الملحة إلى توفير بيئة رقمية آمنة تضمن حماية البيانات الشخصية وخصوصية المستخدمين، إذ لا تقتصر فعالية التوثيق الإلكتروني على الجوانب القانونية والتنظيمية فحسب، بل تعتمد بشكل كبير على مدى جاهزية البنية التحتية التقنية، وكفاءة الوسائل المعتمدة في حماية المعلومات وتسييرها[5].

في السياق الجزائري، ورغم الخطوات التشريعية المتخذة، إلا أن الواقع الميداني يكشف عن عدد من التحديات التقنية والعملية التي تعرقل التفعيل السليم لمنظومات التوثيق الرقمي، من بين هذه التحديات: ضعف أنظمة الأمن السيبراني، غياب منصات رقمية موثوقة وشاملة، محدودية استخدام التوقيع الإلكتروني، بالإضافة إلى نقص التكوين لدى الموارد البشرية المكلفة بإدارة هذه المنظومات.

يُعد تأمين المعطيات الرقمية وحماية خصوصية المستخدمين من أبرز ركائز بناء الثقة في منظومات التوثيق الإلكتروني، ذلك أن القيمة القانونية لأي وثيقة رقمية لا تستمد مشروعيتها من نص القانون فقط، بل كذلك من سلامتها التقنية وسرية محتواها، وعدم تعرّضها لأي تعديل غير مشروع أو اختراق خارجي، في الجزائر ورغم صدور عدة نصوص قانونية تُؤسس لمشروعية التوثيق الإلكتروني، إلا أن التطبيق العملي يواجه

[5] براهي خليل ممدوح، التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2010، ص 63.

تحديات تقنية ومؤسساتية تهدد مصداقية الوثائق الرقمية، وتُضعف من أثر الحماية القانونية المنصوص عليها نظرياً.

1. ضعف البنية التحتية للأمن السيبراني في المؤسسات العمومية

يُعتبر الأمن السيبراني الضمانة الأساسية لسلامة الوثائق الرقمية، غير أن الممارسة تكشف عن ضعف كبير في المنظومات الأمنية المعلوماتية لدى عدد من المؤسسات العمومية الجزائرية، فهذه المؤسسات، التي من المفترض أن تكون حاضنة لمعاملات قانونية موثقة إلكترونيًا، لا تتوفر على أنظمة متخصصة لرصد التهديدات السيبرانية أو منع التلاعب بالبيانات ، هذا الخلل ينعكس بشكل مباشر على شرط الحماية التقنية الذي يفترضه القانون 15-04[6] المتعلق بالتوقيع والتصديق الإلكترونيين، والذي ربط الاعتراف القانوني بالوثيقة الإلكترونية بمدى احترامها للمعايير التقنية المتعلقة بالسرية، التكامل، وعدم الإنكار، إن عدم توفر وسائل فعالة للكشف عن أي خرق أو تعديل في الوثائق يُضعف من حجيتها أمام القضاء ويُعقّد من إجراءات الإثبات، خاصة في غياب جهات مختصة قادرة على تقديم تقارير تقنية معتمدة حول مدى صحة الوثائق الرقمية.

2. غياب الثقافة الرقمية داخل الهيئات الإدارية والقانونية

لا يقتصر الضعف في منظومة التوثيق الإلكتروني على الجوانب التقنية فحسب، بل يمتد ليشمل العنصر البشري، إذ أن العديد من الموظفين والموثقين لا يتوفرون على تكوين كافٍ في التعامل مع الأنظمة الرقمية أو إدارتها وفق معايير الأمان المعتمدة ، هذا النقص في الثقافة الرقمية يؤدي إلى وقوع أخطاء بشرية جسيمة، من قبيل: تخزين الوثائق على وسائط غير آمنة، استخدام كلمات مرور ضعيفة، أو مشاركة بيانات حساسة دون اعتماد بروتوكولات مشفّرة ، هذه السلوكات وإن بدت بسيطة، قد تشكل في نظر القانون إخلالاً بمبدأ الحيطة والحذر الواجب توفره في كل من يتولى حفظ أو إدارة وثائق ذات طابع قانوني، كما أنها تُعرّض الجهات المعنية لمسؤوليات مدنية أو تأديبية في حال تسرب البيانات أو التلاعب بمحتوى الوثائق، مع صعوبة تحديد المسؤولية بدقة بسبب غياب نظام رقمي يوثّق العمليات التي تتم على كل وثيقة.

