

سفارات البيانات والاستمرارية السيادية السعودية: إطار مقارن قابل للاختبار

ورقة عمل تحليلية تقارن بين الحماية القانونية لسفارة البيانات، وتجارب استمرارية السجلات تحت الحرب والكوارث، وتقنيات التوزيع التشفيري؛ وتقتراح معايير اختبار قبل أي تطبيق سعودي.

تاريخ المادة الكاتب
18 أكتوبر 2026 صفوان المضيان

الكلمات المفتاحية: سفارة البيانات · الاستمرارية السيادية · السيادة الرقمية · التشفير ذو العتبة · استمرارية الحكومة · إدارة المخاطر

ورقة عمل تحليلية مشتقة من مقالة المؤلف ومصادر مفتوحة حتى 18 أكتوبر 2026. ليست بحثاً محكماً، ولا رأياً قانونياً، ولا تقريراً عن تجربة منفذة أو نتائج حكومية فعلية.

isafwan.com/ar/research/data-embassies-sovereign-continuity/

الملخص

تبحث هذه الورقة في الاستمرارية السيادية (Sovereign Continuity)، وفي الشروط التي تجعل الاستضافة الخارجية للبيانات الحكومية أداة لها بدل أن تبقى نسخة احتياطية بعيدة أو مصدر اعتماد جديد. وتنطلق من أن استمرار الدولة وظيفته تجمع السجل والبرمجيات والهوية والتوقيع والاتصال والتفويض القانوني، وأن سلامة البيانات لا تساوي وحدها إمكان استعمالها أو صحة محتواها.

تستخدم الورقة منهجاً وثائقيًا مقارنًا، فتقرأ اتفاق إستونيا ولوكسمبورغ بوصفه حالة قانونية، وتقرأ أوكرانيا وكشمير وسوريا والسودان وسفالبارد بوصفها حالات تكشف أنماطًا مختلفة من الفشل أو الاسترداد. ثم تربط هذه المقارنة بأدبيات التعافي، والفشل النمطي المشترك، وتقاسم الأسرار، وسلامة السجلات، والضوابط السعودية لنقل البيانات والحوسبة السحابية. [1] [16]

النتيجة التحليلية هي إطار اختبار، لا نتيجة تجربة: ينبغي تقييم أي نموذج سعودي على استقلال نقاط الفشل، وإمكان تشغيل وظائف محددة ضمن هدف زمن الاسترداد وهدف نقطة الاسترداد، وصحة التفويض، وقابلية التحقق من سلسلة المنشأ، والامتثال النظامي، والقدرة على تغيير المضيف والموارد والخوارزمية. ولا تدعي الورقة أن الاستضافة الخارجية لازمة لكل وظيفة أو جائزة نظامًا لكل فئة من البيانات.

سؤال البحث وحدوده

السؤال الرئيس هو: تحت أي شروط قانونية وتقنية وتشغيلية يمكن لترتيب متعدد المواقع، وبعضه خارج المملكة، أن يقلل احتمال فقد قدرة الدولة السعودية على إثبات الحقوق وتشغيل وظائف سيادية محددة عند تعطل مواقع أو شبكات أو سلطات إدارية؟

يتفرع منه أربعة أسئلة: ما الذي تضيفه الحماية القانونية فوق عقد الاستضافة؟ ما الحد الأدنى الذي يجب أن ينتقل مع البيانات حتى تصبح قابلة للتشغيل؟ كيف توزع المفاتيح والنسخ من دون أن تنشأ سلطة خارجية منفردة؟ وكيف تُختبر الفائدة والمخاطر قبل استعمال بيانات حساسة؟

لا تقيم الورقة مشروعية مشروع بعينه، لأن ذلك يتطلب معرفة فئة البيانات وغرض المعالجة وبنية التشغيل والدول المضيفة والجهات المختصة. ولا تقدم تقديرًا كمياً لاحتمالات الحرب أو أثرًا ماليًا متنبأ به، ولا تدعي إثبات علاقة سببية بين سفارات البيانات واستقرار الأسواق.

