

المنظومة الوطنية لحوكمة البيانات في الجزائر:

قراءة قانونية - تقنية في المرسوم الرئاسي رقم 25-320

The National Data Governance System in Algeria:

A Legal-Technical Analysis of Presidential Decree No. 25-320

د. مناصرة يوسف *

جامعة يوسف بن خدة - الجزائر

menasra@hotmail.com

تاريخ نشر المقال: 06-06-2026

تاريخ قبول المقال: 25-04-2026

تاريخ إرسال المقال: 21-01-2026

الملخص:

يتناول هذا المقال تطوّر مقاربة المشرّع الجزائري لتنظيم البيانات، منتقلاً من منطق حماية المعطيات الشخصية الذي كرّسه القانون رقم 18-07 إلى تبني منظور أشمل يقوم على حوكمة البيانات بموجب المرسوم الرئاسي رقم 25-320. يهدف هذا المقال إلى تحليل الإطار القانوني والتنظيمي لحوكمة البيانات في الجزائر، في ضوء المرسوم الرئاسي، وبيان ما إذا كان هذا التحول يعكس نضجاً تشريعياً يتجاوز المقاربة التقليدية لحماية المعطيات الشخصية التي أرساها القانون رقم 18-07. ويسعى المقال إلى تحديد الغايات الحقيقية للمنظومة الوطنية لحوكمة البيانات من حيث تنظيم دورة حياة البيانات وضبط استعمالها، وتعزيز قيم النجاعة والشفافية والسيادة الرقمية. كما يبرز المقال حدود النموذج الجزائري وإمكاناته، ويقترح سبل تعزيز التنسيق المؤسساتي وتوضيح الأدوار بما يضمن تحقيق حماية البيانات وخدمة المصلحة العامة.

الكلمات المفتاحية: البيانات، حوكمة البيانات، حماية المعطيات الشخصية، السيادة الرقمية.

Abstract:

This article examines the evolution of the Algerian legislator's approach to data regulation, moving from a logic centered on the protection of personal data as enshrined in Law No. 18-07 to the adoption of a broader perspective based on data governance under Presidential Decree No. 25-320. The article aims to analyze the legal and regulatory framework for data governance in Algeria in light of the presidential decree, and to determine whether this shift reflects a level of legislative maturity that goes beyond the traditional approach to personal data protection established by Law No. 18-07. It seeks to identify the genuine objectives of the national data governance system in terms of organizing the data life cycle, regulating data use, and promoting the values of efficiency, transparency, and digital sovereignty. The article also highlights the limits and potential of the Algerian model and proposes avenues for strengthening institutional coordination and clarifying roles in a manner that ensures data protection and serves the public interest.

KEY WORDS: Data, Data Governance, Personal Data Protection, Digital Sovereignty.

* المؤلف المرسل

1- المقدمة:

لم تعد حوكمة البيانات مسألة اختيارية أو تنميقا تنظيمياً، بل أضحت التزاماً موضوعياً تفرضه طبيعة الاقتصاد الرقمي وكثافة المعالجة الآلية للبيانات¹. فالمؤسسات اليوم تحتفظ بكميات هائلة من البيانات المتعلقة بالأشخاص الطبيعيين والمعنويين، واستخدام هذه البيانات دون إطار حوكمي واضح يعرضها لمخاطر قانونية وتقنية جسيمة. ومن ثم، فإن حوكمة البيانات تمثل شرطاً مسبقاً لاستغلال البيانات بشكل مشروع وفعال، وليس مجرد أداة لتحسين الأداء.

وما يعزز هذا التوجه من زاوية قانونية وتنظيمية، هو تشريعات حماية المعطيات الشخصية، وعلى رأسها مبدأ المسؤولية Accountability ومبدأ دقة البيانات وواجب الأمن والسرية². فحوكمة البيانات تضمن موثوقية المعطيات وإمكانية تتبعها وتوثيقها، وتحدد قواعد الولوج إليها داخل المؤسسة، وهو ما يجعلها وسيلة عملية لاحترام متطلبات المشروعية والشفافية وحماية الحقوق الأساسية للأشخاص المعنيين بالبيانات. لذا فإن حوكمة البيانات هنا ليست خياراً إدارياً، بل امتداداً طبيعياً للالتزامات القانونية.

ويمثل انتقال المشرع الجزائري من القانون رقم 07/18، الذي ركّز أساساً على حماية المعطيات الشخصية، إلى إقرار منظومة وطنية لحوكمة البيانات بموجب المرسوم الرئاسي 25-320³، تعبيراً عن نضج تشريعي واضح. إذ لم يعد الهدف مقتصرًا على الحماية فقط، بل اتجه نحو تنظيم البيانات باعتبارها مورداً استراتيجياً يتطلب التنظيم والتنسيق والتبادل الآمن وحسن الاستغلال ويقتضي حوكمة شاملة توازن بين الاستغلال الآمن للبيانات ومتطلبات الأمن الرقمي مع ضمان حقوق وحرّيات الأشخاص الطبيعية.

-أهمية الموضوع

تكتسي حوكمة البيانات أهمية متزايدة في ظل التحول الرقمي الذي تشهده الإدارة العمومية⁴، لما لها من دور محوري في تحسين جودة القرار الإداري، وتعزيز النجاعة والشفافية، وضمان الاستغلال

¹ الإعتبار الأول من اللائحة (الاتحاد الأوروبي) رقم 868/2022 الصادرة عن البرلمان الأوروبي والمجلس المؤرخة في 30 ماي 2022 المتعلقة بحوكمة البيانات الأوروبية، والمعدّلة لللائحة (الاتحاد الأوروبي) رقم 1724/2018 لائحة حوكمة البيانات.

² د-مناصرة، يوسف، "الموازنات الكبرى بين متطلبات الأمن العام وحماية المعطيات الشخصية"، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 59، العدد 03، 2022، ص 448-465.

³ المرسوم الرئاسي رقم 25-320، المؤرخ في 10 رجب عام 1447 هـ الموافق 30 ديسمبر سنة 2025، يتضمن وضع منظومة وطنية لحوكمة البيانات. جريدة رسمية رقم 87، عدد 87 ص 4 بتاريخ 30 ديسمبر 2025.

⁴ ويرجع هذا التحول في الأهمية إلى جملة من الاتجاهات الأساسية، أبرزها الارتفاع الهائل في حجم البيانات المنتجة عالمياً، حيث يُتوقع أن يرتفع حجم البيانات السنوي من 4.4 زيتابايت سنة 2013 إلى نحو 44 زيتابايت بحلول سنة 2020. وقد أدى هذا التضخم في البيانات، القادمة من مصادر متعددة ومتباينة، إلى تفاقم مشكلات عدم الاتساق وجودة

الأمثل للبيانات العمومية. كما تبرز أهمية الموضوع من زاوية قانونية بالنظر إلى تدخل حوكمة البيانات مع حماية المعطيات ذات الطابع الشخصي، وما يثيره ذلك من تحديات تتعلق باحترام الحقوق والحريات الأساسية، لاسيما الحق في الخصوصية، في مقابل متطلبات المصلحة العامة وتبادل البيانات بين الهيئات العمومية.

-الإشكالية-

تتطلب الدراسة من إشكالية مفادها التساؤل حول مدى قدرة الإطار القانوني المنظم لحوكمة البيانات في الجزائر على تحقيق توازن فعلي بين تسهيل تبادل البيانات داخل الإدارة العمومية من جهة، وضمان حماية المعطيات ذات الطابع الشخصي من جهة أخرى.

-الفرضيات-

نفترض الدراسة أن المشرع الجزائري سعى من خلال النصوص القانونية والتنظيمية ذات الصلة إلى إرساء منظومة لحوكمة البيانات تقوم على مبدأ التدرج في مستوى حساسية البيانات، وتكريس ضوابط قانونية وتقنية لتبادلها. غير أن فعالية هذه المنظومة تبقى رهينة بمدى وضوح آليات التصنيف والفهرسة، وتكاملها مع قواعد حماية المعطيات الشخصية، وكذا بقدرة الهياكل المكلفة على التطبيق السليم للنصوص.

-المنهجية المتبعة-

للإجابة على الإشكالية، تعتمد الدراسة على المنهج التحليلي الوصفي، من خلال تحليل النصوص القانونية والتنظيمية المتعلقة بحوكمة البيانات وحماية المعطيات الشخصية في الجزائر، مع الاستعانة بالمنهج المقارن عند الاقتضاء لإبراز بعض التجارب المقارنة من خلال تبني خطة ثنائية متوازنة تتناول أولا الإطار المفاهيمي والمقارن لحوكمة البيانات الذي يعالج حوكمة البيانات في التجارب المقارنة و يميّط اللثام عن المفاهيم القريبة منها، أما في المسألة الثانية نشرح فيها المنظومة الوطنية لحوكمة البيانات في الجزائر وفق المرسوم الرئاسي أين نبين نطاق هذا الأخير ومقاصده التنظيمية ثم نخرج على مكونات وآليات عمل المنظومة الوطنية لحوكمة البيانات و ننتهي بخاتمة معصدة بالنتائج المتوصل إليها مع التوصيات.

2- الإطار المفاهيمي والمقارن لحوكمة البيانات

إن تعدد المقاربات الفقهية والتقنية لمفهوم حوكمة البيانات، وغياب تعريف معياري موحد له في الأبحاث الأكاديمية والتطبيقية، يطرح إشكالا حقيقيا على مستوى الضبط المفاهيمي والتأطير القانوني.