3. الاعتماد على تقنيات رقمية أجنبية: تهديد للسيادة المعلوماتية

في غياب صناعة رقمية محلية متطورة، تلجأ بعض المؤسسات الجزائرية إلى الاعتماد على حلول تكنولوجية أجنبية لمعالجة البيانات أو حفظ الوثائق، وهو ما يطرح إشكالية السيادة الرقمية وحماية المعطيات الوطنية من الناحية القانونية، يُعد هذا الاعتماد مصدر تهديد مباشر للحقوق المحمية بموجب القانون رقم 18-07

[6] المادة 11 القانون 15-04 المؤرخ 2015/02/01 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني

المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، لا سيما في حالة تخزين البيانات على خوادم خارج الإقليم الوطني فالمادة 44 من هذا القانون تُقيّد إمكانية نقل البيانات إلى الخارج بشروط صارمة، أهمها توفر مستوى حماية مماثل، والحصول على ترخيص مسبق من السلطة الوطنية المختصة، وهي شروط كثيرًا ما تُغفل في الواقع العملي.

4. غموض في إثبات المسؤولية القانونية عن التسريبات الرقمية

من الإشكاليات القانونية التي تُثيرها حالات اختراق أو تسرب الوثائق الرقمية الموثقة، هو عدم وضوح المسؤولية القانونية، لا سيما إذا كانت الوثيقة قد مرت بعدة أطراف أو مخزّنة على منصات خارجية، فالقانون الجزائري رغم اعترافه بالمحررات الإلكترونية، لا يقدّم بعد تصورًا متكاملًا حول كيفية تحديد الطرف المسؤول عن فشل في تأمين الوثيقة، أو المعايير التي يتم بموجبها تحميله المسؤولية ، هذه الثغرة تتطلب تدخلًا تشريعيًا أو تنظيميًا لتحديد المسؤوليات بدقة، سواء في مواجهة الإدارة، أو موفّري الخدمة الرقمية، أو حتى الأطراف الخاصة المعنية بالمعاملة[7].

5. قصور في التكوين المتخصص في الأمن الرقمي

يتأكد من خلال التقييم الواقعي أن الكوادر الإدارية والقانونية في الجزائر لا تتلقى تكوينًا كافيًا ومنتظمًا في مجال الأمن الرقمي، رغم حساسية المهام التي يتولونها، ويُشكّل هذا الضعف أحد العوامل الرئيسية في هشاشة منظومة التوثيق الإلكتروني، إذ لا يمكن ضمان سلامة العمليات الرقمية دون موارد بشرية متمكنة من الأدوات التقنية، وقادرة على التصرف عند وقوع اختراق أو تسرب أو خلل في الأنظمة ، القانون وحده لا يكفي ما لم يتم ترجمته إلى ممارسة مهنية تعتمد الكفاءة والجاهزية التقنية، وهو ما يقتضي إقرار برامج وطنية للتكوين المستمر، بشراكة بين وزارة العدل، وزارة الرقمنة، والهيئات التقنية المختصة، كسلطة ضبط البريد والمواصلات، والهيئة الوطنية للأمن السيبراني.

إن التحديات التقنية والعملية التي تواجه منظومة التوثيق الرقمي في الجزائر لا تنفصل عن الإطار القانوني المنظّم لها، بل تكشف حدود النص التشريعي حين لا يقترن ببيئة مؤسساتية قوية، وبنية تحتية مؤمنة، وموارد بشرية مؤهلة، ويتطلب الوضع الراهن مقاربة تكاملية، تُعزّز التنسيق بين الفاعل القانوني والتقني، وتُكرّس ثقافة رقمية راسخة داخل الإدارة، مع توفير ضمانات حقيقية لحماية البيانات واحترام خصوصية المستخدم، وفقًا لأفضل المعايير الدولية.