المنهج الوثائقي واختيار الحالات

يعتمد التحليل على مصادر أولية أو قريبة من الواقعة حيث أمكن: النص الرسمي لاتفاق إستونيا ولوكسمبورغ؛ إفادات حكومية وقضائية عن أوكرانيا وكشمير؛ مصادر حقوقية وإنسانية عن سوريا والسودان؛ توثيق مستودع سفالبارد؛ اللوائح والضوابط السعودية؛ والمصادر الأصلية أو المعيارية لشامير وNIST. تُعامل الأخبار والتصريحات بوصفها نوافذ محدودة، ولا تُرفع إلى مرتبة تحقق مستقل حين لا تكون كذلك.

اختيرت الحالات بحسب الوظيفة التحليلية، لا بقصد الادعاء أنها متكافئة. تقدم إستونيا أداة قانونية للاستضافة؛ وتقدم أوكرانيا مثالاً على بقاء سجلات حرجة بعد ضرب موقع؛ وتظهر كشمير وسوريا أثر فقد السجل على الحق؛ ويكشف السودان انفصال حفظ البيانات عن الاتصال؛ وتوضح سفالبارد معنى استعادة القدرة لا حفظ النسخة. [1] [2] [3] [4] [5] [6] [7] [8] [9]

تُقارن الحالات عبر ستة أبعاد: نوع الأصل المحمي، ونوع التهديد، واستقلال الموقع، وإمكان الاسترداد والتشغيل، وسلطة إصدار أمر الاسترداد، وحدود الدليل المتاح. لا تسمح هذه الطريقة بتعميم إحصائي، لكنها تكشف شروطًا ينبغي تحويلها إلى فرضيات واختبارات في نموذج أولي.

التعريفات التشغيلية

سفارة البيانات (Data Embassy) في هذه الورقة موقع استضافة خارجي لبيانات وأنظمة حكومية يتمتع بوضع قانوني محدد باتفاق بين الدولتين؛ ولا يعني نقل الإقليم أو حصانة دبلوماسية تلقائية. أما الاستمرارية السيادية فهي قدرة الدولة على إبقاء وظائف عامة مختارة قابلة للتشغيل والتحقق تحت تعطلات جسيمة مع بقاء القرار القانوني والتحكم النهائي لديها.

التعافي من الكوارث (Disaster Recovery) يعيد موردًا تقنيًا بعد الانقطاع؛ واستمرارية الحكومة (Continuity of Government) تبقي وظائف الحكم الجوهرية خلال الانقطاع أو تعيدها ضمن حدود مقبولة. لذلك قد ينجح الاسترداد التقني ويفشل الأثر العام إذا عاد النظام بعد انتهاء المدة التي يحتملها الحق أو الخدمة.

سلسلة المنشأ (Provenance) هي القدرة على تتبع أصل البيانات ومسار تعديلها والسلطة التي أجازت التغيير. وسلامة البيانات (Integrity) تعني كشف التغيير غير المصرح به، ولا تثبت وحدها أن الإدخال الأول صحيح. والفشل النمطي المشترك (Common-Mode Failure) هو سقوط حلول متكررة بسبب علة مشتركة؛ وهو ما يجعل التنوع الحقيقي أهم من التوزيع الجغرافي الشكلي.^[10]

المقارنة: حالات ودروس

تكشف الحالة الإستونية أن القيمة القانونية لا تنبع من الاسم، بل من نص يحدد حرمة الموقع والدخول والاتصالات والقانون الواجب التطبيق والنزاع والإنهاء والتسليم. ويؤكد النص أن اتفاقية فيينا غير كافية وحدها. والاتفاق لا يحول الموقع إلى أرض إستونية؛ إنه ينشئ حماية تعاقدية دولية ذات حدود معلومة.^[1]