هذا التباين لا يعكس قصورًا معرفيًا بقدر ما يجسّد حادثة المفهوم وتداخله مع مفاهيم قريبة كإدارة البيانات وحمايتها واستغلالها. ومن ثم، يصبح من الضروري التوقف عند الإطار المفاهيمي لحوكمة البيانات، قصد توضيح مضمونها، وتحديد عناصرها المميزة، وبيان حدودها الوظيفية والتنظيمية، تمهيدًا لتحليل تجلياتها القانونية في التشريع الجزائري⁵.

يُقصد بحوكمة البيانات الإطار القانوني والتنظيمي الذي يضبط كيفية جمع البيانات وتنظيمها وتبادلها واستعمالها داخل المؤسسات بهدف إرساء أجندة موحّدة على مستوى المؤسسة ككل فيما يخص البيانات⁶، مع تحديد المسؤوليات وضمان الجودة⁷ والأمن والشفافية⁸. وهي مفهوم يتجاوز الإدارة التقنية للبيانات، ليشمل وضع قواعد ومعايير واضحة تحكم دورة حياة البيانات كاملة، بما يضمن حسن استغلالها مع احترام القوانين ذات الصلة وعلى رأسها حماية المعطيات ذات الطابع الشخصي⁹ ومتطلبات الأمن المعلوماتي.

وعلى المستوى المقارن، اتجهت عدة تشريعات حديثة إلى تكريس حوكمة البيانات كخيار استراتيجي، خاصة في التجربة الأوروبية التي أرست إطارًا متكاملًا من خلال قانون حوكمة البيانات وقانون البيانات، بهدف تعزيز تقاسم البيانات في بيئة آمنة قائمة على الثقة. كما اعتمدت دول أخرى مقاربات تنظيمية متفاوتة تراعي خصوصياتها المؤسسية، وهو ما يعكس وعيًا متزايدًا بأن حوكمة البيانات أصبحت أداة أساسية لتحقيق النجاعة الإدارية، والسيادة الرقمية، وحماية الحقوق في آن واحد.

1.2- حوكمة البيانات في التجارب المقارنة

إن تجربة الاتحاد الأوروبي من خلال قانون حوكمة البيانات¹⁰ Data Governance Act، ثم التجربة المكتملة المتمثلة في قانون البيانات¹¹ Data Act من الأمثلة الرائدة التي نستشهد بها حيث يُعدّ

⁵ Zorn, T. E., & Campbell, N. (2006). *Improving the writing of literature reviews through a literature integration exercise*. Business Communication Quarterly, 69(2), 172–183, p. 175.

⁶ Dyché, J., & Levy, E., *Customer Data Integration: Reaching a Single Version of the Truth*, Wiley, 2006, p. 150.

⁷ Kim, Y., & Cho, J., “Data quality management,” *Sustainability*, 2018, p. 386.

⁸ DAMA International, 2009, p. 41; Morabito, V, *Big Data and Analytics*, Springer, 2015, p.99.

⁹ القانون رقم 07-18 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص

الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر عدد 34، ص 11 بتاريخ 10 يونيو 2018.

¹⁰ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

<http://data.europa.eu/eli/reg/2022/868/oj>

¹¹ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

القانون امتدادًا طبيعيًا للائحة العامة لحماية البيانات RGPD¹² وللاستراتيجية الأوروبية للبيانات إضافة إلى تجربة المملكة المتحدة في مجال استعمال البيانات والوصول إليها Data Use and Access و هو ما نستعرضه كمثال من دول القانون المكتوب و السوابق ثم بالمختصر نعرض في لمحة جد وجيزة على التجارب العربية التي اعتمدت تنظيمات قطاعية أو توجيهات إدارية دون إقرار قانون شامل لحوكمة البيانات، مع بيان وجه القصور الكلي مقارنة بالنماذج الأوروبية.

2-1-1- التجارب الدولية الرائدة

هناك تجارب وتشريعات مماثلة للتشريع الجزائري الذي سبقته واستقى منها أحكامه في دول ومنظمات دولية تتناول حوكمة البيانات في إطار قانوني لتنظيم تبادلها واستعمالها بأمان وفعالية، بعضها يقارب من حيث المبدأ ما نصّ عليه المرسوم الرئاسي الجزائري رقم 25-320 (منظومة وطنية لحوكمة البيانات)، مع اختلافات في التركيز والمضمون حسب السياقات القانونية والسيادية.

ولعل تجربة الاتحاد الأوروبي في قانون حوكمة البيانات، أول مصدر نستذكره كمنبع لكثير من النصوص القانونية للدول، فلقد أصدر الاتحاد الأوروبي اللائحة (EU) رقم 868/2022 المؤرخة في 30 ماي 2022، المعروفة باسم قانون حوكمة البيانات DGA، والمنشورة في الجريدة الرسمية للاتحاد الأوروبي¹³ حيث يهدف هذا النص إلى وضع إطار قانوني موحد لحوكمة البيانات داخل الاتحاد الأوروبي، من خلال تنظيم إعادة استعمال البيانات التي تحتفظ بها الهيئات العمومية، وتسهيل تبادل البيانات بين الإدارات والفاعلين الاقتصاديين، مع احترام قواعد حماية المعطيات الشخصية والأمن العام. ويسعى هذا التنظيم إلى تعزيز القيمة الاقتصادية للبيانات، ودعم السيادة الرقمية الأوروبية، وخفض كلفة الوصول إلى البيانات ومعالجتها، مع تنظيم إعادة استعمال بعض بيانات القطاع العام، وتأطير خدمات وساطة البيانات، وتشجيع الاستعمال الايثاري للبيانات لأغراض المصلحة العامة، تحت رقابة سلطات وطنية مختصة في مجال البيانات مع احترام صارم لقواعد الأمن وعدم تعارض نقل البيانات دوليًا مع التشريع الأوروبي¹⁴.

¹² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

¹³ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) Published in the Official Journal of the European Union (L 152) — يسري اعتبارًا من 24 سبتمبر 2023.

¹⁴ د. مناصرة يوسف، المعطيات الشخصية و الجريمة في التشريع الجزائري و المقارن، دار الخلدونية، 2025.

ويُعد هذا القانون أقرب نموذج مقارنة للمرسوم الجزائري، من حيث التركيز على تنظيم تداول البيانات العمومية، ووضع آليات مؤسسية وتقنية لضمان التشغيل البيئي وتبادل البيانات بشكل منظم وآمن.

إلى جانب قانون حوكمة البيانات، اعتمد أيضا الاتحاد الأوروبي قانون البيانات Data Act ، وهو تشريع يُنشئ إطاراً قانونياً موحداً لتنظيم الوصول إلى البيانات المتولدة عن الأشياء المتصلة واستعمالها وتحديد قواعد مشاركتها بين الهيئات العمومية والفاعلين الاقتصاديين بهدف تعزيز اقتصاد بيانات أكثر انفتاحاً وتنافسية داخل الاتحاد الأوروبي. ويعزز هذا الإطار حقوق مستخدمي هذه الأشياء، من خلال تمكينهم من الوصول إلى بياناتهم ومشاركتها مع أطراف ثالثة بشروط عادلة وشفافة، مع فرض التزامات جديدة على المصنعين وحائزي البيانات، ولا سيما منذ مرحلة التصميم. كما ينظم القانون تبادل البيانات ويمنع الشروط التعاقدية التعسفية، ويسهل الانتقال بين مزودي الخدمات السحابية، مع التأكيد على أولوية تطبيق اللائحة العامة لحماية البيانات GDPR كلما تعلّق الأمر ببيانات شخصية، وعلى التكامل مع قانون حوكمة البيانات DGA في تشجيع تقاسم البيانات بشكل آمن ومنظم¹⁵.

ويُكمل هذا النص الإطار الأوروبي لحوكمة البيانات، ويعكس توجهاً عاماً نحو اعتبار البيانات مورداً استراتيجياً يتطلب تنظيماً قانونياً خاصاً، وهو نفس المنطق الذي تبناه المرسوم الجزائري.

وثاني تجربة من دول القانون الانجلوساكسوني بالمملكة المتحدة (قانون استعمال والوصول إلى البيانات)، أين أصدر البرلمان البريطاني قانون Data Use and Access Act لسنة 2025، الفصل 18 ، والمنشور في الموقع الرسمي للتشريعات البريطانية¹⁶. وهو تشريع بريطاني حديث يهدف إلى تحديث الإطار القانوني المنظم لاستعمال البيانات وتبادلها خاصة داخل القطاع العام مع تبسيط الإجراءات وتعزيز فعالية استخدام البيانات في تقديم الخدمات العمومية، دون المساس بضمانات حماية الحياة الخاصة.

ويأتي هذا القانون ليطور أحكام القواعد القائمة، ولا سيما اللائحة العامة لحماية البيانات في صيغتها البريطانية UK GDPR، من خلال إدخال قدر أكبر من المرونة التنظيمية وتبسيط آليات تقاسم البيانات. كما ينص على اعتماد نظم «البيانات الذكية» على غرار الخدمات المصرفية المفتوحة، ويوضح القواعد المتعلقة باتخاذ القرارات المؤتمتة، ويعزز حقوق أصحاب البيانات في تقديم الشكاوى، مع تسهيل

¹⁵ Federico Casolari, Carlotta Buttaboni, Luciano Floridi, The EU Data Act in context: a legal assessment, International Journal of Law and Information Technology, Volume 31, Issue 4, Winter 2023, Pages 399–412, <https://doi.org/10.1093/ijlit/eaee005>

¹⁶ Data (Use and Access) Act 2025 (c. 18) (DUAA). Department for Science, Innovation and Technology, Data (Use and Access) Act factsheet: UK GDPR and DPA, published on 27 June 2025, accessed on 08/01/2026

استخدام ملفات تعريف الارتباط لأغراض التحليل¹⁷. وإلى جانب ذلك، يعيد القانون تنظيم هيئة حماية البيانات بإنشاء مفوضية معلومات جديدة، على أن يتم تطبيق أحكامه بشكل تدريجي ما بين منتصف عامي 2025 و 2026، في إطار يسعى إلى تحقيق توازن دقيق بين الاستغلال الاقتصادي للبيانات ووصون الحقوق والحريات الفردية¹⁸.

