International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
IJLRS
Vol. (5), No. (11) November 2026 الإصدار (5)، العدد (11)

ترسيخ السيادة الرقمية في الدولة الذكية: دراسة في الأسس التشريعية والتقنية

محمد حسين المجالي
أستاذ القانون الإداري المشارك، جامعة الزيتونة، الأردن
Moh.almajali@zuj.edu.jo

ملخص

يتناول هذا البحث موضوع السيادة الرقمية بوصفها مفهوماً قانونياً واستراتيجياً محورياً برز بقوة موازية لتسارع التحول الرقمي وتنامي نموذج الدولة الذكية إذ لم يعد قيام الدولة بوظائفها العامة مقتصراً على المجال المادي التقليدي بل امتد ليشمل الفضاء الرقمي وما يتصل به من قواعد بيانات ومراكز تشغيل وبنى تحتية ومنصات ذكية وأنظمة خوارزمية.

وينطلق البحث من فرضية جوهرية ترى أن تعزيز السيادة الرقمية في الدولة الذكية لا يتحقق من خلال المعالجة التقنية وحدها ولا عبر التنظيم التشريعي المجرد وإنما من خلال بناء منظومة متكاملة (تشريعية، وتقنية، ومؤسسية) تضمن للدولة السيطرة الفاعلة والمشروعة على بياناتها وبناها التحتية وتصون استقلال قرارها العام في مواجهة تحديات التبعية الرقمية والانكشاف السيبراني.

ولتحقيق هذه الغاية يسعى البحث إلى استجلاء الأسس التشريعية والتقنية اللازمة لترسيخ السيادة الرقمية باحثاً في دور القواعد المنظمة لحوكمة البيانات والأمن السيبراني وحماية الخصوصية والبنية التنظيمية للإدارة الرقمية إلى جانب تفكيك الأسس التقنية المرتبطة بالحوسبة السحابية والذكاء الاصطناعي والمنصات الرقمية.

وقد اعتمدت الدراسة على (منهجية تكاملية مركبة) تجمع بين المنهج التحليلي لاستنطاق النصوص التشريعية والمنهج الوصفي لتأطير التحولات البنيوية والمنهج المقارن لاستقراء أفضل الممارسات التشريعية العالمية.

وتبرز أهمية البحث في قدرته على تقديم تصور علمي متكامل يوازن ببراعة بين مقتضيات الابتكار التكنولوجي ومتطلبات المشروعية القانونية وحماية المصلحة العامة.

وتخلص الدراسة إلى جملة من النتائج والتوصيات أبرزها ضرورة إحداث تحديث تشريعي عميق وتوطين للقدرات التقنية بما يكفل بناء سيادة رقمية فاعلة تحمي الأمن القومي المعلوماتي وتعزز كفاءة الدولة الذكية واستقلال إرادتها في البيئة الرقمية المعاصرة.

الكلمات المفتاحية: السيادة الرقمية، الدولة الذكية، الأمن السيبراني، حوكمة البيانات، حماية البيانات الشخصية، الحوكمة الرقمية.

Establishing Digital Sovereignty in the Smart State: A Study of Legislative and Technical Foundations

Mohmmad Hussien Almajali
Associate Professor of Administrative Law, Al-Zaytuna University, Jordan
Moh.almajali@zuj.edu.jo

Abstract

This study addresses the concept of "Digital Sovereignty" as a pivotal legal and strategic framework that has emerged prominently alongside the accelerating digital transformation and the evolution of the "Smart State" model. The traditional execution of state functions is no longer confined to the physical domain; rather, it has expanded to encompass the digital sphere,

including databases, processing centers, infrastructure, smart platforms, and algorithmic systems.

The research operates on a core hypothesis: enhancing digital sovereignty within a smart state cannot be achieved solely through technical solutions or abstract legislative regulation. Instead, it requires building an integrated framework—legislative, technical, and institutional—that guarantees the state's effective and legitimate control over its data and infrastructure, thereby safeguarding its public decision-making autonomy against digital dependence and cyber exposure.

To achieve this objective, the study explores the legislative and technical foundations essential for consolidating digital sovereignty. It examines the regulatory principles governing data governance cybersecurity, privacy protection, and the organizational framework of digital administration, while deconstructing the technical foundations associated with cloud computing, artificial intelligence, and digital platforms.

Methodologically, the study adopts a "composite integrative approach," combining analytical methodology to interpret legislative texts, descriptive methodology to contextualize structural transformations, and comparative methodology to review best international legislative practices. The significance of this research lies in its capacity to provide a comprehensive scientific framework that meticulously balances technological innovation, legal legitimacy, and the protection of the public interest.

The study concludes with several key findings and recommendations, emphasizing the necessity of deep legislative reform and the localization of technical capabilities. These measures are essential for establishing effective digital sovereignty, protecting national information security, and enhancing the smart state's efficiency and autonomous decision-making in the contemporary digital environment.

Keywords: Digital Sovereignty, Smart State, Cybersecurity, Data Governance, Personal Data Protection, Digital Governance.

المقدمة

تمر الدولة المعاصرة بـ "تحول بنيوي غير مسبوق" فرضته الثورة الرقمية وتسارع تطبيقات الذكاء الاصطناعي والحوسبة السحابية فلم تعد وظائف الإدارة العامة وآليات سير المرافق ووسائل تقديم الخدمات الإدارية محكومة بالوسائل المادية أو الأطر التنظيمية التقليدية بل أصبحت ترتكز بصورة كليّة على بنى تحتية رقمية معقدة ومنصات ذكية وقواعد بيانات ضخمة مترابطة وأنظمة خوارزمية قادرة على توجيه القرار العام وإدارة الشأن العام بكفاءة فائقة.

وفي ظل هذا الانتقال النوعي نحو نموذج "الدولة الذكية" لم يتوقف الأثر عند حدود تحسين الأداء الإداري وتسهيل الإجراءات بل أفضى إلى إعادة تشكيل الركائز القانونية العميقة لنظرية الدولة وفي مقدمتها مفهوم "السيادة الوطنية" في امتدادها المعلوماتي المعاصر.

فالسيادة في صورتها الحديثة لم تعد تقف عند حدود السلطة القانونية التي تمارسها الدولة داخل إقليمها الجغرافي البري والبحرية والجوي فحسب بل اتسع نطاقها ليشمل "الفضاء الرقمي الوطني".

وتتجلى هذه السيادة الرقمية في القدرة الفعلية والمشروعة للدولة على التحكم في بياناتها الوطنية وتأمين بنيتها المعلوماتية الحيوية وإخضاع المنصات والشبكات والنظم الرقمية – المحلية منها والعابرة للحدود – لسلطان القانون الوطني، بما يضمن استقلال الإرادة العامة وصيانة القرار الإداري والسياسي من صور التبعية أو الهيمنة التقنية الخارجية.

ومن هذا المنطلق يكتسب البحث في "الأسس التشريعية والتقنية لترسيخ السيادة الرقمية في الدولة الذكية" أهمية استثنائية في الفقه القانوني والإداري المعاصر إذ أضحى ترسيخ هذه السيادة رهيناً ببناء منظومة متكاملة يتكامل فيها النص التشريعي مع الممكنات التقنية وتتفاعل فيها قواعد القانون العام مع ضرورات الأمن السيبراني وحوكمة البيانات واستقلال البنية الرقمية.

وبذلك يغدو القانون أداة إرساء وضبط للمشروعية وتغدو التقنية أداة تمكين وحماية حقيقية لتغدو الدولة الذكية دولةً لا تكتفي بتوظيف التكنولوجيا كأداة إجرائية بل تمارس من خلالها "سيادة رقمية رشيدة ومستقلة" تحمي أمنها المعلوماتي وتحصن وظائفها السيادية في عالم متسارع ومفتوح.

مشكلة الدراسة

أدى التحول نحو نموذج "الدولة الذكية" إلى نقل مركز ثقل الوظيفة الإدارية والسيادية إلى الفضاء الرقمي حيث أصبحت ممارسة الدولة لاختصاصاتها الأساسية قائمة على منظومات معلوماتية متطورة تشمل قواعد البيانات الضخمة والمنصات الذكية وتقنيات الذكاء الاصطناعي والحوسبة السحابية.

غير أن الإشكالية الرئيسية والدقيقة التي تفجرها هذه الدراسة تكمن في "الفجوة الهيكلية المتزايدة بين التسارع التقني المذهل الذي تقوم عليه الدولة الذكية وبين الأطر التشريعية والتنظيمية التي غالباً ما تأتي متأخرة أو عاجزة عن استيعاب هذا التحول وإخضاعه لمنطق المشروعية القانونية".

إن ضعف التكامل البنيوي بين المنظومة التشريعية والقدرات التقنية الذاتية للدولة يفضي إلى "انكشاف سيادي خطير" فيجعل البيئة الرقمية الوطنية عرضة للتبعية التقنية المطلقة للشركات التكنولوجية العالمية والفاعلين العابرين للحدود أو الاختراقات السيبرانية المساس باستمرارية سير المرافق العامة الحيوية فضلاً عن القصور في الحماية القانونية لبيانات المواطنين والأمن القومي المعلوماتي.

وتأسيساً على ذلك تتحدد مشكلة الدراسة في "بيان وكشف الأسس التشريعية والتقنية الكفيلة بترسيخ السيادة الرقمية في الدولة الذكية وتأصيل كيفية بناء منظومة قانونية وتكنولوجية متكاملة تضمن للدولة السيطرة الفعلية والمشروعة على فضاءها الرقمي وتكفل استقلال قرارها العام، مع إحداث التوازن الدقيق بين مقتضيات الابتكار الرقمي ومتطلبات المشروعية واستقلال الدولة العام من التبعية التقنية والاختراقات السيبرانية.

غير أن الإشكال الرئيس يتمثل في أن التطور التقني المتسارع الذي تقوم عليه الدولة الذكية لا يقابله في كثير من الأحيان تطور موازٍ في الأطر التشريعية والتنظيمية القادرة على استيعابه وضبطه.

كما أن ضعف التكامل بين البنية القانونية والبنية التقنية يفضي إلى إضعاف قدرة الدولة على ممارسة سيادتها الرقمية ممارسة فعالة، ويجعل المجال الرقمي عرضة للهيمنة الخارجية أو للتبعية التقنية أو للقصور في الحماية القانونية للبيانات والمرافق والخدمات العامة الرقمية.

ومن ثم تتمحور مشكلة هذه الدراسة حول بيان الأسس التشريعية والتقنية اللازمة لترسيخ السيادة الرقمية في الدولة الذكية على نحو يكفل حماية المجال الرقمي الوطني ويضمن استقلال القرار العام، ويحقق التوازن بين متطلبات الابتكار الرقمي ومقتضيات المشروعية وسيادة الدولة.

أسئلة الدراسة

1. ما الأسس التشريعية والتقنية اللازمة لترسيخ السيادة الرقمية في الدولة الذكية بما يكفل للدولة حماية بنيتها الرقمية وبياناتها وقرارها العام في ظل التحول الرقمي المتسارع؟
2. ما التأصيل المفاهيمي والقانوني لمفهوم السيادة الرقمية وكيف ترتبط بعلاقة عضوية بوظائف الدولة المعاصرة ونموذج الدولة الذكية؟
3. ما طبيعة التحديات التشريعية والأمنية التي تواجهها الدولة الذكية في فضاءها الرقمي وكيف تنعكس على استقلال قرارها العام؟
4. ما الأسس التشريعية والتنظيمية الواجب توافرها لحوكمة البيانات وحماية الخصوصية وتحقيق الأمن السيبراني في الدولة الذكية؟

5. ما الدور الذي تضطلع به البنية التحتية الرقمية، والحوسبة السحابية والذكاء الاصطناعي بوصفها مكونات تقنية أساسية لدعم السيادة الرقمية؟
6. ما التصور المقترح لبناء منظومة متكاملة (تشريعية وتقنية) تكفل ترسيخ السيادة الرقمية وتعزيز كفاءة أداء الدولة الذكية واستقلالها؟

أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق جملة من الغايات العلمية والعملية الأصيلة التي تتكامل مع مشكلة البحث، وتتمثل في الآتي:

1. التأصيل المفاهيمي والنظري: بناء إطار مفاهيمي وقانوني دقيق ومحكم لمفهوم السيادة الرقمية، وتحديد أبعادها ووظائفها في بيئة الدولة الذكية المعاصرة.
2. تشخيص الفجوة والإشكالات: رصد وتحليل التحديات التشريعية والتقنية التي تواجهها الإدارة العامة في الدولة الذكية وتحديد مظاهر الانكشاف السيادي في مواجهة الفاعلين الرقميين العابرين للحدود.
3. تحليل الأسس التشريعية وحوكمة البيانات: استجلاء الأطر القانونية اللازمة لحوكمة البيانات الوطنية وتوفير الحماية القانونية للخصوصية والأمن السيبراني والمنصات الرقمية الحيوية.
4. بيان الممكنات التقنية: إبراز الدور الوظيفي للبنية التحتية الرقمية ومراكز البيانات والحوسبة السحابية وتقنيات الذكاء الاصطناعي كأدوات تمكين حقيقية لدعم السيادة الرقمية.
5. تقديم تصور استراتيجي مقترح: الخروج بتوصيات وتصور منهجي متكامل يربط بين القواعد القانونية والمقوم التقني، بما يسهم في ترسيخ السيادة الرقمية للدولة الذكية وتعزيز استقلال قرارها العام بكفاءة واستدامة.