تقدم الإفادة الرسمية الأوكرانية مثالاً على أن توزيع السجلات وتهئية موارد بديلة قبل اكتمال الخطر قد يمنع ضربة مادية من إيقاف سجل حرج، من دون أن تكون تدقيقاً مستقلاً لتوافر كل نظام. وتكشف كشمير وسوريا أن فقد الوثيقة يضعف قابلية إثبات الحق حتى حين تبقى الدعوى القانونية نظرياً. ويكشف السودان أن سلامة الأرشيف لا توفر الخدمة إذا انقطعت الاتصالات أو الهوية أو وسائل الدفع.^{[3] [4] [5] [6] [7]}

وتقدم سفالبارد مقياساً مفاهيمياً: نجاح الحفظ عندما استُخرجت العينات وزُرعت وأُكثرت وأُعيد إبداعها. وبالمقياس التحليلي، لا تعد نسخة الوزارة قدرة مستمرة حتى يمكن تشغيل البرمجيات والتحقق من الهوية والتوقيع واستعمال السجل ضمن إجراء مخول. القياس لا يجعل البذور والبيانات شيئاً واحداً؛ إنه يوضح معيار الاستعادة الوظيفية.^[8]

الإطار القانوني: حماية محددة لا فراغ سيادي

يمنح اتفاق إستونيا ولوكسمبورغ المكان حرمة من التفتيش والحجز والتنفيذ، ويشترط موافقة ممثل إستونيا على الدخول. ولا تفترض الموافقة في الطوارئ إلا لحماية فورية من خطر على السلامة. وتعامل المادة السادسة البيانات والأنظمة كأرشيف إستوني، وتحمي الاتصالات الرسمية وتتيح التشفير. لكن المادة الثامنة تُبقي القانون الدولي وقانون الاتحاد الأوروبي وقانون لوكسمبورغ حيث ينطبق، وتنظم التحكيم.^[1]

تجعل المادة العاشرة الإنهاء نافذًا بعد أربعة وعشرين شهرًا من الإخطار، وتفصل تسليم الأصول إلى الممثل المأذون عن حالة تعذر تحديده، حين تُحمى الأصول ولا تسلم إلا إلى ممثل قانوني. هذه الأحكام مهمة لأنها تحدد مصير الأرشيف عند تدهور العلاقة أو إشكال التمثيل بدل تركه لتقدير مشغل مركز البيانات.^[1]

في السياق السعودي، تخضع البيانات الشخصية المنقولة إلى الخارج لشروط تشمل الأمن الوطني والمصالح الحيوية والحد الأدنى اللازم والحماية وحقوق الأفراد وتقييم الملاءمة أو الضمانات والحالات المحددة. الاتفاق الدولي مسار محتمل ضمن إجراءات الجهة المختصة، لا موافقة تلقائية. وضوابط الأمن السيبراني للحوسبة السحابية، (Cloud Cybersecurity Controls) (CCC) إطار أمني ضمن نطاقه، وليست بديلًا عن نظام حماية البيانات أو تصنيف المعلومات والاشتراطات القطاعية.^[14]^[15]

الإطار التقني: توزيع البيانات والسلطة

يلزم الفصل بين ثلاث تقنيات: التشفير الموثق (Authenticated Encryption)، وترميز المحو (Erasure Coding)، والتشفير ذو العتبة (Threshold Cryptography). يحمي الأول السرية ويكشف العبث، ويوزع الثاني الأجزاء لتوفير المحتوى رغم الفقد، ويوزع الثالث سلطة المفاتيح أو العمليات. الخلط بينها يجعل وجود إحدى الطبقات يبدو علاجًا لوظائف لا تؤديها.

