

حوكمة البيانات كمدخل للتحويل الرقمي الآمن في الجزائر: دراسة تحليلية لأحكام المرسوم الرئاسي رقم 25-320

Data Governance as a Gateway to Secure Digital Transformation in Algeria: An Analytical Study of the Provisions of Presidential Decree No. 25-320



د. العلجة موسى^{*1}

كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو، (الجزائر)¹

Dr. Laldja Mouaci^{1*}

Faculty of Law and Political Science Department of Law

University of Tizi Ouzou - Algeria¹

تاريخ الاستلام: 2026/04/09 تاريخ القبول للنشر: 2026/05/15 تاريخ النشر: 2026/06/30



ملخص: تشهد الجزائر مرحلة انتقالية حاسمة نحو الدولة ما بعد الحديثة التي تعتمد في تسيير شؤونها على البيانات الضخمة والخوارزميات لتعزيز كفاءة المرافق العامة. وفي هذا الإطار صدر المرسوم الرئاسي رقم 25-320، ليضع إطارا قانونيا وتنظيميا لمنظومة وطنية متكاملة تهدف الى تنظيم وتأمين تدفق المعلومات والبيانات بين مختلف المؤسسات و الهيئات العمومية، و ذلك من خلال تصنيفها و فهرست مصادرها ووضع آليات لتبادلها بين مختلف الهيئات العمومية.

كما حدد المرسوم الرئاسي، الهيئات التي تشرف على منظومة حوكمة البيانات، مع بيان حدود تطبيق هذه المنظومة في ضوء الاستثناءات التي نصّ عليها، خاصة تلك المتعلقة بالمعطيات ذات الطابع الشخصي والمجالات التي تخضع للاعتبارات أمنية أو قضائية.

الكلمات المفتاحية: حوكمة البيانات، البيانات العمومية، فهرسة البيانات، التشغيل البيئي، الرقمنة.

Abstract: Algeria is going through a decisive transition toward a post-modern state model, where the management of public affairs increasingly relies on big data and algorithmic systems to enhance the efficiency of public services.

In this context, Presidential Decree No. 25-320 was adopted to establish a legal and regulatory framework for an integrated national system. Its purpose is to organize and secure the flow of information and data between various public bodies, regulate how data are classified and how their sources are indexed, and set mechanisms for data exchange among public institutions.

The decree also identifies the authorities responsible for overseeing the data governance system and clarifies the scope of its application, particularly in light of the exceptions it provides. These exceptions mainly concern personal data and sectors subject to security or judicial considerations.

Keywords: Data Governance, Public Data, Data Indexing, Interoperability, Digitization

مقدمة:

أدى التحول الرقمي الذي شهدته الإدارة العمومية في السنوات الأخيرة إلى ظهور واقع جديد، حيث أصبحت البيانات عنصراً أساسياً في تحسين أداء المرافق العامة وإعداد السياسات العمومية، وفي توجيه القرار الإداري. غير أن هذا التحول، رغم أهميته، لم يكن دائماً مصحوباً بإطار تنظيمي متكامل يضبط كيفية إنتاج البيانات العمومية وتداولها واستعمالها بين مختلف الإدارات والهيئات والمؤسسات المكلفة بأداء خدمة عمومية، وهو ما أدى عملياً إلى تشتت مصادر المعلومة، وتعدد قواعد البيانات، وضعف التنسيق بين الإدارات.

فقد كان تنظيم المجال المعلوماتي العمومي يتم بصورة جزئية ومتفرقة، من خلال نصوص قانونية متخصصة، على غرار النصوص المتعلقة بحماية المعطيات ذات الطابع الشخصي⁽¹⁾، أو أمن الأنظمة المعلوماتية⁽²⁾، حماية المعلومات والوثائق الإدارية⁽³⁾، ورغم أهمية هذه النصوص، إلا أنها عالجت البيانات من زوايا قطاعية محددة، دون أن تؤسس إطاراً عاماً ومشتزجاً ينظم البيانات العمومية في حد ذاتها بوصفها مورداً إدارياً مشتركاً.

وقد ترتب عن هذا الوضع عدد من العراقيل العملية، من أبرزها غياب مرجع موحد لتصنيف البيانات، وتكرار نفس المعطيات لدى أكثر من إدارة، وصعوبة تبادل البيانات بين المؤسسات، الإدارات والهيئات المكلفة بأداء خدمة عمومية، إضافة إلى تفاوت كبير في مستوى جاهزية الأنظمة المعلوماتية. وهو ما جعل مسألة تنظيم البيانات لا تتعلق فقط بالجوانب التقنية، بل تطرح إشكالاً قانونياً وتنظيمياً يمس فعالية العمل الإداري ككل.

في هذا السياق، جاء المرسوم الرئاسي رقم 25-320 المتضمن إحداث منظومة وطنية لحوكمة البيانات⁽⁴⁾، ليشكل إطار تنظيمي موحد يضبط المفاهيم الأساسية المرتبطة بالبيانات العمومية، ويحدد آليات تنظيمها وتبادلها، ويرسم معالم البنية المؤسسية المشرفة على حوكمتها. ويُلاحظ أن المشرع لم يتجه إلى سنّ

1 - قانون رقم 18-07، مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34، صادر بتاريخ 10 جوان 2018 المعدل والمتمم، بالقانون رقم 25-11، المؤرخ في 24 يوليو 2025، جريدة رسمية عدد 48، صادر في 24 يوليو 2025.

2 - مرسوم رئاسي رقم 20-05، مؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، معدل ومتمم بموجب المرسوم الرئاسي رقم 25-298، المؤرخ في 10 نوفمبر 2025، جريدة رسمية عدد 80، صادر في 30 نوفمبر 2025.

3 - أمر رقم 21-09، مؤرخ في 8 يونيو 2021، يتعلق بحماية المعلومات والوثائق الإدارية، جريدة رسمية عدد 45، صادر في 9 يونيو 2021.

4 - مرسوم رئاسي رقم 25-320، مؤرخ في 30 ديسمبر 2025، يتضمن وضع منظومة وطنية لحوكمة البيانات، جريدة رسمية عدد 87، صادر في 30 ديسمبر 2025.

قانون جديد ذي بعد حقوقي، بل اختار أداة تنظيمية تهدف أساسًا إلى إعادة تنظيم النشاط الإداري في مجاله المعلوماتي، مع الإبقاء على النصوص السابقة المتخصصة كل في مجالها.

وتهدف هذه الدراسة إلى قراءة وتحليل أحكام هذا القانون، من خلال الوقوف على كيفية تنظيم المشرع لإدارة وهيكلية البيانات، والآليات التي اعتمدها لتحقيق التوازن بين الاستعمال الإداري للبيانات من جهة، وضمان حمايتها من جهة أخرى

وانطلاقًا من ذلك، تطرح هذه الدراسة الإشكالية الآتية: إلى أي مدى أسهم المرسوم الرئاسي المتعلق بحكومة البيانات في إرساء إطار تنظيمي موحد لإدارة البيانات العمومية، دون المساس بمقتضيات الأمن والسيادة الوطنية؟

وللإجابة عن هذه الإشكالية، تم الاعتماد على المنهج التحليلي، من خلال تحليل أحكام القانون محل الدراسة. وقد تم تقسيم الدراسة إلى محورين رئيسيين، يتناول الأول، الإطار القانوني لإعادة هيكلة البيانات العمومية، بينما يخص الثاني لدراسة آليات تفعيل حوكمة البيانات .

المبحث الأول: إعادة هيكلة بيانات المؤسسات العمومية

قبل صدور قانون حوكمة البيانات لسنة 2025، لم يكن تنظيم البيانات داخل الإدارة العمومية في الجزائر يقوم على إطار موحد، إذ كانت كل جهة تنشئ قواعد بياناتها وتديرها بشكل مستقل، ما أدى إلى تشتت المعطيات وتكرار جمعها وصعوبة تبادلها بين الإدارات، وهو ما أثر سلبيًا على فعالية المرافق العامة وجودة القرار الإداري.