أهمية الدراسة

تتحدد أهمية هذه الدراسة عبر مسارين متكاملين: أحدهما علمي نظري والآخر عملي تطبيقي يعكسان معاً عمق الإشكالية المطروحة:

أولاً: الأهمية العلمية (النظرية):

- تأصيل فكري استراتيجي لنظرية الدولة المعاصرة: تنبع الأهمية العلمية لهذه الدراسة من كونها تخوض في صميم التحولات البنيوية التي تعصف بمفاهيم القانون العام التقليدية لاسيما إعادة تمركز فكرة "السيادة الوطنية" وانتقالها من نطاقها الجغرافي البحت إلى فضاء السيادة الرقمية والمعلوماتية في عصر الدولة الذكية.
- تجاوز المقاربات المجزأة: تقدم الدراسة نموذجاً تحليلياً مركباً يتجاوز الانفصام التقليدي بين الفقه القانوني والبعد التقني من خلال ربط التشريع بالممكنات التكنولوجية مما يثري المكتبة القانونية والسياسية العربية بمرجعية علمية متكاملة حول حوكمة الفضاء الرقمي.
- سد الفراغ المعرفي في دراسات الإدارة العامة الرقمية: ترد الدراسة على التساؤلات المتجددة حول حدود السلطة العامة في البيئة الافتراضية وتقدم إطاراً مفاهيمياً دقيقاً يفكك إشكالية "التبعية والارتهان التقني" ويؤصل لاستقلال القرار الإداري والسياسي.

ثانياً: الأهمية العملية (التطبيقية):

- توجيه المشرع وصناع القرار: تمثل الدراسة بوصلة استراتيجية للمشرع الوطني ومؤسسات الإدارة العامة إذ تقدم رؤية تشريعية وتنظيمية دقيقة تساعد في صياغة سياسات وطنية محكمة لحوكمة البيانات وتحقيق الأمن السيبراني وصون البنية التحتية الرقمية الحيوية.
- تحصين الإدارة العامة الذكية ضد الانكشاف السيادي: تسهم مخرجات هذه الدراسة في تقديم حلول وتوصيات عملية تعزز من مناعة الدولة الذكية وتضمن كفاءة أداء المرافق العامة واستمراريتها دون الوقوع في فخ التبعية للشركات التقنية العابرة للحدود.

- بناء نموذج إداري آمن ومستدام: توفر الدراسة تصوراً عملياً متعلماً يوازن بدقة بين متطلبات الابتكار الرقمي والتطوير الإداري وبين مقتضيات المشروعية القانونية وحماية الحقوق والحريات الأساسية للمواطنين في الدولة الذكية.

منهجية الدراسة

تقتضي طبيعة الموضوع المركبة واستثنائية إشكاليته في تقاطع القانون العام مع الفضاء الرقمي تبني منهجية تكاملية مركبة لا تكتفي بالوصف السطحي بل تغوص في تفكيك البنى القانونية وتأصيل الممكنات التقنية في إطار الدولة الذكية.

وتستند هذه المنهجية إلى ركائز متكاملة تتوزع كالتالي:

- **المنهج الأول المنهج التحليلي:**

تعتمد الدراسة بصفة رئيسة على المنهج التحليلي وذلك لاستنطاق النصوص التشريعية وتفكيك البنى المفاهيمية للسيادة الرقمية ودراسة أبعادها القانونية والوظيفية في بيئة الدولة الذكية بما يتيح تقييم مدى كفاءة الأطر القانونية القائمة في مواجهة التحديات السيبرانية.

- **المنهج الثاني المنهج الوصفى:**

تُستعان بالمنهج الوصفي لتأطير ظاهرة التحول الرقمي وتوصيف التحولات البنيوية والانتقال من الإدارة التقليدية إلى الإدارة الذكية وعرض المفاهيم والمصطلحات التقنية والقانونية ذات الصلة بموضوع البحث بدقة علمية متسقة.

- **المنهج الثالث المنهج المقارن:**

توظف الدراسة المنهج المقارن في الحدود التي تقتضيها طبيعة البحث من خلال استقراء ومقارنة أحدث الاتجاهات التشريعية والتنظيمية العالمية والمقارنة المتعلقة بحوكمة البيانات والأمن السيبراني وصون البنية التحتية الحرجة للاستفادة من النماذج الناجحة في صياغة الإطار المقترح.

- **المنهج الرابع مقاربة القراءة المتسأصلة (الجدلية بين القانون والتقنية):**

يقوم البناء المنهجي لهذه الدراسة على فلسفة فريدة ترفض الفصل الجزئي بين النص القانوني والواقع التقني إذ تفترض المنهجية أن دراسة السيادة الرقمية تستوجب عقلاً فقهياً قادراً على تلمس الأثر القانوني للبرمجيات والخوارزميات وقراءة النصوص التشريعية في ضوء البنية التحتية الرقمية مما يضمن الخروج بنتيجة علمية محكمة ومتكاملة تعزز من استقلال الدولة الذكية وسيادتها في البيئة المعاصرة.

المبحث الأول: الإطار المفاهيمي للسيادة الرقمية وعلاقتها بالدولة الذكية

تمثل دراسة الإطار المفاهيمي للسيادة الرقمية في الدولة الذكية المدخل الأساس لفهم هذا الموضوع في أبعاده القانونية والعملية ذلك أن السيادة الرقمية لم تعد مفهوماً تابعاً للتطور التكنولوجي أو أثراً فرعياً من آثاره بل أضحت أحد المرتكزات الجوهرية في إعادة تشكيل الدولة المعاصرة ووظائفها في البيئة الرقمية. ومع اتساع الاعتماد على الأنظمة الذكية والبنى التحتية الرقمية وقواعد البيانات والخدمات المترابطة إلكترونياً لم يعد تطوير الأداء الحكومي مسألة تقنية محضة وإنما أصبح وثيق الصلة بقدرة الدولة على بسط سلطتها المشروعة على مجالها الرقمي وصون استقلال إرادتها التنظيمية والإدارية في مواجهة صور التبعية التقنية والاختراقات السيبرانية والهيمنة الرقمية العابرة للحدود [1].

ومن هذا المنطلق فإن الإحاطة بهذا المبحث تقتضي البدء بتأصيل مفهوم السيادة الرقمية وبيان علاقتها بمفهوم الدولة الذكية باعتبار أن ضبط المفهوم يعد أساساً لازماً لبناء أي معالجة قانونية منضبطة.

[1] Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

كما تقتضي الوقوف على الجوانب التنظيمية والتقنية التي تمنح السيادة الرقمية مضمونها العملي من خلال ما توفره البنية التحتية الرقمية وأمن الشبكات وحوكمة البيانات والتقنيات الذكية من أدوات تمكين حقيقية للدولة في ممارسة وظائفها العامة بكفاءة وأمان واستقلال.

وعلى هذا الأساس يتوزع هذا المبحث إلى مطلبين: يتضمن المطلب الأول منه التأصيل القانوني والمفاهيمي لمفهوم السيادة الرقمية بينما يتضمن المطلب الثاني بيان علاقة السيادة الرقمية بمفهوم الدولة الذكية ووظائفها. [1]

المطلب الأول :التأصيل المفاهيمي للسيادة الرقمية ومقوماتها القانونية والتقنية:

يقتضي تناول موضوع السيادة الرقمية في إطار الدولة الذكية البدء بضبطها مفهوماً وتأصيلاً لأن سلامة التحليل القانوني في هذا الموضوع لا تتحقق من غير تحديد دقيق لمضمونها وحدودها، وتمييزها عما يجاورها من مفاهيم متداخلة كالأمن السيبراني وحوكمة البيانات والتحول الرقمي والاستقلال التقني.

فالسيادة الرقمية ليست مجرد وصف سياسي حديث ولا هي تعبير إنشائي عن الرغبة في مواكبة التطور التكنولوجي وإنما تمثل امتداداً معاصراً وتطوراً بنيوياً لفكرة السيادة الوطنية في بعديها الوظيفي والتنظيمي بعد أن أضحى الفضاء الرقمي جزءاً أصيلاً من النطاق الذي تمارس فيه الدولة اختصاصاتها العامة وتباشر فيه سلطاتها الإدارية والتنظيمية. [2]

وقد اتجهت الأدبيات القانونية والمؤسسية الحديثة إلى ربط السيادة الرقمية بالقدرة الذاتية للدولة على تصميم بنيتها الرقمية الوطنية، وتطويرها والتحكم الفعلي فيها وحمايتها بما يحقق الاستقلال الرقمي والأمن المعلوماتي ويحدّ من صور التبعية والارتهان لمقدمي التكنولوجيا والشركات العابرة للحدود.

وعلى هذا الأساس يمكن تعريف السيادة الرقمية بأنها: "قدرة الدولة، قانوناً وفعلاً على تنظيم مجالها الرقمي الوطني والتحكم المشروع في بياناتها وبناها التحتية ونظمها ومنصاتها وخدماتها الرقمية بما يكفل استقلال القرار العام وصون المصلحة العامة وحماية الوظائف السيادية والإدارية من صور التبعية التقنية أو الهيمنة الرقمية أو التعرض غير المشروع للبيانات والأنظمة". [3]

ويكشف هذا التأصيل المفاهيمي أن السيادة الرقمية لا تنحصر في حماية البيانات وحدها ولا تختزل في امتلاك أدوات أمنية تقنية فحسب بل تقوم على ثلاثة أبعاد وركائز متكاملة تُشكل مقوماتها الأساسية: بعد تنظيمي قانوني يخول الدولة وضع القواعد القانونية والتنظيمية الحاكمة للمجال الرقمي وبسط اختصاصها القضائي والإداري على الفضاء المعلوماتي الوطني وبعد تقني عملي يضمن امتلاك الدولة للقدرة الفعلية والتشغيلية على إدارة البنى التحتية الرقمية ومراكز البيانات ومفاهيم التشفير وتأمينها من الاختراقات والتعطيل وبعد وظيفي مؤسسي يضمن بقاء ممارسة الاختصاص العام وإدارة المرافق والخدمات الحيوية بيد الإدارة العامة للدولة، ومن زاوية النظرية العامة للقانون الإداري تكتسب السيادة الرقمية أهمية مضاعفة لأنها تمس جوهر الوظيفة العامة الإدارية لا مجرد الوسائل التنفيذية.

فالإدارة العامة لم تعد تباشر نشاطها الإداري عبر الوثيقة الورقية والإجراء المادي المباشر وحدهما بل أضحت تعتمد على قواعد بيانات ضخمة ومترابطة ومنصات تقديم خدمات ذكية ونظم تحقق للهوية الرقمية وتقنيات الحوسبة السحابية وأدوات التحليل والتنبؤ الخوارزمي التي تسهم في صنع القرار الإداري وتوجيه المرافق العامة. [4]

---

[1] Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. Government Information Quarterly, 37(3), Article 101493. https://doi.org/10.1016/j.giq.2020.101493
Misra, S., Barik, K., & Kvalvik, P. (2025). Trust in Digital Sovereignty: A Review of Security, Privacy, and Governance Challenges. Public Organization Review, 1-23. https://doi.org/10.1007/s11115-025-00968-0

[2] Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

[3] Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. Digital Society, 3(3), 59. https://doi.org/10.1007/s44206-024-00146-7

[4] Boul, M. (2018). Réflexions sur la notion de donnée publique. Revue française d'administration publique, 167(3), 471–478. https://doi.org/10.3917/rfap.167.0471

ولهذا فإن أي قصور أو ضعف في السيطرة القانونية أو التقنية على هذه الأدوات لا يعد مجرد خلل فني عارض بل يمس مباشرة مبدأ المشروعية الإدارية واستمرارية سير المرافق العامة بنظام وطرود وسلامة الإرادة في القرار الإداري وقدرة الدولة على ممارسة سلطاتها التنظيمية والضبطية بصورة مستقلة وآمنة.

وتأكيداً لذلك، فإن المفاهيم الحديثة للحوكمة الرقمية تبين أن الإدارة الرقمية لم تعد وسيلة لتحسين الكفاءة الإجرائية فحسب بل محركاً استراتيجياً يجعل السياسات العامة أكثر فاعلية واستقلالاً ويصون كرامة الدولة وسيادتها في البيئة المعلوماتية المعاصرة. [1]

ممارسة الاختصاص العام وإدارة المرافق والخدمات الحيوية بيد الإدارة العامة للدولة، دون الارتهان المطلق للفاعلين التقنيين المحليين أو العابرين للحدود. [2]

ومن زاوية النظرية العامة للقانون الإداري تكتسب السيادة الرقمية أهمية مضاعفة لأنها تمس جوهر الوظيفة العامة الإدارية لا مجرد الوسائل التنفيذية.