يعطي تقاسم السر لشامير (Shamir's Secret Sharing) ضمانًا حديًا: في التنفيذ الرياضي الصحيح تستعيد العتبة السر ولا تكشف مجموعة دونها معلومة عنه. مثال ثلاث من خمس يبين تحمل فقد حصتين، لكنه لا يثبت توافر البيانات أو صحة التفويض أو أمن الحواسيب التي تحمل الحصص. يلزم استقلال الأمناء، وحماية الحصص، وتدويرها، ومراقبتها، واختبار استبدال أمين متعذر أو غير موثوق.^[11]

وقد تسمح الحوسبة متعددة الأطراف (Multi-Party Computation) والتوقيعات ذات العتبة (Threshold Signatures) بعمليات لا تجمع المفتاح كاملاً في موضع واحد، مع وحدات أمن عتادية (Hardware Security Modules, HSMs). لكن التعقيد البروتوكولي يزداد عبء التدقيق والاستجابة للحوادث. المعيار ليس حداثة التقنية، بل خفضها خطرًا محددًا مع إمكان تشغيلها في أسوأ ظروف المؤسسة.

سلامة السجل وصحة الواقعة وسلطة التعديل

يمكن لبصمة تشفيرية (Cryptographic Hash) أو شجرة ميركل (Merkle Tree) أو سجل كاشف للعبث (Tamper-Evident Log) أن يثبت أن نسخة مرتبطة ببصمة موثقة لم تتغير دون كشف. وتصف وثائق البنية التحتية للتوقيع عديم المفاتيح (Keyless Signature Infrastructure, KSI) إمكان التحقق من وقت التوقيع وسلامة البيانات وترتيبها وبصمة المدخل. مصدر هذا الوصف هو مزود التقنية، ولذلك لا يُعامل كتحقق مستقل من كل ادعاء تسويقي.^[12]

ولا يثبت دليل السلامة أن الواقعة الأصلية صحيحة، أو أن الموظف الذي أدخلها كان مخولاً، أو أن تعديلاً قانونياً لم يُمنع خطأ. يجب تصميم ثلاث طبقات مترابطة: صحة الإدخال عبر إجراءات العمل والأدلة؛ وسلامة النسخة عبر التشفير والسجلات؛ وسلطة التعديل عبر الهوية والتوقيع والمراجعة القانونية.

تعطي سلسلة المنشأ قيمة عملية حين تسمح بتحديد النسخة المعروفة السلامة، ومن عدّ لها، وبأي صلاحية، وما الذي يجب التراجع عنه. وهي تصبح أكثر أهمية مع تسميم البيانات (Data Poisoning) وانتحال الهوية والأتمتة التي قد تنشر التغيير الخطأ بسرعة إلى النسخ كلها.

نموذج السلطة في الطوارئ

يجب ألا تتطابق القدرة التقنية على الاسترداد مع السلطة القانونية لإصداره. يقترح الإطار أربع وظائف منفصلة: صاحب الصلاحية القانونية الذي يقرر؛ وأمناء حصص المفاتيح الذين ينفذون ضمن عتبة؛ ومشغل البيئة البديلة؛ ومدقق مستقل يتحقق من الطلب والسجل والنتيجة.

يحتاج النموذج إلى حالات طوارئ معرفة مسبقاً، وترتيب خلافة، وقنوات اعتراض، وسياسة لتعارض الأوامر، وسجل قرارات لا يستطيع طرف واحد محوه. كما يحتاج إلى طريقة لإثبات هوية صاحب الطلب إذا تعطل مزود الهوية الأساسي، وإلى اختبارات تشمل غياب مسؤول أو انقسام الاتصال بين الجهات.

لا ينبغي للمضيف الأجنبي أو المورد التجاري أن يحسم نزاعاً دستورياً. الاتفاق والعقد والبروتوكول التقني يجب أن تحدد جميعاً ما يستطيع المضيف فعله وما يُمنع عنه، وكيف يحفظ الأصول عند تعذر تحديد الممثل، وكيف تُنقل إلى مضيف بديل.