ولمعالجة هذا الوضع، تدخل المشرع لإرساء منظومة قانونية تهدف إلى إعادة تنظيم وهيكلية البيانات الوطنية، وذلك من خلال: ضبط المفاهيم الأساسية المرتبطة بها (المطلب الأول)، واعتماد معايير موحدة لإدارتها (المطلب الثاني)، وتحديد فئات البيانات المستثناة من التصنيف والفهرسة لاعتبارات تتعلق بحماية الخصوصية وصون السيادة الوطنية (المطلب الثالث).

المطلب الأول: ضبط المفاهيم القانونية لحوكمة البيانات

خصص المشرع جزءًا مهمًا من المرسوم لتحديد المفاهيم المرتبطة بحوكمة البيانات، وهو ما يدل على أهمية ضبط المصطلحات قبل الانتقال إلى تنظيم الآليات (الفرع الأول) وطبيعة الالتزامات الملقة على عاتق المؤسسات والهيئات العمومية (الفرع الثاني). ومن ثم، فإن دراسة هذه المفاهيم تسمح بفهم الكيفية التي يتعامل بها النص مع البيانات بوصفها موردًا إداريًا يتطلب تنظيمًا خاصًا في البيئة الرقمية (الفرع الثالث).

الفرع الأول: مفهوم البيانات الرقمية واتساع نطاقها القانوني

بالرجوع الى قانون حوكمة البيانات نجد أن المشرع الجزائري اعتمد بعض المصطلحات والمفاهيم القانونية التي تعكس بعدا تقنيا وتنظيميا، من ثم فإن الوقوف على مدلول هذه المفاهيم يشكل خطوة أساسية لفهم طبيعة الحوكمة التي يراد إرساؤها.

استعمال المشرع لمصطلح حوكمة لم يكن عفويا بل جاء محملا بدلالات قانونية تتجاوز مجرد ادارة تقنية للمعلومات، اذ يعبر هذ المفهوم عن الانتقال من منطق التعامل الجزئي مع البيانات إلى تصور أشمل يقوم على التنظيم والتوجيه وتوزيع المسؤوليات⁽¹⁾.

لهذا تختلف حوكمة البيانات عن إدارة البيانات في كون إدارة البيانات تركز بشكل عام على تحديد عنصر البيانات وكيفية تخزينه ونقله أي تعامل فيزيائي مادي، بينما حوكمة البيانات فهي الإطار العام أي تشمل مجموعة من العمليات التي تضمن إدارة ومعالجة أصول البيانات والمعلومات المهمة والحاسمة بشكل رسمي وتحسين أمنها وجودتها⁽²⁾.

فقد حددت المادة الثانية، البيانات الرقمية على أنها كل معلومة مقدّمة في شكل يمكن معالجته وتخزينه بطريقة رقمية. ويُلاحظ أن هذا التعريف لم يُقَيّد بطبيعة المعلومة ولا بمصدرها، كما لم يربطه بنوع معين من الأنشطة الإدارية. فاعتماد تعريف شامل يسمح بإدراج مختلف أشكال البيانات التي تنتجها سواء المؤسسات والادارات العمومية والهيئات المكلفة بحكم نشاطها بتقديم خدمة عمومية، سواء تعلّقت بتسيير الموارد، أو بالخدمات المقدمة للمواطنين، أو بإعداد السياسات العمومية، وهو ما يعكس إرادة واضحة في توسيع نطاق تطبيق المنظومة.

كما لم يفصل بشكل واضح بين البيانات باعتبارها معطيات أولية، والمعلومات بوصفها ناتجا عن معالجتها. مما يسمح بتوسيع نطاق التطبيق ليشمل كل محتوى قابل للمعالجة الرقمية، حتى لو كان ذلك على حساب الدقة الاصطلاحية المعروفة في التمييز بين المفهومين⁽³⁾.

1 - وهذا ما نصت عليه المادة 1 من المرسوم الرئاسي رقم 25-320، مرجع سابق.

2 - عامر عبد الرزاق عبد المحسن، أحمد زهر توفيق، "التحديات المعاصرة لحوكمة بيانات الحوسبة السحابية في مراكز المعلومات، دراسة تحليلية"، المجلة الاقتصادية والادارية للعلوم المجلد 25، عدد 115، ص 176.

3 - ذلك أنه يوجد فرق بين البيانات والمعلومات، فالبيانات هي معطيات أولية خام، مثل الأرقام أو الكلمات أو الرموز، لا تحمل في ذاتها معنى واضح، وإنما تمثل حقائق مجردة تحتاج إلى معالجة. أما المعلومات فهي نتيجة تنظيم تلك البيانات وتحليلها وترتيبها بطريقة تجعلها مفهومة وذات دلالة، وقابلة للاستفادة منها في الفهم واتخاذ القرار، للمزيد من التفصيل راجع : جوهري قويدر صامت، "الضوابط القانونية لمعالجة البيانات الشخصية الكترونيا"، مجلة الدراسات القانونية المقارنة، المجلد 6، عدد 2، 2020، ص 469 - 470.

كما يظهر من خلال هذا المرسوم أنه ميز بين حوكمة البيانات وحماية البيانات الشخصية حيث تبقى هذه الأخيرة خاضعة للتشريع خاص مما يعكس حرص المشرع على عدم الخلط بين البعد التنظيمي والبعد الحقوقي⁽¹⁾.

الفرع الثاني: مفهوم مصدر البيانات ومستخدمها

اعتمد المرسوم مفاهيم جديدة تتمثل في كل من: "مصدر البيانات" و"مستخدم البيانات" واستغلال البيانات، ضمن أحكامه⁽²⁾، و يقصد بالبيانات تلك الحقائق أو الرسائل أو الإشارات غير المنظمة و غير مفسرة مثل الأرقام أو الرموز أو الإحصاءات الخام التي ليس لها علاقة ببعضها البعض⁽³⁾ أما منتج البيانات فهو الجهة العمومية التي تتولى توليد البيانات وتصنيفها وفهرستها وضمان جودتها، في حين يُقصد بمستعمل البيانات الجهة التي تستفيد منها في إطار أداء مهامه، أما استغلال البيانات فيمكن أن يتم بطرق مختلفة كتسجيلها وتنظيمها أو حفظها وتشغيلها⁽⁴⁾.

و الملاحظ أن المشرع لم يربط إنتاج البيانات أو استعمالها بشخص طبيعي، وإنما أسند هذه الأدوار إلى المؤسسات والإدارات والهيئات المكلفة بخدمة عمومية، وهو ما يعكس انتقالاً من منطق المسؤولية الفردية إلى منطق المسؤولية المؤسسية. فهذا الاختيار يسمح بتحديد واضح للأدوار داخل الإدارة العمومية، ويحدّ من الغموض الذي كان يكتنف مسألة من يتحمل مسؤولية صحة البيانات أو تحيينه⁽⁵⁾.

كما أن الفصل بين منتج البيانات ومستعملها يعكس أهمية تداول البيانات بين الإدارات، دون المساس بمصدرها الأصلي. فالإدارة التي تنتج البيانات تظل مسؤولة عن جودتها، حتى وإن استعملت من قبل جهة أخرى، وهو ما يساهم في تعزيز الثقة في تبادل البيانات داخل المنظومة الإدارية.

1 - انظر المادة 4 من المرسوم الرئاسي رقم 25-320، مرجع سابق.

2 - يقصد بالبيانات لغتا لفظ مشتق من كلمة بَيّن و المشتقة بدورها من لفظ بيان أي ما تبين به الشيء من الدلالة و غيرها، راجع فوزية بن عيدة، رقية جومي، "حوكمة البيانات في مؤسسات التعليم العالي: الآليات الاستراتيجية، العوائق"، المجلة المغربية للمخطوطات، المجلد 20، العدد الأول، 2024، ص 158.

3 - فوزية بن عيدة، رقية جوم، مرجع نفسه، ص 158.