فالإدارة العامة لم تعد تباشر نشاطها الإداري عبر الوثيقة الورقية والإجراء المادي المباشر وحدهما بل أضحت تعتمد على قواعد بيانات ضخمة ومترابطة ومنصات تقديم خدمات ذكية ونظم تحقق للهوية الرقمية وتقنيات الحوسبة السحابية وأدوات التحليل والتنبؤ الخوارزمي التي تسهم في صنع القرار الإداري وتوجيه المرافق العامة. [3]

ولهذا فإن أي قصور أو ضعف في السيطرة القانونية أو التقنية على هذه الأدوات لا يعد مجرد خلل فني عارض بل يمس مباشرة مبدأ المشروعية الإدارية واستمرارية سير المرافق العامة بنظام وطرود، وسلامة الإرادة في القرار الإداري، وقدرة الدولة على ممارسة سلطاتها التنظيمية والضبطية بصورة مستقلة وآمنة.

وتأكيداً لذلك فإن المفاهيم الحديثة للحوكمة الرقمية تبين أن الإدارة الرقمية لم تعد وسيلة لتحسين الكفاءة الإجرائية فحسب بل محركاً استراتيجياً يجعل السياسات العامة أكثر فاعلية واستقلالاً ويصون كرامة الدولة وسيادتها في البيئة المعلوماتية المعاصرة. [4]

المطلب الثاني: علاقة السيادة الرقمية بمفهوم الدولة الذكية ووظائفها:

بدايةً تجدر الإشارة إلى أن مفهوم "الدولة الذكية" لا ينصرف إلى دولة تستخدم التكنولوجيا استخداماً جزئياً أو شكلياً بل إلى دولة تعيد بناء إدارة الشأن العام على أساس الاستخدام المنهجي للبيانات والتقنيات الرقمية والأنظمة الذكية في تصميم السياسات العامة تقديم الخدمات إدارة الموارد والتفاعل مع الأفراد والمؤسسات.

وتظهر الأدبيات الدولية الحديثة ولا سيما تقارير الأمم المتحدة ومنظمة التعاون والتنمية الاقتصادية (OECD) أن التطور الانتقالي من "الحكومة الإلكترونية" إلى "الحكومة الرقمية" وصولاً إلى "الدولة الذكية" يعني الانتقال من مجرد رقمنة الإجراءات والوثائق إلى إعادة هندسة العمل الإداري الحكومي على أساس التكامل بين البيانات والمنصات والبنية الرقمية وصنع القرار العام القائم على المعرفة.

كما أن البنية الرقمية العامة لم تعد مرفقاً تقنياً تابعاً بل أضحت جزءاً بنيوياً من قدرة الدولة على إنجاز وظائفها الإدارية والسيادية بكفاءة اتساق واستدامة. [5]

---

[1] Cluzel -Métayer, L. (2018). La construction d'un service public de la donnée. Revue française d'administration publique, 167(3), 491–500. https://doi.org/10.3917/rfap.167.0491

[2] Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305–2322. https://doi.org/10.1177/1461444819865984

[3] Boul, M. (2018). Réflexions sur la notion de donnée publique. Revue française d'administration publique, 167(3), 471–478. https://doi.org/10.3917/rfap.167.0471

[4] Cluzel -Métayer, L. (2018). La construction d'un service public de la donnée. Revue française d'administration publique, 167(3), 491–500. https://doi.org/10.3917/rfap.167.0491

[5] Glybovets, A., & Mohammad, A. (2017). E-government versus smart government: Jordan versus the United States. EUREKA: Social and Humanities.

ومن ثم فإن العلاقة بين السيادة الرقمية والدولة الذكية هي علاقة عضوية وتكاملية لا عرضية فالدولة الذكية بحكم اعتمادها الكثيف والمباشر على قواعد البيانات المنصات الخدمات المترابطة والأنظمة الخوارزمية لا تستطيع أداء وظائفها أداءً مستقلاً وفعالاً ما لم تكن قادرة على إخضاع تلك البيئة الرقمية لمقتضيات القانون الوطني والمشروعية الإدارية.

كما يلتزم هذا النموذج بحماية البنية المعلوماتية الوطنية من أخطار الاختراق والتعطيل أو السيطرة والهيمنة الخارجية وضبط حركة البيانات وتداولها بما ينسجم مع مقتضيات المصلحة العامة وصيانة الحقوق والحريات الأساسية. [1]

وبالمقابل فإن السيادة الرقمية لا تظهر في صورتها التطبيقية والعملية الأوضح إلا داخل نموذج الدولة الذكية لأن هذا النموذج المؤسسي الحديث هو الذي يكشف على نحو تطبيقي مدى قدرة الدولة على الجمع بين الكفاءة التقنية المشروعية القانونية والاستقلال المؤسسي.

وعليه تُمثل السيادة الرقمية الشرط البنيوي والأساسي لقيام الدولة الذكية على أسس تنظيمية وقانونية سليمة في حين تُشكل الدولة الذكية الإطار الوظيفي والعملي الذي تتجسد فيه هذه السيادة واقعاً وممارسة إدارية ملموسة. [2]

المبحث الثاني: الإطار التشريعي المنظم للسيادة الرقمية في الدولة الذكية

لا يكفي في دراسة القوانين المنظمة للمجال الرقمي الوقوف عند نصوصها وأحكامها المجردة بل يقتضي التحليل القانوني السليم الرجوع إلى الأسباب الموجبة التي دعت السلطة التشريعية إلى إصدارها لأن هذه الأسباب تكشف الغاية التشريعية وتوضح المصلحة العامة التي استهدفها المشرّع وتعين على فهم اتجاه النصوص وتفسيرها في ضوء سياقها الوظيفي والتنظيمي.

وتزداد أهمية ذلك في التشريعات المرتبطة بالتحول الرقمي لأن هذا النوع من القوانين لا يصدر في فراغ وإنما يأتي استجابة لتحولات عميقة مست بنية الدولة الحديثة وأعادت تشكيل وسائل الإدارة العامة وأنماط تقديم الخدمات وحدود التدخل التنظيمي في البيئة الرقمية. [3]

وفي هذا الإطار يمكن القول إن أبرز الأسباب الموجبة لإصدار القوانين محل الدراسة التحول المتسارع نحو الدولة الذكية بما فرضه هذا التحول من انتقال الإدارة العامة من الوسائل التقليدية إلى الاعتماد على قواعد البيانات والمنصات الرقمية والخدمات الإلكترونية والحوسبة السحابية والأنظمة الذكية في ممارسة اختصاصاتها.

وقد أوجد هذا الواقع حاجة تشريعية ملحة إلى وضع إطار قانوني يحكم هذا الانتقال ويمنح العمل الإداري الرقمي أساسه المشروع ويحدد ضوابطه وحدوده وآثاره القانونية. [4]

---

[1] Donnelly, S., Rios Camacho, E., & Heidebrecht, S. (2024). Digital sovereignty as control. https://doi.org/10.1080/13501763.2023.2295520
Pierucci, F. (2025). Sovereignty in the digital era: Rethinking territoriality and governance in cyberspace. Digital Society, 4(1), 27. https://doi.org/10.1007/s44206-025-00189-4

[2] Fratini, S., et al. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. Digital Society, 3(3), 59. https://doi.org/10.1007/s44206-024-00146
Misra, S., Barik, K., & Kvalvik, P. (2025). Trust in Digital Sovereignty: A Review of Security, Privacy, and Governance Challenges. Public Organization Review, 1-23. https://doi.org/10.1007/s11115-025-00968-0

[3] Boul, M. (2018). Réflexions sur la notion de donnée publique. Revue française d'administration publique, 167(3), 471–478.
Cluzel-Métayer, L. (2018). La construction d'un service public de la donnée. Revue française d'administration publique, 167(3), 491–500.

[4] Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. Government Information Quarterly, 37(3), Article 101493
Glybovets, A., & Mohammad, A. (2017). E-government versus smart government: Jordan versus the United States. EUREKA: Social and Humanities.

فالإدارة الرقمية مهما بلغت من الكفاءة التقنية لا يمكن أن تستقيم قانوناً إلا إذا أحيطت بتنظيم تشريعي يضمن مشروعيتها ويحفظ حجية أعمالها ويضبط مسؤولياتها ويكفل خضوعها لسيادة القانون.

لنرى بأن دور التشريع في هذا السياق حدود يتجاوز التنظيم الشكلي ليغدو صمام الأمان الذي يحمي المنظومة الإدارية من مخاطر الفوضى الرقمية ويوفر الحصانة القانونية اللازمة لاستمرار تقديم الخدمات العامة بكفاءة واستقرار مما يرسخ دعائم الثقة المؤسسية ويحول البنية الرقمية من أداة تقنية بحتة إلى مرفق عام ذكي محكوم بقواعد المشروعية وسيادة القانون.

وبناءً عليه فقد تم تقسيم هذا المبحث الى مطلبين: تضمن المطلب الأول الأسباب الموجبة لإصدار التشريعات المرتبطة بالسيادة الرقمية ويتضمن المطلب الثاني دور التشريعات في تعزيز السيادة الرقمية وحماية البنية الرقمية للدولة. [1]

المطلب الأول: الأسباب الموجبة لإصدار التشريعات المرتبطة بالسيادة الرقمية:

تتمثل الأسباب الموجبة في الحاجة الملحة إلى حماية المجال الرقمي الوطني باعتباره أحد المكونات الحديثة للسيادة فمع اتساع اعتماد الدولة على البنية الرقمية في تشغيل المرافق العامة وحفظ السجلات وتقديم الخدمات وإدارة الاتصال المؤسسي لم يعد المجال الرقمي شأناً فنياً أو إجرائياً بحسب بل أصبح جزءاً من النطاق الذي تمارس الدولة داخله سلطتها التنظيمية والإدارية.

ومن ثم فإن تعرض هذا المجال للاختراق أو التعطيل أو الوصول غير المشروع أو التبعية التقنية غير المنضبطة لا ينعكس على الجانب التقني وحده بل يمتد أثره إلى انتظام المرفق العام وسلامة القرار الإداري وأمن البيانات الوطنية واستقلال الإرادة العامة للدولة.

ولهذا كان التدخل التشريعي ضرورياً لتقرير الحماية القانونية للمجال الرقمي ووضع القواعد المنظمة له وإرساء الأساس النظامي الذي يمكن الدولة من بسط سلطانها المشروع على فضائها الرقمي. [2]

ويتصل بذلك سبب موجب آخر يتمثل في إعادة تنظيم العلاقة القانونية بين الإدارة العامة والأفراد والبيانات والفاعلين التقنيين.

فقد أفرز التحول الرقمي مراكز قانونية جديدة لم تكن معروفة بذات الكثافة في البيئة التقليدية كالمراكز القانوني للبيانات الشخصية وحجية السجلات والمعاملات الرقمية وحدود المعالجة الإلكترونية للبيانات ومسؤولية الجهات القائمة على تشغيل الأنظمة الذكية والضمانات الواجبة للأفراد في مواجهة القرارات أو الإجراءات الرقمية.

ومن ثم كان لزاماً على السلطة التشريعية أن تتدخل لضبط هذه العلاقات في إطار قانوني يوازن بين مقتضيات الكفاءة الإدارية من جهة وضمانات الحقوق والحريات من جهة أخرى بما يمنع الانكشاف المعلوماتي أو التعسف التقني أو التوسع غير المشروع في جمع البيانات أو استعمالها أو تداولها. [3]

ومن الأسباب الموجبة أيضاً مواجهة القصور التشريعي الذي يظهر عادة في المراحل الأولى للتحول الرقمي حيث تكون الأحكام ذات الصلة موزعة بين نصوص عامة أو متفرقة ولا تكفي وحدها لتوفير حماية متكاملة للمجال الرقمي ولا لتحديد الاختصاصات والمسؤوليات والضمانات على نحو دقيق.

ومن هنا فإن إصدار القانون دراسة محل الدراسة يُعد النظير إليه بوصفه استجابة تشريعية تهدف إلى تجاوز التشتت التنظيمي وبناء مرجعية قانونية أكثر تخصيصاً واتساقاً قادرة على استيعاب خصوصية البيئة الرقمية وعلى تنظيمها وفق منطق قانوني موحد يحقق الوضوح والاستقرار وقابلية النفاذ.

وفي الإطار الأردني تبدو الأسباب الموجبة لإصدار قانون حماية البيانات الشخصية رقم 24 لسنة 2023 وقانون الجرائم الإلكترونية رقم 17 لسنة 2023 متصلة اتصالاً يتبدل موقع الدولة نفسها داخل المجال الرقمي.