مصفوفة المخاطر المقترحة

تصف المصفوفة المخاطر على محورين: احتمال تحقق العلة، وأثرها في الوظيفة السيادية. وتشمل فئات الخطر المادي، والسيبراني، والتشغيلي، والقانوني، والسياسي، وخطر المورد، وخطر السلطة الداخلية. ويُسجل لكل خطر الأصل المتأثر، ونقطة الفشل المشتركة، وإجراء المنع، وإجراء الكشف، ومسار الاسترداد، والدليل المطلوب لإغلاق الاختبار.

أمثلة السيناريوهات: فقد موقعين؛ انقطاع مسار اتصال دولي؛ حظر قانوني مفاجئ في دولة مضيضة؛ تعطل واجهة إدارة مشتركة؛ سرقة حصة مفتاح؛ حذف مشروع لكنه خاطئ ينتشر بالمزامنة؛ تعارض طلبات الاسترداد؛ وعجز عن تحديث خوارزمية تشفير. قد يكون احتمال بعض السيناريوهات منخفضاً، لكن أثرها مرتفع بما يبرر تمريناً أو تصميمًا مضاداً.

ينبغي أن تظهر المصفوفة المخاطر المتبقية بعد الضوابط، لأن تحول كل خانة إلى اللون الأخضر. كما يجب أن تفرق بين خطر فقد السرية وخطر فقد التوافر وخطر فساد الدليل وخطر استعمال صلاحية صحيحة لغرض غير مشروع. معالجة أحدها قد تزيد الآخر؛ ورفع العتبة قد يحسن مقاومة الاستيلاء ويبطئ الاسترداد.

فرضيات تحليلية للاختبار

تقترح الورقة فرضية أولى: لا يخفض التوزيع الجغرافي زمن التعطل إلا إذا امتد إلى اعتماديات التشغيل، ومنها الهوية والمفاتيح والإدارة والاتصال. يمكن اختبار ذلك بمقارنة استعادة موزعة المواقع لكنها موحدة الإدارة، باستعادة تستخدم مسار إدارة وهوية بديلين، مع تثبيت الوظيفة والبيانات قدر الإمكان.

والفرضية الثانية أن توزيع سلطة المفاتيح يقلل خطر الاستيلاء المنفرد، لكنه قد يرفع زمن الاسترداد ومعدل فشل الإجراء البشري. تُختبر بتغيير العتبة وعدد الأمناء وغياب بعضهم، وقياس زمن التفويض والأخطاء والطلبات المرفوضة. لا تُفترض أفضلية صيغة ثلاث من خمس؛ تختار النتيجة بعد نمذجة الخطر والتمرين.

والفرضية الثالثة أن نسخة ذات سلسلة منشأ قابلة للتحقق تقلل زمن اكتشاف النسخة السليمة بعد حادث عبث، بشرط أن تكون بصمات الثقة وسجلات السلطة مستقلة عن النظام المتضرر. أما الرابعة فتري أن التشغيل المتدهور المنضبط (Controlled Degraded Mode) يعيد ناتجاً عاماً نافعاً أسرع من استعادة النظام الكامل، من دون تجاوز حدود الحقوق، إذا حُدثت وظائفه مسبقاً وخضع كل استعمال للمراجعة.

هذه الفرضيات لا تحمل نتائج ضمنية. قد يكشف الاختبار أن التعقيد ألغى الفائدة، أو أن وظيفة محددة لا تتحمل الاستضافة الخارجية، أو أن مساراً وطنياً مستقلاً أقل كلفة وأكثر ثباتاً. قيمة النموذج الأولي أنه يسمح بهذه الإجابات قبل بناء اعتماد طويل الأجل.

إطار التقييم الاقتصادي

ينبغي أن يقارن التقييم بين تكلفة دورة الحياة وتكلفة الانقطاع، لا بين فاتورة التخزين وعدم الإنفاق. تشمل دورة الحياة الإنشاء والربط والاختبار والتدريب والتدقيق والعقود وتدوير المفاتيح وتغيير الخوارزميات والخروج من المورد. وتشمل تكلفة الانقطاع المعاملات المفقودة، والعمل اليدوي، وتأخر الحقوق، واستعادة الثقة، وآثار التعطل على جهات أخرى.