4 - التفسير طريقة تعتمد على خوارزميات رياضية، تستخدم لتحويل الرسالة من كلام واضح و مقروء الى كلام غير مفهوم، ولا يستطيع قراءتها إلا من يملك مفتاحا سريا يعيدها الى حالتها الأصلية المقروءة، للزبد من الفصيل راجع: حزام فتيحة، "حماية الأنظمة الرقمية بين الآليات التقنية و أجهزة الحماية: قراءة في أحكام المرسوم الرئاسي 20-05"، مجلة الحقوق و العلوم الإنسانية، العدد الثالث، 2020، ص 175.

5 - انظر المادة 3 من المرسوم الرئاسي رقم 25-320، المرجع نفسه.

ومع ذلك، فإن فعالية هذا التقسيم تبقى مرتبطة بمدى وضوح الإجراءات العملية التي تضبط العلاقة بين المنتج والمستعمل، خاصة في الحالات التي تتعدد فيها الجهات المستفيدة من نفس البيانات، وهو ما يجعل هذا المفهوم إطاراً تنظيمياً يحتاج إلى تفعيل دقيق على المستوى التطبيقي العملي .

الفرع الثالث: جودة البيانات كمعيار قانوني للتبادل

لم يكتفِ المشرع بتنظيم تداول البيانات بين الإدارات العمومية، بل أدرج مفهوم جودة البيانات ضمن المفاهيم الأساسية، و يقصد بها مجموعة من الخصائص التي تحدد مدى ملائمة البيانات للاستخدام، محدداً عناصرها بدقة، بما يربط سلامة الأداء الإداري باحترام هذه الخصائص. فاشتراط المطابقة للواقع لأن المعلومة غير الصحيحة قد تمثل خطراً قانونياً يؤدي إلى انحراف القرار الإداري، في حين يعكس معيار الشمولية إدراك أثر البيانات الناقصة في إنتاج معرفة إدارية غير مكتملة. كما يهدف معيار غياب التعارض إلى ضمان الانسجام بين الأنظمة المعلوماتية داخل الإدارة العمومية والحدّ من تضارب المعطيات بين الهيئات، بينما يربط معيار التوفر في الوقت المناسب جودة البيانات بمتطلبات السرعة التي تفرضها المرافق العمومية الحديثة.

ويُعدّ التحديث المستمر من أبرز مؤشرات الطابع الديناميكي لجودة البيانات، إذ لا تُقيّم البيانات عند إنتاجها فقط، بل طيلة دورة حياتها، وهو ما يعزز مبدأ المسؤولية المستمرة للإدارة عن بياناتها⁽¹⁾.

المطلب الثاني: توحيد المعايير التقنية وإنهاء التشتت الإداري للبيانات

بعد أن ضبط المشرع المفاهيم الأساسية المرتبطة بحوكمة البيانات، انتقل إلى وضع معايير تنظيمية تهدف إلى معالجة مظاهر التشتت التي كانت تسود إدارة البيانات داخل الإدارة العمومية. من بينها توحيد طرق تصنيف البيانات (الفرع الأول)، ووضع مرجع لفهرسة البيانات من أجل تحديد الجهة الأصلية المنتجة للبيانات (الفرع الثاني).

الفرع الأول: مرجع تصنيف البيانات كأداة للضبط الإداري

نصّ المشرع الجزائري، على ضرورة إرساء مرجع موحد لتصنيف البيانات، يقوم على اعتماد معايير واضحة لتحديد درجة حساسيتها، وتحديد مجالات استخدامها، وكذا نوع الحماية التي ينبغي أن تُطبّق على كل فئة منها، بما يضمن تنظيمًا أكثر انسجامًا لمعالجة البيانات داخل الهيئات والمؤسسات العمومية. ويعكس هذا الخيار رغبة تشريعية في تجاوز الممارسات السابقة التي كانت تترك لكل إدارة حرية تحديد طبيعة بياناتها وكيفية التعامل معها، وهو ما أدى في كثير من الأحيان إلى تفاوت المعايير وغياب الانسجام بين القطاعات العمومية.

1 - سوزان أحمد سلطان، أثر القحطاني، " استراتيجيات تعزيز جودة البيانات في نظم ادارة المعلومات: تحليل للتحديات و الفرص"، المجلة العربية الدولية لادارة المعرفة، المجلد الرابع، العدد الرابع، 2025، ص 21، 27

وفي هذا السياق، تنص المادة 6، على أن مرجع تصنيف البيانات هو الأداة الأساسية التي تُحدّد من خلالها المعايير المعتمدة في هذا المجال. ويشمل هذا المرجع، في المقام الأول، تحديد مستويات حساسية البيانات، من خلال تصنيفها إلى بيانات عامة، وبيانات سرية، وبيانات ذات سرية عالية، بما يسمح بضبط نطاق الولوج إليها وتحديد الجهات أو الأشخاص المخوّلين قانوناً بالاطلاع عليها أو معالجتها.

كما يعتمد مرجع التصنيف على معيار مجال استعمال البيانات، حيث تُربط كل فئة بالسياق الوظيفي أو القطاعي الذي تُستعمل فيه، سواء تعلق الأمر بالمجال الإداري أو الاقتصادي أو الصحي أو غيره. ويهدف هذا المعيار إلى تكريس مبدأ تخصيص الغرض، ومنع استعمال البيانات خارج الإطار الذي جُمعت من أجله.

ويُدرج المرسوم ضمن معايير التصنيف كذلك تحديد أنواع الحماية والتدابير الأمنية الواجب اعتمادها لكل فئة من البيانات، بما يتناسب مع درجة حساسيتها. وتشمل هذه التدابير الإجراءات التقنية والتنظيمية اللازمة لحماية البيانات من مخاطر الاختراق أو التسريب أو الاستعمال غير المشروع⁽¹⁾.

الفرع الثاني: مرجع فهرسة مصادر البيانات وإنهاء الازدواجية المعلوماتية

عالج المرسوم الرئاسي إلى جانب تصنيف البيانات، إشكالية لا تقل أهمية، تتمثل في تعدد مصادر نفس البيانات داخل الإدارة العمومية. فقد كانت المعطيات نفسها تُجمع وتُخزّن من قبل أكثر من هيئة دون تنسيق فعلي، مما أدى إلى ازدواجية في الجهد، وتضارب في المعلومات، وهدر للموارد البشرية والتقنية.

ولمواجهة هذا الوضع، أقرّ المشرّع إنشاء مرجع وطني لفهرسة مصادر البيانات، يهدف إلى تحديد الجهة الأصلية المنتجة لكل نوع من البيانات، وتمكين باقي الإدارات من التعرف على مصدرها الرسمي. وتكمن أهمية هذا المرجع في إعادة تنظيم خريطة البيانات داخل المؤسسات والهيئات والإدارة العمومية، وتحديد المسؤولية المؤسسية عن إنتاج المعطيات وتحيينه⁽²⁾.

ويساهم هذا المرجع في تكريس مبدأ الاعتماد على المصدر الواحد للبيانات، بما يقلّل من الحاجة إلى إعادة جمع نفس المعلومات، ويُحسّن من دقة المعطيات المتداولة بين الإدارات. غير أن فعالية هذه الآلية تظل رهينة بالتزام الإدارات بالإفصاح عن قواعد بياناتها وتحيين المعلومات المرتبطة بها بصفة منتظمة، وهو ما يجعل الفهرسة عملية ديناميكية مستمرة لا تقتصر على مرحلة الإنشاء.

وعليه، يمكن القول إن فهرسة وتصنيف البيانات لم يعودا مجرد أدوات تقنية مساعدة، بل أصبحت ركيزة أساسية لحوكمة البيانات العمومية. فبفضلها تتحول البيانات من تراكم معلوماتي غير منظم إلى أصول رقمية

1 - حيث تصنف الوثائق والمعلومات الإدارية حسب حساسيتها إلى سرية جدا، سري، واجب الكتمان وإخيرا ذات توزيع محدود، وهذا ما نصت عليه المادة 6 من الأمر رقم 21-09، المتعلق بحماية المعلومات والوثائق الإدارية، مرجع سالف الذكر.