---

[1] Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. Digital Society, 3(3), 59.
Misra, S., Barik, K., & Kvalvik, P. (2025). Trust in Digital Sovereignty: A Review of Security, Privacy, and Governance Challenges. Public Organization Review, 1-23

[2] الدهشان، يحيى (2023). الحماية الجنائية للبيانات في ظل التحول الرقمي، مجلة الدراسات القانونية والاقتصادية، 9(3)، 1500-1551.

[3] الزهراني، ايناس، (2024) التحول الرقمي وتأثيره على الإدارة العامة. مركز البحث وتطوير الموارد البشرية (رماح)، (12)، 9-21

فالأول جاء في السياق الحاجة إلى تنظيم جمع البيانات الشخصية ومعالجتها وتخزينها ونقلها وتحديد الحقوق والالتزامات والجهات الرقابية ذات الصلة بينما جاء الثاني في سياق مواجهة الأفعال غير المشروعة المرتكبة عبر الشبكات والأنظمة المعلوماتية وحماية المجتمع والدولة من الأخطار الناشئة عن الاستخدام الإجرامي للتكنولوجيا.

ويدل صدور هذين القانونين في المدى الزمني نفسه تقريباً على أن المشرع الأردني بات يتعامل مع المجال الرقمي لا بوصفه حيزاً تقنياً هامشياً بل بوصفه مجالاً قانونياً يحتاج إلى ضبط مزدوج: ضبط وقائي تنظيمي من جهة وضبط زجري من جهة أخرى. [1]

المطلب الثاني: دور التشريعات في تعزيز السيادة الرقمية وحماية البنية الرقمية للدولة:

أما من حيث دور هذه الأسباب الموجبة في تعزيز السيادة الرقمية فإن أثرها لا يقف عند مرحلة التفسير التشريعي بل يمتد إلى البنية الوظيفية للقانونين نفسيهما.

فهذه الأسباب تكشف أن الغاية من التدخل التشريعي لم تكن مجرد إدخال وسائل تقنية حديثة إلى الإدارة، وإنما بناء حماية قانونية للمجال الرقمي الوطني وتمكين الدولة من إدارة بياناتها وبنيتها الرقمية وخدماتها على نحو منظم وآمن ومستقل.

وبذلك تسهم هذه التشريعات في تعزيز السيادة الرقمية على مستويين متكاملين: مستوى حمائي من خلال وضع القواعد الكفيلة بصون البيانات والأنظمة والبنى الرقمية من الاعتداء أو العبث أو الوصول غير المشروع ومستوى تمكيني من خلال منح الدولة الإطار القانوني الذي يمكنها من تنظيم التحول الرقمي وتحديد اختصاصات الجهات العامة، وضبط البيئة الرقمية بما يخدم المصلحة العامة.

ومن منظور القانون الإداري تتجلى القيمة القانونية للأسباب الموجبة في أنها تعكس تحوّلاً في وظيفة التشريع ذاته.

فالتشريع لم يعد يقتصر على تنظيم النشاط الإداري في صورته المادية أو التقليدية بل أصبح أداة لتأسيس مشروعية الإدارة الرقمية وضمان استمرارية المرفق العام الرقمي وحماية الثقة العامة في المعاملات والخدمات الإلكترونية وتأمين المشروعية في مجال أصبحت فيه الدولة تمارس جزءاً مهماً من اختصاصاتها عبر الوسائط الرقمية. وعليه، فإن الأسباب الموجبة لإصدار القانونين محل الدراسة لا تمثل مجرد خلفية تفسيرية للنصوص، وإنما تكشف عن وعي تشريعي بأن السيادة الرقمية ليست نتيجة عفوية للتطور التكنولوجي بل ثمرة لبناء قانوني منظم ومقصود يستهدف حماية استقلال الدولة في المجال الرقمي وتمكينها من ممارسة وظائفها العامة في بيئة تقنية متغيرة ومتداخلة. [2]

وبناء على ذلك فإن الأسباب الموجبة لإصدار القانونين محل الدراسة تؤدي دوراً محورياً في ترسيخ السيادة الرقمية لأنها تعكس إدراك السلطة التشريعية لضرورة الانتقال من المعالجة التقنية الجزئية إلى البناء القانوني المتكامل للمجال الرقمي الوطني.

فهي تكشف من جهة عن الحاجة إلى حماية البنية الرقمية والبيانات والخدمات العامة وتكشف من جهة أخرى عن إرادة تشريعية تتجه إلى إعادة ضبط العلاقة بين الدولة والتقنية في إطار يحفظ المشروعية، ويضمن الاستقلال، ويعزز القدرة التنظيمية للدولة الذكية.

ولهذا فإن دراسة هذه الأسباب لا تعد مسألة تمهيدية فحسب بل تمثل جزءاً أصيلاً من فهم الأساس الذي تقوم عليه السيادة الرقمية في صورتها التشريعية المعاصرة.

وفي مصر يلاحظ ذات الاتجاه المتبع في الإطار الأردني ولكن في صورة مزدوجة: حماية البيانات عبر قانون 151 لسنة 2020، وحماية البنية الرقمية ومكافحة الاعتداءات عبر قانون 175 لسنة 2018.

---

[1] قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023؛ وقانون الجرائم الإلكترونية الأردني رقم (17) لسنة 2023، الجريدة الرسمية الأردنية.

[2] محمد، سامي الطيب إدريس. (2024) دواعي وآثار خرق السيادة في ظل المتغيرات الدولية. مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة السادات، المجلد 12، العدد 2، ص 1408–1413

وهذه الثنائية المقارنة مفيدة جداً لأنها تكشف أن التشريعات الحديثة تتجه إلى تقسيم الحماية الرقمية إلى شقين متلازمين: شق تنظيمي يضبط البيانات وحقوق أصحابها وشق جنائي/حمائي يواجه الجرائم الرقمية والأفعال الماسة بأمن الأنظمة والمواقع والشبكات.

وهو منطق قريب من البناء الأردني الحديث ويؤكد أن الأسباب الموجبة للتدخل التشريعي لا تتعلق فقط بالتنظيم ولا فقط بالتجريم بل ببناء منظومة قانونية متكاملة تضمن أن يكون المجال الرقمي خاضعاً للسيادة القانونية للدولة لا مبعثراً بين قواعد عامة عاجزة عن مواكبة خصوصيته.

ومن زاوية القانون الإداري تتجلى أهمية هذه الأسباب الموجبة في أنها تكشف عن تحول وظيفة التشريع الإداري ذاته، فالمشرّع لم يعد معنياً فقط بتنظيم القرار الإداري أو المرفق العام أو السلطة الضبطية في صورتها التقليدية بل أصبح معنياً أيضاً بتقنين الإدارة الرقمية وتحديد ضوابط معالجة البيانات داخل الجهات العامة وتأمين الخدمات الإلكترونية وحماية المرفق العام الرقمي من الانقطاع أو العبث أو الاستغلال غير المشروع.

وبهذا المعنى فإن القوانين محل الدراسة لا تؤدي وظيفة موضوعية مستقلة عن النظرية العامة للقانون الإداري بل تمثل امتداداً حديثاً لها فهي تشريعات تضمن استمرار المرفق العام في صورته الرقمية وتؤمن مشروعية أدوات الإدارة الذكية وتدعم سلطة الدولة التنظيمية في بيئة تتسم بالتعقيد التقني والتداخل العابر للحدود.

وهذا تحديداً هو الموضع الذي تتحول فيه الأسباب الموجبة من مجرد خلفية تشريعية إلى عنصر كاشف عن بنية السيادة الرقمية نفسها. [1] وعليه فإن دور الأسباب الموجبة في تعزيز السيادة الرقمية يظهر على مستويين متكاملين.

الأول مستوى حمائي يتمثل في أنها تبرر إقامة بنية قانونية تحمي البيانات والأنظمة والشبكات والمنصات والخدمات من الاعتداء والاختراق والاستعمال غير المشروع.

والثاني مستوى تمكيني يتمثل في أنها تؤسس لسلطة الدولة في تنظيم المجال الرقمي وإدارته وفق قواعد واضحة بما يعزز الاستقلال التنظيمي ويرفع منسوب الثقة العامة ويدعم قدرة الإدارة على التحول الذكي دون أن تفقد سيطرتها القانونية على أدواتها الرقمية.

ومن ثم فإن هذه الأسباب لا ينبغي النظر إليها بوصفها مقدمات تفسيرية هامشية بل بوصفها جزءاً من الفلسفة التشريعية التي يقوم عليها بناء السيادة الرقمية في الدولة الذكية. [2]

وبناءً على ما تقدم يخلص هذا المطلب إلى أن صدور التشريعين الأردنيين محل الدراسة لم يكن استجابة عرضية لظاهرة تقنية طارئة بل جاء تعبيراً عن إدراك تشريعي متقدم بأن الدولة الحديثة إذا أرادت أن تنتقل إلى نموذج الدولة الذكية انتقالاً آمناً ومشروعاً فلا بد أن تؤسس هذا الانتقال على قواعد تحمي بياناتها وتصون بنيتها الرقمية وتضبط العلاقة بين الإدارة والأفراد والفاعلين التقنيين، وتمنع تحول المجال الرقمي إلى نقطة ضعف تمسّ استقلال القرار العام.

ومن هنا تتأكد الصلة الوثيقة بين الأسباب الموجبة وهذه القوانين وبين ترسيخ السيادة الرقمية في معناها القانوني والإداري المعاصر.

المبحث الثالث: الأسس التقنية للسيادة الرقمية وأثرها في بناء الدولة الذكية

لا يتحقق ترسيخ السيادة الرقمية في الدولة الذكية عبر البناء التشريعي وحده لأن فعالية الحماية القانونية في هذا المجال تظل مشروطة بوجود بنية تقنية وطنية قادرة على حمل تلك الحماية وإنفاذها عملياً.

فالقانون قد يقرر ضوابط حماية البيانات أو ينظم المعاملات الرقمية أو يجرم الاعتداء على الأنظمة والشبكات إلا أن هذه القواعد تبقى محدودة الأثر إذا لم تستند إلى أدوات تقنية تمكن الدولة من السيطرة الفعلية على بيئتها الرقمية.

---

[1] وزارة الاقتصاد الرقمي والريادة. (2024) معايير اعتماد مراقب حماية البيانات الشخصية الصادرة بموجب أحكام الفقرة (ب) من المادة (17) من قانون حماية البيانات الشخصية رقم (24) لسنة 2023 . عمّان، الأردن: وزارة الاقتصاد الرقمي والريادة.

[2] المركز الوطني للأمن السيبراني. (2018) الاستراتيجية الوطنية للأمن السيبراني 2018–2023 .عمّان، الأردن: المركز الوطني للأمن السيبراني.

ومن ثم، فإن السيادة الرقمية لا تنصرف فقط إلى سلطة الدولة في التنظيم بل تمتد إلى قدرتها الواقعية على إدارة البيانات وتأمين الشبكات وتشغيل المنصات وضمان استمرارية المرافق والخدمات الرقمية من غير ارتهان تقني يضعف استقلال القرار العام. [1]

وقد أكدت التقارير الدولية ومنظمة التعاون الاقتصادي والتنمية (OECD) أن البنية الرقمية العامة لم تعد مجرد وسيلة لتحسين الكفاءة بل أصبحت جزءاً مركزياً من تنفيذ سياسات الحكومة الرقمية ورفع اتساقها وفعاليتها. وفي هذا السياق العضوي يتبين أن التلاحم بين التقنية والسيادة يمثل عصب الدولة المعاصرة إذ لا سيادة في الفضاء الافتراضي لمن لا يمتلك مفاتيح تشغيله وتأمينه ذاتياً مما يحتم على الدولة امتلاك سيادتها التقنية كدرع استراتيجي يحمي أمنها القومي المعلوماتي. [2]

وقد تم تقسيم هذا المبحث إلى مطلبين: يتضمن المطلب الأول المرتكزات التقنية للسيادة الرقمية ويتضمن المطلب الثاني أثر الأسس التقنية في دعم وظائف الدولة الذكية وتحقيق الكفاءة الرقمية. [3]

المطلب الأول: المرتكزات التقنية للسيادة الرقمية:

ويتمثل الأساس التقني الأول في البنية التحتية الرقمية الوطنية بما تشتمل عليه من شبكات اتصال ومراكز بيانات ومنصات حكومية مشتركة وسجلات أساسية وأنظمة ربط وتبادل معلومات بين الجهات العامة. فالدولة الذكية لا تقوم على رقمنة متفرقة للخدمات وإنما على بنية مترابطة وآمنة وقابلة للتشغيل البيني تسمح بتدفق البيانات والقرارات والخدمات عبر مؤسسات الدولة على نحو منظم. وتقرر (OECD) أن من المكونات الجوهرية للبنية الرقمية العامة: الهوية الرقمية وأنظمة مشاركة البيانات والمدفوعات الرقمية والبريد الرقمي، والسجلات الحكومية الأساسية وأنان الحكومات تضطلع بدور محوري في تصميم هذه البنية وتطويرها وإدارتها. كما أن الاستراتيجية الأردنية للتحول الرقمي (2020-2026) جعلت من بناء أردن رقمي آمن وممكن رقماً أحد مرتكزاتها وربطت التحول الرقمي بالثقة الرقمية والبيانات والذكاء الاصطناعي وتكامل الخدمات. وهذا يدل على أن امتلاك بنية التحتية الرقمية أو السيطرة الوطنية عليها ليس خياراً فنياً صرفاً بل أحد المظاهر الأساسية للسيادة الرقمية لأن الدولة التي لا تتحكم في الطبقات الأساسية لبنيتها الرقمية لا تملك في الواقع السيطرة الكاملة على أدواتها الإدارية الحديثة. [4]