وعلى الرغم من أن هذا القانون لا ينشئ منظومة وطنية لحوكمة البيانات بالمعنى التنظيمي الصارم، إلا أنه يشترك مع المرسوم الجزائري في السعي إلى عقلنة استخدام البيانات العمومية وتحسين تبادلها داخل الإدارة.

2-1-2- التجارب العربية وحدود المقاربة التنظيمية

في بعض الدول العربية، لا توجد إلى حدّ الآن قوانين شاملة ومتكاملة لحوكمة البيانات، لكن وُضعت سياسات وطنية أو أطر تنظيمية تمهيدية. و الملاحظ أن العديد من البلدان العربية لم تصدر بعد قوانين متكاملة لحوكمة البيانات مثل تلك الموجودة في أوروبا أو بريطانيا، وإنما بدأ بعضها بإصدار سياسات وطنية للبيانات المفتوحة أو أطر تنظيمية أولية تمهيداً لتشريعات لاحقة و تركز الأطر الحالية غالباً على البيانات الحكومية غير الحساسة وتحسين الوصول إليها وتنظيم نشرها وشفافيتها أكثر من تنظيم شامل لإدارة البيانات العامة والخاصة داخل منظومة وطنية.

توجد حالياً ديناميكيات متسارعة في المنطقة نحو تبني تشريعات أوسع تشمل حوكمة البيانات وحماية المعطيات الشخصية على حد سواء، خاصة في مصر وعُمان والسعودية.

ففي جمهورية مصر العربية، تم اعتماد سياسة البيانات المفتوحة سنة 2025، وهي وثيقة تنظيمية تهدف إلى تنظيم إتاحة البيانات الحكومية وتبادلها، مع الإعلان عن مشروع مستقبلي لإنشاء هيئة لحوكمة البيانات¹⁹.

أما في المملكة العربية السعودية، فقد تم تطوير منصات وطنية للبيانات المفتوحة، في إطار سياسات تنظيمية، دون صدور قانون موحد خاص بحوكمة البيانات إلى غاية الآن²⁰.

¹⁷ Information Commissioner's Office, The Data Use and Access Act 2025 (DUAA) - what does it mean for organisations?. <https://ico.org.uk/>. [09/01/2026]

¹⁸ Guidance, Data (Use and Access) Act 2025: data protection and privacy changes. A summary of changes to the UK's data protection and privacy legislation in the Data (Use and Access) Act. <https://www.gov.uk/guidance/>

¹⁹ نصت السياسة الوطنية للبيانات المفتوحة، كإطار انتقالي، على إنشاء «الهيئة المصرية لحوكمة البيانات EDGA بوصفها الجهة التي يُفترض أن تنقل الإتاحة من وعود عامة إلى ممارسة قابلة للتنفيذ. وفي المرحلة الحالية، يشرف المجلس الوطني للذكاء الاصطناعي على التنفيذ، على أن تنتقل المهام لاحقاً إلى الهيئة بعد إنشائها تشريعياً.

<https://ai.gov.eg/>. [15/01/2026]

يتبين من خلال هذه التجارب أن المرسوم الرئاسي الجزائري رقم 25-320 يندرج ضمن اتجاه دولي عام يهدف إلى تنظيم تداول البيانات العمومية وضمان التشغيل البيئي بين الإدارات و حماية المعطيات الحساسة وتكريس دور الدولة في حوكمة البيانات باعتبارها مورداً سيادياً. فالنموذج الجزائري بكونه نصاً تنظيمياً مباشراً ينشئ منظومة وطنية واضحة المعالم، في حين اعتمدت بعض الدول الأخرى مقاربة تشريعية تدريجية أو قطاعية.

2-2- الإطار المفاهيمي لحوكمة البيانات وتمييزها عن المفاهيم القريبة

استُخدم مصطلح الحوكمة على نطاق واسع خلال العقدين الأخيرين، غير أن معناه لا يزال يتسم بالغموض ومن خلال النقاشات القائمة في علم السياسة ودراسات المخاطر تُفهم الحوكمة باعتبارها «تعدّد الفاعلين والعمليات التي تقضي إلى اتخاذ قرارات جماعية مُلزِمة»²¹ وتشير الحوكمة بوجه عام، إلى شبكة الفاعلين المنخرطين في عملية إدارة نظام ما، مع اختلاف أدوارهم ومسؤولياتهم. ويؤكد هذا المصطلح القطيعة مع نموذج «الأمر والضبط» التقليدي الذي تمارسه الدولة، ويُقرّ في المقابل بأن إدارة المجتمعات أصبحت تشارك فيها مجموعة أوسع من الفاعلين والمؤسسات، بما في ذلك القطاع الخاص والمجتمع المدني وغيرها من الكيانات غير الحكومية²².

وتُعرّف حوكمة البيانات بأنها ممارسة السلطة والرقابة على إدارة البيانات داخل المنظمة، بما يشمل وضع القواعد وتحديد المسؤوليات وآليات الإشراف على دورة حياة البيانات²³.

يوضح هذا الفرع أن حوكمة البيانات لا تُعد إدارة بيانات بالمعنى التقني، ولا إدارة بيانات مرجعية MDM، كما لا تختزل في Data Stewardship و يُبرز الفروق الوظيفية والتنظيمية. كما يُبرز العلاقة التكاملية بين حوكمة البيانات وإدارة البيانات المرجعية ودور القائمين على البيانات داخل منظومة الحوكمة خاصة في البيئات الرقمية المعقّدة كالحوسبة السحابية.

²⁰ Strigence. "From Compliance to Competitiveness: The Rise of Data Governance in the GCC." Strigence Advisory Desk, 6 June 2025, www.strigence.com/blog/from-compliance-to-competitiveness-the-rise-of-data-governance-in-the-gcc. [18/11/2025].

²¹ Van Asselt, Marjolein BA et RENN, Ortwin. Risk governance. Journal of risk research, 2011, vol. 14, no 4, p. 431-449.

²² Marina Micheli, Marisa Ponti, Max Craglia, Anna Berti Suman, Emerging models of data governance in the age of datafication.,journal Big Data\ Society, Vol.7 N°2 , 2020. doi:10.1177/2053951720948087

Marina Micheli, Marisa Ponti, Max Craglia, Anna Berti Suman

²³ DAMA International, *The DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK)*, 1st ed., Technics Publications, 2009, p. 19.

2-2-1- التمييز بين حوكمة البيانات والمفاهيم التقنية المجاورة

غالبًا ما يتم الخلط بين حوكمة البيانات ومفاهيم أخرى قريبة منها، مثل إدارة البيانات وتسيير البيانات المرجعية MDM²⁴. ويرجع هذا الخلط إلى تداخل هذه المفاهيم في الممارسة العملية، رغم اختلافها من حيث الدور والمستوى الوظيفي داخل المنظمة²⁵. فحوكمة البيانات لا تعني القيام بالمعالجة التقنية للبيانات بحد ذاتها، وإنما وضع الإطار الذي ينظم كيفية هذه المعالجة ومن يتحمل مسؤوليتها.

أ - حوكمة البيانات ليست هي إدارة البيانات

تعني إدارة البيانات تسيير جميع احتياجات المؤسسة المتعلقة بالبيانات، من جمعها وتخزينها ومعالجتها وتأمينها واستغلالها. أما حوكمة البيانات فهي تمثل الركيزة الأساسية داخل هذا النظام الشامل، إذ تقوم بدور التنسيق والربط بين مختلف التخصصات المرتبطة بالبيانات، مثل جودة البيانات، وإدارة البيانات المرجعية، وأمن البيانات، وإدارة قواعد البيانات، وإدارة البيانات الوصفية (الميتاداتا)، ومستودعات البيانات. وبذلك، يمكن القول إن حوكمة البيانات لا تنفذ العمليات، بل تضع القواعد التي تحكم تنفيذها²⁶.

ب - حوكمة البيانات ليست إدارة البيانات المرجعية

تركّز إدارة البيانات المرجعية على تحديد الكيانات الأساسية داخل المؤسسة، مثل الزبائن أو الموردين أو المرضى، ثم تحسين جودة البيانات المتعلقة بها لضمان دقتها واكتمالها. ونظرًا لأن هذه الكيانات تُستعمل من قبل مختلف المصالح، فإن البيانات المرجعية تهدف إلى توحيد الرؤى الجزئية في رؤية شاملة واحدة. ورغم أن هذا المجال يتجاوز من حيث التطبيق نطاق حوكمة البيانات، إلا أنه لا يمكن تصوّر إدارة بيانات مرجعية فعالة دون وجود حوكمة بيانات سليمة تحدد النماذج الأساسية للبيانات، وقواعد الاحتفاظ بها، وصلاحيات الإدخال والتعديل والاطلاع²⁷.

ج - حوكمة البيانات ليست Data Stewardship

تختلف حوكمة البيانات عن مفهوم الإشراف على البيانات Data Stewardship من حيث المستوى والدور. فحوكمة البيانات تعمل على المستوى الاستراتيجي والتنظيمي حيث تحدد السياسات والأدوار والهياكل والقواعد العامة. أما الإشراف على البيانات فينصرف إلى الجانب التنفيذي، إذ يهدف إلى ضمان أن تكون البيانات دقيقة ومضبوطة وسهلة الاكتشاف والاستعمال من قبل الفاعلين المعنيين²⁸.

