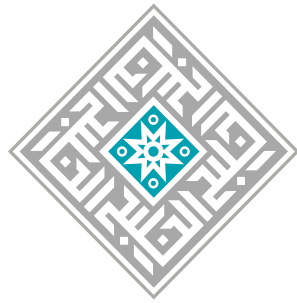




السيادة الرقمية على البيانات والبنى السحابية الوطنية: حدود الولاية القانونية والقضائية العابرة للحدود نموذجاً لـ CLOUD Act و Schrems II

د. فاطمة علي فهد الحويل
زميلة باحثة – أستاذة القانون الدولي الخاص
مركز الكويت للبحوث والدراسات





الآراء الواردة في هذا المقال تعبر عن رأي الكاتب وحده، ولا تعكس بالضرورة سياسة أو توجه مركز الخليج للأبحاث

السيادة الرقمية، سيادة البيانات، الحوسبة السحابية السيادية، التوطين المادي للبيانات، التوطين القضائي والتنفيذي، الاختصاص القضائي، الاختصاص القانوني، القانون الدولي الخاص، مفاتيح التشفير، **Act CLOUD**، **II Schrems**.

ملخص تنفيذي

تتجه دولة الكويت ودول مجلس التعاون الخليجي إلى توسيع الاعتماد على الحوسبة السحابية والذكاء الاصطناعي عبر شراكات متنامية مع كبار مزودي الخدمات السحابية العالميين. ويحقق توطين مراكز البيانات والمناطق السحابية داخل الدولة مزايا تتصل بسرعة الخدمات واستمرارية الأعمال والأمن والامتثال التنظيمي. **إلا أن التوطين المادي لا يكفي بذاته لإثبات تحقق السيادة الرقمية؛** إذ قد تظل السيطرة القانونية أو التقنية أو التشغيلية على البيانات، أو مفاتيح تشفيرها، أو طبقات إدارتها وتحكمها، مرتبطة بكيان أجنبي يمكن أن يمتد إليه اختصاص قضائي أجنبي.

وتنطلق الورقة من فرضية مؤداها أن السؤال السيادي لا ينبغي أن ينحصر في: أين توجد البيانات؟ وإنما يمتد إلى: من يملك القدرة القانونية والتقنية والتشغيلية على الوصول إليها أو التحكم فيها أو الإفصاح عنها؟ وبذلك تنتقل دراسة السيادة الرقمية من معيار الموقع المادي إلى معيار السيطرة الفعلية ومصادر السلطة التي تحكمها.

وتختبر الورقة هذه الفرضية في ضوء الإطار القانوني الكويتي وقانون Act CLOUD الأمريكي، مع تحليل قضية Ireland Microsoft بوصفها نموذجًا كاشفًا للتوتر بين موقع البيانات والاختصاص الواقع على الكيان المسيطر عليها. كما تُستخدم قضية II Schrems كمقارنة محدودة لإظهار أن الحماية التعاقدية لا تكفي بذاتها لمنع الآثار القانونية المترتبة على صلاحيات سلطة عامة أجنبية.

وتقترح الورقة بناءً على ذلك معيارًا عمليًا قابلاً للتدقيق في عقود الحوسبة السحابية، يفحص هوية الكيان الحائز للبيانات، ومراكز الإدارة والتحكم، وحياسة مفاتيح التشفير، وحدود صلاحيات مقدم الخدمة، وآليات التعامل مع طلبات الإفصاح الأجنبية، وقابلية نقل البيانات والأنظمة. كما تطرح نموذجًا مرحليًا يبدأ بإحكام السيطرة على مفاتيح التشفير وإعادة هندسة العقود والضوابط التشغيلية، ويتدرج نحو بيئة سحابية ذات سيطرة وطنية مشددة للأحمال والبيانات الأكثر حساسية.



“

**التوطين المادي لا يكفي
بذاته لإثبات تحقق السيادة
الرقمية**

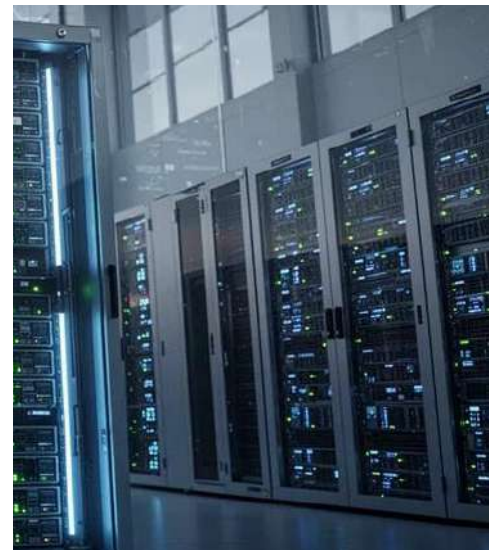
أصبحت السيادة في البيئة الرقمية الحديثة لا تقاس فقط بقدرة الدولة على حماية إقليمها وبنيتها التحتية، وإنما كذلك بقدرتها على تحديد نطاق السلطة التي تحكم أصولها الرقمية، ومن يملك الوصول إليها، وتحت أي اختصاص يمكن إلزام الكيانات التي تديرها أو تتحكم في تشغيلها. وقد أوجد الانتقال إلى الحوسبة السحابية والذكاء الاصطناعي طبقات متعددة للملكية والحيازة والإدارة والتحكم، بحيث لم يعد الموقع المادي للبنية التقنية كافيًا وحده لتحديد مركز السيطرة على البيانات.

ومن هنا تبرز إشكالية هذه الورقة : كيف يمكن لدولة أن تحقق توطيئًا ماديًا لبنيتها السحابية، بينما تظل بعض عناصر السيطرة على البيانات أو تشغيلها أو مفاتيحها مرتبطة بكيانات قد تخضع لاختصاص قضائي وقانوني أجنبي؟ وهل يكفي العقد أو اختيار القانون أو موقع مركز البيانات داخل الإقليم لاحتواء الآثار المترتبة على ذلك الاختصاص؟

وتكتسب هذه الإشكالية بعدًا عمليًا مع توسع دولة الكويت في استخدام البنى السحابية العالمية ضمن مسار التحول الرقمي الوطني؛ ومن ثم، تتعامل الورقة مع السيادة الرقمية باعتبارها مسألة قانونية وتشغيلية تتصل بتوزيع السيطرة على البيانات بين الدولة ومقدم الخدمة والكيانات المرتبطة به.

وعلى هذا الأساس، تبحث الورقة حدود التوطن المادي للبيانات وعلاقته بالاختصاص القانوني والقضائي الأجنبي وقابلية آثاره للنفذ عبر الحدود، ثم تحلل نموذج **Act CLOUD** وقضية **Ireland Microsoft**، قبل بحث حدود الحماية التعاقدية والتشفير والتحكم، وصولًا إلى إطار عملي لقياس مستوى السيطرة السيادية على البيئة السحابية الوطنية.

“ لم يعد الموقع المادي للبنية التقنية كافيًا وحده لتحديد مركز السيطرة على البيانات ”



السياق القانوني والاستراتيجي للتحول السحابي والسيادة الرقمية في دولة الكويت

تتجسد هذه الإشكالية في دولة الكويت مع توسع الاعتماد المؤسسي على البنية السحابية العالمية ضمن مسار التحول الرقمي الوطني. فقد أبرمت الدولة شراكة استراتيجية مع **Microsoft**¹ في مارس ٢٠٢٥، أعقبها انتقال أول جهة حكومية إلى **Azure Microsoft** في أغسطس ٢٠٢٥ باستخدام **Azure VMware Solution**. كما أقامت حكومة الكويت تحالفًا استراتيجيًا متعدد السنوات مع **Google Cloud**²، فيما سبق ذلك تعاون مؤسسي مع **Am-Services Web azon** في مجال حوكمة الحوسبة السحابية.^٣

ولا تعني هذه التطورات -بذاتها- خضوع البيانات الحكومية لاختصاص أجنبي؛ فذلك يتوقف على طبيعة الكيان المتعاقد، وموقع الحيازة والسيطرة، والبنية التشغيلية للخدمة، والقواعد القانونية التي تحكم مقدم الخدمة والكيانات المرتبطة به. غير أنها تكشف انتقال البيئة السحابية من بنية تقنية مساندة إلى جزء من البنية التشغيلية التي تُدار من خلالها أصول رقمية وطنية.

ولا تنفصل هذه الإشكالية عن النقاش الأوسع في دول الخليج حول السيادة على البيانات والاستقلال الاستراتيجي في البيئة الرقمية؛ إذ أصبحت السيطرة على البيانات والبنية الرقمية جزءًا من النقاش المتعلق بقدرة الدول على حماية أصولها الرقمية وتقليل مواطن الارتهاق الخارجي. وتأتي الحالة الكويتية ضمن هذا السياق الإقليمي، مع خصوصيتها القانونية والتنظيمية التي تقتضي الانتقال من النقاش العام حول السيادة الرقمية إلى تحديد عناصر السيطرة التي يمكن قياسها وتدقيقها داخل العلاقة السحابية.^٤

ولا يلزم أن تتطابق الجهة التي تتعاقد معها الدولة مع الجهة التي تدير البنية التقنية أو تقدم الدعم أو تدير الهوية والصلاحيات أو تتحكم في مفاتيح التشفير. كما أن وجود الخوادم أو مراكز البيانات داخل الكويت لا يحسم، بذاته، مكان ممارسة السيطرة القانونية أو التشغيلية على البيانات.

