الأمم المتحدة A/CN.9/WG.IV/WP.154

الجمعية العامة

Distr.: Limited
12 September 2018
Arabic
Original: English

لجنة الأمم المتحدة للقانون التجاري الدولي
الفريق العامل الرابع (المعني بالتجارة الإلكترونية)
الدورة السابعة والخمسون
فيينا، ١٩-٢٣ تشرين الثاني/نوفمبر ٢٠١٨

المسائل القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة

مذكِّرة من الأمانة

المحتويات

270918 270918 V.18-05924 (A)

أولاً- مقدِّمة

١- توضِّح هذه المذكرة جوانب معيَّنة لبعض المواضيع التي اعتبرها الفريق العامل مناسبة لنظره في المسائل القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة (A/CN.9/936، الفقرة ٥٨) من أجل تيسير المضي قدماً في مناقشتها. وهي تهدف على وجه الخصوص إلى تسليط الضوء على المسائل الرئيسية واقتراح حلول ممكنة بشأنها وهي لا تبغي الحد من إمكانية النظر في مواضيع إضافية أو بحث بعض المواضيع معاً، حسب الاقتضاء. وتوضح ورقة العمل A/CN.9/WG.IV/WP.153 جوانب معينة لمواضيع أخرى اعتبرها الفريق العامل ذات صلة بنظره في المسائل القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة.

٢- ويمكن الاطلاع على معلومات أساسية عن أعمال الفريق العامل بشأن المسائل القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة في الفقرات من ٦ إلى ١٧ من ورقة العمل A/CN.9/WG.IV/WP.152. ويمكن الاطلاع على قائمة بالوثائق الإضافية ذات الصلة في الفقرة ١٨ من ورقة العمل A/CN.9/WG.IV/WP.152.

ثانياً- مسائل مناسبة للأعمال المقبلة بشأن الجوانب القانونية لإدارة الهوية وخدمات توفير الثقة

ألف- التصديق على أهلية مقدِّمي خدمات إدارة الهوية وتوفير الثقة

٣- يمكن لعمليات التصديق، بما يشمل التصديق الذاتي والاعتماد والمراجعة المستقلة، أن تساعد مساعدة كبيرة في إشاعة الثقة بمقدِّمي خدمات إدارة الهوية وتوفير الثقة. وقد يتأثر اختيار الشكل الأنسب للتصديق بنوع الخدمات المقدَّمة والتكلفة ومستوى الضمان المطلوب.

٤- واللائحة التنظيمية لخدمات التحديد الإلكتروني للهوية وتوفير الثقة في المعاملات الإلكترونية في السوق الداخلية ("لائحة الخدمات الإلكترونية") تتوخى نظاماً شاملاً للإشراف والتصديق على خدمات توفير الثقة، حيث تنص في المادة ١٧ منها على أن تسمي الدول الأعضاء هيئات تكون مسؤولة عن القيام بمهام إشرافية منتظمة على مقدِّمي خدمات توفير الثقة المؤهلين ومهام عرضية على غيرهم من مقدِّمي خدمات توفير الثقة، أمَّا المادة ١٧ (٤)، فتورد قائمة بالمهام المحددة التي ينبغي للهيئة المشرفة القيام بها.

٥- ومما يجدر بالذكر أنَّ لائحة الخدمات الإلكترونية تجعل من وجود هيئة إشرافية ضرورة لاعتبار مقدِّم خدمات توفير الثقة مؤهلاً. وتوجب اللائحة بوجه خاص، في المادة ٢٠، أن يخضع مقدِّم خدمات توفير الثقة المؤهل لعملية مراجعة كل ٢٤ شهرا على الأقل تقوم بها جهة معنية بتقييم الامتثال وتقدم تلك الجهة بناء على ذلك تقريراً عن مدى امتثاله إلى هيئة الإشراف. والتقاعس عن الامتثال لطلبات هيئة الإشراف يمكن أن يؤدي إلى حرمان مقدِّم الخدمات نفسه أو بعض خدماته من صفة الأهلية.

٦- ولا تجيز لائحة الخدمات الإلكترونية بدورها إلاَّ لمقدِّمي خدمات توفير الثقة المؤهلين تقديم خدمات توفير الثقة المؤهلة التي ترتبط بآثار قانونية معينة، مثل افتراض الصحة، فاللائحة تنص مثلاً،

في المادة ٢٥ (٢) منها، على أنَّ للتوقيع الإلكتروني المؤهل أثراً قانونيًّا مكافئاً للتوقيع بخط اليد. والخلاصة، أنَّ وجود هيئة إشرافية يتيح توفير خدمات مؤهلة لتوفير الثقة ذات أثر قانوني.