²⁴ Master Data Management, OR MDM

²⁵ DataGalaxy. "Gouvernance des données : définition, enjeux et bonnes pratiques." DataGalaxy Blog, (<http://www.datagalaxy.com/fr/blog/gouvernance-des-donnees-definition/>). [08/01/2026]

²⁶ Talend. "Guide de la gouvernance des données." Talend Resources, Talend, (<http://www.talend.com/fr/resources/guide-gouvernance-donnees/>). Accessed 18. 01. 2026.

²⁷ Ibid.

²⁸ Ibid

2-2-2- العلاقة التكاملية بين الحوكمة، إدارة البيانات، والقائمين عليها

تتجلى أهمية حوكمة البيانات في كونها تضع الأسس التي تُبنى عليها إدارة البيانات المرجعية، مثل تعريف المفاهيم الأساسية (من هو العميل؟ ما هو المنتج؟)، وتحديد قواعد حفظ البيانات، وتوزيع الأدوار والمسؤوليات بين من يُدخل البيانات، ومن يجمعها، ومن يملك حق الولوج إليها. ومن دون هذه القواعد، تصبح إدارة البيانات المرجعية مجرد عملية تقنية معزولة، معرضة للتناقض والأخطاء²⁹.

ويتولى القائمون على البيانات Data Stewards أو Arbitres de données إدارة عناصر البيانات عملياً، والسهر على مطابقتها لمخطط حوكمة البيانات المعتمد. كما يضمنون ترابط البيانات مع غيرها والتحكم في جودتها واحترامها لمتطلبات الامتثال والأمن. وبهذا المعنى، فإنهم يشكلون حلقة الوصل بين الإطار النظري لحوكمة البيانات والتطبيق العملي اليومي داخل المؤسسة³⁰.

أخيراً نصل إلى نتيجة أن حوكمة البيانات هي الإطار الناظم الذي يحدد "من يقرر" و"وفق أي قواعد"، بينما تتكفل إدارة البيانات وMDM وData Stewardship بتنفيذ هذه القرارات عملياً. وكلما كان هذا الإطار واضحاً ومُحكماً كلما كانت منظومة البيانات أكثر موثوقية وفعالية.

3- المنظومة الوطنية لحوكمة البيانات في الجزائر وفق المرسوم الرئاسي 25-320

لاستكمال سيادة المشرع الجزائري على البيانات الوطنية انتقل من قانون حماية المعطيات الشخصية رقم 07/18 إلى اعتماد مفهوم حوكمة البيانات الذي صدر حديثاً بموجب المرسوم الرئاسي رقم 25-320 في الجريدة الرسمية الجزائرية رقم 87 بتاريخ 30 ديسمبر 2025، وهو نص تنظيمي يتضمن وضع منظومة وطنية لحوكمة البيانات على مستوى الإدارة العمومية في الجزائر.

وينشئ المرسوم إطاراً وطنياً موحداً لحوكمة البيانات داخل الإدارة العمومية، يتناول تنظيم تبادل البيانات وحمايتها وتسييرها بين المؤسسات والإدارات العمومية ويتضمن النص تنظيماً تقنياً ومؤسسياً لإنشاء النظام الوطني للتشغيل البيئي ومراجع التصنيف والفهرسة وأدوار الجهات المعنية مثل مجلس أمن الأنظمة المعلوماتية والسلطة الوطنية لحماية المعطيات الشخصية والمحافظة السامية للرقمنة.

²⁹ Talend. "Guide de la gouvernance des données." Talend Resources, Talend, . Accessed 18. 12. 2026

³⁰ Nielsen, J. A., Persson, J. S., & Madsen, S., "Challenges of enterprise architecture," *Journal of Enterprise Architecture*, 2018, p. 22.

كما يستثنى من تطبيقه بيانات الأمن والدفاع الوطني، وكذلك البيانات المرتبطة بالسلطة القضائية والعمليات القضائية والتحقيقات.

و قد ورد النص في 20 مادة قانونية، موزعة على الإطار المفاهيمي والتعريف (المواد 1-4)، والبنية التقنية والتنظيمية لمنظومة حوكمة البيانات (المواد 5-13)، وتوزيع الاختصاصات بين الهيئات المشرفة (المواد 14-17)، الاستثناءات الجوهرية ولاسيما ما يتصل بالأمن الوطني والسلطة القضائية (المادة 18)، وأحكام النفاذ والتنفيذ (المواد 19-20).

1.3- نطاق المرسوم الرئاسي ومقاصده التنظيمية

يتناول هذا الجزء مقاصد المرسوم الرئاسي ومزايا اعتماد حوكمة البيانات على مستوى الإدارة العمومية، من حيث تحسين الأداء و ضمان الأمن وتعزيز الثقة في تداول البيانات. و يُحلّل العلة من استثناء القطاع الخاص من نطاق التطبيق و يبين البيانات المستثناة من التنظيم، مع توضيح الخلفيات القانونية والأمنية لهذه الاختيارات.

1.3-1- أهداف المرسوم ومزايا حوكمة البيانات

الأصل في قوانين الحوكمة أنها تحقق مقاصد ومبادئ كبرى³¹ تتمثل إستراتيجية حوكمة و ضبط للمحركات التشغيلية، حماية للبيانات الحساسة، وتوضيح نسبي للأدوار والمسؤوليات³². و بتمعن دقيق في المرسوم الرئاسي، أعتقد أنه يحقق هذه المقاصد بدرجة معتبرة من حيث البناء المفاهيمي والتنظيمي، لكنه يحققها على نحو تدريجي ومشروط بالتنفيذ، وليس على نحو مكتمل وفوري كما تقترضه نماذج حوكمة البيانات المتقدمة في بيئات الـ Big Data. لكنه يظل إطاراً تأسيسياً يحتاج إلى استكمال بنصوص تطبيقية، وبنضج مؤسسي وتقني، حتى يرقى إلى نموذج حوكمة بيانات متكامل بالمعايير المعتمدة في أنظمة الـ Big Data والامتثال المقارن على رأسها النموذج الأوروبي و ذلك للإعتبارات التالية المستخلصة من المواد العشرين للمرسوم الرئاسي:

أولاً، من زاوية وجود إستراتيجية واضحة لحوكمة البيانات، فإن المرسوم يؤسس فعلاً لإطار استراتيجي وطني لحوكمة البيانات العمومية، من خلال توحيد المبادئ الحاكمة لمعالجة البيانات، وضبط أغراض استعمالها، وتنظيم تبادلها البيئي بين الإدارات. هذا التوجه ينسجم مع الفكرة الجوهرية التي وردت في النص الفرنسي، والتي تجعل من الحوكمة أداة لتحقيق الانسجام وتقاسم المسؤوليات وتوحيد الإجراءات. غير أن المرسوم، بطبيعته كنص تنظيمي عام، لا يفصل الإستراتيجية التشغيلية الدقيقة

³¹ DAMA International. DAMA-DMBOK: Data Management Body of Knowledge. 2nd ed., Technics Publications, 2017, pp. 19-41. <https://dama.org/dmbok2r-infographics/>

³² Khatri, V., & Brown, C. V., "Designing data governance" *MIS Quarterly*, 2010, p. 151

الخاصة بكل قطاع، بل يترك ذلك للنصوص التطبيقية والسياسات القطاعية، وهو ما يعني أن الإستراتيجية موجودة كإطار موجّه أكثر منها كخطة تشغيلية مكتملة التفاصيل.

ثانياً، فيما يتعلق بالمحركات التشغيلية (moteurs opérationnels)، فإن المرسوم يستجيب لها من حيث المبدأ، لا سيما عندما يربط بين طبيعة البيانات ومستوى حساسيتها، ويفرض تصنيفها وفهرستها وتحديد شروط الولوج إليها. هذا يسمح نظرياً بتحديد أي البيانات يجب التحكم فيها بدقة أكبر، وما هي المنافع المنتظرة من ذلك، سواء تعلق الأمر بتحسين الأداء الإداري، أو تقليص المخاطر القانونية، أو حماية حقوق الأفراد. غير أن تحويل هذه المحركات إلى نتائج ملموسة يظل مرتبطاً بمدى قدرة كل إدارة على ترجمة هذه الالتزامات إلى إجراءات تقنية وتنظيمية فعلية، وهو تحدّي عملي لا يعالجه المرسوم وحده. ثالثاً، وبخصوص حماية البيانات الحساسة، مثل بيانات الصحة وضمان السرية والتتبع والامتثال، فإن المرسوم ينسجم مع هذا المقصد من حيث الفلسفة، إذ يكرس مبدأ المعالجة الآمنة، وتقيد الاستعمال بالغرض، وربط الولوج بالمشروعية. كما أن منطق التتبع (traceabilité) وحفظ السجلات، وإن لم يُفصل تقنياً كما هو الحال في القانون رقم 07/18، يظل حاضراً ضمناً من خلال إلزام الإدارات بتحديد المسؤوليات ومصادر البيانات وشروط استغلالها. غير أن الفارق الجوهرى هو أن المرسوم لا يرقى بعد إلى مستوى تنظيم دقيق لمتطلبات الاحتفاظ التاريخي بالبيانات وتوثيق التعديلات بنفس التفصيل الذي يفرضه التنظيم الأوروبي، ما يجعله أقرب إلى إطار امتثال عام منه إلى نظام تدقيق دقيق بالمعنى التقني الصارم.

رابعاً، من حيث تحديد الأدوار والمسؤوليات داخل منظومة حوكمة البيانات، فإن المرسوم يحقق مقصداً أساسياً يتمثل في إنهاء الغموض الذي كان يحيط بمسؤولية البيانات داخل الإدارة. فهو يكرس مبدأ تحديد المستخدم، مصدر البيانات، ومسؤولية المعالجة، وهو ما يشكل نواة صلبة لتوزيع الأدوار على المستويات الاستراتيجية والتكتيكية والتنفيذية. ومع ذلك، فإن اكتمال هذا الإطار يظل مرهوناً بإرساء وظائف متخصصة فعلية (مسؤولي بيانات، أمناء نظم معلومات، لجان حوكمة داخلية)، وهي عناصر لا يفرضها المرسوم صراحة، بل يفترضها ضمناً.