ومن هنا تميز الورقة بين أربعة مستويات مترابطة: **الموقع المادي للبنية التي تستضيف البيانات أو تعالجها؛ والسيطرة التقنية والتشغيلية؛ والاختصاص القانوني القادر على إلزام الكيان الحائز أو المسيطر؛ وقابلية تنفيذ الأمر الأجنبي أو مقاومته عبر الحدود.** ويشكل هذا التمييز أساس تحليل حدود التوطين المادي وقدرته على إنتاج حماية سيادية فعلية.

1 البوابة الإلكترونية الرسمية لدولة الكويت، «الكويت توقع اتفاقية شراكة مع (مايكروسوفت) لتعزيز التحول الرقمي والذكاء الاصطناعي»، ٥ مارس ٢٠٢٥؛ وزارة المالية الكويتية، «وزارة المالية أول جهة حكومية تفعل اتفاقية الشراكة مع مايكروسوفت وتنتقل إلى Microsoft Azure باستخدام Azure VMware Solution»، ١٠ أغسطس ٢٠٢٥؛ والجهاز المركزي للمناقصات العامة، وثيقة طلب التعاقد المباشر بشأن الشراكة الاستراتيجية مع Microsoft.

2 «The Government of Kuwait Selects Google Cloud to Commence Nationwide Digital Transformation Roadmap5»، Google Cloud، ٢٠٢٣؛ و «Kuwait Alliance Framework Agreement» AFA، Google Cloud، يناير 2023؛ و

3 الهيئة العامة للاتصالات وتقنية المعلومات، «CITRA، AWS sign coop deal»، ٥ سبتمبر ٢٠١٨؛ والهيئة العامة للاتصالات وتقنية المعلومات، «Kuwait، Amazon to put framework for cloud services in gov't sector»، ٣ أكتوبر ٢٠١٨.

4 زينب أشكناني، «Data Sovereignty and Strategic Autonomy in the Gulf»، مركز الخليج للأبحاث، يونيو ٢٠٢٦.

العمق التحليلي للحالة الكويتية والخصوصية التشريعية: من موقع الخادم إلى بنية السيطرة

أ. القانون الكويتي لا يجعل موقع الخادم معيارًا حاسمًا بذاته

تقتضي معالجة البيئة السحابية من منظور القانون الدولي الخاص تحديد طبيعة العلاقة القانونية محل النزاع وتكييفها، إذ قد تتصل البيانات بعلاقة تعاقدية، أو بحقوق ملكية فكرية، أو بسر تجاري، أو بحماية البيانات الشخصية، أو بسرية المعلومات الحكومية، أو بالتزامات تنظيمية. ومن ثم، لا يمكن افتراض أن «البيانات» تمثل في جميع الأحوال محلًا قانونيًا واحدًا يخضع لضابط إسناد واحد.

وتكتسب المادة (٣١) من القانون رقم (٥) لسنة ١٩٦١ بتنظيم العلاقات القانونية ذات العنصر الأجنبي أهميتها؛ إذ تجعل القانون الكويتي مرجعًا في تكييف العلاقات القانونية متى كان تحديد نوع العلاقة لازمًا لتعيين القانون الواجب التطبيق من قبل القاضي الكويتي^٥، متى انعقد له الاختصاص وفق قواعد قانون المرافعات الكويتي^٦. وبذلك لا تبدأ المسألة من مكان الخادم، وإنما من طبيعة العلاقة أو الحق محل النزاع ثم ضابط الإسناد الملائم.

أما المادة (٥٢)، فتقرر بالنسبة إلى المنقول أن قانون الجهة التي يوجد فيها المنقول وقت تحقق السبب المنشئ للحيازة أو الملكية أو الحق العيني أو الناقل له هو القانون الواجب التطبيق على هذه المسائل. وقد تكون ذات صلة بالخوادم والمعدات المادية إذا انصب النزاع على حق عيني في البنية ذاتها؛ لكنها لا تؤسس لقاعدة مفادها أن موقع الخادم يحدد القانون الذي يحكم البيانات أو جميع العلاقات القانونية المتصلة بها. فالمساواة بين موقع الأصل المادي وموقع البيانات أو مركز السيطرة القانونية عليها تتجاوز نطاق قاعدة الإسناد التي قررتها المادة.

وفي البيئة السحابية، قد يوجد الخادم داخل الكويت بينما تكون البيانات محل العلاقة التعاقدية أو التنظيمية مرتبطة بالجهة الحائزة لها أو بمقدم الخدمة أو بالبنية التي تتيح إدارتها والوصول إليها. ومن ثم، يظل الموقع المادي عنصرًا من عناصر التحليل، لكنه لا يمثل ضابطًا جامعيًا لتحديد القانون الواجب التطبيق على جميع الآثار القانونية المرتبطة بالبيانات.

أما المادة (٥٩)، فتتناول القانون الواجب التطبيق على العقد من حيث شروطه الموضوعية وآثاره، وتعتد بالمواطن المشترك للمتعاقدين، وعند اختلافه بقانون الدولة التي تم فيها العقد، مع الاعتداد باتفاق المتعاقدين أو بما تكشف عنه الظروف من إرادة تطبيق قانون آخر. وتكتسب هذه القاعدة أهمية خاصة في العقود السحابية الحكومية؛ إذ يمكن أن تنظم العلاقة القانون الواجب التطبيق، والاختصاص، والسرية، والإخطار، وقيود نقل البيانات، وتوزيع المسؤوليات، وإدارة مفاتيح التشفير، والتعامل مع الطلبات الحكومية أو القضائية.

5 المرسوم بالقانون رقم (٥) لسنة ١٩٦١ في شأن تنظيم العلاقات القانونية ذات العنصر الأجنبي، ولا سيما المواد ٣١، ٥٢، ٥٩، ٦٨-٧٣.
6 المرسوم بالقانون رقم (٣٨) لسنة ١٩٨٠ بإصدار قانون المرافعات المدنية والتجارية وتعديلاته، الكتاب الثاني، الباب الأول، الفصل الأول، المواد ٢٣-٢٨.

غير أن اختيار القانون في العقد لا ينشئ حصانة من اختصاص قانوني أو قضائي أجنبي خارج نطاق العقد. فالعقد ينظم العلاقة بين أطرافه في الحدود التي يسمح بها القانون، لكنه لا يستطيع بذاته إلغاء قاعدة أمره تنطبق على كيان خاضع لاختصاص دولة أخرى، ولا منع محكمة أجنبية من ممارسة اختصاصها متى توافرت أسسه وفق قانونها. وهنا يظهر الفارق بين القانون الواجب التطبيق على العلاقة التعاقدية وبين الاختصاص القانوني والقضائي الذي قد يمارس على أحد أطرافها أو على الكيان الحائز أو المسيطر على البيانات.

وتؤكد المواد (٦٨) إلى (٧٣) من القانون ذاته أولوية النص الخاص أو المعاهدة الدولية النافذة، وإحالة ما لم يرد فيه نص إلى مبادئ القانون الدولي الخاص، وتنظيم نطاق تطبيق القانون الأجنبي، ثم استبعاد أحكامه المخالفة للنظام العام أو الآداب في الكويت.

غير أن النظام العام يؤدي وظيفته أساسًا في مرحلة تحديد القانون الواجب التطبيق أو استبعاد أثر قانون أجنبي أمام الجهة القضائية الكويتية؛ ولا ينبغي تحميله وظيفة منع سلطة أجنبية من إصدار أمر إلى كيان خاضع لاختصاصها. فهذه المسألة تتعلق بالاختصاص القضائي الأجنبي، والقوة القانونية للأمر الصادر عنه، ومدى إمكان إنفاذه أو مقاومته خارج الدولة التي أصدرته.

وعليه، لا تقود القراءة السليمة للإطار الكويتي إلى قاعدة ثنائية من نوع «الخدم داخل الكويت = القانون الكويتي»، أو «المزود أجنبي = القانون الأجنبي»، وإنما إلى تفكيك العلاقة إلى عناصرها القانونية والفعلية، وتحديد طبيعة الحق، والكيان الحائز أو المسيطر، ومصدر السلطة القانونية عليه، ثم فصل القانون الواجب التطبيق عن الاختصاص القضائي وقابلية تنفيذ آثاره عبر الحدود.

ب. معيار الكيان المسيطر: من «مزود الخدمة» إلى مركز السلطة الفعلية

لا يكفي تحديد اسم مقدم الخدمة أو الشركة الظاهرة في العقد؛ لأن الكيان المتعاقد ليس بالضرورة هو الكيان الذي يملك السيطرة التقنية أو التشغيلية أو القدرة القانونية الفعلية على الوصول إلى البيانات.

ولا يقصد بالسيطرة مجرد الملكية التجارية للبيانات، وإنما القدرة الفعلية على الوصول إليها أو إدارتها أو استعادتها أو نقلها أو فك تشفيرها أو تمكين الغير من الوصول إليها، مقرونة بالقدرة القانونية على إلزام الجهة التي تملك هذه القدرة.