٧- وفيما يتعلق بخدمات توفير الثقة، تعتبر المادة ١٠ (هـ) و(و) من لائحة الخدمات الإلكترونية وجود إجراءات للاعتماد والمراجعة والتصديق الذاتي عنصراً واحداً من العناصر التي يمكن أن تكون مناسبة لتقييم مدى إمكانية الوثوق بالنظم التي يستخدمها مقدِّم خدمات توفير الثقة. ومن هنا، يعتبر ذلك النهج أنَّ وجود هيئة إشرافية ومخططات للاعتماد مسألة اختيارية وأنَّ تقدير مدى أهمية ذلك الوجود مسألة تقديرية.

٨- والتصديق (بما في ذلك التصديق الذاتي) هو عنصر ضروري في نماذج الاعتراف القانوني المتبادل، التي تستخدم قوائم بالنظم الموثوقة (انظر A/CN.9/WG.IV/WP.153، الفقرات ٦١-٧٣ و٧٦-٧٩)، من أجل تقييم مخططات إدارة الهوية التي تستخدم معايير قائمة على النتائج. وقد يكون من الضروري إعداد مجموعة مسبَّقة من المواصفات الأساسية لكي تستخدم في هذا التقييم.

٩- ولعلَّ الفريق العامل يودُّ أن ينظر فيما إذا كان وجود إجراءات للتصديق، بما يشمل التصديق الذاتي والاعتماد والمراجعات المستقلة، ينبغي أن يقترن بآثار قانونية معينة، وأن يحدد تلك الآثار إذا ما رأى ذلك، أو أن يقوم بوضع قائمة تتضمن عناصر يمكن أن تكون مناسبة لتقييم مقدِّمي خدمات إدارة الهوية وتوفير الثقة من حيث إمكانية التعويل عليهم والوثوق بهم وغير ذلك من الصفات اللازمة لهم. ولعلَّ الفريق العامل يودُّ أيضاً خلال المداولات أن يشير إلى ما إذا كان ينبغي أن يكون استخدام التصديق، بما يشمل التصديق الذاتي والاعتماد والمراجعات المستقلة، إلزاميًّا أو اختياريًّا.

باء- مستويات الضمان

١- إدارة الهوية

١٠- مستوى الضمان هو مقياس لموثوقية عمليات تأكيد الهوية يستند إلى الإجراءات المستخدمة. وهناك تعاريف مختلفة لمستويات الضمان متاحة من كيانات عامة وخاصة. ويجري تحديث صيغة تلك المستويات بانتظام في ضوء التطورات الجارية في التكنولوجيا والعمليات التجارية. وفي ضوء اعتماد مبدأ الحياد التكنولوجي، لا تؤخذ في الاعتبار إلاَّ مستويات الضمان المحايدة تكنولوجيا في صياغتها.

١١- ويحدد المعهد الوطني للمعايير والتكنولوجيا بالولايات المتحدة الأمريكية ثلاثة مستويات مختلفة للضمان المتعلق بالهوية، هي فيما يلي: مستوى ضمان الهوية ومستوى ضمان أداة الاستيقان ومستوى ضمان الاتحاد.(١) ويشير مستوى ضمان الهوية إلى عملية تدقيق الهوية ويشير مستوى ضمان أداة الاستيقان إلى عملية الاستيقان ويشير مستوى ضمان الاتحاد إلى بروتوكول التأكيد المستخدم في البيئة الاتحادية لإبلاغ الطرف المعول بالاستيقان ومعلومات عن النعوت (عند الانطباق).

١٢- ويشير مستوى ضمان الهوية بشكل أدق إلى قوة عملية تدقيق الهوية من أجل تحديد هوية الفرد بشكل موثوق؛ أمَّا مستوى ضمان أداة الاستيقان فيشير إلى قوة عملية الاستيقان نفسها

(١) انظر: NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, section 2، على العنوان الإلكتروني: https://doi.org/10.6028/NIST.SP.800-63-3.

والربط بين أداة الاستيقان ومحدِّد معين لهوية الفرد؛ ويشير مستوى ضمان الاتحاد إلى قوة بروتوكول التأكيد الذي يستخدمه الاتحاد لإبلاغ الطرف المعول بالاستيقان ومعلومات عن النعوت في حال استخدام بنية هوية متحدة.(٢)

١٣- ولكل مستوى من مستويات ضمان الهوية درجة خاصة من القوة مشفوعة ببعض المقتضيات، ففي الدرجة الأولى من مستوى ضمان الهوية، على سبيل المثال، تكون النعوت، إن وجدت، مؤكدة ذاتيًّا أو ينبغي أن تعامل على هذا النحو، أمَّا في الدرجة الثانية من ذلك المستوى، فتلزم عملية تدقيق للهوية عن بعد أو تدقيق شخصي لها، كما تلزم عملية تحقق شخصي أو عن بعد من النعوت المحددة للهوية تستخدم على أقل تقدير إجراءات محددة. وأمَّا في الدرجة الثالثة من المستوى نفسه، فيلزم إجراء عملية تدقيق شخصي للهوية ويجب التحقق من صحة النعوت المحددة للهوية على يد مقدِّم خدمات تصديق مأذون له بذلك من خلال فحص الوثائق المادية وفقاً لإجراءات محددة.