---

[7] عاطف عبد الحميد حسن، التوقيع الالكتروني ، مفهومه ، صوره، حجيته في الإثبات في نطاق المعاملات المدنية، دار النهضة العربية، القاهر ، 9 ،ص 70

في ضوء التطور المتسارع الذي يشهده العالم في مجال الرقمنة القانونية، تظهر أهمية بناء منظومة توثيق إلكتروني تتسم بالكفاءة، الشفافية، والحماية القانونية والتقنية، بما يضمن انخراط الدولة في بيئة رقمية تتماشى مع التزاماتها الدستورية والدولية في حماية الحقوق الأساسية للأفراد، وعلى رأسها الحق في حماية الحياة الخاصة وسرية البيانات، ويُفترض في هذا السياق أن يكون الإطار القانوني، بمختلف مكوناته، مرآة واضحة تعكس فلسفة الدولة في الانتقال الرقمي، من خلال بناء قواعد قانونية واضحة، ومؤسسات فاعلة قادرة على مواكبة التحديات التي يفرضها هذا الانتقال.

وفي التجربة الجزائرية، تبيّن أن المنظومة القانونية، رغم تطورها النسبي في السنوات الأخيرة، لا تزال تعاني من ثغرات متعددة على مستوى الإحاطة الشاملة بالمعاملات الرقمية، وخصوصًا تلك المتعلقة بالتوثيق الإلكتروني، فقد تميّز القانون رقم 15-04 بوضع أساس قانوني للاعتراف بالتوقيع والتصديق الإلكترونيين، مكرّسًا بذلك مبدأ المساواة في الحجية القانونية بين التوقيع الرقمي والتوقيع الخطي، شرط احترام الضوابط التقنية المنصوص عليها. إلا أن هذا الاعتراف، وإن شكّل تطورًا تشريعيًا مهمًا، لم يصاحبه تحديد دقيق للآليات العملية التي تضمن التحقق الفعلي من صحة الوثيقة الرقمية، أو كيفية الطعن في صحتها عند حدوث نزاع، ما يجعل من هذا الاعتراف القانوني إطارًا نظريًا في كثير من الأحيان، غير مدعوم بضمانات تطبيقية كافية.

وفي سياق موازٍ، يُعدّ القانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي إطارًا مرجعيًا لحماية خصوصية المستخدمين في البيئة الرقمية، حيث يُلزم الجهات المعنية بمعالجة البيانات باحترام مبدأ الشرعية، الغرض المشروع، الأمن، والسرية.

في إطار تعزيز الحماية القانونية للبيانات ذات الطابع الشخصي، أنشأت الجزائر السلطة الوطنية لحماية المعطيات الشخصية(ANPDP) ، بموجب القانون رقم 18-07 الصادر سنة 2018[8]، تُعد هذه الهيئة المستقلة الجهة الرسمية المكلفة بمراقبة وتطبيق التشريعات المتعلقة بحماية المعطيات الشخصية، بما في ذلك تلك المستخدمة في منظومات التوثيق الإلكتروني.

تتمثل مهام السلطة في متابعة مدى التزام مختلف الجهات، سواء كانت عمومية أو خاصة، بالقواعد القانونية التي تحكم جمع، معالجة، وتخزين البيانات الشخصية، وذلك بهدف ضمان احترام الحقوق الفردية المتعلقة

[8] شهد قانون حماية المعطيات الشخصية في الجزائر، المعروف بالقانون 18-07، تعديلات حديثة في يوليو 2025 لتعزيز حماية خصوصية الأفراد في ظل الرقمنة المتزايدة، وتضمنت هذه التعديلات فرض تعيين "مندوب لحماية البيانات" (DPO)، إلزامية الاحتفاظ بسجلات دقيقة لأنشطة معالجة البيانات والانتهاكات، إنشاء أقطاب جهوية للمراقبة داخل السلطة الوطنية لحماية المعطيات، وفرض ضوابط صارمة على النقل الدولي للبيانات.