ومن ثم، لا يكفي اسم مقدم الخدمة أو موقع الخادم للوصول إلى نتيجة بشأن الخضوع لاختصاص أجنبي، وإنما يتعين تفكيك بنية العلاقة وتحديد مركز السيطرة الفعلية، ثم التحقق من الصلة القانونية التي قد تجعل هذه السيطرة خاضعة لاختصاص قانوني أو قضائي أجنبي.

“ لا يكفي تحديد اسم مقدم الخدمة أو الشركة الظاهرة في العقد لأن الكيان المتعاقد ليس بالضرورة هو الكيان الذي يملك السيطرة التقنية أو التشغيلية أو القدرة القانونية الفعلية على الوصول إلى البيانات ”

وتأسيسًا على ذلك، تعتمد الورقة **معياريًا عمليًا** لتحديد الكيان المسيطر، يقوم على أربعة مستويات مترابطة:

المستوى الأول: تحديد مركز الحياة

١. من هو الكيان المتعاقد مع الحكومة الكويتية؟
٢. من يحوز البيانات أو يحتفظ بها؟
٣. أين توجد البنية المادية التي تستضيف البيانات أو تعالجها؟
٤. هل توجد كيانات أخرى تشارك في الاستضافة أو المعالجة أو النسخ أو النقل؟

المستوى الثاني: تحديد مركز السيطرة التقنية والتشغيلية

١. من يدير طبقات الإدارة والتحكم والهوية والصلاحيات؟
٢. أين توجد وظائف الدعم الفني والإداري التي يمكنها الوصول إلى البيئة؟
٣. من يستطيع استعادة البيانات أو نسخها أو نقلها أو تمكين الوصول إليها؟

المستوى الثالث: تحديد السيطرة على التشفير

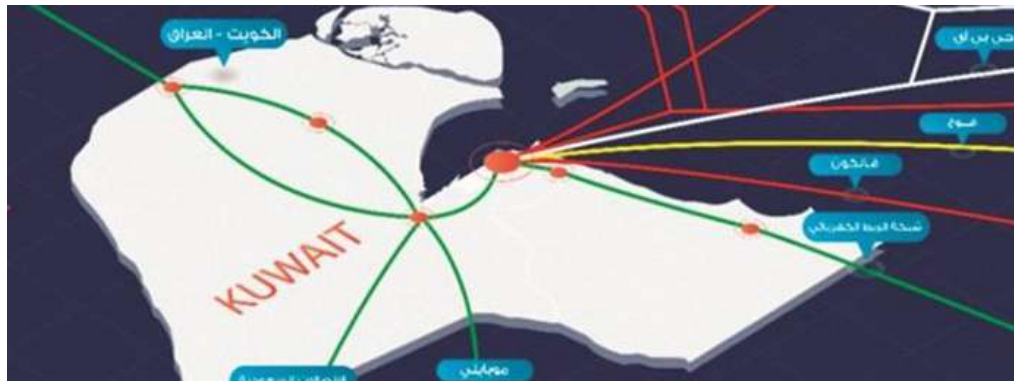
١. من يملك مفاتيح التشفير؟
٢. من يملك القدرة الفعلية على فك التشفير والوصول إلى المحتوى؟

المستوى الرابع: تحديد مركز السلطة القانونية

١. ما العلاقة القانونية والتشغيلية بين الشركة المتعاقدة والشركات التابعة أو الأم، وأي كيان منها يملك القدرة الفعلية على الوصول إلى البيانات، ومن ثم قد يكون عرضة لطلب أو أمر صادر عن سلطة قانونية أو قضائية أجنبية؟

ولا يفترض هذا المعيار أن الجنسية الأمريكية لمقدم الخدمة تكفي وحدها لإثبات خضوع البيانات للقانون الأمريكي، كما لا يفترض أن وجود الخادم داخل الكويت يستبعد تلقائيًا الاختصاص الأجنبي. فكلًا الاستنتاجين يحتاج إلى إثبات مستقل لعناصر السيطرة والاختصاص.

ومن ثم، فإن السؤال الحاسم لا ينتهي عند مكان البيانات أو الخادم، بل يمتد إلى تحديد الكيان الذي تقع تحت سيطرته القدرة على الوصول إليها، والسلطة القانونية التي تستطيع إلزامه، والوسيلة القضائية التي يمكن من خلالها تحويل تلك السلطة إلى أمر نافذ.



السيناريو التنفيذي: ماذا يحدث عندما يصدر أمر قضائي أمريكي بشأن بيانات موجودة في الكويت؟

هنا ينتقل التحليل إلى التنفيذ الفعلي. ولنفترض أن جهة حكومية كويتية تضع بيانات حساسة في منطقة سحابية داخل الكويت، وأن البيانات مملوكة لها والخوادم موجودة ماديًا في الكويت، بينما تقدم الخدمة مجموعة تقنية دولية يوجد ضمن هيكلها كيان خاضع للاختصاص الأمريكي يملك أو يسيطر، بصورة مباشرة أو غير مباشرة، على القدرة القانونية أو التقنية أو التشغيلية ذات الصلة بالبيانات.

في هذه الحالة، لا يكون موقع الخادم نقطة الحسم الوحيدة؛ بل يبدأ التحليل من تحديد الكيان الذي يمكن أن يخضع للطلب الأمريكي، وطبيعة البيانات المطلوبة، ومدى وقوعها ضمن حيازته أو عهده أو سيطرته، ثم آثار تعارض الالتزامات الأمريكية مع القيود القانونية أو التنظيمية في الكويت.

أ. صدور الطلب القانوني

إذا صدر إجراء قانوني أمريكي مستند إلى الصلاحية المناسبة، فإن السؤال الأول لا يكون: أين يوجد الخادم؟ وإنما: هل البيانات أو المعلومات المطلوبة تقع ضمن حيازة مقدم الخدمة المشمول أو عهده أو سيطرته؟

فقد قرر U.S.C. § 2713 18 أن مقدم الخدمة المشمول يلتزم بحفظ البيانات أو نسخها احتياطيًا أو الإفصاح عن محتوى الاتصالات أو السجلات أو المعلومات المتعلقة بالعميل أو المشترك التي تقع ضمن حيازته أو عهده أو سيطرته، بغض النظر عن كون البيانات موجودة داخل الولايات المتحدة أو خارجها.^٧

وعليه، فإن وجود البيانات داخل الكويت لا ينهي التحليل، وإنما ينقل مركزه من موقع البيانات إلى علاقة الكيان المطلوب منه الاستجابة بالبيانات وقدرته القانونية والتقنية على الوصول إليها وإنتاجها.

ب. تحديد مفهوم الحيازة والعهد والسيطرة

إذا كانت البيانات محفوظة في بيئة مادية داخل الكويت، لكن كيانًا خاضعًا للاختصاص الأمريكي يملك القدرة الفعلية على الوصول إليها أو استعادتها أو إنتاجها، فإن موقع الخادم لا يكون وحده كافيًا لنفي إمكانية انطباق § ٢٧١٣.

وفي المقابل، لا يجوز استنتاج أن وجود شركة أم أمريكية يعني تلقائيًا خضوع كل بيانات تحتفظ بها شركة تابعة أجنبية للقانون الأمريكي. فالمعيار يرتبط بالكيان الذي تكون البيانات ضمن حيازته أو عهده أو سيطرته، وبالأساس القانوني الذي يربطه بالإجراء الأمريكي.

7 U.S.C. § 2713 18 6، كما أضيف بموجب (Clarifying Lawful Overseas Use of Data Act (CLOUD Act)، Pub. L. No. 115-141, div. V, § 103(a)(1), 1214 Stat. 2018 March 23.

ج. إخطار الحكومة الكويتية

ينبغي أن ينظم العقد مسبقًا كيفية تعامل المزود مع أي طلب حكومي أو قضائي أجنبي يتعلق بالبيانات الكويتية، في حدود ما يسمح به القانون.

ويشمل ذلك، متى كان الإخطار جائزًا قانونًا، إبلاغ الجهة الحكومية بالطلب قبل الإفصاح، وبيان طبيعته ونطاقه والبيانات المطلوبة والمهلة المحددة للاستجابة، وما إذا كان المزود يستطيع الاعتراض أو طلب تضيق نطاقه.

ولا يعني ذلك قدرة الكويت على إلغاء الأمر الأجنبي، وإنما تمكينها من معرفة الطلب قبل تنفيذه وإتاحة الوقت لاتخاذ الإجراءات القانونية المناسبة.

د. هل يستطيع المزود الاعتراض؟

لا يعني خضوع المزود للقانون الأمريكي أن الإفصاح واجب في جميع الحالات دون إمكانية للاعتراض أو طلب تعديل الأمر. ويتيح القانون، في حالات محددة، طلب تعديل الأمر أو إلغائه، ومن أبرزها ما ينظمه (h) 2703 U.S.C. عند تعارض الإفصاح المطلوب مع قانون دولة أجنبية مؤهلة.⁸

وتنظر المحكمة في مدى وجود التعارض وفي الاعتبارات التي حددها القانون، ومنها مصالح الولايات المتحدة والدولة الأجنبية وطبيعة التعارض والآثار المترتبة على مقدم الخدمة.