2 - وهذا ما نصت عليه المادة 7 من المرسوم الرئاسي رقم 25-320، مرجع سابق.

قابلة للاستغلال الرشيد في تحسين الأداء الإداري وجودة الخدمة العمومية. وفي غياب هذا التنظيم، تبقى الرقمنة مجرد نقل للفوضى الورقية إلى الفضاء الإلكتروني، دون تحقيق الأهداف المرجوة منها في تحديث الإدارة وتعزيز فعاليتها

المطلب الثالث: حدود تطبيق حوكمة البيانات

لم يكن تنظيم حوكمة البيانات العمومية بمعزل عن الاعتبارات المرتبطة بحماية الحقوق والحريات الأساسية، وعلى رأسها الحق في حماية المعطيات ذات الطابع الشخصي. فخصوصية هذا الصنف من البيانات، وما ينطوي عليه من مخاطر في حال سوء المعالجة أو التبادل غير المنضبط، فرضت على المشرع التمييز بين البيانات بوصفها مورداً إدارياً، وبين المعطيات الشخصية بوصفها امتداداً للحياة الخاصة للأفراد (الفرع الأول) إلى جانب إقرار مجموعة من الاستثناءات التي تعكس اعتبارات قضائية وسيادية (الفرع الثاني).

الفرع الأول: استثناء البيانات ذات طابع شخصي من منظومة الحوكمة

استثنى المرسوم الرئاسي رقم 25-320 صراحة المعطيات ذات الطابع الشخصي من نطاق تطبيق منظومة حوكمة البيانات، وإخضاعها للتشريع الخاص المنظم لحمايتها. فالمشرع تبنى منطق الفصل الوظيفي بين نظامين قانونيين مختلفين في الطبيعة والغاية، أحدهما يهدف إلى تنظيم تبادل البيانات العمومية وتحسين الأداء الإداري، والآخر يُعنى بحماية حقوق الأفراد واحترام خصوصيتهم⁽¹⁾.

ولا يُعدّ هذا الاستثناء قصوراً تشريعياً، بل يعكس رغبة واعية في تجنب التداخل بين قواعد تنظيمية إدارية ومبادئ حمائية ذات طابع حقوقي، لا سيما وأن نظام حماية المعطيات الشخصية يقوم على أسس خاصة، كالموافقة، وتناصب المعالجة، وحماية الحياة الخاصة، وهي مبادئ يصعب إدماجها ضمن نص تنظيمي موجّه أساساً للإدارة.

غير أن الإحالة العامة على التشريع القائم، وعلى رأسه القانون رقم 18-04، المعدل والمتمم، تطرح إشكالية عملية تتعلق بتنسيق تطبيق النصوص وتحديد المسؤوليات بين مختلف المتدخلين، خاصة في ظل تعدد الهيئات المشرفة على معالجة وتبادل البيانات في البيئة الرقمية.

لكن، رغم أن المشرع استثنى المعطيات ذات الطابع الشخصي من نطاق تطبيق حوكمة البيانات، فإنه لم يُخرجها تماماً من الإطار التنظيمي المصاحب للمنظومة. فقد أخضع استعمالها لشروط دقيقة وصارمة، أهمها ضرورة الحصول على موافقة مسبقة من الجهة المصدرة للبيانات قبل القيام بأي معالجة أو تبادل لها. ويعكس ذلك حرصاً على تكريس مبدأ التحكم في البيانات، ومنع تداولها أو استخدامها دون ترخيص صريح وواضح..

1 - وهذا ما نصت عليه المادة 4 من المرسوم الرئاسي رقم 25-320، مرجع سابق.

كما قيّد المرسوم استعمال المعطيات الشخصية بالغرض الذي جُمعت من أجله، تكريسًا لمبدأ تخصيص الغرض، وهو ما يشكّل ضماناً أساسية للحد من مخاطر إعادة توظيف البيانات خارج سياقها القانوني⁽¹⁾. ويُضاف إلى ذلك إلزامية التصنيف المسبق للبيانات، وفق مرجع وطني يحدّد درجة حساسيتها ومستوى الحماية الواجب توفيره لها قبل إدماجها في أي مسار رقمي⁽²⁾.

وعلى المستوى المؤسسي، أسند المشرّع للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي مهمة الرقابة على عمليات التصنيف والمعالجة، بما يشكّل إطاراً رقابياً يهدف إلى ضبط الممارسات الإدارية ومنع التجاوزات المحتملة. غير أن فعالية هذه الضمانات تظل مرتبطة بمدى التنسيق بين الجهات المتدخلة، وبقدرة أجهزة الرقابة على التدخل في الوقت المناسب⁽³⁾.

الفرع الثاني: استثناء البيانات ذات الطابع الأمني والقضائي

أقرّ المرسوم الرئاسي، مجموعة من الاستثناءات المتعلقة بالبيانات المرتبطة بالأمن الوطني والدفاع، وبنشاط السلطة القضائية، وهي استثناءات تعكس الطابع السيادي لبعض الوظائف الأساسية للدولة.

وقد استُثنت، في المقام الأول، البيانات المرتبطة بالدفاع الوطني والأمن الوطني من مجال تطبيق المرسوم، إذ يظل أي تبادل للبيانات لأغراض دفاعية أو أمنية خاضعاً لأنظمة خاصة صارمة، لا ينسجم طبيعتها مع منطق التشغيل البيني الإداري، بالنظر إلى ما تنطوي عليه هذه المعطيات من حساسية مباشرة تمس أمن الدولة واستقرارها.

كما شمل الاستثناء البيانات المتعلقة بصلاحيات السلطة القضائية، تكريسًا لمبدأ استقلال القضاء، وحماية لسرية العمل القضائي وحسن سير العدالة. ويمتد هذا الاستثناء ليشمل البيانات المرتبطة بالعمل القضائي والجنائي، لا سيما تلك المتعلقة بالوقاية من الجرائم، والكشف عنها، وإجراء التحريات والتحقيقات، والمتابعات القضائية، وتنفيذ العقوبات، وهي مجالات تتطلب مستوى عاليًا من السرية والانضباط الإجرائي لا يتلاءم مع التبادل الرقمي الواسع⁽⁴⁾.

وإلى جانب هذه الاستثناءات المحددة صراحة، أتاح المرسوم إمكانية استثناء فئات أخرى من البيانات في حالات خاصة، شريطة تقديم طلب معلّل من مصدر البيانات، والحصول على موافقة المجلس الوطني لأمن

1 - وهذا ما نصت عليه المادة 13، المرجع نفسه.

2 - وهذا ما نصت عليه المادة 6، المرجع نفسه.

3 - راجع المادة 15، من المرسوم الرئاسي رقم 25-320، مرجع سابق.

4 - وهذا ما نصت عليه المادة 18، المرجع نفسه.

الأنظمة المعلوماتية. ويعكس هذا التوجه حرص المشرع على إدخال قدر من المرونة، دون الإخلال بالضوابط الأمنية العامة للمنظومة⁽¹⁾.

الفرع الثالث: أثر الاستثناءات على فعالية منظومة حوكمة البيانات

رغم أن الاستثناءات القانونية تُقيد من شمولية منظومة حوكمة البيانات، إلا أنها لا تُفقد قيمتها. فهي في الواقع تُحدد مجال تطبيقها بما يتماشى مع طبيعة الدولة ووظائفها السيادية. وإذا طُبقت هذه الاستثناءات في حدودها الضيقة، فإنها لا تعرقل تنظيم البيانات العمومية، بل تساعد على تحقيق توازن ضروري بين متطلبات التحول الرقمي من جهة، وحماية الأمن والسيادة والحقوق الأساسية من جهة أخرى.

غير أن قراءة أحكام المرسوم الرئاسي رقم 25-320 تظهر أن التحدي الحقيقي لا يكمن في النص القانوني ذاته، بل في شروط تطبيقه. فالمنظومة بُنيت على افتراض جاهزية رقمية متقدمة لدى جميع الإدارات، دون الإشارة بوضوح إلى مراحل انتقالية تراعي تفاوت الإمكانيات بينها. وهذا قد يخلق صعوبات عملية عند الانتقال من الإطار النظري إلى التنفيذ الفعلي.