بالخصوصية وحماية المعطيات من كل شكل من أشكال المعالجة غير المشروعة أو التعسفية. وتشمل اختصاصاتها:

- منح التراخيص والموافقات اللازمة لنقل المعطيات الشخصية إلى خارج التراب الوطني، مع التأكد من توفر معايير الحماية الملائمة في الدول المستقبلة.
- استقبال ودراسة الشكاوى التي تقدم من قبل الأفراد أو الهيئات المتضررة من انتهاكات خصوصية البيانات، واتخاذ الإجراءات المناسبة.
- إصدار التوصيات والإرشادات التقنية والقانونية التي تساعد الجهات المعنية على الامتثال للقانون، وتعزيز ثقافة حماية المعطيات.
- متابعة التطورات التقنية والتشريعية على المستويين الوطني والدولي لضمان تحديث الإطار التنظيمي بما يتلاءم مع متطلبات العصر الرقمي.

رغم هذا الدور الهام تواجه السلطة تحديات متعددة على مستوى التطبيق، أبرزها محدودية الموارد البشرية والتقنية، وضعف الوعي الرقمي لدى بعض المؤسسات، ما ينعكس على صعوبة تنفيذ مهام الرقابة بفعالية، وخاصة في ظل انتشار المعاملات الرقمية المتزايد، بالإضافة إلى ذلك، ما تزال بعض الجهات الإدارية تعتمد على نظم تقنية غير متكاملة، أو تلجأ إلى حلول أجنبية، ما يعرقل مراقبة تطبيق القانون ويضعف من قدرة السلطة على ضمان حماية حقيقية للبيانات.

بذلك تشكل السلطة الوطنية لحماية المعطيات الشخصية ركيزة أساسية في منظومة الحماية القانونية للمعطيات الرقمية، ولعب دورها بفعالية يتطلب استراتيجيات دعم متكاملة تشمل تطوير بنيتها التحتية، تعزيز التنسيق مع باقي الجهات القانونية والمؤسساتية، والتوعية المستمرة للمستخدمين والموظفين على حد سواء.

في ضوء التطور المتسارع الذي يشهده العالم في مجال الرقمنة القانونية، تظهر أهمية بناء منظومة توثيق إلكتروني تتسم بالكفاءة، الشفافية، والحماية القانونية والتقنية، بما يضمن انخراط الدولة في بيئة رقمية تتماشى مع التزاماتها الدستورية والدولية في حماية الحقوق الأساسية للأفراد، وعلى رأسها الحق في حماية الحياة الخاصة وسرية البيانات، ويُفترض في هذا السياق أن يكون الإطار القانوني، بمختلف مكوناته، مرآة واضحة تعكس فلسفة الدولة في الانتقال الرقمي، من خلال بناء قواعد قانونية واضحة، ومؤسسات فاعلة قادرة على مواكبة التحديات التي يفرضها هذا الانتقال ، ويتعمّق هذا التباين عند الانتقال من البعد القانوني إلى الجانب التطبيقي، حيث تُواجه الجزائر جملة من التحديات التقنية الجوهرية التي تمسّ بصلب مفهوم الثقة الرقمية. فالافتقار إلى بنية تحتية سيبرانية متينة لدى عدد كبير من المؤسسات العمومية، يجعلها غير قادرة على

كشف الهجمات أو التصدي لها في الوقت المناسب، وهو ما يجعل سلامة الوثائق عرضة للاختراق أو التلاعب، دون إمكانية التتبع التقني أو القانوني الدقيق للمسؤول عن ذلك، لغياب منظومة PKI وطنية، تُتيح إنشاء، توزيع، وتدبير الشهادات الرقمية المعتمدة والموثوقة ، ويُضاف إلى ذلك غياب التكوين الكافي والمتخصص في مجال الأمن الرقمي لدى العاملين في الإدارات القانونية أو لدى الموثقين، مما يُضعف قدرتهم على إدارة الوثائق الرقمية بطريقة احترافية، ويجعلهم عُرضة للوقوع في أخطاء بشرية جسيمة، قد تؤدي إلى فقدان المعطيات، أو تعريضها للتسريب غير المقصود، وهذا النقص في الكفاءة الرقمية يؤكد أن فعالية النصوص القانونية ليست مستقلة عن العنصر البشري، بل إن نجاح التوثيق الرقمي مرهون بتوافر بيئة بشرية مؤهلة ومدربة، قادرة على تفعيل الضمانات التقنية في إطار منضبط قانونيًا.