1.3-2- نطاق التطبيق والاستثناءات

ينحصر نطاق تطبيق المرسوم الرئاسي رقم 25-320 في تنظيم حوكمة البيانات الرقمية داخل الإدارة العمومية والهيئات والمؤسسات المكلفة بخدمة عمومية، وذلك من خلال وضع إطار وطني لتصنيف البيانات وفهرسة مصادرها وضمان تبادلها بطريقة آمنة ومنظمة عبر النظام الوطني للتشغيل البيني. ولا يمتد هذا النطاق إلى القطاع الخاص بصفته العامة، كما لا يمسّ بالأحكام الخاصة بحماية

المعطيات ذات الطابع الشخصي الخاضعة للقانون 18-07، ولا بالبيانات المرتبطة بالأمن والدفاع والمجال القضائي إلا في الحدود التي يحددها التشريع والتنظيم المعمول بهما.

أ- استثناء القطاع الخاص من نطاق تطبيق المرسوم الرئاسي رقم 25-320

يُستنتج من نص المادة 2 من المرسوم أنه تم استثناء القطاع الخاص من نطاق تطبيق المرسوم الرئاسي رقم 25-320 لأن هذا النص يندرج ضمن فئة النصوص التنظيمية الموجهة أساساً إلى الإدارة العمومية، ويهدف إلى ضبط كيفية إنتاج وتبادل واستعمال البيانات داخل أجهزة الدولة بما يخدم المرفق العام ويحسن أداء السياسات العمومية. ويعود هذا الاستثناء إلى اختلاف المركز القانوني للقطاع الخاص، الذي يقوم على مبدأ حرية المبادرة والاستقلال في التسيير، ويخضع في مجال البيانات لأطر قانونية خاصة، لاسيما القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي طبقاً لأحكام المادة 4 من المرسوم الرئاسي والتشريعات التجارية والمهنية. كما أن إدماج القطاع الخاص ضمن منظومة وطنية موحدة لحوكمة البيانات ذات طابع سيادي وتقني وأمني، قد يطرح مخاطر تتعلق بأمن الأنظمة المعلوماتية وحماية البيانات الحساسة للدولة، فضلاً عن احتمال المساس بحرية النشاط الاقتصادي. وعليه، فإن استثناء القطاع الخاص يُعدّ خياراً تشريعياً وظيفياً ومنهجياً، يعكس رغبة المشرع في حصر المنظومة في الفضاء الإداري العمومي في مرحلة أولى، مع إمكانية توسيعها لاحقاً بنصوص خاصة تضمن التوازن بين متطلبات الحوكمة وحماية الحقوق والحريات الاقتصادية.

ب- البيانات المستثناة من التنظيم في إطار المرسوم الرئاسي رقم 25-320

يُستخلص من نص المادة 18 من المرسوم الرئاسي رقم 25-320 أن الاستثناءات الواردة فيها لا ترمي إلى إقصاء بيانات أجهزة إنفاذ القانون أو المجال القضائي من أي تنظيم قانوني، بل تهدف أساساً إلى تحديد المجال الوظيفي الدقيق لمنظومة حوكمة البيانات التي أنشأها المرسوم. فهذه المنظومة تقوم على منطق إداري وتقني قوامه التشارك، التشغيل البيئي، وتدفق البيانات بين الإدارات العمومية لتحسين الأداء العمومي وصنع القرار. أما بيانات الأمن والتحقيقات القضائية، فهي بطبيعتها بيانات سيادية وحساسة، لا تتلاءم مع فلسفة التبادل والتشغيل البيئي، بل تخضع لمنطق مغاير يقوم على السرية، التقييد، والتحفّظ، حمايةً للنظام العام وحسن سير العدالة.

وعلى الرغم من أن القانون رقم 18-07 ينظم معالجة المعطيات ذات الطابع الشخصي، بما فيها تلك التي تعالجها أجهزة إنفاذ القانون والسلطة القضائية، إلا أن مجال تطبيقه يظل محصوراً في ضمان مشروعية المعالجة وحماية الحقوق والحريات الفردية، ولا يمتد إلى تنظيم البنية التقنية أو المؤسسية لتبادل البيانات ضمن منظومة وطنية موحدة. ومن ثمّ، فإن إخضاع بيانات التحقيقات القضائية أو الأعمال الأمنية لمنظومة حوكمة البيانات الإدارية قد يؤدي إلى تداخل غير محمود بين نظامين

قانونيين مختلفين: نظام حماية المعطيات الشخصية من جهة، ونظام إدارة وتدفق البيانات العمومية من جهة أخرى، بما قد يخلّ بالتوازن الدقيق الذي يفرضه العمل القضائي والأمني.

فالمادة 4 من المرسوم 25-320 تُقرّ مبدأً أساسياً مفاده أن المعطيات ذات الطابع الشخصي، حتى داخل المنظومة الوطنية لحوكمة البيانات، لا تخرج عن الخضوع للأحكام المقررة في القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. ومنه فإن المرسوم يعترف منذ بدايته بأن حوكمة البيانات لا تُنشئ نظاماً قانونياً موازياً أو ناسخاً لقواعد حماية المعطيات، بل تعمل في إطارها واحترامها.

وانطلاقاً من هذا المبدأ، جاءت المادة 18 لتجسّد التطبيق العملي لمبدأ الفصل الوظيفي، إذ استبعدت صراحةً البيانات المرتبطة بالأمن الوطني وأجهزة إنفاذ القانون والمجال القضائي، ليس لأنها غير منظمة، بل لأنها منظمة أصلاً بنصوص خاصة أشدّ صرامة، وعلى رأسها القانون 07-18 وقوانين الإجراءات، التي تفرض منطق السرية والتحفّظ لا منطق التداول والتشغيل البيني.

وبالتالي، فإن العلاقة بين المادتين 4 و18 علاقة تكامل لا تعارض للأسباب التالية:

تُقرّ المادة 4 سمو قواعد حماية المعطيات الشخصية داخل منظومة الحوكمة، والمادة 18 تُحدّد حدود هذه المنظومة عندما يتعلق الأمر بوظائف سيادية حساسة، كالأمن والتحقيق القضائي.

وهذا يعكس وعي المشرّع بأن حوكمة البيانات الإدارية لا يمكن أن تمتد إلى حيث تبدأ سرّية العدالة ومتطلبات النظام العام، دون مساس بالإطار القانوني القائم أو باستقلال السلطة القضائية.

كما تهدف هذه الاستثناءات إلى تكريس مبدأ استقلال السلطة القضائية وحماية خصوصية عمل أجهزة إنفاذ القانون، وذلك بمنع أي تأثير غير مباشر لآليات الحوكمة الإدارية على مجريات التحقيقات أو الإجراءات القضائية. إخضاع بيانات التحقيق لآليات التصنيف المشترك أو التشغيل البيني قد يمس بسرية التحقيق، أو بقرينة البراءة، أو بسلامة الأدلة والإجراءات. وعليه، فإن المادة 18 جاءت لتؤكد أن هذه البيانات تظل خاضعة حصرياً لقوانينها الخاصة، ولا سيما قانون الإجراءات الجزائية والقانون رقم 07-18، خارج نطاق المنظومة الوطنية لحوكمة البيانات، بما يحقق الفصل الوظيفي بين الحوكمة الإدارية للبيانات و الحماية القضائية والأمنية للمعطيات الحساسة .

2.3- مكونات وآليات عمل المنظومة الوطنية لحوكمة البيانات

يتعين الحديث عن مكونات وآليات عمل المنظومة الوطنية لحوكمة البيانات في أي مرسوم تنظيمي، لأنه بدون تحديد هذه المكونات تصبح حوكمة البيانات مجرد فكرة عامة دون إطار عملي واضح. و إن تحديد المكونات مثل الهياكل التنظيمية و قواعد تصنيف البيانات و مستويات الحساسية، وآليات الإشراف والمتابعة يضمن وجود إطار تشغيلي متكامل يسمح بتطبيق المبادئ الاستراتيجية

للوكمة على أرض الواقع ، ناهيك على أن هذا التحديد يساهم أيضاً في تبيان مسؤوليات الأطراف المختلفة، سواء المؤسسات العامة أو الخاصة، ويحد من الفوضى أو التضارب في إدارة البيانات. كما أن تضمين آليات العمل والإشراف في التشريع ليس ترفاً، بل هو معيار موجود في التشريعات المقارنة، خصوصاً في التجارب الأوروبية مثل Data Governance Act (DGA) و Data Act، حيث تنص هذه القوانين على هيكلية واضحة للجهات المعنية، آليات التصنيف، مشاركة البيانات، وآليات الرقابة لضمان الشفافية والامتثال القانوني. بالتالي، فإن دمج هذه العناصر في مرسوم رئاسي يعزز فعالية الحوكمة ويقربها من أفضل الممارسات الدولية بما يحقق أهداف المنظومة الوطنية من كفاءة، أمان وامتثال قانوني.

نعالج في هذا الفرع من المقال المرجع الوطني لتصنيف البيانات وأهميته في تحديد مستويات الحساسية إلى جانب فهرسة مصادر البيانات وضمان وحدتها، مع الإشارة إلى المعايير القانونية والفنية المعتمدة في الجزائر، كما نتناول آليات التطبيق العملي لتحديد الحساسية و شروط استخدام البيانات واستغلالها، إلزام المؤسسات بالتصنيف والفهرسة ودور الهيئات المختصة في الإشراف والتكامل المؤسسي.