وتزداد هذه الصعوبات عندما تُمنح الإدارة المصدرة للبيانات سلطة تصنيفها وتحديد درجة حساسيتها. ففي غياب رقابة لاحقة فعالة، قد يتم تصنيف عدد كبير من البيانات ضمن مستويات حماية مرتفعة دون مبرر كافٍ، وهو ما قد يؤدي عملياً إلى الحد من تبادلها، ويُضعف بذلك مبدأ التشغيل البيني. لذلك تبقى فعالية النظام مرتبطة بوجود آليات تدقيق تكشف أي تصنيف مبالغ فيه أو غير دقيق، سواء أفضى إلى حماية مفرطة أو إلى مساس غير مقصود بالخصوصية.

كما أن اشتراط الحصول على موافقة مُصدر البيانات قبل تبادلها قد يتحول، إن لم يُنظم بطريقة مرنة، إلى عبء إجرائي يُبطئ العمل الإداري بدل أن يُيسره. ويزداد الأمر تعقيداً عند التعامل مع المعطيات الشخصية أو البيانات ذات الطابع السيادي، حيث يصبح من الضروري تحقيق توازن دقيق بين تحسين الأداء الإداري وضمان احترام الخصوصية والمتطلبات الأمنية.

بناءً على ذلك، يمكن القول إن المرسوم وضع إطاراً قانونياً وتقنياً متقدماً، لكنه يفترض في المقابل مستوى عالياً من التنسيق والجاهزية الرقمية. ونجاح المنظومة لا يتوقف فقط على وضوح النصوص، بل على قدرة الإدارات على تطوير أنظمتها المعلوماتية، وتأهيل مواردها البشرية، والتكيف مع منطق جديد يقوم على الانضباط التقني بقدر ما يقوم على التنظيم القانوني.

ومن هنا تبرز أهمية اعتماد مرحلة انتقالية مرنة تسمح بإدماج الإدارات تدريجياً في المنظومة، بما يضمن تطبيقاً واقعياً ومتوازناً، ويحافظ في الوقت نفسه على متطلبات الأمن السيبراني وحسن سير المرفق العام.

1 - راجع الفقرة الثالثة من المادة 18، المرجع نفسه.

المبحث الثاني: آليات تفعيل حوكمة البيانات

لم يعد نجاح السياسات العمومية مرتبطاً فقط بوفرة النصوص القانونية أو بتعدد الهياكل الإدارية، بل أصبح رهيناً بمدى قدرة الإدارة على إدارة بياناتها بكفاءة، وضمان انسيابها بين مختلف المتدخلين في إطار من التنسيق والضبط القانوني. وفي هذا الإطار، سعى المشرع إلى إرساء جملة من الآليات التقنية (المطلب الأول) والمؤسسية لتفعيل وتطبيق منظومة حوكمة البيانات (المطلب الثاني).

المطلب الأول: النظام الوطني للتشغيل البيئي كآلية تقنية لتكريس تبادل البيانات العمومية

يعد النظام الوطني للتشغيل البيئي الإطار الحصري والوحيد لتبادل البيانات في الجزائر. ويطرح هذا الخيار التنظيمي عدة أبعاد متداخلة، تتعلق بأهمية هذا النظام داخل منظومة حوكمة البيانات (الفرع الأول)، وبالضمانات المقررة للحفاظ على سيادة الإدارة على بياناتها (الفرع الثاني)، دون إغفال ما يواجهه هذا النظام من صعوبات عملية قد تحدّ من فعاليته رغم وجاهته من الناحية القانونية (الفرع الثالث).

الفرع الأول: الأهمية العملية لنظام التشغيل البيئي

يُعدّ النظام الوطني للتشغيل البيئي أحد المكونات الأساسية لمنظومة حوكمة البيانات، إذ يهدف إلى تمكين الإدارات والهيئات العمومية من تبادل البيانات الرقمية فيما بينها بطريقة آمنة ومنظمة⁽¹⁾. ولا يقتصر هذا النظام على مجرد نقل تقني للمعلومة، بل يقوم على إرساء إطار مؤسسي يسمح بتكامل الأنظمة المعلوماتية المختلفة داخل الإدارة العمومية، بما يخدم أهداف العمل الإداري المشترك. ففكرة التشغيل البيئي لا تقوم على تجميع البيانات أو نزع السيطرة عنها، وإنما على تنظيم تداولها بين الإدارات عند الحاجة، وفق قواعد تضمن احترام مصدرها والغرض الذي خُصصت من أجله، وقد اختار المشرع اعتماد نظام التشغيل البيئي كأداة مركزية لتسريع المعاملات الإدارية، انطلاقاً من قناعة مفادها أن بطء الإدارة لا يعود فقط إلى كثرة الإجراءات، بل أساساً إلى صعوبة الوصول إلى المعلومة وتشتتها بين الإدارات. ومن هذا المنطلق، يسمح النظام بانتقال البيانات مباشرة بين الهيئات العمومية، بدل تحميل المواطن عبء نقلها.

فحين تحصل الإدارة على المعلومة من مصدرها الأصلي، يصبح اتخاذ القرار أسرع وأكثر دقة، كما تساهم النماذج التقنية الموحدة في ضمان استمرارية الخدمة العمومية دون عراقيل تقنية.

الفرع الثاني: ضمانات حوكمة البيانات في إطار نظام التشغيل البيئي.

1 - وهذا ما نصت عليه المادة 9 من المرسوم الرئاسي رقم 25-320، مرجع سابق.

يقوم النظام الوطني للتشغيل البيني على مبدأ سيادة الإدارة على بياناتها، إذ لا يقوم على نزع السيطرة عن الجهة المنتجة، بل على تنظيم تداول البيانات بما يحفظ سلطة مُصدرها ويضبط شروط استعمالها.

ويتجلى هذا المبدأ من خلال اشتراط الموافقة الصريحة لمُصدر البيانات قبل أي عملية تبادل، حيث تظل الإدارة المنتجة صاحبة القرار في تحديد قابلية البيانات للتشارك، والجهة المستفيدة منها، والغرض الإداري المحدد لاستعمالها. وبذلك، ينتقل تبادل البيانات من ممارسة إدارية غير منضبطة إلى تصرف قانوني منظم تحكمه قواعد واضحة.

كما يفرض النظام على مستخدم البيانات الالتزام الصارم باحترام الغرض الذي طُلبت من أجله المعلومة، تكريسًا لمبدأ تخصيص الغرض، وهو ما يحدّ من مخاطر إعادة توظيف البيانات خارج سياقها القانوني أو الإداري⁽¹⁾.

ويُعزّز هذا التنظيم اشتراط تصنيف البيانات وفهرسة مصادرها قبل إدماجها في نظام التشغيل البيني، إذ لا تُدرج البيانات إلا بعد ضبط طبيعتها ومستوى حساسيتها وقابلية تبادلها، بما يجعل قرار المشاركة قرارًا واعيًا ومبنيًا على معرفة دقيقة بمحتوى البيانات وأهميته⁽²⁾.

في إطار التشغيل البيني يقتصر دور المحافظة السامية للرقمنة على توفير بنية تحتية وطنية مؤمنة تضمن سلامة البيانات أثناء انتقالها بين الإدارات، دون التدخل في مضمونها أو في القرارات المرتبطة باستعمالها. ويعكس هذا الدور تمييزًا واضحًا بين الوظيفة التقنية المتمثلة في التأمين، والوظيفة القانونية المتعلقة بالتحكم في البيانات، بما يدعم مبدأ السيادة الإدارية على بياناتها⁽³⁾.