أما الأساس الثاني فيتمثل في حوكمة البيانات والسيطرة على السجلات الأساسية ودفعات المعلومات. فالدولة الذكية تستمد قسطاً مهماً من قدرتها الإدارية والتنظيمية من البيانات العامة: تجمعها وتحقق منها وتربط بينها وتستند إليها في صنع القرار وفي توجيه الموارد وفي الرقابة وفي تصميم الخدمة العامة. ولهذا لم تعد البيانات مجرد مورد معلوماتي بل أصبحت أصلاً سيادياً يرتبط به استقلال القرار العام. وتقرر (OECD) أن حوكمة البيانات تعني الأطر التي تنظم دورة حياة البيانات وقيمتها واستخدامها ومشاركتها على نحو يحقق الفائدة العامة مع الحد من المخاطر المرتبطة بالسيطرة والخصوصية والجودة. ومن ثم فإن السيادة الرقمية تقتضي وجود هندسة مؤسسية وتقنية لإدارة البيانات الحكومية، تضمن سلامة المصدر وإمكانية التتبع وقابلية التشغيل البيني، ومنع التكرار، وضبط النفاذ، وتحديد ما يجوز مشاركته وما يجب أن يظل في دائرة الحماية المقيدة. ومن زاويتي القانون الإداري فإن حسن إدارة البيانات لا يمثل فقط شرطاً لتحسين الخدمة بل يعد شرطاً لصحة القرار الإداري الرقمي، لأن القرار القائم على بيانات ناقصة أو غير مضمونة أو خارجة عن الرقابة الفعلية للدولة يظل قراراً منقوص الأساس من حيث المشروعية والفعالية معاً. [5]

ويقوم الأساس الثالث على الأمن السيبراني باعتباره الضمانة الفعلية لاستقرار المجال الرقمي الوطني فكل توسع في الاعتماد على الأنظمة الرقمية والخدمات الحكومية الإلكترونية والحوسبة السحابية وتبادل البيانات يقابله ارتفاع في مستويات التعرض

---

[1] كامل، أحمد، (2024). البنى التحتية لتكنولوجيا المعلومات في العصر الرقمي، المجلة الدولية للعلوم الإدارية والاقتصادية والمالية، 3(8)، 1-14

[2] Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. Digital Society, 3(3), 59.

[3] وهدان، نيفين، (2026)، الحوكمة الذكية في الإدارة العامة في عصر الذكاء الاصطناعي: نموذج وساطة وتعديل في إطار إعادة هندسة السياسات العامة دراسة تطبيقية على مصر مع تحليل مقارن للنماذج الدولية، المجلة الأكاديمية للعلوم الاجتماعية، 26(4)، ص1-53

[4] وزارة الاقتصاد الرقمي والريادة الأردنية، الاستراتيجية الوطنية للتحول الرقمي والخطة التنفيذية (2021–2025)، المملكة الأردنية الهاشمية، 2021، ص 10–14، وص 34–35

[5] العبدلية، رقية بنت خلفان، والحراصي، نبهان بن حارث بن ناصر، والكندي، سالم سعيد علي (2024). انعكاسات تطبيق حوكمة البيانات في المؤسسات الحكومية العمانية .المجلة العلمية للمكتبات والوثائق والمعلومات، المجلد 6، العدد 19، ص 6–22

للهجمات الرقمية والاختراق والتعطيل وتسريب المعلومات والعبث بالخدمات العامة. ولهذا فإن الأمن السيبراني لا يعد عنصراً مكملاً للسيادة الرقمية بل أحد شروط وجودها.

والاستراتيجية الوطنية للأمن السيبراني 2018-2023 نصت على إنشاء إطار وطني يقود تنفيذ الأمن السيبراني وتطويره وعلى حماية البنى التحتية الحيوية والأنظمة الوطنية وتنسيق التنسيق الوطني في هذا المجال. وهذا يبين أن الدولة الأردنية نظرت إلى الأمن السيبراني باعتباره جزءاً من أمن الدولة وقدرتها على حماية خدماتها الرقمية ومعلوماتها الحيوية.

وفي الفقه الإداري الحديث، ينعكس التحول نحو المرافق العامة الرقمية بصورة مباشرة على مبدأ استمرارية المرفق العام وانتظام سيره؛ إذ لم يعد ضمان الاستمرارية مقتصراً على توفير الموارد البشرية والمادية اللازمة لتشغيل المرفق، بل أصبح يشمل أيضاً المحافظة على جاهزية البنية التحتية التقنية واستمرار عمل المنصات والأنظمة الإلكترونية التي تقدم الخدمات العامة. ومن ثم، فإن تعرض المرفق الرقمي للتعطيل أو الاختراق أو الأعطال الفنية التي تحول دون تقديم خدماته، من شأنه أن يشكل إخلالاً بمبدأ استمرارية المرفق العام، حتى وإن ظلت بنيته التنظيمية قائمة من الناحية الشكلية؛ ذلك أن وجود المرفق لا يحقق غايته القانونية والوظيفية ما لم يكن قادراً على تقديم خدماته للمنتفعين بصورة منتظمة ومستمرة. كما أن تكرار هذه الاختلالات قد يؤدي إلى زعزعة ثقة الجمهور بالإدارة العامة وإضعاف اطمئنانهم إلى كفاءة الخدمات الرقمية وسلامتها. [1]

أما الأساس الرابع فهو الحوكمة السيادية للحوسبة السحابية والخدمات المستضافة. ذلك أن السحابة توفر مرونة تشغيلية وقابلية للتوسع وخفضاً في التكاليف لكنها في المقابل تثير أسئلة دقيقة تتعلق بمكان البيانات والولاية القانونية عليها والجهة المتحكمة في مفاتيح الوصول والاعتماد على مزود واحد وإمكانية النقل والتعافي من الحوادث وإنهاء التعاقدات أو تعديلها. ولهذا فإن السيادة الرقمية لا تعني رفض الحوسبة السحابية بل تعني إخضاعها لمتطلبات سيادية وقانونية واضحة: تصنيف البيانات وتحديد البيانات المسموح بها وفرض معايير أمنية واعتمادية وضمان عدم الوقوع في الارتهان التقني لمزود بعينه. وقد أبرزت ENISA في إطارها الأمن للسحب الحكومية أن هذا النموذج يحقق قابلية للتوسع والمرونة والأداء العالي لكنه يتطلب نماذج دقيقة لتقييم المخاطر التنظيمية والأمنية وسياسات واضحة للرقابة والامتثال. ومن ثم فإن الدولة الذكية لا تكفيها الاستفادة من السحابة بل يلزمها أن تحكمها وفق تصور سيادي يضمن السيطرة الفعلية على البيانات والخدمات الحيوية بيدها أو ضمن بيئات موثوقة تخضع لرقابتها القانونية. [2]

ويتمثل الأساس الخامس في الهوية الرقمية والتشغيل البيني والسجلات الحكومية الأساسية. فالخدمات الذكية لا تكون ذكية بحق إلا إذا أمكن التحقق من الشخصية والصفة بأهلية بطريقة موثوقة وإذا كانت الأنظمة الحكومية قادرة على التفاعل فيما بينها من غير تضارب أو ازدواج أو انقطاع. وتؤكد OECD أن الهوية الرقمية ومشاركة البيانات والسجلات الأساسية عناصر محورية في البنية الرقمية العامة لأنها تتيح تقديم الخدمات على نحو متكامل وآمن وشامل وهذا البعد له قيمة قانونية واضحة وحدة الإدارة العامة في صورتها الرقمية ليست مجرد وسيلة تقنية للدخول إلى الخدمة بل هي أداة قانونية لإسناد التصرف والطلب والقرار والسجل إلى صاحبه بما يضمن حجية الإجراءات وسلامة آثارها.

كما أن التشغيل البيني بين الجهات العامة يجسد، من الناحية المؤسسية وحدة الإدارة العامة في صورتها الرقمية ويمنع تحول الدولة إلى جزر تقنية متباعدة وهو ما ينعكس إيجاباً على سرعة الإجراءات ودقة البيانات وكفاءة الرقابة وسلامة التنسيق بين الأجهزة العامة.

ولا يقل عن ذلك أهمية العنصر البشري والقدرات المؤسسية فالبنية الرقمية مهما بلغت من التقدم لا تنتج سيادة رقمية حقيقية إذا لم تتوافر للدولة كوادر قادرة على إدارة الأنظمة وتحليل البيانات ومراقبة الامتثال والاستجابة للحوادث وبناء الحلول الوطنية والتعامل الفني والقانوني الرشيد مع الموردين ومقدمي الخدمات. والاستراتيجية الأردنية للتحول الرقمي 2026-2028 تؤكد على بناء القدرات والمهارات الرقمية وتعزيز البيئة الممكنة للابتكار واعتماد التقنيات المستقبلية.

---

[1] المناصير، صهيب، (2023)، مسؤولية الإدارة العامة عن إدارة مرافقها الإلكترونية، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، 4(1)، ص 9، 22

[2] European Union Agency for Network and Information Security (ENISA), Security & Resilience in Governmental Clouds: Making an Informed Decision (Heraklion: ENISA, January 2011), pp. 6–8, 40–41.

وهذا يعني أن السيادة الرقمية لا تقوم على الأجهزة والبرمجيات فحسب، بل تستند أيضا إلى القدرة الوطنية على فهمها وإدارتها وتطويرها وصيانتها وضمان استدامة تشغيلها. فامتلاك البنية التحتية الرقمية دون توافر الكفاءات البشرية القادرة على إدارتها والتحكم في مكوناتها يحد من قدرة الدولة على تحقيق استقلالها التقني. وفي هذا السياق، أكدت الاستراتيجية الأردنية للتحول الرقمي والخطة التنفيذية (2026–2028) أهمية تنمية المهارات الرقمية المتخصصة لدى الموظفين الحكوميين، من خلال التدريب في مجالات الذكاء الاصطناعي وتحليل البيانات والأمن السيبراني وتطوير البرمجيات، بما يعزز الكفاءات الوطنية ويرفع جاهزية القطاع العام للتعامل مع متطلبات التحول الرقمي، ومن منظور القانون العام، يرتبط هذا العنصر بكفاءة الإدارة واستمرارية المرفق العام؛ إذ إن اعتماد الإدارة اعتمادا كليا على الخبرات الفنية الخارجية في تشغيل بنيتها التحتية الحيوية وصيانتها وتطويرها قد يؤدي إلى إضعاف استقلالها التقني والحد من قدرتها على ضمان استمرارية خدماتها الرقمية. [1]

المطلب الثاني: أثر الأسس التقنية في دعم وظائف الدولة الذكية وتحقيق الكفاءة الرقمية:

وبناء على ما تقدم من بيان المرتكزات التقنية للسيادة الرقمية، يتضح أن هذه المرتكزات لا تمثل جانباً فنياً منفصلاً عن البناء القانوني للدولة الذكية، وإنما تشكل البنية الوظيفية التي تستند إليها الدولة في ممارسة اختصاصاتها العامة وتحقيق أهدافها. فالبنية التحتية الرقمية توفر البيئة اللازمة لممارسة النشاط الإداري إلكترونياً، وحوكمة البيانات تتيح للإدارة الاستفادة من المعلومات في تطوير أدائها وتحسين عملية صنع القرار، في حين يسهم الأمن السيبراني في حماية الأنظمة والبيانات وضمان سلامة تشغيلها. كما تؤدي الحوسبة السحابية الخاضعة للحوكمة السيادية دوراً في تنظيم الاستضافة والتحكم في الموارد الرقمية، بينما تسهم الهوية الرقمية والتشغيل البيني في تحقيق التكامل بين الجهات الحكومية وتيسير تبادل البيانات وتقديم الخدمات بصورة مترابطة، وتضمن القدرات البشرية المتخصصة استدامة هذه المنظومة وقدرتها على التطور والتكيف مع المستجدات التقنية. [2]