يمكن بناء خط أساس من حوادث واختبارات داخلية مجهلة، ثم قياس الفرق في زمن العودة ومقدار فقد البيانات وساعات العمل وكلفة التحويل إلى التشغيل البديل. ولا ينبغي تحويل حركة سوق أو حالة حرب واحدة إلى معامل مالي ثابت؛ أثر الاستمرارية يعتمد على الوظيفة ومدة الانقطاع ووجود البدائل وتوقعات الأطراف.

كما يجب تسعير خطر الارتهان للمورد والدولة المضيفة: ما تكلفة الانتقال إذا تغير القانون أو العقد؟ وما المدة اللازمة لاستخراج البيانات والمفاتيح والسجلات بصيغ قابلة للاستخدام؟ اختبار الخروج الدوري يقدم رقماً أدق من بند تعاقدى لم يُجرب، ويكشف إن كان التنوع المعلن قابلاً للتشغيل أم قائماً على الورق.

معايير تقييم قابلة للاختبار

المعيار الأول وظيفي: تُحدد لكل خدمة حرجة نتيجة دنيا يمكن للمواطن أو الجهة استعمالها، لا مجرد تشغيل خادم. والمقياسان الزمانيان هما هدف زمن الاسترداد (Recovery Time Objective, RTO)، أي أقصى زمن انقطاع قبل أثر غير مقبول، وهدف نقطة الاسترداد (Recovery Point Objective, RPO)، أي النقطة التي يمكن الرجوع إليها ومقدار فقد البيانات المقبول قياساً إلى أحدث نسخة.^[13]

المعيار الثاني هو الاستقلال: ينجح الاختبار مع فقد العدد المفترض من المواقع أو الأمناء، ومع تعطيل المورد أو الهوية أو مسار الاتصال المشترك. ويقاس الاستقلال بعدد الاعتماديات المشتركة المكتشفة، لا بعدد المدن على الخريطة. والمعيار الثالث سلامة الاستعادة: يجب اكتشاف نسخة مسممة أو غير مصرح بها قبل إعادة الخدمة وإثبات سلسلة المنشأ للنسخة المختارة.

المعيار الرابع صحة السلطة: لا ينفذ طلب ناقص العتبة أو صادر من جهة غير مخولة، ويعمل ترتيب الخلافة عند غياب مسؤول. والخامس قابلية الخروج: يمكن نقل البيانات والمفاتيح والبرمجيات وسجلات التدقيق إلى مضيف بديل ضمن زمن وكلفة معينين. والسادس الامتثال: يثبت التصنيف والغرض والأساس النظامي وتقليل البيانات وقرارات الجهات المختصة قبل إدخال بيانات فعلية. هذه مقاييس مقترحة؛ لا تدعي الورقة أنها اجتازت اختباراً لم يُنفذ.

تصميم نموذج أولي مرحلي

تبدأ المرحلة الأولى ببيانات تركيبية (Synthetic Data) وخدمة غير حساسة تحاكي بنية وظيفة حكومية حقيقية. يرسم الفريق سلسلة الاعتماد، ويحدد RTO وRPO، ثم يبني حفظاً مشفراً وبيئة تشغيل بديلة وآلية مفاتيح موزعة وسجل تدقيق. لا تستخدم بيانات شخصية فعلية لإثبات فكرة يمكن اختبارها من دونها.

في المرحلة الثانية تُجرى تمارين فشل مركبة تحت مراقبة مستقلة: فقد مواقع، وغياب أمناء، وقطع اتصال، ونسخة مسممة، وطلب غير مخول، وانتقال إلى مورد بديل. تُسجل الأزمنة والقرارات والفشل اليدوي ونقاط الاعتماد التي لم تظهر في الرسم النظري. ولا يعد نجاح استعادة واحدة دليلاً على الجاهزية الدائمة.