الفرع الثالث: حدود فعالية نظام التشغيل البيني في الواقع العملي

رغم ما يحمله نظام التشغيل البيني من إيجابيات واضحة، إلا أن فعاليته تظل رهينة بعدة شروط عملية، في مقدمتها تقارب مستوى الجاهزية الرقمية بين المؤسسات والإدارات العمومية. غير أن الواقع يكشف أن العديد من الإدارات والمؤسسات والهيئات المكلفة بخدمة عمومية ما تزال تعتمد أنظمة معلوماتية تقليدية أو غير متجانسة، ما يجعل عملية إعادة تكييف هذه الأنظمة لتتلاءم مع المتطلبات الجديدة مسارًا معقدًا يتطلب مجهودًا تقنيًا وبشريًا وزمنيًا معتبرًا. ويؤدي هذا التفاوت إلى تأخر اندماج بعض القطاعات في النظام الوطني للتشغيل البيني، بما يخلق تفاوتًا عمليًا في الاستفادة من التحول الرقمي، ويحدّ من شمولية تطبيق منظومة الحوكمة.

1 - المادة 13 من المرسوم الرئاسي رقم 25-320، مرجع سابق.

2 - المادة 12، المرجع نفسه.

3 - انظر المادة 10، المرجع نفسه.

كما أن نجاح النظام يفترض وجود ثقة متبادلة في جودة البيانات المتبادلة، في حين أن غياب هذه الثقة قد يدفع بعض الإدارات إلى الاستمرار في طلب الوثائق من المواطن، مما يُبقي بعض مظاهر البيروقراطية قائمة. ويُضاف إلى ذلك أن السرعة التقنية قد تصطدم أحياناً بالضوابط القانونية المتعلقة بالموافقة، وتحديد الغرض، وحماية المعطيات الشخصية، وهو ما قد يُفرغ النظام من فعاليته إذا لم تُؤاكب مرونة تنظيمية مناسبة.

ومن جهة أخرى، فإن القيد التقني الذي يمنع استعمال البيانات خارج الغرض المصرح به، رغم كونه ضماناً قوية نظرياً، يظل رهيناً بمدى فعالية أنظمة المراقبة اللاحقة وقدرتها على كشف أي تحايل أو إساءة استعمال غير ظاهرة تقنياً. فالحماية التقنية، مهما بلغت دقتها، لا تُغني كلياً عن الرقابة القانونية والبشرية المستمرة.

وعليه، يمكن القول إن آلية الموافقة التقنية تمثل خطوة متقدمة في مسار حوكمة البيانات، لكنها تظل بحاجة إلى استكمالها بضمانات، مثل تحديد آجال للرد، وتوحيد معايير منح الموافقة، وتعزيز الرقابة اللاحقة على استعمال البيانات. فبدون هذه العناصر، قد تفقد الموافقة التقنية جزءاً من فعاليتها، وتتحول من أداة تسهيل إلى آلية ضبط مفرطة تحدّ من أهداف التشغيل البيئي.

المطلب الثاني الهيئات المكلفة بتنفيذ منظومة الحوكمة

اعتمد المشرع في تنظيم الإشراف على منظومة حوكمة البيانات مقارنة تقوم على توزيع الاختصاصات بين عدة هيئات، لكل منها دور محدد يتماشى مع طبيعة مهامها الأصلية. ويكشف هذا التعدد عن رغبة في الإحاطة بمختلف أبعاد البيانات، من حيث التنظيم، والحماية، والأمن، والتنسيق الرقمي ومن بينها نجد: السلطة الوطنية لحماية المعطيات ذات طابع شخصي (الفرع الأول)، وكل من المجلس والوكالة الوطنية لأمن الأنظمة المعلوماتية (الفرع الثاني)، إضافة إلى المحافظة السامية لأمن الأنظمة المعلوماتية (الفرع الثالث).

الفرع الأول: السلطة الوطنية لحماية المعطيات ذات طابع شخصي

لم يتعامل المشرع الجزائري مع مسألة حوكمة البيانات بوصفها مسألة تقنية فقط، بل ربطها أساساً بحماية الحقوق الأساسية للأفراد، وعلى رأسها الحق في الخصوصية باعتباره حقاً دستورياً⁽¹⁾ ولهذا أسند دوراً محورياً للسلطة الوطنية المكلفة بحماية المعطيات ذات الطابع الشخصي، باعتبارها آلية رقابية تضمن أن تتم معالجة البيانات في إطار قانوني وآمن⁽²⁾.

1 - وهذا ما تم تأكيده في نص المادة 47، من المرسوم الرئاسي رقم 20-442، المؤرخ في 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020، جريدة رسمية عدد 82، صادر في 30 ديسمبر 2020.

2 - راجع المادة 4 من المرسوم الرئاسي رقم 25-320، مرجع سابق.

ولقد تم انشائها بموجب القانون رقم 18-07، المتعلق بحماية المعطيات ذات طابع شخصي، كهيئة مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والإداري⁽¹⁾، تزود بأقطاب جهوية تتكفل بمهام المراقبة والتدقيق على مستوى الهيئات والأشخاص المعالجين للمعطيات ذات طابع شخصي⁽²⁾.

وتتمثل مهمتها الأساسية في السهر على احترام التشريع المتعلق بحماية المعطيات الشخصية أثناء جمعها أو معالجتها أو استعمالها، سواء من طرف الإدارات العمومية أو الهيئات الأخرى⁽³⁾.

وتبرز أهمية هذه السلطة بشكل خاص في إطار حوكمة البيانات، لأنها تمثل جهاز الرقابة الذي يضمن ألا تتحول عمليات استغلال البيانات إلى مساس بالحياة الخاصة للأفراد. فهي تتدخل قبل المعالجة من خلال نظام التصريح أو الترخيص، حيث تلزم كل جهة ترغب في معالجة معطيات شخصية بالحصول على موافقتها المسبقة، وتمسك لهذا الغرض سجلاً وطنياً للتصريحات والتراخيص. كما تراقب عمليات نقل البيانات إلى الخارج، ولا تسمح بها إلا إذا توفرت ضمانات كافية لحماية هذه المعطيات أو في الحالات التي يجيزها القانون.

ولا يقتصر دورها على الرقابة المسبقة فقط، بل يمتد إلى الرقابة اللاحقة أيضاً، إذ تستقبل شكاوى الأشخاص المعنيين، وتتحقق من مدى احترام حقوقهم، ويمكنها أن تأمر بتصحيح المعطيات أو سحبها أو إتلافها إذا ثبت أنها عولجت بطريقة غير قانونية. كما تقوم بتقديم الاستشارات⁽⁴⁾ وبذلك، يتضح أن إدراج هذه السلطة ضمن المنظومة القانونية المرتبطة بحوكمة البيانات يعكس توجهاً تشريعياً يهدف إلى تحقيق توازن بين متطلبات استغلال البيانات لأغراض إدارية وتنموية، وبين ضرورة حماية المعطيات الشخصية وصون حرمة الحياة الخاصة.

الفرع الثاني: الهيئات المختصة بأمن الأنظمة المعلوماتية

في إطار إرساء منظومة وطنية لحوكمة البيانات، لم يكتفِ المشرع الجزائري بوضع قواعد لتنظيم تداول المعطيات داخل الإدارة العمومية، بل حرص أيضاً على إسناد دور واضح لهيئات مختصة تضمن أن تتم هذه الحوكمة في بيئة رقمية آمنة. وفي هذا السياق، يبرز دور كل من: المجلس الوطني لأمن الأنظمة المعلوماتية ووكالة أمن الأنظمة المعلوماتية، كأداتين أساسيتين لحماية البيانات وتأمين استعمالها.

- 1 - انظر المادة 22 من القانون رقم 18-07، مرجع سابق.
- 2 - وهذا ما نصت عليه المادة 27 مكرر من القانون رقم 25-11، المعدل والمتمم للقانون رقم 18-07، مرجع سابق.
- 3 - يقصد بالمعطيات ذات الطابع الشخصي، كل معلومة بغض النظر عن دعائها متعلقة بشخص معرف أو قابل للتعريف بصفة مباشرة أو غير مباشرة، وتشمل هذه المعطيات كل ما يرتبط بهويته مثل خصائصه البدنية، الجينية، الاقتصادية، الثقافية، والاجتماعية، راجع: العيداني محمد، يوسف زروق، "حماية المعطيات الشخصية في الجزائر على ضوء القانون 18-07"، مجلة معالم للدراسات القانونية والسياسية، العدد الخامس، 2018، ص ص 118-119.
- 4 - وهذا ما أشارت إليه المادة 25 من القانون رقم 18-07، مرجع سابق.