ويظهر أثر هذه المرتكزات في دعم وظائف الدولة الذكية من خلال تمكين الإدارة العامة من تقديم خدمات أكثر كفاءة وانتظاماً، وتعزيز قدرتها على الاستناد إلى البيانات في اتخاذ القرارات، وتطوير وسائل الرقابة والمتابعة الإدارية، فضلاً عن حماية المرافق العامة والسجلات والبيانات الحكومية من المخاطر التقنية والاختراقات. وبذلك، فإن تكامل هذه المرتكزات لا يقتصر على تحسين الأداء الإداري، بل يسهم في تعزيز قدرة الدولة على إدارة مواردها الرقمية وممارسة اختصاصاتها بصورة مستقلة وآمنة وفعالة، بما يحقق سيادة رقمية فعلية تتجاوز مجرد امتلاك الأدوات والتقنيات إلى القدرة الحقيقية على التحكم فيها وتوجيه استخدامها، وعلى هذا الأساس، لا يمكن النظر إلى التقنية في الدولة الذكية باعتبارها مجرد وسيلة مادية لتنفيذ الوظائف العامة، بل أصبحت عنصراً بنيوياً في تنظيم النشاط الإداري وضمان فاعلية ممارسة الاختصاصات العامة في البيئة الرقمية. غير أن هذه الأهمية لا تنفصل عن ضرورة إخضاع استخدام التقنية للقواعد القانونية والضمانات المؤسسية التي تكفل المشروعية والأمن والمساءلة، حتى لا تتحول التبعية التقنية أو ضعف السيطرة على البيانات والأنظمة إلى عوامل تحد من استقلال الدولة في إدارة شؤونها الرقمية. [3]

المبحث الرابع: التطبيقات التشريعية المقارنة للسيادة الرقمية في الأنظمة المعاصرة

تقوم السيادة الرقمية في جوهرها القانوني على قدرة الدولة على إخضاع المجال الرقمي لقواعد قانونية وطنية نافذة بما يكفل لها السيطرة المشروعة على البيانات والبنى التحتية الرقمية والخدمات الإلكترونية، والفضاء المعلوماتي الذي تمارس من خلاله جزءاً متزايداً من وظائفها العامة. ومن ثم فإن الحديث عن السيادة الرقمية لا يستقيم في غياب إطار تشريعي منظم يحدد حدود السلطة العامة في البيئة الرقمية ويضبط العلاقة بين الإدارة العامة والأفراد والفاعلين التقنيين، ويوازن بين مقتضيات الأمن الرقمي ومتطلبات حماية الحقوق والحريات. فالتشريع في هذا المجال لا يؤدي دوراً تنظيمياً هامشياً بل ينهض بوظيفة تأسيسية لأنه يحول السيادة الرقمية من فكرة سياسية أو تقنية إلى مركز قانوني منظم تستند إليه الدولة في إدارة فضائها الرقمي وصيانة استقلالها التنظيمي وضبط بنيتها المعلوماتية على نحو مشروع وفعال. وهذا ما تؤكده الاتجاهات التشريعية الحديثة التي باتت تربط بوضوح بين السيادة الرقمية وبين التنظيم القانوني للبيانات والأنظمة والمنصات والخدمات الرقمية في إطار

[1] وزارة الاقتصاد الرقمي، الاستراتيجية الأردنية للتحول الرقمي والخطة التنفيذية (2026–2028)
[2] Christopher Tullis, Jordan Digital Public Infrastructure Diagnostic (Washington, DC: World Bank, 2024), p6-9
[3] Organisation for Economic Co-operation and Development. (2026). Digital government outlook 2026: From foundations to transformational impact. OECD Publishing. https://doi.org/10.1787/0496b2bc-en

يضمن خضوعها للشرعية القانونية ولأهداف المصلحة العامة. وعليه فقد تم تقسيم هذا المبحث الى مطلبين: يتضمن المطلب الأول التنظيم التشريعي للسيادة الرقمية في البيئة القانونية المعاصرة والمطلب الثاني التطبيقات المقارنة للسيادة الرقمية في كل من الولايات المتحدة الأمريكية والمملكة الأردنية الهاشمية. [1]

المطلب الأول: التنظيم التشريعي للسيادة الرقمية في البيئة القانونية المعاصرة:

وينبني هذا الإطار في المقام الأول على الأساس الدستوري والوظيفي لاختصاص الدولة في تنظيم المجال الرقمي. فالدولة بوصفها صاحبة الاختصاص الأصيل في حماية النظام العام وضان انتظام المرافق العامة وصون الحقوق والحريات تملك من حيث المبدأ سلطة التدخل التشريعي كلما أصبح الفضاء الرقمي مجالاً مؤثراً في ممارسة الوظائف العامة أو في استقرار المجتمع أو في سلامة البنية المؤسسية.

ولما كانت الدولة الذكية تمارس جزءاً متزايداً من اختصاصاتها من خلال البيانات والمنصات والخدمات الرقمية والهوية الرقمية والتكامل الإلكتروني بين المؤسسات فإن تنظيم هذا المجال لم يعد مجرد خيار تحديثي بل أصبح مظهراً من مظاهر ممارسة الدولة لاختصاصها السيادي في صورته المعاصرة. ومن هنا فإن إخضاع البيئة الرقمية لقواعد تشريعية خاصة يعد امتداداً طبيعياً لاختصاص الدولة في الضبط والتنظيم والحماية لا خروجاً على وظائفها التقليدية وإنما تطويراً لها بما يتلاءم مع التحول الرقمي المتسارع. [2]

ويتمثل العمود التشريعي الأول للسيادة الرقمية في التشريعات المنظمة للبيانات الشخصية وحوكمتها لأن البيانات أصبحت في البيئة الرقمية المعاصرة أصلاً قانونياً ووظيفياً لا غنى عنه لمباشرة الاختصاص العام. وفي هذا السياق جاء قانون حماية البيانات الشخصية الأردني رقم 24 لسنة 2023 ليضع إطاراً قانونياً متخصصاً ينظم جمع البيانات الشخصية ومعالجتها والإفصاح عنها ونقلها والرقابة عليها بما يكفل حماية الحقوق المرتبطة بها ويضع قيوداً قانونية على الجهات التي تتعامل معها. وتنبع أهمية هذا النوع من التشريعات من أنه لا يحمي خصوصية الأفراد فحسب بل يرسخ أيضاً أهم أوجه السيادة الرقمية وهو السيطرة القانونية على دورة البيانات داخل النطاق الوطني ومنع معالجتها أو تداولها أو استثمارها في غير الحدود المشروع. فالدولة التي تفتقر إلى إطار قانوني لحوكمة البيانات لا تستطيع في الواقع أن تدير فضاءها الرقمي إدارة سيادية كاملة لأن البيانات فيها تظل عرضة للتشتت وللاستغلال غير المنضبط أو للنفاد غير المشروع، بما يضعف الثقة العامة ويقوض أسس الإدارة الرقمية الرشيدة. وفي المقارنة المصرية جاء قانون حماية البيانات الشخصية رقم 151 لسنة 2020 في الاتجاه نفسه بما يؤكد أن التشريعات الحديثة باتت تعد حماية البيانات أحد الأعمدة الرئيسية لبناء السيادة الرقمية.

قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023 وقانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020 الجريدة الرسمية:

أما العمود التشريعي الثاني فيقوم على التشريعات الحماية والزجرية الخاصة بالبنية الرقمية والأنظمة والشبكات. ذلك أن السيادة الرقمية لا تكتمل إذا اقتصر المشرع على تنظيم التعامل المشروع مع البيانات، من غير أن يواجه الأفعال غير المشروعة التي تستهدف الأنظمة أو المواقع أو الشبكات أو الخدمات الرقمية، أو وسائل الاتصال الإلكتروني. ومن هنا تبرز أهمية قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023 بوصفه جزءاً أصيلاً من البناء التشريعي الحاكم للسيادة الرقمية لأنه يعبر عن وظيفة الدولة في حماية الفضاء الرقمي من صور الاعتداء التي قد تمس سلامة البيانات أو استقرار الخدمات أو الثقة العامة أو الأمن المعلوماتي للدولة والمجتمع. وهذا الاتجاه يجد نظيره المقارن في قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 الذي اتجه بدوره إلى تجريم طيف واسع من الأفعال الماسة بالأنظمة والبيانات والمواقع والخدمات الرقمية.

ويدل ذلك على أن البيئة القانونية المعاصرة أصبحت تميل إلى بناء سيادة رقمية على شقين متلازمين: شق تنظيمي يضبط الاستخدام المشروع وشق حمائي يردع الاعتداء والانتهاك.

---

[1] لشقار، محمد (2017). التنظيم القانوني للفضاء الرقمي، سؤال الماهية ومستقبل القانون، مجلة دفاتر القانونية، 3(2)، 9-48.

[2] قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023 وقانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020 الجريدة الرسمية.

قانون الجرائم الإلكترونية الأردني رقم (17) لسنة 2023 وقانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018:

ويتمثل العمود التشريعي الثالث في القواعد الناظمة للإدارة الرقمية والمعاملات والخدمات الإلكترونية فالسيادة الرقمية لا تقتصر على الحماية من الاعتداء أو على تنظيم البيانات بل تجلى أيضاً في قدرة الدولة على إضفاء الحجية القانونية على أعمالها الرقمية، وعلى تنظيم المرفق العام الإلكتروني وعلى ضمان مشروعية المعاملات والإجراءات التي تتم عبر الوسائط الرقمية، ولهذا يحتفظ قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2023 بأهمية تأسيسية في البناء التشريعي للسيادة الرقمية لأنه منح الاعتراف القانوني للمعاملات الإلكترونية وأرسى قواعد حجيتها وآثارها وممهد بذلك انتقال الإدارة العامة إلى مستويات أكثر تقدماً من العمل الرقمي.

ومن منظور القانون العام، تكتسب هذه القواعد أهمية خاصة لارتباطها المباشر بصحة الإجراء الإداري وسلامة القرار الرقمي وحجية المستند والسجل الإلكتروني والخدمات المقدمة عبر الوسائل الرقمية. وبذلك تضمن ألا يكون التحول نحو الدولة الذكية مجرد تحول تقني، بل تحولا قائما على قواعد قانونية تحقق مبدأ المشروعية وتكفل استقرار المراكز القانونية الناشئة عنه. [1]

ويقوم العمود التشريعي الرابع على التشريعات والسياسات المعيارية المرتبطة بالبنية المعلوماتية العامة، والانفتاح المنظم للبيانات، والتشغيل البيني واختيار الحلول التقنية القابلة للسيطرة الوطنية وهذا البعد يظهر بجلاء في التجربة الفرنسية ولا سيما في قانون الجمهورية الرقمية لعام 2016 الذي لم يقتصر على حماية الحقوق الرقمية أو الوصول إلى البيانات بل عبر عن توجه تشريعي يجعل من إدارة البنية الرقمية العامة وتشجيع الصيغ المفتوحة وتسهيل الوصول المنظم إلى البيانات العامة جزءاً من سياسة قانونية تهدف إلى تقوية استقلال الدولة ومؤسساتها في المجال الرقمي. وقيمة هذا البعد المقارن تكمن في أنه يكشف أن السيادة الرقمية لا تبنى فقط عبر نصوص الحظر والعقاب بل أيضاً عبر النصوص التي توجه اختيارات الإدارة العامة في بناء نظمها الرقمية وتتقلل من الارتهان للحلول المغلقة أو البيئات التقنية التي تضعف القدرة الوطنية على التحكم والتطوير. [2]

المطلب الثاني: التطبيقات المقارنة للسيادة الرقمية في كل من الولايات المتحدة الأمريكية والمملكة الأردنية الهاشمية:

تُعد السيادة الرقمية مفهوماً متعدد الأوجه يعكس قدرة الدولة على التحكم في بنيتها الرقمية وتدفقات بياناتها وأصولها التكنولوجية وأطر سياساتها يوضح هذا التحليل المقارن أن السيادة الرقمية ترتبط ارتباطاً وثيقاً بالقوة الاقتصادية والقدرة التكنولوجية والنضج المؤسسي ويُفهم هذا المفاهيم على نحو أفضل باعتباره طيفاً متدرجاً لا حالة ثنائية. [3]

تجسد الولايات المتحدة نموذجاً شاملاً وناضجاً للسيادة الرقمية يتميز بالريادة التكنولوجية وقدرات الأمن السيبراني المتكاملة وآليات حوكمة البيانات القوية وبيئة اقتصادية وابتكارية مؤثرة عالمياً.

يُظهر نهجها التفاعل بين التطور المؤسسي والاستقلال الاستراتيجي ما يسمح بالسيطرة المحلية والتأثير الرقمي الدولي.

وتتبنى الولايات المتحدة نهجاً لا ممركزاً وموجهاً نحو السوق للسيادة الرقمية تتوزع الحوكمة على المستويات الفيدرالية والولائية والمحلية مع مشاركة قوية من القطاع الخاص.

[1] المواد (6، 15، 16، 17) من قانون المعاملات الإلكترونية رقم (15) لسنة 2023
[2] قانون الجمهورية الرقمية الفرنسي لعام 2016 (Loi pour une République numérique)
[3] لشقار، محمد. التنظيم القانوني للفضاء الرقمي، سؤال الماهية ومستقبل القانون، مرجع سابق، 9-48.