لكن هذه الحماية ليست تلقائية ولا مطلقة، ولا تمنح الكويت حقًا في إلغاء الأمر الأمريكي، ولا تعني أن كل تعارض بين القانونين سيؤدي إلى وقف الإفصاح. ومن ثم، يظل الاعتراض وسيلة دفاع عند نشوء النزاع، لا ضمان مسبق لحماية البيانات.

هـ. ماذا لو تعارض القانونان؟

إذا كان القانون الكويتي أو التزام تنظيمي أو تعاقدني نافذ يمنع الإفصاح، في حين يكون مقدم الخدمة ملزمًا بموجب القانون الأمريكي بالاستجابة لأمر صحيح صادر إلى كيان خاضع للاختصاص الأمريكي، فقد يواجه المزود التزامين متعارضين.

ولا يعني وجود القانون الكويتي أن الكويت تستطيع تلقائيًا منع المحكمة أو السلطة الأمريكية من إصدار الأمر، كما لا يعني صدور الأمر الأمريكي أن القانون الكويتي يفقد أثره داخل الكويت. فكل نظام قانوني يعمل في نطاق اختصاصه، وتبقى المسألة العملية مرتبطة بالكيان المخاطب ومكان وجوده ومدى خضوعه للسلطات الكويتية أو الأمريكية.

8 (U.S.C. § 2703(h))، بشأن طلب تعديل أو إلغاء الإجراء القانوني في حالات محددة عند وجود تعارض جوهري مع قانون دولة أجنبية مؤهلة، مع مراعاة الشروط والاعتبارات المنصوص عليها في النص

وهنا يجب التمييز بين الاختصاص القضائي والقدرة على تنفيذ الأمر عبر الحدود. فقد تستطيع الكويت إصدار أمر ملزم داخل إقليمها، دون أن يعني ذلك امتلاك وسيلة مباشرة لإجبار كيان أجنبي خارج نطاق سلطتها التنفيذية على الامتناع عن تنفيذ أمر صادر عن قضاء دولته. وبالعكس، قد يكون الأمر الأمريكي ملزمًا للكيان الخاضع للاختصاص الأمريكي رغم وجود البيانات ماديًا في الكويت.

ومن ثم، فإن توطين الخوادم داخل الكويت لا يكفي وحده لضمان قدرة الدولة على التحكم في تنفيذ الأوامر الأجنبية؛ والسؤال الحاسم هو: هل تملك الكويت السيطرة القانونية والتقنية والتنفيذية على الجهة التي تستطيع الوصول إلى البيانات عند وقوع النزاع؟

و. التطبيق العملي: أين تقع نقطة الانكشاف الفعلية؟

قد تتوزع الوظائف المرتبطة بقاعدة بيانات حكومية بين مالك مركز البيانات، والكيان المتعاقد مع الحكومة، وكيانات أخرى تتولى التشغيل أو الدعم الفني أو إدارة الهوية أو النسخ الاحتياطي أو الإدارة والتحكم. ولذلك لا يكفي اسم المزود أو موقع الخادم لتحديد الجهة القادرة فعليًا على الوصول إلى البيانات أو إنتاجها.

وعند صدور أمر أمريكي، لا يكون السؤال الحاسم هو هل البيانات كويتية، بل أي كيان صدر إليه الأمر، وما طبيعة البيانات المطلوبة، وهل تقع ضمن حيازته أو عهده أو سيطرته؟

وقبل التعاقد، ينبغي أن تجيب الجهة الحكومية بصورة موثقة عن الأسئلة الآتية:

- إلى أي كيان يمكن أن يوجّه الطلب؟
- ما البيانات التي يمكن أن يشملها؟
- أي كيان يحتفظ بها أو يستطيع الوصول إليها أو إنتاجها؟
- هل الوصول مباشر أم من خلال كيان آخر؟
- من يملك صلاحيات الإدارة والاستعادة؟
- من يملك مفاتيح التشفير؟
- هل توجد نسخ احتياطية أو سجلات وصول أو بيانات وصفية في بيئات أخرى؟
- ما القيود القانونية أو التنظيمية الكويتية التي قد تتعارض مع الإفصاح؟

فإذا كان المزود يملك صلاحيات تمكّنه فعليًا من الوصول إلى البيانات أو استعادتها أو إنتاجها، فإن هذه القدرة تمثل عنصرًا مهمًا في تقييم السيطرة. أما إذا كانت البيانات مشفرة بمفاتيح لا يملكها المزود ولا يستطيع الوصول إليها، فإن قدرته على إنتاج محتوى مقروء تكون أكثر محدودية، دون أن يعني ذلك استحالة جميع أشكال الوصول؛ فقد يشمل الطلب بيانات وصفية أو سجلات وصول أو معلومات حساب أو بيانات تشغيلية أو نسخة مشفرة.

ولهذا يجب أن تطلب الجهة الحكومية خريطة واضحة لبنية السيطرة تبين الكيانات القانونية ذات الصلة، وموقع البنية، ومواقع النسخ الاحتياطية، وصلاحيات الإدارة والوصول، وآلية إدارة المفاتيح، والجهة القادرة على الاستعادة أو النقل أو تغيير إعدادات الوصول.

وفي حالات الطوارئ، ينبغي أن يرتبط بند الإخطار بآلية واضحة للاستجابة للطلبات العاجلة، تحدد جهة الاتصال ووسيلة الإخطار والمعلومات الواجب تقديمها وإجراءات حفظ البيانات، والتزام المزود - بالقدر الذي يسمح به القانون - بالسعي إلى تضيق الطلب أو الاعتراض عليه.

ولا ينبغي كذلك الاعتماد على التعويض المالي وحده عند وقوع إفصاح مخالف؛ لأن التعويض قد يعالج أثرًا ماليًا لاحقًا دون أن يعيد السرية إلى بيانات تم الإفصاح عنها. ومن ثم، يبقى منع نقطة الانكشاف خط الدفاع الأول.

ز. من يملك البيانات ليس بالضرورة من يستطيع إنتاجها

قد تكون الجهة الحكومية صاحبة البيانات وصاحبة السلطة القانونية عليها، لكنها لا تملك بالضرورة حساب الإدارة أو النسخة التشغيلية أو مفاتيح التشفير أو القدرة التقنية على استخراجها. وبالمقابل، قد يملك المزود القدرة التقنية على الوصول إليها أو إنتاجها دون أن يكون مالكًا لها قانونًا.

ولهذا ينبغي أن تتحول الأسئلة السابقة إلى قائمة تحقق تعاقدية وتشغيلية تشمل:

١. المالك أو صاحب السلطة القانونية.
٢. الحائز الفعلي.
٣. المشغل.
٤. صاحب صلاحيات الإدارة العليا.
٥. صاحب القدرة على الإنتاج.
٦. حائز مفاتيح التشفير.
٧. صاحب القدرة على فك التشفير.
٨. الكيان المعرض للاختصاص الأجنبي.
٩. صاحب القرار التشغيلي في الأزمة.
١٠. قابلية الانفصال والترحيل.

وتكتسب النقطتان التاسعة والعاشر أهمية خاصة؛ لأن ضعف السيطرة في لحظة الأزمة أو عدم القدرة على الانتقال إلى بيئة بديلة قد يحول الحماية القانونية إلى حماية نظرية.

ولا يعني وجود عنصر أجنبي انعدام السيادة الرقمية تلقائيًا، وإنما تتأثر درجة السيطرة الوطنية بمدى اعتماد الدولة على كيانات خارجية في الوظائف التي تحدد القدرة على الوصول إلى البيانات أو إنتاجها أو نقلها.

الخطوة السادسة: ماذا تستطيع دولة الكويت فعليًا أن تفعل؟

قبل النزاع، تستطيع الكويت تحديد فئات البيانات ذات المتطلبات السيادية المرتفعة، واختيار بنية تقلل تركّز وظائف السيطرة الجوهرية خارج الدولة، وإحكام السيطرة على مفاتيح التشفير حيث يكون ذلك ممكنًا، ووضع آليات للإخطار والتعامل مع الطلبات الأجنبية، وإجراء تدقيق مستقل، وضمان قابلية نقل البيانات والأنظمة وتقليل الاعتماد على مزود واحد.

أما بعد صدور الأمر، فتستطيع الجهة الحكومية، بحسب طبيعة الإجراء والكيان المخاطب والقانون الواجب التطبيق، استخدام الوسائل القانونية والتنظيمية والتعاقدية المتاحة، وطلب من المزود ممارسة حقوق الاعتراض أو التعديل التي يتيحها القانون.

لكن لا ينبغي بناء مفهوم السيادة على افتراض القدرة المطلقة على منع القضاء الأجنبي من إصدار إجراء إلى كيان خاضع لاختصاصه. **فأفضل حماية سيادية ليست القدرة على خوض النزاع بعد صدور الأمر، وإنما إعادة تصميم البنية مسبقًا بحيث تقل قدرة الكيان الأجنبي على الوصول إلى البيانات القابلة للإفصاح، وتبقى للدولة قدرة فعلية على إدارة الأزمة والانتقال إلى بديل عند الضرورة.**

“ أفضل حماية سيادية ليست القدرة على خوض النزاع بعد صدور الأمر
وإنما إعادة تصميم البنية مسبقًا



من موقع البيانات إلى السيطرة على مقدم الخدمة، قضية Ireland Microsoft

تقدم قضية Ireland Microsoft مثالاً قضائياً مهماً لفهم التحول من التركيز على موقع البيانات إلى العلاقة بين البيانات ومقدم الخدمة الخاضع للاختصاص الأمريكي.