3.2-1- المرجع الوطني لتصنيف البيانات وفهرسة مصادرها

إن تحديد مستوى حساسية البيانات يُعد من الركائز الأساسية لأي نظام لحماية البيانات الشخصية، سواء على المستوى الدولي أو الجزائري، ويقوم على مجموعة من المعايير القانونية والفنية يمكن عرضه على النحو التالي:

أ- المرجع الوطني لتصنيف البيانات وأهميته

تُشكل المنظومة الوطنية لحوكمة البيانات الإطار القانوني والتنظيمي الأساسي لتحديد مستويات حساسية البيانات في الجزائر، ويعتمد هذا التصنيف على مرجع تصنيف البيانات ومرجع فهرسة مصادر البيانات و النظام الوطني للتشغيل البيئي كما نصت عليه المادة 5 من المرسوم. ويهدف هذا المرجع إلى توحيد معايير التصنيف لكل المؤسسات والإدارات العامة، بما يضمن حماية البيانات ذات الطابع الشخصي أو البيانات الحساسة ويضمن كذلك سلامة الإجراءات المتعلقة بالمعطيات القضائية أو الأمنية أو ذات الطابع المالي أو الصحي.

إن اعتماد مرجع موحد يعزز من قدرة المؤسسات على التعامل مع البيانات وفق مستوى حساسيتها مع مراعاة المخاطر المترتبة على أي استخدام غير مشروع، كما يحقق انسجاماً بين التشريعات الوطنية والتزاماتها الدولية، خصوصاً فيما يتعلق بحماية البيانات الشخصية وحماية حقوق الأفراد. فتصنيف البيانات وفق هذا المرجع لا يقتصر على الجانب الفني فقط، بل يتعداه إلى الربط بين طبيعة

البيانات والأطر القانونية والإجراءات الأمنية الواجب اتباعها بما يتيح ضمان التوازن بين حماية الخصوصية وفعالية استخدام البيانات.

ب- المعايير والإجراءات لتحديد مستوى الحساسية

وفقاً للمادة 6 من المرسوم، يتضمن مرجع تصنيف البيانات المعايير والإجراءات المتبعة لتحديد مستوى الحساسية، والتي تشمل طبيعة البيانات، مجال استخدامها، مستوى تأثير تسربها، والإجراءات الأمنية الواجب اتخاذها لكل نوع من البيانات. ومن خلال هذه المادة يصبح من الممكن تصنيف البيانات إلى فئات مختلفة من الحساسية مثل البيانات العادية، والبيانات الحساسة، والبيانات ذات الحساسية العالية، مع ربط كل فئة بالإجراءات القانونية والأمنية المناسبة.

كما يوضح المرجع الإجراءات العملية لتقييم البيانات قبل معالجتها، بما في ذلك تحديد المخاطر المحتملة على الأفراد أو المؤسسات أو الأمن الوطني، وتقدير الإجراءات الوقائية التي يجب تطبيقها، بما يضمن حماية الحقوق والحفاظ على السرية. ويتعين على كل مؤسسة أو إدارة عامة اتباع هذا التصنيف، ومراجعة مستويات الحساسية بشكل دوري بما يتناسب مع تغير الظروف أو ظهور بيانات جديدة، وهو ما يؤكد ديناميكية النظام الوطني لتصنيف البيانات وفاعليته في ضمان الأمن المعلوماتي.

ج- فهرسة مصادر البيانات ووحدتها

تنص المادة 7 على أن مرجع فهرسة مصادر البيانات يهدف إلى توحيد تعريف المصادر عبر نموذج موحد، يتيح الوصول الآمن إلى البيانات ويضمن جودة المعلومات وعدم تكرارها. ويعتبر هذا الفهرس أداة أساسية لربط مستوى حساسية البيانات بمصدرها القانوني والأمني، فالمصادر الرسمية، الصادرة عن الهيئات العامة، تخضع لإجراءات محددة مقارنة بالبيانات المستمدة من جهات خارجية أو غير رسمية.

ويتيح الفهرس سهولة تتبع البيانات وربطها بالإجراءات الأمنية الملائمة، كما يضمن أن كل مستوى حساسية مرتبط بسياق استخدامه القانوني والوظيفي. ومن خلال هذا التنظيم الموحد، يمكن للهيئات والمؤسسات تبادل البيانات ضمن النظام الوطني للتشغيل البيئي بطريقة آمنة ومنظمة، مع الحفاظ على سرية البيانات ذات الحساسية العالية، وتجنب ازدواجية الجهود أو تضارب المعلومات بين الجهات المختلفة.

2.3-2- آليات التطبيق، الاستغلال، والإشراف المؤسساتي

تقوم آليات تطبيق منظومة حوكمة البيانات على إلزام الإدارات والمؤسسات العمومية بتصنيف بياناتها وفهرسة مصادرها وفق المرجع الوطني المعتمد، وربطها بالنظام الوطني للتشغيل البيئي. ويُشترط في استغلال البيانات الحصول المسبق على موافقة مصدرها وحصر استخدامها في الغرض المحدد قانونًا. أما الإشراف المؤسساتي، فينقسمه كلٌّ من المحافظة السامية للرقمنة من حيث التسيير التقني، والهيئات المختصة بالأمن وحماية المعطيات الشخصية من حيث الرقابة وضمان الامتثال القانوني.

أ- آلية التطبيق والمتابعة

تقرض المواد 8 و9 على الوزارات السامية للرقمنة إعداد مرجع تصنيف البيانات ومرجع فهرسة المصادر، ومتابعة تحديثهما، وضمان تطبيقهما عبر جميع المؤسسات والإدارات العامة. ويتم هذا التطبيق وفق معايير واضحة تتضمن مستوى حساسية البيانات وطبيعة استخدامها، مع مراعاة المخاطر القانونية والأمنية المرتبطة بكل نوع من البيانات. ويؤكد المرسوم على أن كل تصنيف يجب أن يتم من قبل المصدر وفق المرجع الوطني، لضمان التوافق والانسجام بين الجهات المختلفة وتقليل المخاطر الناتجة عن التعامل مع البيانات الحساسة.

وتنص المواد 10 و11 و12 على وجوب تصنيف البيانات داخل نظم المعلومات لدى كل مؤسسة أو إدارة عامة أو هيئة مكلفة بخدمة العموم وفق المرجع الوطني، مع القدرة على إدماج هذه البيانات ضمن النظام الوطني للتشغيل البيئي عند الحاجة. كما تلتزم المؤسسات بمتابعة تحديث تصنيف البيانات وتحسين الإجراءات الأمنية باستمرار، بما يضمن التوازن بين حماية الخصوصية وتسهيل استخدام البيانات في الأغراض المشروعة.

هذا النظام يعزز من شفافية التعامل مع البيانات ويحقق الرقابة القانونية الفعّالة على جميع مستويات الحساسية، كما يوفر آلية لتقوية التعاون بين الإدارات المختلفة في إطار قانوني واضح، وهو ما يضمن حماية الحقوق الفردية والمصلحة العامة معًا.

ب- شروط استخدام البيانات واستغلالها

تنص المادة 13 من المرسوم الرئاسي على أن مستعمل البيانات يجب أن يحصل على موافقة صريحة من مصدر البيانات عبر النظام الوطني للتشغيل البيئي قبل استغلال أي بيانات رقمية للأغراض المطلوبة. ويُعني ذلك أن أي استخدام للبيانات لا يكون مشروعًا إلا إذا تم وفق التشريع والتنظيم المعمول بهما، بما يضمن أن استغلال المعلومات الرقمية يخضع للإطار القانوني المنظم ويحمي حقوق المصدر والمستفيد معًا.

ويترتب على هذه المادة أن المؤسسات أو الأفراد الذين يرغبون في استخدام البيانات لأغراض تحليلية، بحثية، أو إدارية، لا يمكنهم ذلك إلا بعد التحقق من موافقة المصدر وإدراجها ضمن النظام الوطني بطريقة رسمية وموثقة. وهذا يعزز من الشفافية القانونية ويحد من أي استخدام غير مشروع للبيانات الحساسة أو الشخصية.

وبذلك، يشكّل هذا الإجراء ضماناً إضافياً لتطبيق المعايير الأمنية وقواعد الخصوصية، حيث يرتبط استغلال البيانات دائماً بالغاية المصرح بها وبالموافقة القانونية الصريحة، مما ينسجم مع فلسفة المرسوم في تنظيم التعامل مع البيانات الرقمية الحساسة، ويكفل حماية الحقوق الفردية والمصلحة العامة على حد سواء.

ج- إشراف وتكامل الهيئات المختصة

إن صاحبة الإقتراح التشريعي لهذا المرسوم الرئاسي هي المحافظة السامية للرقمنة لكن لم يقتصر الأمر عليها فقط في الإشراف على المنظومة الوطنية، بل شملت هيئات أخرى وطنية كلا في مجال تخصصها و مهامها، فطبقاً للمادة 14 تم تكليف المجلس الوطني لأمن الأنظمة المعلوماتية بالإشراف على كل ما يتعلق بوظيفة المنظومة الوطنية للبيانات. ويرمي هذا الإشراف إلى ضمان توازن الرقابة الفنية والتقنية مع الرقابة التنظيمية، وتفاذي أي تداخل محتمل بين مسؤوليات المحافظة السامية للرقمنة والهيئات الأخرى.

ووضعت المادة 15 على عاتق السلطة الوطنية المكلفة بالمعطيات ذات الطابع الشخصي مهمة الرقابة على فهارس وتصنيف البيانات، بما يتوافق مع التشريع والتنظيم، لتأكيد فصل المهام التنظيمية عن المهام الأمنية، وضمان التوزيع الواضح للاختصاصات.