قانون حماية البيانات الفيدرالي والتشريعات التقنية الأمريكية (US Federal Cybersecurity and Data Governance Frameworks).

في المقابل يمثل الأردن نموذجاً ناشئاً للسيادة الرقمية تشكل من خلال التطور المؤسسي التدريجي والاعتماد على التقنيات المستوردة والتركيز على بناء قدرات أساسية في الأمن السيبراني وحوكمة البيانات والبنية التحتية الرقمية.

يُبرز النهج الأردني القيود التي تواجهها الاقتصاديات النامية مسلطاً الضوء على أهمية الاستثمار الاستراتيجي في الابتكار المحلي ورأس المال البشرى وأطر السياسات لتعزيز الاستقلالية الرقمية تدريجياً.

International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
Vol. (5), No. (11)
November 2026
الإصدار (5)، العدد (11)



ومن خلال هذه المراجع التي تُبرز الأبعاد المقارنة في الجدول أدناه الركائز الأساسية للسيادة الرقمية التي نوقشت في هذا التحليل. تُوضح الأطر المؤسسية والقانونية هياكل الحوكمة الأساسية التي تُمكّن من الإشراف الاستراتيجي وإنفاذ السياسات. تُسلط قدرات الأمن السيبراني الضوء على التوازن بين القدرات الدفاعية والهجومية اللازمة لحماية الأصول الرقمية الوطنية. تُعكس حوكمة البيانات آليات التحكم في تدفق المعلومات وتخزينها واستخدامها وتنظيمها. تُجسد القوة الاقتصادية دور النظم

البيئية الرقمية والابتكارية في تمكين الريادة التكنولوجية والتأثير في السوق. وأخيرًا، يُؤكد الاستقلال التكنولوجي على مدى قدرة الدولة على تطوير ونشر وصيانة التقنيات الرقمية الحيوية بشكل مستقل. تُقدم هذه الأبعاد مجتمعةً رؤيةً دقيقةً لكيفية احتلال الولايات المتحدة والأردن مواقع متميزة على طيف السيادة الرقمية، مما يُتيح فهمًا أعمق للتحديات والاستراتيجيات المرتبطة بتعزيز الاستقلال الرقمي الوطني.

البعد	الأردن	الولايات المتحدة
الإطار المؤسسي والقانوني	أطر تنظيمية ناشئة مع تطوير مؤسسي تدريجي	هياكل حوكمة ناضجة ومعقدة ذات تأثير عالمي كبير
قدرات الأمن السيبراني	التركيز على التدابير الدفاعية وبناء القدرات	قدرات سيبرانية هجومية ودفاعية متقدمة متكاملة عبر القطاعين الحكومي والخاص
حوكمة البيانات	تطوير قوانين حماية البيانات والسياسات الرقمية	السيطرة على تدفقات البيانات العالمية عبر شركات التكنولوجيا الكبرى؛ تنظيم مرن قائم على السوق
القوة الاقتصادية	اقتصاد رقمي ناشئ بموارد محدودة	اقتصاد عالمي رائد مع أنظمة بيئية قوية للابتكار وتأثير سوقي كبير
الاستقلالية التكنولوجية	الاعتماد على التقنيات المستوردة	مستوى عالٍ من الاكتفاء الذاتي التكنولوجي وقيادة الابتكار

وبمطالعة الجدول أعلاه يُبرز عدة اختلافات جوهرية بين الولايات المتحدة والأردن في نهجهما تجاه السيادة الرقمية. فبينما تُظهر الولايات المتحدة نموذجًا متكاملًا يستفيد من النفوذ العالمي، وريادة القطاع الخاص، والاستقلالية التكنولوجية لتعزيز موقعها الاستراتيجي، يتسم نموذج الأردن بالتطوير التدريجي الحذر الذي يهدف إلى بناء قدرات أساسية. والجدير بالذكر أن قدرة الولايات المتحدة على التحكم في تدفقات البيانات العالمية والحفاظ على مستوى عالٍ من الاكتفاء الذاتي التكنولوجي تتناقض بشكل حاد مع اعتماد الأردن على التقنيات المستوردة والأدوات التنظيمية الناشئة [1].

وبالمثل، تعكس الفجوة في نضج الأمن السيبراني اختلاف الأولويات: فالولايات المتحدة تجمع بين الاستراتيجيات الهجومية والدفاعية عبر مختلف القطاعات [2]، بينما يركز الأردن على بناء القدرات الدفاعية تُسلط هذه الفروقات الضوء على أن السيادة الرقمية ليست مسألة سياسية فحسب، بل هي أيضًا مسألة قدرة هيكلية وتشغيلية، مما يكشف عن المسارات المتباينة التي تتبعها الدول تبعًا لمواردها، ونضجها المؤسسي، وطموحاتها الاستراتيجية.

لهذه الفروقات آثار بالغة الأهمية على استراتيجية السيادة الرقمية للأردن. لتحقيق تقدم ملموس نحو مزيد من الاستقلالية، يتعين على الأردن إعطاء الأولوية للاستثمار في التطوير التكنولوجي المحلي، بما في ذلك مراكز البيانات المحلية، والبنية التحتية للأمن السيبراني، وبيئات الابتكار. وسيسهم تعزيز الأطر التنظيمية وموائمتها مع المعايير الدولية في جذب الشراكات الأجنبية مع الحفاظ على المصالح الوطنية. إضافةً إلى ذلك، يُعد بناء رأس المال البشري من خلال التعليم والتدريب المتخصص ونقل المعرفة أمراً بالغ الأهمية للحد من الاعتماد على التقنيات المستوردة. ومن خلال تبني نهج تدريجي واستراتيجي يوازن بين بناء القدرات والإصلاحات السياسية التدريجية، يستطيع الأردن تعزيز مرونته، وتوسيع نفوذه تدريجياً في المجال الرقمي، ورسم مسار مستدام نحو سيادة رقمية شاملة.

الخاتمة

يخلص هذا البحث الموسوم بـ «الأسس التشريعية والتقنية لترسيخ السيادة الرقمية في الدولة الذكية» إلى أن السيادة الرقمية لم تعد مجرد مفهومٍ طارئ أو مظهر ترفي ملحق بمسارات التحول الرقمي بل غدت في الدولة المعاصرة مقوماً جوهرياً وركناً مكتملاً لمباشرة الاختصاصات العامة وإدارة الشأن الوطني. فالدولة الذكية بما تختزنه من بنى بيانات حيوية ومنصات خدمية وشبكات مترابطة لم تعد تقاس كفاءتها الإدارية والتنفيذية بمدى السرعة واليسر في تقديم الخدمات فحسب بل أصبحت تُقاس بالقدر ذاته بمدى اقتدارها المؤسسي والقانوني على إخضاع فضاءها الرقمي لسيادة القانون وصون استقلال قرارها السيادي

[1] Glybovets, A., & Mohammad, A. (2017). E-government versus smart government: Jordan versus the United States. EUREKA: Social and Humanities.

[2] Pierucci, F. (2025). Sovereignty in the digital era: Rethinking territoriality and governance in cyberspace. Digital Society, 4(1), 27. https://doi.org/10.1007/s44206-025-00189-4

وتحصين أمن بياناتها ومرافقها من صور التبعية التقنية أو الارتهان الخارجي أو المخاطر السيبرانية المحدقة وقد أثبت البحث عبر استقراء التطور التشريعي في المملكة الأردنية الهاشمية ولا سيما صدور قانون حماية البيانات الشخصية رقم 24 لسنة 2023 وقانون الجرائم الإلكترونية رقم 17 لسنة 2023 أن المشرّع اتجه بوضوح نحو هندسة إطار تنظيمي متخصص ومستقل يناسب الطبيعة المركبة للمجال الرقمي متجاوزاً بذلك حالة التشتت التنظيمي السابقة وهو ما يتلاقى بوضوح مع اتجاهات التجارب التشريعية المقارنة كالتجربتين الفرنسية والمصرية اللتين تؤكدان أن التأسيس للسيادة الرقمية يتطلب بيئة قانونية تكاملية تدمج بين الحوكمة والضبط الزجري وتأمين البنية الرقمية العامة.

وقد انتهى البحث في أبعاده المفاهيمية والتأصيلية إلى أن السيادة الرقمية تتجاوز الاختزال النظري الذي يحصرها في حدود الأمن السيبراني أو مجرد حماية الخصوصية الرقمية إذ تتمثل روح هذه السيادة في قدرة الدولة قانوناً وواقعاً على بسط سلطانها المشروع على الفضاء المعلوماتي الوطني والتوجيه الذاتي للبيانات والمنصات والخوارزميات التي تُبنى عليها القرارات الإدارية والخدمية. ومن هذا المنطلق تتكشف العلاقة بين السيادة الرقمية والدولة الذكية بوصفها علاقة وجودية وبنيوية فلا يمكن تصور دولة ذكية تمتلك المشروعية وتضمن الاستدامة دون إرساء سيادة رقمية تحمي مكوناتها التقنية والتنظيمية من الانكشاف. كما كشف التحليل أن دواعي التدخل التشريعي لم تعد مجرد معالجة لآثار التطور التقني بل أصبحت استجابة استراتيجية تهدف إلى تنظيم الممارسة القانونية بين الإدارة والأفراد والفاعلين التكنولوجيين وإعادة صياغة مفاهيم المشروعية واستمرارية المرفق العام والضبط الإداري في البيئة الرقمية الذكية.

كما يتأكد عبر نتائج الدراسة أن السيادة الرقمية لا يمكن أن تبلغ مداها المأمول استناداً إلى النصوص التشريعية المجردة وحدها ما لم تكن مسنودة بـ سيادة تقنية واقعية تتمثل في امتلاك قدرات وطنية مستقلة على إدارة البنى التحتية الحرجة وتأمين مراكز البيانات وتنفيذ حوكمة سيادية للأنظمة السحابية وضمان التشغيل البيني الآمن وتحصين الهوية الرقمية. فالتقنية في مفهوم الدولة الذكية ليست أداة تنفيذية محايدة بل هي وسيلة تمكين سيادي وركن وظيفي يرتبط بشرعية القرار الإداري وحجية التصرفات القانونية. وتُبرز استقراءات الاستراتيجيات الأردنية للتحول الرقمي والأمن السيبراني إدراكاً رسمياً متقدماً لهذه الحقيقة مما يرسخ النتيجة المحورية التي توصل إليها البحث ومفادها أن السيادة الرقمية الناجعة هي ثمرة للتلاحم العضوي والتكامل الوظيفي بين النص التشريعي المحكم والتمكين التقني المستقل بحيث لا يستغني أحدهما عن الآخر.

وتأسيساً على هذا التأصيل الشامل يُجمل البحث نتائجه في نموذج متكامل يقوم على أربعة مرتكزات متساندة لترسيخ السيادة الرقمية في الدولة الذكية:

- أولاً: إطار تشريعي وحوكمي متخصص يضبط دورة حياة البيانات ويحدد الالتزامات والأحكام الخاصة بالمعاملات والخدمات الرقمية.
- ثانياً: منظومة حماية قانونية وزجرية متطورة تردع صور الاعتداء السايكولوجي والسيبراني على البنى التحتية والأنظمة الوطنية.
- ثالثاً: بنيوية تقنية سيادية محصنة تخضع للرقابة المؤسسية الوطنية وتضمن التشغيل البيني والمرونة ومواجهة المخاطر التقنية.
- رابعاً: مقاربة فقهية وقانونية معاصرة تعيد قراءة أركان القانون الإداري العام وقواعد المشروعية وضمانات الحقوق وحريات الأفراد في ضوء التطبيقات الرقمية الذكية. وبناءً عليه فإن معيار النضج والدقة في الدولة الذكية لم يعد يتوقف عند حدود الابتكار والسرعة التقنية بل بمدى تحويل هذا الابتكار إلى سيادة رقمية رشيدة ومستدامة توازن بدقة واقتدار بين مقتضيات الأمن والتطوير وتحمي استقلال الدولة وتصون حقوق الأفراد وثقتهم بالبيئة الرقمية الوطنية.

النتائج

1. خلص البحث إلى أن السيادة الرقمية لم تعد مفهوماً طارئاً أو مظهر ترفي ملحق بمسارات التحول الرقمي بل غدت في الدولة المعاصرة مقوماً جوهرياً وركناً مكتملاً لمباشرة الاختصاصات العامة وإدارة الشأن الوطني.
2. أثبت البحث أن الدولة الذكية بما تختزنه من بنى بيانات حيوية ومنصات خدمية وشبكات مترابطة لم تعد تقاس كفاءتها الإدارية والتنفيذية بمدى السرعة واليسر في تقديم الخدمات فحسب بل أصبحت تُقاس بالقدر ذاته بمدى اقتدارها المؤسسي

والقانوني على إخضاع فضاءها الرقمي لسيادة القانون وصون استقلال قرارها السيادي وتحصين أمن بياناتها ومرافقها من صور التبعية التقنية والمخاطر السيبرانية المحدقة.