بدأ النزاع عندما طلبت السلطات الأمريكية من Microsoft، بموجب أمر صادر في إطار **Communications- Stored**، تسليم محتوى بريد إلكتروني مخزن في مركز بيانات تابع لها في دبلن. وفي عام ٢٠١٦، قضت محكمة الاستئناف للدائرة الثانية بأن القانون بصيغته آنذاك لا يمتد إلى محتوى الاتصالات المخزن خارج الولايات المتحدة، واعتبرت تطبيق الأمر على ذلك المحتوى تطبيقاً خارج الإقليم.^٩

غير أن المحكمة العليا الأمريكية لم تفصل في المسألة من حيث الموضوع. فبعد إقرار الكونغرس **CLOUD Act** في ٢٣ مارس ٢٠١٨، أضيف § ٢٧١٣، ونص على التزام مقدم الخدمة المشمول بحفظ أو نسخ أو الإفصاح عن البيانات الواقعة ضمن حيازته أو عهده أو سيطرته، بغض النظر عن وجودها داخل الولايات المتحدة أو خارجها. وبعد حصول الحكومة على أمر جديد يتعلق بالمعلومات نفسها، اعتبرت المحكمة العليا النزاع الأصلي غير ذي موضوع، وأبطلت حكم محكمة الاستئناف وأعادت القضية.^{١٠}

ومن ثم، لا يصح الاستناد إلى Ireland Microsoft بوصفها حكماً للمحكمة العليا قرر أن «السيطرة» هي المعيار الحاكم؛ لأن المحكمة العليا لم تحسم أصل النزاع. وتكمن أهمية القضية في تسلسلها؛ كشف النزاع الأول أثر الاعتماد على موقع البيانات في تحديد النطاق الإقليمي للقانون، ثم جاء التدخل التشريعي ليقرر صراحة أن موقع البيانات لا يمنع الالتزام إذا كانت البيانات ضمن حيازة مقدم الخدمة أو عهده أو سيطرته.

ولا يعني ذلك أن وجود مزود أمريكي يؤدي تلقائياً إلى خضوع كل بيانات موجودة في الكويت للقانون الأمريكي، كما لا يعني وجود البيانات داخل الكويت منع الاختصاص الأجنبي. وإنما يتوقف التحليل على الكيان المخاطب بالإجراء، وعلاقته بالبيانات، ومدى وقوعها ضمن حيازته أو عهده أو سيطرته، وطبيعة الإجراء والأساس القانوني له.^{١١}

وهذا هو الدرس الأهم للحالة الكويتية: إثبات وجود البيانات داخل الكويت يثبت عنصرًا مهمًا من التوطين المادي، لكنه لا يكفي وحده لإثبات سيطرة الدولة القانونية والتقنية على إمكانية الوصول إليها.

9 Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016).
 10 United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018) (per curiam)
 11 U.S. Department of Justice, Criminal Division, «CLOUD Act Resources» ٢٤، October 2023.

الحماية القانونية والتقنية: مفاتيح التشفير ليست حصانة قانونية

يمثل التشفير أحد أهم عناصر الحماية التقنية للبيانات، لكنه لا يشكل بديلاً عن الحماية القانونية أو حصانة تلقائية من الطلبات القضائية الأجنبية.

فإذا كانت البيانات مشفرة وكانت مفاتيح فك التشفير تحت إدارة جهة وطنية مستقلة، بحيث لا يملك مقدم الخدمة الخارجي المفاتيح ولا يستطيع استخدامها للوصول إلى المحتوى، فإن قدرته التقنية على إنتاج **محتوى مقروء** تكون أكثر محدودة، بما يعزز قدرة الدولة على التحكم في أحد أهم عناصر السيادة التقنية.

لكن التشفير لا يسقط، بذاته، الالتزام القانوني إذا كان مقدم الخدمة خاضعاً لإجراء قانوني صحيح. فقد يشمل الطلب، بحسب نطاقه وطبيعة الخدمة، بيانات وصفية أو سجلات وصول أو معلومات حساب أو بيانات تشغيلية أو نسخاً مشفرة، كما قد توجد بيانات أخرى في بيئات أو نسخ احتياطية تخضع لضوابط مختلفة.

ومن ثم، يجب التمييز بين الحماية التقنية والحماية القانونية: فالأولى تحد من القدرة الفعلية على الوصول إلى البيانات أو إنتاج محتواها المقروء، بينما تحدد الثانية الالتزامات والحقوق والاختصاصات التي تحكم الجهات المتصلة بها. ولا تتحقق الحماية السيادية القوية من أحدهما منفرداً، وإنما من تكاملهما.

وعليه، ينبغي أن تقتصر الحماية التقنية بقاعدة قانونية وتنظيمية واضحة، وعقد يحدد إجراءات التعامل مع الطلبات الأجنبية وآلية الإخطار والاعتراض بالقدر الذي يسمح به القانون، وبنية تشغيلية تحتفظ الدولة من خلالها بالسيطرة على الوظائف الحساسة، وفي مقدمتها إدارة مفاتيح التشفير.

ومن هنا، لا ينبغي أن تكون إدارة مفاتيح التشفير مجرد إجراء أمني، بل جزءاً من تحديد مركز السيطرة الفعلية على البيانات. فكلما كان المزود الخارجي يملك المفاتيح الأساسية أو يستطيع الوصول إليها منفرداً، ازدادت قدرته التقنية على إنتاج المحتوى المقروء؛ أما عندما تكون المفاتيح تحت سيطرة جهة مستقلة، فتقلص قدرته على الوصول إلى المحتوى، دون أن ينهي ذلك جميع صور التعرض القانوني.



من يملك البيانات ومن يستطيع إنتاجها؟ نموذج التدقيق السيادي

بعد تحديد مركز السيطرة القانونية والتقنية على البيانات، ينبغي نقل التحليل إلى مرحلة ما قبل التعاقد. فلا يكفي معرفة صاحب البيانات من الناحية القانونية، بل يجب تحديد الجهات التي تملك الحيازة أو القدرة التقنية والتشغيلية على الوصول إليها أو استعادتها أو إنتاجها، والكيانات التي يمكن أن تخضع لإجراء قانوني أو قضائي أجنبي.

وتكتسب هذه التفرقة أهمية خاصة في ضوء §٢٧١٣؛ إذ يرتبط الالتزام بالبيانات التي تقع ضمن حيازة مقدم الخدمة أو عهده أو سيطرته، بصرف النظر عن مكان وجودها. ومن ثم، ينبغي أن يتجه التدقيق إلى **بنية الحيازة والسيطرة والقدرة على الوصول والإنتاج**.

ولهذا ينبغي أن تتضمن عملية اعتماد البيئة السحابية الحكومية خريطة موثقة للسيطرة على البيانات تشمل:

أولاً: الصفة القانونية للبيانات

من هي الجهة الحكومية صاحبة البيانات أو السلطة القانونية عليها؟ وما الالتزامات القانونية والتنظيمية التي تحكمها؟

ثانياً: الحيازة والتخزين

أين توجد البيانات والنسخ الاحتياطية؟ وأي كيان يحتفظ بها أو يدير البيئة المستضيفة؟

ثالثاً: الإدارة والتشغيل

من يدير البنية والمنصة؟ ومن يملك صلاحيات الإدارة والاستعادة وتغيير إعدادات الوصول؟

رابعاً: الوصول والإنتاج

من يستطيع الوصول إلى البيانات أو استعادتها أو استخراجها أو إنتاج نسخة منها؟ وهل يفعل ذلك مباشرة أم من خلال كيان آخر؟

خامساً: مفاتيح التشفير

من ينشئ المفاتيح ويحفظها ويديرها؟ وهل يستطيع مقدم الخدمة الوصول إليها أو استخدامها منفرداً؟

سادسًا: الاختصاص القانوني والقضائي

ما الكيانات المرتبطة بالخدمة التي يمكن أن تكون مخاطبة بإجراء قانوني أو قضائي أجنبي؟ وما طبيعة علاقتها بالبيانات وبمقدم الخدمة؟

سابعًا: التعامل مع الطلبات الأجنبية

ما الإجراءات التي يلتزم بها المزود عند تلقي طلب أجنبي؟ وهل يلتزم، بالقدر الذي يسمح به القانون، بالإخطار والمساعدة في تقييم الطلب؟ وهل يستطيع طلب تضيقه أو الاعتراض عليه؟

ثامنًا: الاستمرارية التشغيلية

هل تستطيع الجهة الحكومية استمرار الوصول إلى بياناتها وتشغيل أنظمتها إذا تعذر على المزود الاستمرار في الخدمة بسبب نزاع قانوني أو قيد تنظيمي أو ظرف آخر؟

تاسعًا: قابلية الخروج والترحيل

هل تستطيع الجهة الحكومية نقل البيانات والأنظمة ومفاتيح التشفير إلى بيئة بديلة دون فقدان القدرة على الوصول إليها أو الارتهاق إلى المزود في الوظائف الجوهرية؟

ولا ينبغي أن تظل هذه العناصر إقرارات تعاقدية عامة، وإنما يجب أن تكون قابلة للتحقق من خلال الوثائق الفنية والتعاقدية، وخرائط الصلاحيات، وسجلات الوصول، وبنية إدارة المفاتيح، وتحديد الكيانات القانونية المشاركة.