ولا تنتقل المرحلة إلى بيانات أو وظائف أعلى حساسية إلا بعد مراجعة قانونية وتقنية وخصوصية مستقلة، وإغلاق العيوب الجوهرية، وإثبات القدرة على الخروج. قد تكون النتيجة استبعاد الاستضافة الخارجية لفئة بعينها؛ وهذه نتيجة صحيحة إذا أنتجها الاختبار بدل أن يفرض الشعار نتيجته.

اعتبارات التنفيذ والحوكمة

تحتاج الحوكمة إلى مالك وظيفة، لا مالك تخزين فقط. فالجهة المسؤولة عن السجل تعرف أثر فقده، والجهة الرقمية تدير التكامل، والجهة السيبرانية تختبر الدفاع والاستجابة، والجهة التنظيمية تراجع النقل والخصوصية، والخارجية تفاوض الوضع القانوني. وينبغي أن تكون مسؤولية قبول الخطر مكتوبة لا موزعة حتى تختفي.

تحتاج العقود إلى حقوق تدقيق، وإخطار بالحوادث، وتحديد لمواقع المعالجة والمقاولين، وضمانات لإعادة الأصول وإتلاف النسخ، والتزام بالمساعدة في الانتقال. ويجب ألا يعتمد إثبات الامتثال على تقرير يقدمه المورد وحده. أما الاتفاق بين الدول فيعالج الدخول والحجز والاتصالات والقانون والنزاع والإنهاء والتمثيل.

تحتاج الأصول طويلة العمر إلى قابلية التغيير التشفيري (Cryptographic Agility): جرد للخوارزميات والشهادات والمفاتيح، وفصلها عن التطبيقات قدر الإمكان، وخطة لتدويرها وإعادة التشفير. اعتماد NIST لمعايير FIPS 203 و204 و205 في أغسطس 2024 لا يثبت انهيار التشفير الحالي، لكنه يوضح أن الانتقال الخوارزمي حدث تشغيلي ينبغي تصميم القدرة عليه قبل الحاجة.^[16]

القيود وعدم اليقين

تعتمد بعض الحالات على إفادات حكومية أو صحفية لا تكشف سجلات التشغيل كاملة. لا نعرف من المصادر المفتوحة كل تفاصيل قدرة أوكرانيا على الاسترداد، ولا الحالة الدقيقة لكل وثائق السودان، ولا أثر كل انقطاع على كل خدمة. لذلك تستخدم الوقائع في حدود ما تثبته، لا بوصفها تدقيقاً شاملاً.

المقارنة بين أرشيفات قانونية وبذور وأنظمة حكومية قياس وظيفي محدود، وليست مساواة مادية. كما أن نموذج شامير ضمان رياضي ضمن افتراضاته؛ لا يثبت أمن التنفيذ أو استقلال الأمناء. ووثائق KSI تصف خصائص منتج من مصدره، ولا تثبت صحة البيانات الأصلية أو انتشار الاستخدام في كل خدمة إستونية.

لا تتوافر في هذه الورقة بيانات تكلفة أو قياسات أداء أو تقييم امتثال لتطبيق سعودي. كما أن المخاطر الجيوسياسية والقانونية تتغير بمرور الزمن. أي قرار تنفيذي يحتاج دراسة تهديدات وتصنيف بيانات واختبارات وعقوداً واتفاقات ومراجعات مستقلة في وقت القرار.

ويظل اختيار الحالات عرضة لتحيز التوافر: الأحداث التي وثقتها الحكومات أو القضاء أو الإعلام أسهل في الدراسة من الأعطال التي عولجت داخلياً أو بقيت سرية. كما أن نجاحاً معلناً قد يخفي خدمات ثانوية تعطلت، وفشلاً موثقاً قد يعكس شفافية أعلى لا أداء أسوأ. لذلك لا تستخدم الورقة عدد الحالات لترتيب الدول أو تقدير معدل فشل، بل لاشتقاق أسئلة اختبار يمكن أن تكشف الخطر في بيئة سعودية محددة.