حيث يتولى المجلس الوطني لأمن الأنظمة المعلوماتية دورًا توجيهيًا عامًا، يتمثل في النظر في القضايا الكبرى المرتبطة بأمن الأنظمة المعلوماتية وبالمنظومة الوطنية لحوكمة البيانات وبإعداد استراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية⁽¹⁾. ويعكس هذا الدور رغبة المشرع في إدماج حوكمة البيانات ضمن رؤية شاملة للأمن الرقمي، بحيث لا تُفهم الحوكمة على أنها مجرد تنظيم إداري للبيانات، بل كسياسة عمومية يجب أن تراعي متطلبات الحماية والأمن. وبهذا المعنى، يساهم المجلس في ضبط التوجهات العامة وضمان انسجامها مع الخيارات الاستراتيجية للدولة، دون الدخول في التفاصيل التقنية اليومية⁽²⁾.

أما وكالة أمن الأنظمة المعلوماتية، فهي مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلال المالي⁽³⁾ وتعتبر بمثابة آلية تقنية وتنفيذية لحماية البيانات داخل منظومة حوكمة البيانات. إذ تتولى تحديد مستويات أمن البيانات بحسب طبيعتها ودرجة حساسيتها، وتضع إجراءات الحماية التي تلتزم بها الإدارات والمؤسسات العمومية أثناء تخزين البيانات أو معالجتها أو تبادلها. بالتنسيق مع الهيكل المسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات والذي يجب أن يكون في كل الإدارات والمؤسسات والهيئات العمومية⁽⁴⁾ ويبرز دورها بشكل خاص في مرحلة تبادل البيانات بين الإدارات، حيث تسهر على تأمين هذه العمليات باستعمال وسائل تقنية مناسبة، مثل تصنيف البيانات واعتماد التشفير والاعتماد على شبكات مؤمنة، بما يضمن سلامة البيانات وسريتها.

كما تضطلع الوكالة بدور رقابي وتقني عند وقوع حوادث أو هجمات معلوماتية، من خلال التحقيقات الرقمية وجمع وتحليل المعطيات التقنية⁽⁵⁾، إلى جانب إعداد القواعد والإجراءات التي تهدف إلى رفع مستوى أمن الأنظمة المعلوماتية. وهي، بذلك، تضمن أن تتم حوكمة البيانات في إطار تقني محمي يقلل من مخاطر الاختراق أو الاستعمال غير الآمن للمعطيات⁽⁶⁾.

- 1 - وهذا ما نصت عليه المادة 3 من المرسوم الرئاسي رقم 25-298، المؤرخ في 10 نوفمبر 2025، المعدل والمتمم للمرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، جريدة رسمية عدد 80، صادر في 30 نوفمبر 2025.
- 2 - يظهر ذلك من خلال وضع استراتيجية وطنية لأمن الأنظمة المعلوماتية للفترة الممتدة من 2025 إلى 2029، والتي تم المصادقة عليها بموجب المرسوم الرئاسي رقم 25-321، مؤرخ في 30 ديسمبر 2025، جريدة رسمية عدد 87، صادر في 30 ديسمبر 2025.
- 3 - وهذا ما نصت عليه المادة 17 من القانون رقم 18-04، مرجع سابق.
- 4 - وهذا ما نصت عليه المادة 2 من المرسوم الرئاسي رقم 26-07، مؤرخ في 7 جانفي 2026، يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية وتحديد مهامه وتنظيمه وسيره، جريدة رسمية عدد 4، صادر في 18 جانفي 2026.
- 5 - المادة 18 من القانون رقم 18-07، مرجع سابق.
- 6 - هذا ما نصت عليه المادة 16 من المرسوم الرئاسي رقم 25-320، مرجع سابق.

غير أن دور الوكالة يظل محصوراً في الجانب التقني، فهي تراقب احترام معايير الأمن المعلوماتي، لكنها لا تتدخل في مشروعية استعمال البيانات أو في الأهداف الإدارية لمعالجتها، لأن ذلك يدخل ضمن اختصاص هيئات رقابية أخرى، خاصة تلك المتعلقة بحماية المعطيات ذات الطابع الشخصي. ومن ثم، فإن فعاليتها تتحقق من خلال تكاملها مع باقي آليات الرقابة القانونية.

الفرع الثالث: المحافظة السامية للرقمنة

تعتبر المحافظة السامية للرقمنة مؤسسة عمومية ذات طابع خاص، تتمتع بالشخصية المعنوية والاستقلال المالي وتوضع تحت وصاية رئاسة الجمهورية ولقد اسندت لها عدة صلاحيات بموجب المرسوم الرئاسي رقم 314-23⁽¹⁾، ومن بينها تنظيم ومتابعة تنفيذ لاستراتيجية الوطنية للرقمنة، وضمان توافقها مع متطلبات أمن الأنظمة المعلوماتية بالتشاور مع القطاعات المعنية، وتعزيز السيادة الرقمية بالاهتمام بالمنتج الوطني وتنمية الموارد البشرية والكفاءات الوطنية المطلوبة في مجال الرقمنة⁽²⁾ كما تعتبر الفاعل المحوري في تفعيل منظومة حوكمة البيانات، إذ أسند إليها أيضا المرسوم الرئاسي رقم 25-320 دوراً مركزياً في تنظيم البيانات الوطنية وضبط طرق التعامل معها. فبموجب المادة 8 من المرسوم، أوكلت إلى المحافظة السامية للرقمنة مهمة إعداد المراجع الوطنية لتصنيف البيانات وفهرسة مصادرها، وهي المراجع التي تُشكّل الأساس الذي تُبنى عليه عملية تنظيم البيانات داخل مختلف الهيئات والإدارات والمؤسسات العمومية. وتحدّد هذه المراجع المعايير التقنية والأمنية الواجب احترامها عند تصنيف البيانات واستعمالها، بما يضمن توحيد طرق التعامل معها على المستوى الوطني.

ولا تقوم المحافظة بإعداد هذه المراجع بمعزل عن باقي القطاعات، بل، تعمل على إشراك الجهات المعنية، كلّ حسب مجال اختصاصه، وذلك قصد ملاءمة معايير التصنيف مع طبيعة البيانات المتداولة في كل قطاع. ويهدف هذا التنسيق إلى ضمان واقعية المعايير وقابليتها للتطبيق، وتقادي فرض نماذج موحدة لا تراعي خصوصيات القطاعات المختلفة.

ويمتد دور المحافظة إلى متابعة تنفيذ هذه المعايير ميدانياً، من خلال تقييم مدى التزام الإدارات بها، والعمل على تحيينها وتحديثها كلما دعت الحاجة، خاصة في ظل التطورات التكنولوجية المتسارعة. ويعكس هذا

1 - انظر المرسوم الرئاسي رقم 23-314، المؤرخ في 6 سبتمبر 2023، يتضمن انشاء المحافظة السامية للرقمنة وتحديد مهامها وتنظيمها وسيرها جريدة رسمية عدد 59، صادر في 10 سبتمبر 2023.

2 - وهذا ما نصت عليه المادة 4 من المرسوم الرئاسي رقم 23-314، مرجع سابق.

الدور حرص المشرع على أن تبقى مراجع التصنيف أدوات تنظيمية ديناميكية، لا قواعد جامدة تفقد فعاليتها مع الزمن⁽¹⁾.