وينقل هذا الإطار تقييم السيادة الرقمية من معيار جغرافي بسيط إلى فحص لبنية السيطرة: **من يحوز البيانات؟ ومن يستطيع الوصول إليها أو إنتاجها؟ ومن يملك مفاتيحها؟ وأي كيان يمكن أن يكون مخاطبًا بإجراء أجنبي؟**

ولا يعني وجود عنصر أجنبي فقدان السيادة الرقمية تلقائيًا، كما لا يعني وجود الخادم داخل الكويت استبعاد الاختصاص الأجنبي تلقائيًا؛ وإنما تتحدد درجة الحماية بمدى قدرة الدولة على التحكم في الوظائف الجوهرية، وتقليل اعتمادها على كيان أجنبي، وإدارة مخاطر الاختصاص وضمان الاستمرارية وقابلية الانتقال.

“

لا يعني وجود عنصر أجنبي فقدان السيادة الرقمية تلقائيًا كما لا يعني وجود الخادم داخل الكويت استبعاد الاختصاص الأجنبي تلقائيًا

العقود والتحكيم: أداة حماية وليست درعًا سياديًا

يمكن للعقد الحكومي حماية البيانات من خلال تحديد القانون الواجب التطبيق، وتنظيم الاختصاص القضائي أو التحكيم، وفرض السرية، ومنح حقوق التدقيق، وتنظيم التعامل مع الطلبات الحكومية أو القضائية الأجنبية، وضمان الإخطار متى كان جائزًا قانونًا، ووضع آليات للاعتراض أو تضيق نطاق الإفصاح، وضمان قابلية نقل البيانات والأنظمة.^{١٢}

غير أن هذه الأدوات تظل، في أصلها، أدوات لتنظيم العلاقة بين أطراف العقد. فإذا أصدرت سلطة عامة أجنبية أمرًا إلى كيان خاضع لاختصاصها، فإنها ليست طرفًا في العقد أو شرط التحكيم؛ ومن ثم لا يستطيع شرط التحكيم، بذاته، منعها من ممارسة اختصاصها تجاه الكيان الخاضع لها.

ولا يعني ذلك أن العقد عديم القيمة؛ بل يمكن أن يكون من أهم أدوات تقليل مخاطر الانكشاف، بشرط ألا يعامل باعتباره بديلًا عن السيطرة التقنية والتشغيلية. ولذلك ينبغي ألا يقتصر التصميم التعاقدي على اختيار القانون أو المحكمة، وإنما يمتد إلى تحديد بنية السيطرة نفسها: الكيانات المشاركة، مواقع التخزين والمعالجة والنسخ الاحتياطية، حدود الدعم، صلاحيات الوصول، إدارة المفاتيح، طلبات الإفصاح الأجنبية، الإخطار، حقوق التدقيق، وضوابط التغيير، وحقوق الخروج والترحيل.

وبذلك يصبح العقد أداة لتقليل نقطة الانكشاف، لا وسيلة لإنشاء حصانة تعاقدية في مواجهة سلطة عامة أجنبية.

بذلك يصبح العقد أداة لتقليل نقطة الانكشاف، لا وسيلة لإنشاء حصانة تعاقدية في مواجهة سلطة عامة أجنبية



١٢ لجنة الأمم المتحدة للقانون التجاري الدولي (UNCITRAL)، *Contracts Computing Cloud of Issues Main the on Notes*، ٢٠١٩.

Schrems II: المقارنة المحدودة وحدود الحماية التعاقدية

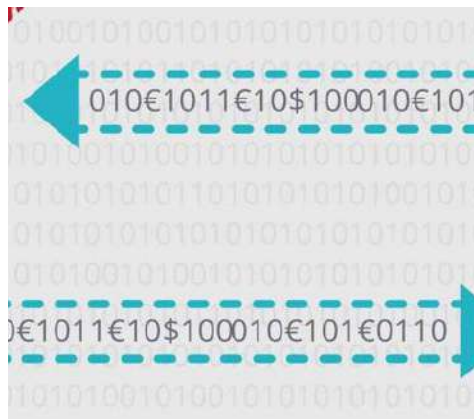
تقدم قضية **Schrems II** أمام محكمة العدل للاتحاد الأوروبي، وهي القضية ٣١١/١٨-٢٠٢٠ الصادر حكمها في ١٦ يوليو ٢٠٢٠، مقارنة مفيدة ولكن محدودة؛ فقد قضت المحكمة ببطلان **Shield Privacy US-EU**، وأكدت صحة شروط حماية البيانات القياسية (Standard Contractual Clauses) مع ضرورة ضمان مستوى حماية مكافئ في الواقع عند نقل البيانات الشخصية إلى دولة ثالثة.^{١٣}

ولا تنطبق القضية مباشرة على البيانات الحكومية الكويتية؛ فقد صدرت في إطار نظام حماية البيانات الشخصية في الاتحاد الأوروبي، وتناولت نقل البيانات الشخصية من الاتحاد الأوروبي إلى دولة ثالثة في ضوء GDPR والحقوق الأساسية.

وتكمن قيمتها المقارنة في إظهار حدود الاعتماد على الحماية التعاقدية وحدها عندما توجد سلطة عامة في دولة ثالثة تملك، بموجب قانونها، صلاحيات قد تؤثر في البيانات المنقولة. فوجود شروط تعاقدية بين الأطراف لا يحول بذاته دون تطبيق القواعد الآمرة التي تحكم السلطات العامة أو الجهات الخاضعة لاختصاص دولة أخرى.

ومن المهم عدم تحميل **Schrems II** أكثر مما تقرر؛ فهي ليست حكمًا بشأن CLOUD Act أو البيانات الحكومية الكويتية، ولا تقرر أن العقد عديم القيمة أمام سلطة أجنبية. وإنما تستخدمها الورقة **كسابقة مقارنة محدودة** لإيضاح أن الحماية التعاقدية لا ينبغي أن تكون الطبقة الوحيدة التي تعتمد عليها الدولة عندما توجد إمكانية قانونية للوصول سلطة عامة أجنبية إلى البيانات.

وبذلك تتكامل المقارنة مع **Ireland Microsoft** دون دمج القضيتين: فـ **Schrems II** تبرز حدود الضمانات التعاقدية في سياق حماية البيانات الأوروبية، بينما تكشف **Ireland Microsoft**، في سياق مختلف، أثر تدخل المشرع الأمريكي في تحديد التزامات مقدم الخدمة بالنسبة إلى البيانات الموجودة خارج الولايات المتحدة.



13 محكمة العدل للاتحاد الأوروبي، *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, Case C-311/18, Judgment, 16 July 2020, ECLI:EU:C:2020:559.

الجانب الكويتي: من التنظيم إلى اختبار الحوكمة السيادية

تبدأ حوكمة الحوسبة السحابية في الكويت من الإطار التنظيمي الذي وضعته الهيئة العامة للاتصالات وتقنية المعلومات CITRA، وما تتضمنه الوثائق التنظيمية لمقدمي الخدمات السحابية من متطلبات تتصل بالترخيص والالتزامات التنظيمية ومواقع البنية التحتية والجهات المشاركة في تقديم الخدمة. ويظهر من الإطار أن التنظيم لا يقتصر على مجرد وجود مركز بيانات داخل الكويت.^{١٤}

وفي المقابل، يجب التمييز بين القواعد التنظيمية القائمة والسياسات أو التصنيفات التي ألغيت لاحقاً. فقد ألغت CITRA بموجب القرار رقم ٣٤/٢٠٢٤ القرارين ٢٠٢١/٩ و٢٠٢١/٩٥ بشأن سياسة تصنيف البيانات وتعديلاتها، ومن ثم لا ينبغي تقديم القيود الواردة في تلك السياسة القديمة باعتبارها قواعد عامة نافذة حالياً.^{١٥}

كما يظهر في السجل التنظيمي الحالي قرار ١١٨/٢٠٢٦ بشأن «دليل إجراءات طلب ترخيص لتقديم خدمات الحوسبة السحابية»، وهو مدرج بوصفه قراراً نافذاً بتاريخ ٢٧ يوليو ٢٠٢٦،^{١٦} ويؤكد ذلك استمرار تطور التنظيم السحابي في الكويت نحو تنظيم إجراءات الترخيص وممارسة النشاط.

لكن التطور التنظيمي لا ينبغي أن يتوقف عند سؤال: أين يوجد مركز البيانات؟ بل يمتد إلى سؤال أكثر اتصالاً بالسيادة الرقمية: من يملك القدرة الفعلية على الوصول إلى البيانات أو التحكم في البيئة التي تستضيفها؟^{١٧}

وعند تقييم أي بيئة سحابية حكومية، ينبغي النظر إلى الكيانات القانونية المشاركة، ومواقع التشغيل والمعالجة والنسخ الاحتياطية، وصلاحيات الإدارة والدعم، وإدارة مفاتيح التشفير، والجهات التي يمكن أن تكون مخاطبة بإجراءات أجنبية، وآليات التعامل مع طلبات الإفصاح، وقابلية نقل البيانات والأنظمة إلى بيئة بديلة.