من الملاحظ كذلك، أن بعض مراحل التوثيق الرقمي في الجزائر تعتمد، بشكل جزئي أو كلي، على حلول تكنولوجية أجنبية، سواء فيما يخص منصات تخزين البيانات أو أدوات التوقيع الرقمي، ورغم أن هذا الخيار قد يكون مؤقتًا في ظل غياب بدائل محلية متطورة، إلا أنه يطرح إشكاليات سيادة معلوماتية، ويُثير تساؤلات قانونية جدية حول مدى خضوع هذه المعطيات للقانون الجزائري، لاسيما في حال وقوع نزاع أو تسرب بيانات محمية. كما أن القانون 18-07، رغم تحديده لشروط نقل البيانات إلى الخارج، لا يوفر، في شكله الحالي، آلية رقابية فعالة لمنع هذا النوع من الاعتماد الخارجي، أو مراقبة مدى امتثال الجهات المتعاملة مع أنظمة أجنبية للضوابط القانونية الوطنية.

من جهة أخرى، يبقى الجانب القضائي في التعامل مع الوثائق الرقمية أحد أهم التحديات العملية التي لم يتم الحسم فيها بعد، سواء من حيث كيفية التحقق من حجية الوثيقة الإلكترونية أمام القضاء، أو المعايير الواجب توفرها لقبولها كدليل، ففي ظل غياب نصوص تنظيمية دقيقة أو دليل قضائي معياري، تختلف الممارسات بين الجهات القضائية، ما يُفقد الوثيقة الرقمية عنصر اليقين القانوني اللازم لاعتمادها في إثبات الحقوق أو الطعن فيها.

إذا ان الهدف من التوثيق الإلكتروني هو تسريع الإجراءات، تخفيف العبء الإداري، وضمان استمرارية الخدمة القانونية، فإن هذه الأهداف تظل محدودة الأثر في غياب منظومة تشريعية متكاملة تراعي التوازن بين الأمان القانوني والتقني، وتعمل على تقليص الهوة بين الواقع والمأمول، كما أن عدم اعتماد معايير

دولية معترف بها[9]، مثل ISO/IEC 27001[10] الخاصة بإدارة أمن المعلومات، يُضعف من فرص تحقيق اعتراف دولي بحجية الوثائق الإلكترونية الجزائرية، خاصة في إطار التعاملات العابرة للحدود.

في ضوء ما سبق، يتبين أن بناء نظام توثيق رقمي فعال وآمن في الجزائر لا يمكن أن يتم بمعزل عن إصلاحات قانونية دقيقة، وتحديث هيكلي للمؤسسات المعنية، إلى جانب إدماج البعد التقني في السياسات القانونية والتشريعية ذات الصلة، إن التحديات الراهنة تُحتّم تبني سياسة عمومية رقمية مندمجة، تُحدد فيها الأدوار، وتُبنى على أسس قانونية واضحة، وتُعززها بنية تحتية سيبرانية وطنية، وتُواكبها برامج تكوين متخصصة لضمان حوكمة رشيدة وآمنة للوثيقة الرقمية.

خاتمة

في الختام، لا يمكن النظر إلى التوثيق الإلكتروني كأداة تقنية فحسب، بل يجب استيعابه كمنظومة متكاملة تستند إلى قواعد قانونية راسخة، مؤسسات متناسقة، وكفاءات مؤهلة، قادرة على بناء ثقة رقمية متينة تضمن حقوق الأفراد وحرياتهم في البيئة الرقمية الحديثة تحقيق هذه الرؤية يتطلب التزامًا وطنيًا شاملاً، واستثمارًا مستدامًا في البنية التحتية، التشريع، والموارد البشرية، لضمان استدامة منظومة توثيق رقمي وطنية آمنة وفعالة.