3. أظهر استقراء التطور التشريعي في المملكة الأردنية الهاشمية ولا سيما صدور قانون حماية البيانات الشخصية رقم 24 لسنة 2023 وقانون الجرائم الإلكترونية رقم 17 لسنة 2023 أن المشرّع اتجه بوضوح نحو هندسة إطار تنظيمي متخصص ومستقل يناسب الطبيعة المركبة للمجال الرقمي متجاوزاً بذلك حالة التشتت التنظيمي السابقة وهو ما يتلاقى بوضوح مع اتجاهات التجارب التشريعية المقارنة كالتجربتين الفرنسية والمصرية اللتين تؤكدان أن التأسيس للسيادة الرقمية يتطلب بيئة قانونية تكاملية تدمج بين الحوكمة والضبط الزجري وتأمين البنية الرقمية العامة.

4. انتهى البحث في أبعاده المفاهيمية والتأصيلية إلى أن السيادة الرقمية تتجاوز الاختزال النظري الذي يحصرها في حدود الأمن السيبراني أو مجرد حماية الخصوصية الرقمية إذ تتمثل روح هذه السيادة في قدرة الدولة قانوناً وواقعاً على بسط سلطانها المشروع على الفضاء المعلوماتي الوطني والتوجيه الذاتي للبيانات والمنصات والخوارزميات التي تُبنى عليها القرارات الإدارية والخدمية.

5. كشف التحليل أن دواعي التدخل التشريعي لم تعد مجرد معالجة لآثار التطور التقني بل أصبحت استجابة استراتيجية تهدف إلى تنظيم الممارسة القانونية بين الإدارة والأفراد والفاعلين التكنولوجيين وإعادة صياغة مفاهيم المشروعية واستمرارية المرفق العام والضبط الإداري في البيئة الرقمية الذكية.

6. أكدت الدراسة أن السيادة الرقمية لا يمكن أن تبلغ مداها المأمول استناداً إلى النصوص التشريعية المجردة وحدها ما لم تكن مسنودة بـ سيادة تقنية واقعية تتمثل في امتلاك قدرات وطنية مستقلة على إدارة البنى التحتية الحرجة وتأمين مراكز البيانات وتنفيذ حوكمة سيادية للأنظمة السحابية وضمان التشغيل البيني الآمن وتحصين الهوية الرقمية.

7. بيّن البحث أن التقنية في مفهوم الدولة الذكية ليست أداة تنفيذية محايدة بل هي وسيلة تمكين سيادي وركن وظيفي يرتبط بشرعية القرار الإداري وحجية التصرفات القانونية.

8. أظهرت استقراءات الاستراتيجيات الأردنية للتحول الرقمي والأمن السيبراني إدراكاً رسمياً متقدماً لهذه الحقيقة مما يرسخ النتيجة المحورية التي توصل إليها البحث ومفادها أن السيادة الرقمية الناجعة هي ثمرة للتلاحم العضوي والتكامل الوظيفي بين النص التشريعي المحكم والتمكين التقني المستقل بحيث لا يستغني أحدهما عن الآخر.

9. انتهت الدراسة إلى نموذج متكامل يقوم على أربعة مرتكزات متساندة تتمثل في إطار تشريعي وحوكمي متخصص يضبط دورة حياة البيانات ومنظومة حماية قانونية وزجرية متطورة تردع صور الاعتداء وبنيوية تقنية سيادية محصنة تخضع للرقابة المؤسسية ومقاربة فقهية وقانونية معاصرة تعيد قراءة أركان القانون الإداري وقواعد المشروعية في ضوء التطبيقات الرقمية الذكية.

التوصيات

1. ضرورة الشروع الفوري في صياغة إطار تشريعي وطني شامل ومتكامل يدمج قواعد حوكمة البيانات والذكاء الاصطناعي والحوسبة السحابية السيادية في مدونة قانونية موحدة تمنع التداخل التشريعي وتوفر مظلة أمان قانونية صلبة لجميع أنشطة الدولة الذكية.

2. العمل على تطوير البنية التحتية التقنية الوطنية من خلال إنشاء مراكز بيانات حكومية سيادية ومملوكة بالكامل للدولة تخضع للولاية القضائية الوطنية حصراً وتتحرر تدريجياً من الارتهان للشركات التقنية الأجنبية الكبرى عابرة القارات بما يضمن استقلال القرار الإداري وحماية الأمن القومي المعلوماتي.

3. تحديث منظومة التشريعات الجزائية والإدارية المرتبطة بالأمن السيبراني لتكون قادرة على استيعاب الجرائم الرقمية المستحدثة وهجمات الاختراق المتقدمة مع إقرار آليات ردع قوية وصارمة تكفل حماية البنى التحتية الحرجة ومفاصل المرافق العامة الرقمية من أي تعطيل محتمل.

4. تأسيس هيئة عليا مستقلة لحوكمة الرقمية والسيادة السيبرانية تتولى التنسيق المؤسسي بين مختلف القطاعات الحكومية والخاصة وتراقب الالتزام بمعايير الأمن الرقمي والتشغيل البيني الآمن وتوجيه الاستثمارات التكنولوجية نحو الابتكار

المحلي وبناء القدرات البشرية الوطنية المتخصصة.

5. تعزيز التعاون الدولي والإقليمي المتبادل مع الدول الشقيقة والصديقة وتبادل الخبرات التشريعية والتقنية بما يحمي المصالح العليا للدولة ويدعم مكانتها في فضاء التجارة والخدمات الرقمية العالمية دون المساس بالاستقلال الوطني.
6. إدماج مفاهيم السيادة الرقمية وأمن المعلومات ضمن المناهج الأكاديمية والتدريبية لكوادر الإدارة العامة والقضائية لرفع مستوى الوعي القانوني والتقني وإعداد جيل قيادي إداري يمتلك القدرة الفائقة على التعامل مع متطلبات الدولة الذكية بكفاءة واقتدار.
7. مراجعة وتطوير أطر المسؤولية الإدارية والمدنية في القانون الإداري الأردني بما يتلاءم مع طبيعة القرارات الخوارزمية الذكية وتأمين ضمانات فعالة للأفراد في مواجهة التعسف التقني أو انتهاك الخصوصية الرقمية لضمان تحقيق التوازن الدقيق بين كفاءة الإدارة العامة وحماية الحقوق والحريات الأساسية في العصر الرقمي.

المراجع

1. الاستراتيجية الوطنية للذكاء الاصطناعي (2019). المجلس الوطني للذكاء الاصطناعي، ص 14.
2. الدهشان، يحيى (2023). الحماية الجنائية للبيانات في ظل التحول الرقمي، مجلة الدراسات القانونية والاقتصادية، 9(3)، 1500-1551.
3. الذكاء الاصطناعي في مصر: الأطر التنظيمية القائمة ومتطلبات تحقيق المستهدفات (2024). مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء، ص 15.
4. دليل القواعد والتعليمات الخاصة بالمعالجة الضريبية لصناع المحتوى (2022). الإصدار الأول، مصلحة الضريبة المصرية، ص 7-8.
5. سعيدي، رغدة (2024). الدفع الإلكتروني: الطريق إلى الاقتصاد غير النقدي في مصر. مجلة كلية السياسة والاقتصاد، جامعة بني سويف، ص 342.
6. محمد، سامي الطيب إدريس (2024). دواعي وآثار خرق السيادة في ظل المتغيرات الدولية. مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة السادات، 10(2)، ص 1408-1413.
7. مرعي، إيمان (2024). المنصات الرقمية: الدور وحدود التأثير. مركز الأهرام للدراسات السياسية والاستراتيجية.
8. الزهراني، ايناس، (2024) التحول الرقمي وتأثيره على الإدارة العامة. مركز البحث وتطوير الموارد البشرية (رماح)، (12)، 9-21
9. العبدلية، رقية بنت خلفان، والحراصي، نبهان بن حارث بن ناصر، والكندي، سالم سعيد علي (2024). انعكاسات تطبيق حوكمة البيانات في المؤسسات الحكومية العمانية. المجلة العلمية للمكتبات والوثائق والمعلومات، المجلد 6، العدد 19، ص 6–22
10. كامل، أحمد، (2024). البنى التحتية لتكنولوجيا المعلومات في العصر الرقمي، المجلة الدولية للعلوم الإدارية والاقتصادية والمالية، 3(8)، 1-14
11. لشقار، محمد (2017). التنظيم القانوني للفضاء الرقمي، سؤال الماهية ومستقبل القانون، مجلة دفاتر القانونية، 3(2)، 9-48.
12. المناصير، صهيب، (2023)، مسؤولية الإدارة العامة عن إدارة مرافقها الإلكترونية، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، 4(1)، ص 9، 22
13. وزارة الاقتصاد الرقمي والريادة الأردنية الاستراتيجية الأردنية للتحول الرقمي والخطة التنفيذية (2026–2028)
14. وزارة الاقتصاد الرقمي والريادة الأردنية، الاستراتيجية الوطنية للتحول الرقمي والخطة التنفيذية (2021–2025)،

المملكة الأردنية الهاشمية، 2021، ص 10–14، وص 34–35

15. وهدان، نيفين، (2026)، الحوكمة الذكية في الإدارة العامة في عصر الذكاء الاصطناعي: نموذج وساطة وتعديل في إطار إعادة هندسة السياسات العامة دراسة تطبيقية على مصر مع تحليل مقارن للنماذج الدولية، المجلة الأكاديمية للعلوم الاجتماعية، 26(4)، ص1-53

القوانين والتقارير العربية الواردة في البحث:

1. قانون الأمن السيبراني الأردني رقم (16) لسنة 2019.
2. قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023.
3. قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015.
4. قانون حماية البيانات الشخصية الأردني رقم 24 لسنة 2023.
5. قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020.
6. قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018.
7. قانون الجمهورية الرقمية الفرنسي لعام 2016 (Loi pour une République numérique).

أولاً: المراجع الإنجليزية:

1. Boul, M. (2018). Réflexions sur la notion de donnée publique. Revue française d'administration publique, 167(3), 471–478.
2. Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305–2322. https://doi.org/10.1177/1461444819865984
3. Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. Digital Society, 3(3), 59.
4. Glybovets, A., & Mohammad, A. (2017). E-government versus smart government: Jordan versus the United States. EUREKA: Social and Humanities.
5. Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. Government Information Quarterly, 37(3), Article 101493. https://doi.org/10.1016/j.giq.2020.101493
6. Misra, S., Barik, K., & Kvalvik, P. (2025). Trust in Digital Sovereignty: A Review of Security, Privacy, and Governance Challenges. Public Organization Review, 1-23. https://doi.org/10.1007/s11115-025-00968-0
7. European Union Agency for Network and Information Security (ENISA), Security & Resilience in Governmental Clouds: Making an Informed Decision (Heraklion: ENISA, January 2011), pp. 6–8, 40–41.
8. Boul, M. (2018). Réflexions sur la notion de donnée publique. Revue française d'administration publique, 167(3), 471–478. https://doi.org/10.3917/rfap.167.0471 Cluzel-Métayer, L. (2018). La construction d'un service public de la donnée. Revue française d'administration publique, 167(3), 491–500. https://doi.org/10.3917/rfap.167.0491

9. Christopher Tullis, Jordan Digital Public Infrastructure Diagnostic (Washington, DC: World Bank, 2024), p6-9
10. Cluzel-Métayer, L. (2018). La construction d'un service public de la donnée. Revue française d'administration publique, 167(3), 491–500. https://doi.org/10.3917/rfap.167.0491
11. Donnelly, S., Rios Camacho, E., & Heidebrecht, S. (2024). Digital sovereignty as control. https://doi.org/10.1080/13501763.2023.2295520
12. Fratini, S., et al. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. Digital Society, 3(3), 59. https://doi.org/10.1007/s44206-024-00146
13. Glybovets, A., & Mohammad, A. (2017). E-government versus smart government: Jordan versus the United States. EUREKA: Social and Humanities.
14. Glybovets, A., & Mohammad, A. (2017). E-government versus smart government: Jordan versus the United States. EUREKA: Social and Humanities.
15. Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. Government Information Quarterly, 37(3), Article 101493. https://doi.org/10.1016/j.giq.2020.101493
16. Misra, S., Barik, K., & Kvalvik, P. (2025). Trust in Digital Sovereignty: A Review of Security, Privacy, and Governance Challenges. Public Organization Review, 1-23. https://doi.org/10.1007/s11115-025-00968-0
17. Organisation for Economic Co-operation and Development. (2026). Digital government outlook 2026: From foundations to transformational impact. OECD Publishing. https://doi.org/10.1787/0496b2bc-en
18. Pierucci, F. (2025). Sovereignty in the digital era: Rethinking territoriality and governance in cyberspace. Digital Society, 4(1), 27. https://doi.org/10.1007/s44206-025-00189-4
19. Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532