ولا تمثل الشراكة مع مزود عالمي -في حد ذاتها، مشكلة سيادية-؛ إذ يمكن أن تحقق مزايا تقنية واقتصادية وأمنية مهمة. وإنما تظهر المخاطر عندما تصبح الوظائف الرقمية الجوهرية غير قابلة للنقل، أو تتركز القدرة على الوصول إلى البيانات أو مفاتيحها أو إدارتها في كيان خارج نطاق السيطرة الوطنية المباشرة.

ج. اختبار حوكمة الشراكات السحابية في الكويت

ينبغي أن تتحول الموافقة على البيئة السحابية الحكومية من قرار تقني لمرة واحدة إلى عملية حوكمة مستمرة. وقبل اعتماد أي بيئة تستضيف بيانات حساسة، ينبغي التحقق من هوية الكيان المتعاقد والكيانات المشاركة، ومركز الحيابة، وصلاحيات الإدارة والوصول، وموقع وظائف الدعم، وإدارة المفاتيح، وآلية التعامل مع الطلبات الأجنبية، والإخطار، وقابلية نقل البيانات والأنظمة.

14 الهيئة العامة للاتصالات وتقنية المعلومات، *Commitments, V1.7 and Regulations Providers Service Cloud*، دولة الكويت.

15 الهيئة العامة للاتصالات وتقنية المعلومات، القرار رقم ٣٤/٢٠٢٤ بشأن إلغاء سياسة تصنيف البيانات، ١٨ فبراير ٢٠٢٤.

16 الهيئة العامة للاتصالات وتقنية المعلومات، القرار رقم ١١٨/٢٠٢٦، «دليل إجراءات طلب ترخيص لتقديم خدمات الحوسبة السحابية»، ٢٧ يوليو ٢٠٢٦.

17 الهيئة العامة للاتصالات وتقنية المعلومات، *Framework, V2.4 Regulatory Computing Cloud*، دولة الكويت.

ولا يكفي توافر هذه المعلومات عند توقيع العقد؛ إذ قد تتغير بنية الخدمة نتيجة إعادة هيكلة الشركات، أو تغيير مواقع المعالجة والنسخ الاحتياطية، أو تعديل إدارة المفاتيح، أو نقل وظائف الدعم، أو تغيير شروط الخدمة، أو نشوء متطلبات قانونية جديدة. ولذلك ينبغي إعادة تقييمها دوريًا وعند حدوث تغيير جوهري.

ويمكن للجهة الحكومية اعتماد **شهادة أو تقرير سيادة رقمية دوري** للبيئات التي تستضيف بيانات حساسة، يثبت الوضع الفعلي للكيانات المشاركة، ومسارات الوصول، ومواقع المعالجة والنسخ، وإدارة المفاتيح، والطلبات القانونية الأجنبية، واختبارات الترحيل والاستمرارية، وأي تغيير جوهري في بنية السيطرة.

ولا يقصد بهذه الشهادة إنشاء مركز قانوني جديد أو الادعاء بوجود معيار تشريعي قائم، وإنما استخدامها كأداة **حوكمة وتدقيق وطنية** تساعد الجهة الحكومية على التحقق المستمر من بقاء مستوى السيطرة المعتمد عند التعاقد.

١.

الأمن السيبراني ليس السيادة القضائية

قد تكون البنية التحتية محمية بدرجة عالية من الاختراق والهجمات السيبرانية، ومع ذلك تبقى معرضة لآثار أمر قانوني أو قضائي أجنبي. فالأمن السيبراني يحمي الأنظمة والبيانات من الدخول أو الاستخدام غير المصرح به تقنيًا، بينما تتصل السيادة القانونية والتشغيلية بمن يملك القدرة على الوصول إلى البيانات أو تمكين الوصول إليها، ومن يمكن أن يخضع لأمر ملزم من سلطة أجنبية.

ومن ثم، فإن وضع البيانات في مركز بيانات آمن داخل الكويت لا يحسم، بذاته، مسألة السيطرة عليها. فإذا احتفظ مزود خارجي بصلاحيات الإدارة أو وسائل الوصول أو مفاتيح التشفير، فقد تكون البيانات محمية تقنيًا مع بقاء جزء من السيطرة عليها خارج الإقليم. ولا يعني ذلك أن خضوع المزود لاختصاص أجنبي يؤدي تلقائيًا إلى الإفصاح، وإنما يعني أن **موقع البيانات وحده لا يكفي لتحديد مستوى الاستقلال القانوني والتشغيلي**.

وبذلك تُفهم السيادة الرقمية باعتبارها منظومة تجمع بين **الأمن التقني، والسيطرة على الوصول، وحياسة مفاتيح التشفير، والاستقلال التشغيلي، والقدرة على إدارة طلبات الإفصاح الأجنبية، وقابلية الانتقال إلى بديل**. فالأمن السيبراني عنصر من عناصر السيادة الرقمية، لكنه لا يقوم مقامها ولا يحسم وحده مسألة الاختصاص القضائي الأجنبي.

“

الأمن السيبراني عنصر من عناصر السيادة الرقمية، لكنه لا يقوم مقامها ولا يحسم وحده مسألة الاختصاص القضائي الأجنبي

الحل السياساتي: من التوطين المادي إلى السيطرة القانونية والتشغيلية

توصي الورقة بالانتقال من سياسة تركيز على مكان استضافة البيانات إلى نموذج تدريجي يفحص أيضًا مركز السيطرة القانونية والتقنية والتشغيلية عليها، من خلال خارطة طريق سياساتية مرحلية تقترحها الورقة، وليست مددًا أو التزامات مفروضة بموجب التشريع الكويتي النافذ. ولا يستلزم ذلك الانسحاب من الخدمات السحابية العالمية، وإنما إعادة تصميم استخدامها وفق درجات مختلفة من الحساسية ومستوى السيطرة المطلوب، وذلك على النحو الآتي:

أولًا: خلال 1-6 أشهر: إنشاء سجل وطني للبيانات والأحمال ذات الحساسية السيادية، وتحديد الفئات التي تستلزم سيطرة وطنية مشددة، ومراجعة العقود السحابية القائمة لتحديد الكيانات الحائزة للبيانات، ومواقع التخزين والمعالجة والنسخ الاحتياطية، وصلاحيات الإدارة، وحياسة مفاتيح التشفير، وآليات التعامل مع طلبات الإفصاح الأجنبية.

ثانيًا: خلال 6-12 شهرًا: إدخال معيار تدقيق السيطرة ضمن إجراءات المناقصات والعقود السحابية الحكومية، بحيث يشمل الكيان المتعاقد والكيانات المرتبطة ومراكز التشغيل والدعم وصلاحيات الوصول وإدارة المفاتيح وإجراءات الإخطار والاعتراض على طلبات الإفصاح الأجنبية، بالقدر الذي يسمح به القانون.

ثالثًا: خلال 12-24 شهرًا: بناء أو تخصيص بيئة سحابية ذات ضوابط سيادية مشددة للأحمال الأعلى حساسية، مع تقليل الاعتماد التشغيلي غير الضروري على أطراف خارجية، واستخدام تقنيات تقلل قدرة المزود الخارجي على الوصول إلى المحتوى المقروء، ولا سيما من خلال فصل إدارة مفاتيح التشفير عنه حيثما كان ذلك ممكنًا ومناسبًا.

رابعًا: خلال 18-30 شهرًا: تطوير القدرات الوطنية اللازمة لإدارة الوظائف التقنية الحساسة، بما في ذلك إدارة الهوية والصلاحيات، ومفاتيح التشفير، والمراقبة، والاستجابة للحوادث، والاستعادة، ونقل الأحمال، بحيث لا تعتمد استمرارية الوظائف السيادية على تدخل تشغيلي دائم من مزود خارجي واحد.

خامسًا: خلال 24-36 شهرًا: ترحيل الأحمال والبيانات المصنفة ضمن الفئات الأعلى حساسية إلى البيئة المناسبة، مع اختبار الاستعادة والطوارئ، وقابلية نقل البيانات والأنظمة، واستمرارية الوصول إلى مفاتيح التشفير.