وبناءً على المادة 16، تُعد وكالة أمن الأنظمة المعلوماتية مسؤولة عن تصنيف مستوى أمان البيانات ضمن المنظومة الوطنية، في حين تبقى المحافظة السامية للرقمنة مسؤولة عن إدارة النظام وضمان أمن البيانات أثناء النقل، بما يحقق حماية فعّالة للبيانات ويحد من التداخل بين الاختصاصات.

كما تحدد المادة 17 مسؤولية المحافظة السامية للرقمنة في وضع حيز إدماج النظام الوطني للتشغيل البيئي وإدارته، مع ضمان تأمين البيانات خلال مراحل نقلها، وفق متطلبات أمن الأنظمة المعلوماتية، بالتنسيق مع المجلس الوطني وأصحاب الاختصاص.

من حيث المنطق التشريعي، فإن إحالة المواد 14-15-16-17 من المرسوم على إشراف عدة هيئات وطنية يمكن قراءته بوصفه تكاملاً مؤسسياً مقصوداً، يعكس الطبيعة العرضية لحوكمة البيانات التي تتقاطع فيها أبعاد قانونية، تقنية، تنظيمية وأمنية. فالمشرع يبدو أنه أراد توزيع الأدوار بحسب

الاختصاص: التخطيط الاستراتيجي، الضبط التقني، حماية المعطيات الشخصية والأمن السيبراني، بدل تركيزها في جهة واحدة قد تعجز عملياً عن الإحاطة بكل هذه الوظائف.

غير أنّ هذا التعدد نفسه يحمل مخاطر كامنة على المدى المتوسط، إذا لم يُدعم بآليات تنسيق فعّالة وواضحة. فغياب ترانتيب دقيقة أو عدم تحديد حدود الاختصاص بدقة بين الهيئات المشرفة، قد يفضي إلى تداخل الصلاحيات وازدواجية القرارات أو تباطؤ مسارات اتخاذ القرار، وهو ما يحوّل الإشراف المتعدد من رافعة للحوكمة إلى عامل كبح و فرملة لها. وتجارب مقارنة كالنموذج الأوروبي قبل ترسيخ دور المنسق المركزي³³، تُظهر أن نجاح هذا الخيار مرهون بوجود جهة تنسيقية محورية وآليات إلزامية لتسوية التعارض وضمان الانسجام بين الفاعلين و هو ما نقترحه للمشرع الجزائري أن يأخذ به.

د- إلزام المؤسسات بتصنيف البيانات وفهرسة مصادرها

تنص المواد 5 إلى 8 و12 من المرسوم الرئاسي على إلزام جميع المؤسسات والإدارات العامة والهيئات المكلفة بالخدمة العامة بتصنيف بياناتها وفهرسة مصادرها ابتداءً من تاريخ نشر المراجع الرسمية لتصنيف البيانات وفهرسة المصادر، وهو ما يضمن توحيد المعايير الوطنية للبيانات. تبدأ العملية بتحديد نوع كل البيانات وطبيعتها ومستوى حساسيتها وأغراض استخدامها، وفق مرجع تصنيف البيانات الذي يبين المعايير والإجراءات المعمول بها لتحديد مستويات الحساسية ومجالات الاستعمال والإجراءات الأمنية الواجب تطبيقها.

على المستوى التقني، تصنف البيانات ضمن فئات محددة—عامة، حساسة، أو شديدة الحساسية—ويتم تطبيق تدابير حماية مناسبة لكل فئة مثل تشفير البيانات، تحديد الصلاحيات المسموح لها بالوصول، وتطبيق سياسات النسخ الاحتياطي والاسترجاع بما يضمن مطابقتها لمستوى الأمان المقرر وفق النظام الوطني للتشغيل البيئي (المواد 9-10). بعد التصنيف تُفهرس مصادر البيانات وفق نموذج موحد يتيح ربط كل بيانات بمصدرها بدقة مع تسجيل الجهة المسؤولة عن جمعها وطبيعة البيانات وطرق الوصول إليها والإجراءات الأمنية المطبقة مما يسهل تبادلها بطريقة منظمة وآمنة بين المؤسسات (المادتين 7 و11).

³³ المادة 29 من لائحة الاتحاد الأوروبي رقم 868/2022 المؤرخة في 30 ماي 2022، المتعلقة بحوكمة البيانات DGA تنص بأنها تنشئ مجلساً أوروبياً لابتكار البيانات European Data Innovation Board، يضم ممثلين عن السلطات المختصة في الدول الأعضاء، واللجنة الأوروبية، وهيئات حماية البيانات، وهيئات مختصة أخرى.

قبل إنشاء EDIB، كان الإطار الأوروبي يتسم بتعدد المتدخلين (هيئات القطاع العام، سلطات حماية البيانات، الجهات التنظيمية القطاعية)، وهو ما كشف عن حاجة عملية إلى هيئة تنسيقية أفقية. فجاء المجلس الأوروبي لابتكار البيانات كآلية مؤسسية لتفادي تداخل الصلاحيات وضمان الانسجام، دون المساس باختصاصات الهيئات القائمة.

تُدمج عملية التصنيف والفهرسة بالنظام الوطني للتشغيل البيئي، حيث تضمن المحافظة السامية للرقمنة متابعة جودة التصنيف والفهرسة والتحقق من تطبيقها فعلياً، مما يحقق التوازن بين الاستغلال القانوني للبيانات وحماية حقوق الأفراد وخصوصيتهم (المادتين 8 و 13). ويتيح هذا الإطار التقني والقانوني ضمان أن كل تبادل للبيانات بين المؤسسات يتم وفق مستويات الأمان المقررة، مع توثيق ومتابعة دقيقة لمصادر البيانات وإجراءات حمايتها، بما يعزز فعالية النظام الوطني ويقلل من مخاطر التداخل أو الاستعمال غير المشروع للبيانات.

المرحلة الأولى: تحديد نطاق البيانات - المادة المرجعية: 6 و 8	المرحلة الثانية: التصنيف الفني والأمني - المادة المرجعية: 6 و 12	المرحلة الثالثة: الفهرسة وتوثيق المصادر - المواد المرجعية: 7, 9, 10, 13, 17
- مراجعة جميع البيانات المتاحة - تحديد طبيعة البيانات - تحديد الغرض من جمعها - تحديد مستوى الحساسية	- إدراج البيانات ضمن الفئة المناسبة (عامة/حساسة/شديدة) - تحديد الإجراءات الأمنية - (تشفير، صلاحيات، مراقبة) - تقييم المخاطر المحتملة	- إنشاء سجل مركزي للبيانات - توثيق المصدر، الجهة المسؤولة - توحيد النموذج للفهرسة - تسهيل تبادل البيانات ضمن النظام الوطني للتشغيل البيئي - متابعة الجودة من المحافظة السامية للرقمنة

4-الخاتمة:

في رأيي، يشكّل المرسوم الرئاسي خطوة متقدمة ومهمة في اتجاه ترسيخ حوكمة الدولة على بياناتها، لكنه يظل إطاراً تأسيسياً أكثر منه حلاً نهائياً لكل الرهانات المعقدة التي يمكن أن نعددها في: أولاً، من حيث النجاعة المؤسسية وحوكمة البيانات، يحسب للمرسوم أنه انتقل بالإدارة من منطق التسيير التقليدي للمعطيات إلى منطق الحوكمة المهيكلية، عبر فرض التصنيف، الفهرسة، توحيد المصادر، وضبط أغراض المعالجة. هذا الاختيار يحدّ مبدئياً من الأخطاء الإدارية، والقرارات المبنية على بيانات غير محدثة أو غير متجانسة، كما يقلل من مخاطر التمييز غير المشروع الناتج عن سوء استعمال البيانات أو تضاربها بين الإدارات. غير أن هذه النجاعة تبقى مرهونة بمدى الالتزام الفعلي للإدارات وبقدرتها التقنية والبشرية على تطبيق المرسوم إذ إن النص مهما بلغت دقته، لا يمنع الانحراف في غياب الرقابة والتكوين.

ثانيًا، فيما يخص الأمن السيبراني وحماية البيانات من الثغرات والاختراقات، فإن المرسوم يتجاوب مع الرهانات الحديثة من خلال ربط التصنيف بمستوى الحساسية، وفرض ضوابط الولوج وتحديد المسؤوليات داخل كل مؤسسة. هذا يعكس وعيًا تشريعيًا بأن الخطر لم يعد قانونيًا فقط، بل تقنيًا واستراتيجيًا. ومع ذلك، تبقى الحماية القانونية غير كافية إذا لم تُدعم باستثمارات حقيقية في البنية التحتية الرقمية، وآليات الرصد والاستجابة للحوادث، وإدماج مثلاً مقاربة الأمن حسب التصميم (Security by Design)، وإلا فإن الثغرات التقنية ستفرغ المرسوم من فعاليته العملية.

ثالثًا، بخصوص رهان السيادة الرقمية في مواجهة الشركات الكبرى (GAFAM)، فإن المرسوم يُعد إعلانًا صريحًا عن إرادة الدولة في استعادة التحكم في بياناتها السيادية، وتقليص التبعية للمنصات الأجنبية، وهو أمر بالغ الأهمية للحفاظ على الكفاءة التشغيلية وثقة المواطنين. غير أن هذا الهدف الاستراتيجي لا يتحقق بالنصوص التنظيمية وحدها، بل يتطلب سياسة رقمية شاملة تشمل: حلول تخزين وطنية-كما حدث خلال سنة 2025 تخزين سحابي وطني ومركز بيانات ضخم - أو سيادية، عقودًا صارمة مع الفاعلين الخواص، ونموذج حوكمة يوازن بين الانفتاح الرقمي وحماية المصالح العليا للدولة. بدون ذلك، تبقى الإدارة عرضة لفقدان السيطرة الفعلية على البيانات، حتى وإن كانت منضبطة قانونيًا.