كما يبرز دور المحافظة بصورة غير مباشرة من خلال اشتراط تصنيف البيانات كشرط أساسي للانضمام إلى النظام الوطني للتشغيل البيئي، إذ لا يُسمح بتبادل البيانات بين الإدارات إلا بعد تنظيمها وتصنيفها وفق المرجع المعتمد. ويُسهم هذا الشرط في دفع الإدارات إلى تحسين تسيير قواعد بياناتها الداخلية، وتعزيز انسجامها مع المنظومة الوطنية لحوكمة البيانات⁽²⁾.

وإلى جانب دورها التنظيمي، تضطلع المحافظة السامية للرقمنة بدور تقني يتمثل في توفير البنية التحتية للشبكة الوطنية المؤمنة، المنفصلة عن شبكة الإنترنت العامة، والتي تشكل الإطار العملي لتبادل البيانات المصنفة بطريقة آمنة⁽³⁾.

مما سبق، ورغم وضوح توزيع الاختصاصات بين الهيئات المكلفة بتطبيق منظومة حوكمة البيانات، إلا أن تعدد الفاعلين المؤسستين قد يؤدي، في غياب تنسيق عملي، صعوبات في اتخاذ القرار أو تداخلا في الأدوار. فالتطبيق السلس للمنظومة يفترض انسجاما دائما بين الجهات المشرفة على التصنيف، والأمن، وحماية المعطيات الشخصية، والتشغيل البيئي.

خاتمة

يتبين من خلال هذه الدراسة أن المرسوم الرئاسي رقم 25-320 المتعلق بإحداث منظومة وطنية لحوكمة البيانات يمثل خطوة هامة في تحديث المنظومة القانونية الجزائرية في المجال الرقمي، فقد ساهم هذا المرسوم في معالجة إشكالات واقعية التي كانت تعاني منها الإدارة العمومية في مجال تنظيم البيانات، والتي كانت تعاني لسنوات من تشتت البيانات، وتعدد مصادرها، وضعف التنسيق بين الإدارات المختلفة. جاء هذا النص استجابة لحاجة تنظيمية حقيقية، تهدف إلى وضع إطار موحد ينظم كيفية إنتاج البيانات العمومية واستعمالها وتبادلها.

وأظهر التحليل أن المشرع الجزائري اتبع في بناء منظومة الحوكمة، بتحديد المفاهيم الأساسية المرتبطة بالبيانات، ثم انتقل إلى وضع آليات عملية لمعالجة الاختلالات القائمة، من خلال توحيد التصنيف، وفهرسة مصادر البيانات، واعتماد نظام وطني للتشغيل البيئي.

1 - وهذا ما نصت عليه المادة 12 من المرسوم الرئاسي رقم 25-320، مرجع سابق.

2 - انظر المادة 17، المرسوم الرئاسي رقم 25-320، مرجع سابق.

3 - انظر المادة 11 من المرسوم الرئاسي رقم 25-320، مرجع نفسه.

كما أبرز المرسوم أهمية الجانب المؤسسي في تفعيل حوكمة البيانات، من خلال توزيع الأدوار بين عدة هيئات، مع إسناد دور تنسيقي محوري للجهات المكلفة بالرقمنة. وفي الوقت نفسه، حرص المشرع على وضع حدود واضحة لتطبيق المنظومة، سواء باستثناء المعطيات ذات الطابع الشخصي وإخضاعها لتشريعها الخاص، أو باستثناء المجالات الأمنية والقضائية، بما يحقق توازنًا بين تنظيم العمل الإداري وحماية المصالح السيادية للدولة.

وعليه، يمكن القول أن هذا المرسوم يمثل خطوة هامة في مسار بناء إدارة عمومية قائمة على البيانات، ومع ذلك، لا يمكن اعتباره حلًا نهائيًا لجميع التحديات المرتبطة بالتحول الرقمي. فنجاح منظومة حوكمة البيانات يعتمد إلى حد كبير على مدى فعالية تطبيق الآليات التي نص عليها المرسوم، بالإضافة إلى قدرة الإدارات والهيئات المعنية على التنسيق فيما بينها.

قائمة المراجع

أولاً- المقالات

- 1- العيداني محمد، يوسف زروق، "حماية المعطيات الشخصية في الجزائر على ضوء القانون 18-07"، مجلة معالم للدراسات القانونية و السياسية، العدد الخامس، 2018، ص ص 115-130.
- 2 - جوهر قويدر صامت، "الضوابط القانونية لمعالجة البيانات الشخصية الكترونياً"، مجلة الدراسات القانونية المقارنة، المجلد 6، عدد 2، 2020، ص ص 465 - 485.
- 3- حزام فتيحة، "حماية الأنظمة الرقمية بين الآليات التقنية و أجهزة الحماية: قراءة في أحكام المرسوم الرئاسي 20-05"، مجلة الحقوق و العلوم الإنسانية، العدد الثالث، 2020، ص ص 172-190.
- 4- سوزان أحمد سلطان، أنير القحطاني، " استراتيجيات تعزيز جودة البيانات في نظم ادارة المعلومات: تحليل للتحديات و الفرص"، المجلة العربية الدولية لادارة المعرفة، المجلد الرابع، العدد الرابع، 2025، ص ص 15-64.
- 5- عامر عبد الرزاق عبد المحسن، "أحمد زهر توفيق"، "التحديات المعاصرة لحوكمة بيانات الحوسبة السحابية في مراكز المعلومات، دراسة تحليلية"، المجلة الاقتصادية والإدارية للعلوم، المجلد 25، عدد 115، 2019، ص ص 172 - 190.

6- فوزية بن عيدة، رقية جومي، " حوكمة البيانات في مؤسسات التعليم العالي: الآليات الاستراتيجية، العوائق"، المجلة المغاربية للمخطوطات، المجلد 20، عدد 01، 2024، ص ص 155-190.

ثانيا - النصوص القانونية:

- 1 - مرسوم رئاسي رقم 20-442 مؤرخ في 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020، جريدة رسمية عدد 82، صادر في 30 ديسمبر 2020.
- 2 - قانون رقم 18-07 مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34، صادر بتاريخ 10 جوان 2018، المعدل والمتمم بالقانون رقم 25-11، المؤرخ في 24 يوليو 2025، جريدة رسمية عدد 48، صادر في 24 يوليو 2025.
- 3 - أمر رقم 21-09، مؤرخ في 8 يونيو 2021، يتعلق بحماية المعلومات والوثائق الإدارية، جريدة رسمية عدد 45، صادر في 9 يونيو 2021.
- 4 - مرسوم رئاسي رقم 20-05، مؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الانظمة المعلوماتية، معدل ومتمم بموجب المرسوم الرئاسي رقم 25-298، المؤرخ في 10 نوفمبر 2025، جريدة رسمية عدد 80، صادر في 30 نوفمبر 2025.
- 5 - مرسوم رئاسي رقم 23-314، مؤرخ في 6 سبتمبر 2023، يتضمن إنشاء المحافظة السامية للرقمنة وتحديد مهامها وتنظيمها وسيرها، جريدة رسمية عدد 59، صادر في 10 سبتمبر 2023.
- 6 - مرسوم رئاسي رقم 25-298 مؤرخ في 10 نوفمبر 2025، يعدل ويتمم المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الانظمة المعلوماتية، جريدة رسمية عدد 80 صادر في 30 نوفمبر 2025.
- 7 - مرسوم رئاسي رقم 25-321 مؤرخ في 30 ديسمبر 2025، يتعلق بوضع استراتيجية وطنية لأمن الانظمة المعلوماتية للفترة الممتدة من 2025 إلى 2029، جريدة رسمية عدد 87، صادر في 30 ديسمبر 2025.
- 8 - مرسوم رئاسي رقم 25-320 مؤرخ في 30 ديسمبر 2025، يتضمن وضع منظومة وطنية لحوكمة البيانات، جريدة رسمية عدد 87، صادر في 30 ديسمبر 2025.
- 9 - مرسوم رئاسي رقم 26-07 مؤرخ في 7 جانفي 2026، يتضمن انشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية وتحديد مهامه وتنظيمه وسيره، جريدة رسمية عدد 4، صادر في 18 جانفي 2026.