يتضح من خلال هذا التحليل أن التوثيق الإلكتروني في الجزائر يشكل خطوة استراتيجية نحو تحديث الإدارة وتطوير الخدمات القانونية، إلا أن تحقيق منظومة توثيق إلكتروني موثوقة وآمنة لا يزال يواجه تحديات جوهرية تعيق بلوغ الثقة الرقمية المنشودة ويمكن تلخيص أبرز النتائج في النقاط التالية:

1. **الاعتراف القانوني بالتوثيق الإلكتروني موجود لكنه نظري في غياب آليات تطبيقية واضحة:** إذ أن النصوص القانونية الجزائرية، مثل القانون رقم 15-04 والقانون رقم

[9] ISO/IEC 27001:2022, Information Security Management Systems – Requirements, International Organization for Standardization.

[10] L'ISO/CEI 27001 est une norme internationale de sécurité des systèmes d'information de l'ISO et la CEI. Publiée en octobre 2005 et révisée en 2013 puis en 2022, son titre est "Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences".

18-07، توفر الإطار التشريعي الضروري، لكنها تفتقر إلى آليات عملية دقيقة للتحقق من صحة الوثائق الرقمية وإثبات مسؤوليات الأطراف المعنية.

2. **الهيئة الوطنية لحماية المعطيات الشخصية تمثل ركيزة قانونية مهمة لكنها تواجه تحديات تنفيذية:** ضعف الموارد التقنية وضعف التنسيق مع الجهات الأخرى يحد من فاعلية مراقبة تطبيق معايير حماية البيانات، ما ينعكس سلبًا على تأمين خصوصية المستخدمين.

3. **تشتت الصلاحيات بين الجهات المعنية يضعف من فعالية الإشراف والتنسيق المؤسسي:** مما يؤخر اعتماد منظومة وطنية موحدة ومتكاملة للتوثيق الإلكتروني ويعرقل توحيد معايير الأمن السيبراني في القطاعين العام والخاص.

4. **النقص في البنية التحتية للأمن السيبراني والاعتماد على تقنيات أجنبية يهددان السيادة الرقمية وأمن الوثائق:** كما أن غياب منظومة PKI وطنية يعرقل بناء الثقة في صحة الوثائق الإلكترونية ويصعب تعقب المسؤوليات في حالات الاختراق أو التلاعب.

5. **ضعف التكوين والتوعية الرقمية للكوادر القانونية والإدارية يحد من قدرة المؤسسات على حماية البيانات وضمان سلامة التوثيق:** الأمر الذي يستدعي تعزيز برامج التكوين المستمر والرفع من مستوى الوعي بسياسات وأدوات الأمن الرقمي.

بناءً على هذه النتائج، يمكن اقتراح **التوصيات التالية** التي تعد أساسية لتطوير منظومة توثيق إلكتروني فعالة وآمنة في الجزائر:

1. **مراجعة وتطوير النصوص التشريعية والتنظيمية لتوفير آليات تطبيقية واضحة،** تحدد الإجراءات القانونية والفنية للتحقق من صحة الوثائق الرقمية، وتُعزز من وضوح المسؤوليات القانونية في حالات الاختراق أو التسرب.

2. **تعزيز دور السلطة الوطنية لحماية المعطيات الشخصية من خلال توفير الموارد التقنية والبشرية اللازمة،** وخلق آليات تعاون منتظمة مع الجهات السيادية والمؤسسات القانونية لضمان الرقابة الفعالة على معالجة البيانات.

3. **إنشاء منظومة وطنية متكاملة للتوثيق الإلكتروني تعتمد على بنية تحتية مؤمنة،** مثل نظام البنية التحتية للمفتاح العام(PKI) ، تضمن سلامة وحماية الوثائق الرقمية وتسهّل التحقق من صحتها أمام القضاء.

4. **توحيد الجهود المؤسسية بين وزارة العدل، سلطة ضبط البريد والمواصلات، الهيئة الوطنية للأمن السيبراني،** والهيئات ذات العلاقة، عبر آليات تنسيق فعالة تضمن تطبيقًا موحدًا لسياسات الأمن السيبراني وحماية المعطيات.

5. **إطلاق برامج تكوين مستمرة ومتخصصة للموثقين، القضاة، الإداريين، والكوادر التقنية،** لتعزيز مهاراتهم في التعامل مع التوثيق الرقمي وأمن المعلومات، مع التركيز على رفع مستوى الوعي بأهمية حماية الخصوصية وأمن البيانات .