الخلاصة

سفارة البيانات أداة محتملة داخل معمارية أوسع، وليست المعمارية نفسها. تضيف الاتفاقات حماية قانونية لا يصنعها اسم تجاري، ويضيف التوزيع مقاومة لبعض الأعطال إذا كانت المواقع والإدارات والمفاتيح مستقلة بالفعل. لكن البيانات لا تصبح وظيفة عامة من دون البرمجيات والهوية والاتصال والتفويض.

الإطار السعودي القابل للدفاع هو إطار انتقائي ومختبر: يبدأ بالوظيفة، ويحدد ما يحتمل من توقف وفقد، ويفصل السلطة عن الحياة، ويعامل سلسلة المنشأ وصحة التفويض كجزء من الاسترداد، ويخضع النقل للأنظمة والجهات المختصة. وقد يختار الداخل لبعض الوظائف، والخارج المحمي لبعضها، وتوزيع المفاتيح أو الأدلة لبعضها الآخر.

القيمة الاستراتيجية ليست في عدد السفارات أو سعة التخزين، بل في إجابة قابلة للبرهنة عن سؤال واحد: بعد فقد مواقع واتصالات وأمناء، هل تستطيع الدولة أن تثبت الحق الصحيح وتشغل الحد الأدنى من الخدمة بقرار مشروع وفي الزمن الذي يحتمله المجتمع؟

بوابات الاستمرارية السيادية (Sovereign Continuity Gates)

4	3	2	1
استعادة مختبرة بسلسلة منشأ (Provenance) قابلة للتحقق	تفويض موزع بعتبة مشروعة (Threshold Authorization)	استقلال قانوني وتقني عن العلة المشتركة (Common-Mode Failure)	هدف زمن الاسترداد (Recovery Time Objective, RTO) وهدف نقطة الاسترداد (Recovery Point Objective, RPO)

لا ينتقل النموذج إلى بيانات فعلية قبل اجتياز البوابات الأربع: تعريف الوظيفة، وخفض الاعتماد المشترك، وصحة السلطة، وإثبات الاستعادة السليمة ضمن الزمن والفقد المقبولين.

المراجع

1. Agreement between Estonia and Luxembourg on the hosting of data and information systems
20 Riigi Teataja يونيو 2017
2. The Legal Status of Data Embassies
International and Comparative Law Quarterly, 01 يناير 2019
3. Ukraine's cybersecurity infrastructure protected state registers during the war
President of Ukraine, 06 سبتمبر 2022
4. Farooq Ahmad Dar v. State of Jammu and Kashmir
High Court of Jammu and Kashmir and Ladakh, 13 أبريل 2022
5. Q&A: Syria's New Property Law
Human Rights Watch, 29 مايو 2018
6. 30 million Sudanese historical documents at risk of deterioration
Asharq Al-Awsat, 26 يونيو 2026
7. Sudan telecommunications joint statement
Norwegian Refugee Council, 03 مايو 2024
8. ICARDA seeds safe back in Lebanon and Morocco
Svalbard Global Seed Vault, 27 أكتوبر 2017
9. Norges tilstedeværelse i Storbritannia under 2. verdenskrig
National Archives of Norway

<u>Engineering Trustworthy Secure Systems</u>	.10
	NIST, 01 مارس 2022
<u>How to Share a Secret</u>	.11
	Communications of the ACM, 01 نوفمبر 1979
<u>KSI Technology</u>	.12
	Guardtime
<u>Contingency Planning Guide for Federal Information Systems</u>	.13
	NIST, 01 مايو 2010
<u>Implementing Regulations for Personal Data Transfer outside the Kingdom</u>	.14
	SDAIA
<u>Cloud Cybersecurity Controls CCC-2:2024</u>	.15
	National Cybersecurity Authority
<u>NIST Releases First 3 Finalized Post-Quantum Encryption Standards</u>	.16
	NIST, 13 أغسطس 2024