سادسًا: بصورة مستمرة: تنويع الموردين والحد من الاحتجاز التقني (Vendor Lock-in)، وضمان قابلية نقل البيانات والأنظمة ومفاتيح التشفير، بحيث لا يتحول الاعتماد على مزود واحد إلى نقطة اختناق تقنية أو قانونية أو جيوسياسية.^{١٨}

“

ولا يستلزم ذلك الانسحاب من الخدمات السحابية العالمية، وإنما إعادة تصميم استخدامها وفق درجات مختلفة من الحساسية ومستوى السيطرة المطلوب

القرار السياساتي المطلوب

لا ينبغي أن يكون الهدف هو الانسحاب من التكنولوجيا العالمية؛ فهذا غير واقعي وغير ضروري. وإنما يتمثل الهدف في **منع تحول الشراكة التقنية إلى تبعية قانونية أو تشغيلية تحد من قدرة الدولة على التحكم في بياناتها أو إعادة تموضعها عند تغير الظروف القانونية أو التقنية أو الجيوسياسية.**

وتتمثل الأولوية في إدخال السيادة الرقمية ضمن معايير تصميم البنية السحابية، وال شراء الحكومي، والتعاقد، وإدارة المخاطر. فإذا كانت البيانات مستضافة داخل الكويت بينما يحتفظ مزود خارجي بمفاتيح التشفير أو بصلاحيات إدارية واسعة أو بقدرة فعلية على الوصول إلى المحتوى، فإن التوطين المادي يكون قد تحقق، لكن درجة السيطرة السيادية تظل محدودة. أما إذا كانت البيانات داخل الكويت، ومفاتيح فك تشفيرها تحت سيطرة وطنية مستقلة، وكانت الوظائف الحساسة وحقوق الوصول وعمليات الترحيل قابلة للإدارة من داخل الدولة، فإن مستوى السيطرة السيادية يرتفع بدرجة جوهرية، مع بقاء بعض مخاطر الاختصاص الأجنبي بحسب الكيان المعني وطبيعة الخدمة والقانون المنطبق.

وعليه، تقترح الورقة تطوير **مؤشر سيادي متعدد العناصر** بوصفه أداة قياس سياساتي مقترحة، لا معياراً قانونياً قائماً، ويمكن أن يقيس:

- نسبة البيانات الحساسة التي تخضع مفاتيح تشفيرها لسيطرة وطنية مستقلة.
 - نسبة الوظائف التشغيلية الحرجة التي يمكن إدارتها من داخل الدولة.
 - نسبة العقود التي تتضمن إجراءات واضحة للتعامل مع طلبات الإفصاح الأجنبية، بالقدر الذي يسمح به القانون.
 - قدرة الجهة الحكومية على نقل البيانات والأنظمة إلى مزود أو بيئة بديلة.
 - عدد البدائل المتاحة لكل وظيفة تقنية حرجة.
 - نسبة الأحمال الأعلى حساسية التي تعمل ضمن بيئة تحقق مستوى السيطرة الوطني المطلوب.
- ولا يقيس هذا المؤشر مكان البيانات فقط، بل مدى السيطرة الفعلية للدولة على البيانات ومفاتيحها ووظائفها التشغيلية وقدرتها على الانتقال وإدارة المخاطر القانونية المرتبطة بها. وكلما ارتفعت هذه القدرة، ارتفع مستوى السيادة الرقمية الفعلية.

تكشف المسألة السحابية عن تحول جوهري في مفهوم السيادة الرقمية؛ إذ قد تحقق الدولة التوطين المادي للبيانات دون أن تكتمل سيادتها الرقمية إذا ظلت البيانات، أو مفاتيح تشفيرها، أو بنيتها التشغيلية خاضعة لسيطرة كيان يمكن أن يمتد إليه اختصاص قانوني أو قضائي أجنبي. ومن ثم، لا ينحصر السؤال السيادي في أين توجد البيانات؟، وإنما يمتد إلى من يملك القدرة القانونية والتقنية والتشغيلية على الوصول إليها أو التحكم فيها أو تمكين الغير من الوصول إليها؟

ويتجلى هذا التحول في قضية **Ireland Microsoft**؛ فقد بدأ النزاع حول الأثر الإقليمي لأمر الإفصاح ومكان تخزين البيانات، قبل أن يعيد **Act CLOUD** صياغة الإطار القانوني على أساس حيازة مقدم الخدمة للبيانات أو وجودها في عهده أو تحت سيطرته، بصرف النظر عن موقعها المادي. وتقدم **II Schrems** -في سياق قانوني مختلف- دلالة مقارنة محدودة؛ إذ تكشف أن الحماية التعاقدية مهما بلغت أهميتها لا تكفي بذاتها لتحديد الآثار القانونية المترتبة على صلاحيات سلطة عامة أجنبية ليست طرفاً في العقد.

أما بالنسبة إلى الكويت، فلا تتمثل النتيجة في رفض الشراكات مع الشركات العالمية، وإنما في إعادة تصميمها على أساس مستوى السيطرة الفعلية المطلوب لكل فئة من البيانات والأحمال. ومن ثم، ينبغي أن ينتقل التعاقد الحكومي من الاكتفاء بالسؤال: «**أين ستُخزن البيانات؟**»، إلى تحديد الكيان الحائز، ومفاتيح التشفير، وصلاحيات الإدارة، ووظائف التشغيل والدعم، والكيان الذي يمكن أن يخضع لأمر أجنبي، وآليات التعامل معه، وقدرة الدولة على الاعتراض أو الترحيل أو استمرار التشغيل دون اعتماد حاسم على المزود.

وبذلك، يصبح التوطين القضائي والتنفيذي مفهوماً تحليلياً وسياساتياً تقترحه الورقة، وليس ادعاءً بوجود مبدأ تشريعي قائم بهذا الاسم. ويقصد به انتقال الدولة من مجرد توطين البيانات مادياً داخل حدودها إلى إحكام السيطرة على عناصرها الحاسمة قانونياً وتقنياً وتشغيلياً، ضمن الحدود التي تسمح بها طبيعة الخدمة والقانون المنطبق. وهنا تنتقل السيادة الرقمية من معيار يركز على مكان الخادم إلى قدرة فعلية على التحكم في البيانات وحمايتها وضمان استمرارية استخدامها وإدارتها، حتى عند تغير الظروف القانونية أو التشغيلية أو نشوء تعارض مع اختصاص أجنبي.



“
وهنا تنتقل السيادة الرقمية
من معيار يركز على مكان
الخادم إلى قدرة فعلية
على التحكم في البيانات
وحمايتها وضمان استمرارية
استخدامها وإدارتها

أولاً: التشريعات والوثائق والقرارات الرسمية الوطنية — دولة الكويت

١. المرسوم بالقانون رقم (٥) لسنة ١٩٦١ في شأن تنظيم العلاقات القانونية ذات العنصر الأجنبي.
٢. المرسوم بالقانون رقم (٣٨) لسنة ١٩٨٠ بإصدار قانون المرافعات المدنية والتجارية وتعديلاته.
٣. الهيئة العامة للاتصالات وتقنية المعلومات، Framework, V2.4 Regulatory Computing Cloud، دولة الكويت.
٤. الهيئة العامة للاتصالات وتقنية المعلومات، Commitments, and Regulations Providers Service Cloud، دولة الكويت، V1.7.
٥. الهيئة العامة للاتصالات وتقنية المعلومات، القرار رقم ٣٤/٢٠٢٤ بشأن إلغاء سياسة تصنيف البيانات، ١٨ فبراير ٢٠٢٤.
٦. الهيئة العامة للاتصالات وتقنية المعلومات، القرار رقم ١١٨/٢٠٢٦، «دليل إجراءات طلب ترخيص لتقديم خدمات الحوسبة السحابية»، ٢٧ يوليو ٢٠٢٦.
٧. البوابة الإلكترونية الرسمية لدولة الكويت، «الكويت توقع اتفاقية شراكة مع (مايكروسوفت) لتعزيز التحول الرقمي والذكاء الاصطناعي»، ٥ مارس ٢٠٢٥.
٨. وزارة المالية الكويتية، «وزارة المالية أول جهة حكومية تُفعّل اتفاقية الشراكة مع مايكروسوفت وتنقل إلى Microsoft Azure باستخدام Azure VMware Solution»، ١٠ أغسطس ٢٠٢٥.
٩. الجهاز المركزي للمناقصات العامة، وثيقة طلب التعاقد المباشر بشأن الشراكة الاستراتيجية مع Microsoft.
١٠. الهيئة العامة للاتصالات وتقنية المعلومات، «deal coop sign AWS, CITRA»، ٥ سبتمبر ٢٠١٨.
١١. الهيئة العامة للاتصالات وتقنية المعلومات، «Kuwait, Amazon put to framework in services cloud for sector t>gov»، ٣ أكتوبر ٢٠١٨.

ثانيًا: التشريعات والوثائق الأجنبية والدولية

12. United States 18 ,U.S.C2713 § ., as added by the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115–141, div. V, § 103(a)(1), 23 March 2018.
13. (United States, 18 U.S.C. § 2703(h).
14. U.S. Department of Justice, Criminal Division, «CLOUD Act Resources», 24 October 2023.
15. United Nations Commission on International Trade Law (UNCITRAL), Notes on the Main Issues of Cloud Computing Contracts, 2019.

ثالثًا: الأحكام القضائية الدولية والدراسات المقارنة

16. Microsoft Corp .v .United States, 829 F.3d 197 (2d Cir. 2016).
17. United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018) (per curiam).
18. Court of Justice of the European Union, Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, Judgment of 16 July 2020, ECLI:EU:C:2020:559.
19. ، مركز الخليج للأبحاث، يونيو 2026Data Sovereignty and Strategic Autonomy in the Gulfزينب أشكناني،



مركز الخليج للأبحاث
المعرفة للجميع

Gulf Research Center

Knowledge for All



مركز الكويت للبحوث والدراسات
KUWAIT RESEARCH AND STUDIES CENTER