كخلاصة نقول بأن المرسوم الرئاسي يلبي جزءًا معتبرًا من رهانات الحوكمة الآمنة للبيانات، ويؤسس لثقافة قانونية وتنظيمية صحيحة، لكنه لا يحقق النجاح الكامل إلا إذا اندمج ضمن رؤية أوسع تشمل الإصلاح الإداري، الأمن السيبراني، والسيادة الرقمية. هو إذن شرط لازم، لكنه غير كافٍ وحده لضمان الثقة، الكفاءة، وحماية الدولة والمواطن في آن واحد.

وعلى ضوء المناقشة القانونية والتقنية لأحكام المرسوم الرئاسي المتعلق بحوكمة البيانات، تم استخلاص النتائج التالية:

- يمثل المرسوم الرئاسي خطوة تأسيسية مهمة نحو إرساء منظومة وطنية لحوكمة البيانات في الجزائر، ويعكس إدراك المشرع لأهمية البيانات كرافعة للرقمنة وصنع القرار العمومي.
- المرسوم الرئاسي يفتقر إلى تعريفات دقيقة ومفصلة لبعض المفاهيم الأساسية مثل: حوكمة البيانات، البيانات العمومية، مستويات الحساسية، مالك البيانات، ودورة حياة البيانات لأن القوانين المقارنة، خاصة الأوروبية DGA، تضبط بشكل صارم التعاريف حتى تحدّ من التداخل في التفسير وتقلّص هامش التعسف الإداري، بينما يترك الغموض في النص الجزائري سلطة تقديرية واسعة للإدارة دون ضوابط دقيقة.

- العلاقة بين منظومة حوكمة البيانات والقانون رقم 18-07 لحماية المعطيات الشخصية ظلت عامة، دون إدماج فعلي لمبادئ حماية المعطيات ضمن منطق الحوكمة وتحتاج المادة 4 لإعادة صياغة تشريعية أو إضافة مواد مستقلة حول المساءلة.
- إلزام الإدارات العمومية بتصنيف وفهرسة بياناتها يعد تقدّمًا نوعيًا، غير أن غياب منهجية تقنية وقانونية دقيقة للتصنيف يضعف قابلية التطبيق الموحد ويحدّ من فعالية الحوكمة.
- لا يعالج المرسوم بشكل تفصيلي المراحل التقنية لدورة حياة البيانات (الجمع، التخزين، المعالجة، التبادل، الأرشفة، الإتلاف)، بينما تعتمد القوانين المقارنة على تصور شامل يعتبر أن كل خلل في مرحلة واحدة قد يؤدي إلى مساس خطير بالحقوق أو بالأمن السيبراني، وتفرض إجراءات تقنية مختلفة حسب كل مرحلة.
- المرسوم لم يربط بشكل صريح بين مستويات تصنيف البيانات والآثار القانونية المترتبة عنها، سواء من حيث شروط النفاذ أو المسؤولية أو الجزاءات عند الإخلال رغم أنه أشار في مقتضيات المرسوم إلى النص المرجعي الوطني لتصنيف الوثائق الإدارية و المعلومات -الأمر رقم 21-09 المؤرخ في 8 جوان 2021-. لكنه من الناحية الصياغية غير كاف.
- اعتماد تعدد الهيئات المشرفة يدل على مقارنة شمولية أمنية و تنظيمية و قانونية، لكنه من المحتمل أن يُفرز تداخلًا في الاختصاصات وغموضًا في تحديد الجهة الحاسمة، خاصة في مسائل تصنيف البيانات وتحديد مستوى حساسيتها.
- غياب آليات تقييم المخاطر، والمراجعة الدورية والتدقيق التقني والقانوني يقلل من قدرة المنظومة على التكيف مع تطور التهديدات السيبرانية.
- النص يغلب عليه الطابع التنظيمي والتوجيهي، ويحتاج إلى تدعيم تشريعي أدق لضمان الفعالية والاستدامة.
- المنظومة الحالية تحتاج إلى مزيد من الانسجام والتكامل حتى تحقق التوازن المطلوب بين الأمن السيبراني، تبادل البيانات، وحماية الحقوق والحريات الأساسية.

التوصيات و الاقتراحات

النتائج المتوصل إليها كانت بشكل نقائص حسب رأيي تستدرك بشكل اقتراحات نختصرها و لا نفصلها كالآتي:

- يوصى بتعديل المادة 3 من المرسوم أو إدراج فصل خاص يتضمن تعريفات دقيقة وموحدة لمفاهيم حوكمة البيانات، وذلك على غرار ما هو معمول به في التشريعات المقارنة.
- يوصى بإدراج مادة تنص صراحة على أن قواعد حوكمة البيانات لا تُطبق بمعزل عن أحكام القانون رقم 07-18، وأن أي معالجة أو تبادل للبيانات ذات الطابع الشخصي يخضع وجوباً لمبادئ الشرعية، التناسب، وتحديد الغرض.
- يوصى بتقسيم البيانات تشريعياً إلى مستويات محددة، مثل: بيانات عمومية، بيانات مهنية داخلية، بيانات حساسة، بيانات عالية الحساسية أو سيادية ويرتبط بكل مستوى نظام قانوني خاص من حيث شروط المعالجة، التبادل، التخزين، ومدد الاحتفاظ.
- التنصيص الصريح على التكامل مع القانون رقم 07-18 لمنع ازدواجية المرجعيات القانونية.
- إرساء نظام قانوني متدرج لتصنيف البيانات وربط التصنيف بآثار قانونية واضحة وعدم الاكتفاء بالأمر رقم 09-21.
- تكريس مبدأ المساواة القانونية وتحديد المسؤوليات في كل مرحلة من دورة حياة البيانات.
- إلزامية اعتماد المعايير التقنية الدولية في مجال أمن المعلومات وحماية البيانات.
- يُستحسن، على غرار التجربة الأوروبية، استحداث آلية تنسيقية مركزية دائمة ضمن المنظومة الوطنية لحوكمة البيانات، تتولى تنسيق أعمال الهيئات المتعددة المشرفة عليها وتوحيد التوجيهات ومنع تداخل الصلاحيات، دون المساس بالاختصاصات القطاعية لكل هيئة، بما يضمن انسجام التطبيق وفعالية الحوكمة على المدى المتوسط والبعيد.

5- المراجع:

5-1- الكتب:

1. د. مناصرة يوسف، المعطيات الشخصية و الجريمة في التشريع الجزائري و المقارن، دار الخلدونية ، 2025.

5-2- المقالات:

1. د- مناصرة، يوسف، "الموازنات الكبرى بين متطلبات الأمن العام وحماية المعطيات الشخصية"، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 59، العدد 03، 2022، ص 448-465.
2. Abraham, r., schneider, j., & vom brocke, j. (2019). Data governance: a conceptual framework, structured review, and research agenda. International journal of information management, 49, 424-438.
3. DAMA International, *The DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK)*, 1st ed., Technics Publications, 2009, p. 19.
4. Dyché, J., & Levy, E., *Customer Data Integration: Reaching a Single Version of the Truth*, Wiley, 2006, p. 150.
5. Federico Casolari, Carlotta Buttaboni, Luciano Floridi, The EU Data Act in context: a legal assessment, International Journal of Law and Information Technology, Volume 31, Issue 4, Winter 2023, Pages 399–412, <https://doi.org/10.1093/ijlit/eaee005>.
6. Information Commissioner's Office, The Data Use and Access Act 2025 (DUAA) - what does it mean for organisations?. <https://ico.org.uk/>
7. Guidance, Data (Use and Access) Act 2025: data protection and privacy changes. A summary of changes to the UK's data protection and privacy legislation in the Data (Use and Access) Act. <https://www.gov.uk/guidance/>
8. Kim, Y., & Cho, J., "Data quality management," *Sustainability*, 2018, p. 386.
9. Khatri, V., & Brown, C. V., "Designing data governance" *MIS Quarterly*, 2010, p. 151.
10. Marina Micheli, Marisa Ponti, Max Craglia, Anna Berti Suman, Emerging models of data governance in the age of datafication., journal Big Data\ Society, Vol.7 N°2 , 2020.
11. Morabito, V, Big Data and Analytics, Springer, 2015, p.99.
12. Nielsen, J. A., Persson, J. S., & Madsen, S., "Challenges of enterprise architecture," *Journal of Enterprise Architecture*, 2018, p. 22.
13. Strigence. "From Compliance to Competitiveness: The Rise of Data Governance in the GCC." Strigence Advisory Desk, 6 June 2025, www.strigence.com/blog/from-compliance-to-competitiveness-the-rise-of-data-governance-in-the-gcc.
14. Thomas, g. Data governance and stewardship: best practices and tools for data governance, data quality, and data stewardship. (2015).
15. Van asselt, marjolein ba et renn, ortwin. Risk governance. *Journal of risk research*, 2011, vol. 14, no 4, p. 431-449.
16. DataGalaxy. "Gouvernance des données : définition, enjeux et bonnes pratiques." DataGalaxy Blog, (<http://www.datagalaxy.com/fr/blog/gouvernance-des-donnees-definition/>). [2025/11/14]
17. Talend. "Guide de la gouvernance des données." Talend Resources, Talend.

5-3- القوانين الوطنية والمقارنة:

1. القانون رقم 07-18 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر عدد 34 ص، 11 بتاريخ 10 يونيو 2018.
2. المرسوم الرئاسي رقم 25-320، المؤرخ في 10 رجب عام 1447 هـ الموافق 30 ديسمبر سنة 2025، يتضمن وضع منظومة وطنية لحوكمة البيانات. جريدة رسمية عدد 87 ص 4 بتاريخ 30 ديسمبر 2025.
3. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).
4. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).