١٤- وتنص المادة ٨ من لائحة الخدمات الإلكترونية على ثلاثة مستويات من الضمان لإدارة الهوية، هي منخفض وأساسي وعال، وكل منها مشفوع بمعايير خاصة، ويلاحظ على وجه الخصوص أنَّ مستوى الضمان "المنخفض" يوفر درجة محدودة من الثقة للهوية المدعاة أو المؤكَّدة للشخص، بينما يوفر المستوى "الأساسي" من الضمان درجة كبيرة من الثقة بالهوية المدعاة أو المؤكَّدة للشخص، أمَّا المستوى "العالي"، فيوفر درجة من الثقة بالهوية المدعاة أو المؤكَّدة للشخص أعلى مما يوفره مستوى الضمان "الأساسي".

١٥- وقد حدد قانون تنفيذي للائحة الخدمات الإلكترونية(٣) مواصفات تقنية وإجراءات دنيا لكي تستخدم في تحديد موثوقية ونوعية عمليات الالتحاق (الانتساب) وإدارة وسائل التحديد الإلكترونية للهوية والاستيقان وإدارة وتنظيم مقدِّمي خدمات إدارة الهوية عبر الحدود. وتلك المواصفات التقنية والإجراءات موصوفة بلغة محايدة تكنولوجيًّا.

١٦- وفي ضوء ما تقدَّم، لعلَّ الفريق العامل يودُّ أن ينظر فيما إذا كان ينبغي استخدام فكرة مستويات الضمان لأغراض الوفاء بالمتطلبات القانونية أو لتحديد الآثار القانونية. وإذا كان الأمر كذلك، فلعله أيضاً يودُّ أن يناقش بخاصة العلاقة بين مستويات الضمان من ناحية ومتطلبات الاعتراف القانوني وآلياته من ناحية أخرى. ولعلَّ الفريق العامل يودُّ أيضاً أن يناقش ما إذا كان عليه أن يدخل في نقاش حول ملامح مستويات الضمان وأن يحدد نطاق ذلك النقاش.

٢- خدمات توفير الثقة

١٧- من المسائل الجوهرية المتعلقة بخدمات توفير الثقة تحديد ما إذا كانت فكرة مستويات الضمان ينبغي أن تطبق أيضاً على تلك الخدمات. ويعترف عدد من القوانين الوطنية المتعلقة بالتوقيعات الإلكترونية بمستويين لهذه التوقيعات، أولهما يشمل جميع أشكال التوقيعات

(٢) انظر: NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, section 2.5، على الموقع الإلكتروني: https://doi.org/10.6028/NIST.SP.800-63-3.

(٣) اللائحة التنفيذية رقم ١٥٠٢/٢٠١٥ الصادرة عن المفوضية الأوروبية بتاريخ ٨ أيلول/سبتمبر ٢٠١٥ بشأن تحديد مواصفات تقنية وإجراءات دنيا من أجل مستويات ضمان وسائل التحديد الإلكتروني للهوية.

الإلكترونية، والثاني يعلق نتائج قانونية معينة، من قبيل افتراض منشأ التوقيع وسلامته، على التوقيعات الإلكترونية التي تفي ببعض المتطلبات. ويمكن أن يؤخذ هذا بمعنى استحداث مستويات مختلفة من الضمان بشأن التوقيعات الإلكترونية.

١٨- وفيما يتعلق بخدمات توفير الثقة، تقدم المادة ٢٤ (١) من لائحة الخدمات الإلكترونية مثالاً لاستخدام مستويات من الضمان في سياق تلبية أحد متطلبات تحديد الهوية من أجل إصدار شهادة مستوفية للشروط. ومن أجل الوفاء بشرط قيام مقدِّم مؤهل لخدمات توفير الثقة بالتحقق من هوية الشخص الذي يصدر له هذه الشهادة المستوفية للشروط، تجيز اللائحة على وجه خاص إجراء عملية التحقق هذه عن بعد باستخدام وسائل للتحديد الإلكتروني للهوية من مستوى الضمان "الأساسي" أو "العالي".

١٩- ولعلَّ الفريق العامل يودُّ أن ينظر فيما إذا كانت فكرة مستويات الضمان ينبغي أن تنطبق أيضاً على خدمات توفير الثقة، وأن يحدد الشكل اللازم إذا ما رأى ذلك.

جيم- المسؤولية

٢٠- قد يكون لنظام المسؤولية المنطبق تأثير كبير على الترويج لاستخدام إدارة الهوية وخدمات توفير الثقة للأغراض التجارية وغير التجارية على السواء، ويجدر بالملاحظة في هذا الصدد أنَّ سبل الانتصاف القانونية من الخطأ في تحديد الهوية في المعاملات التجارية متاحة بوجه عام، غير أنَّ الخطأ في نسب الهوية التأسيسية في المستندات الورقية قد لا تترتب عليه تبعة قانونية إذا كان القانون الوطني لا يُحمِّل الكيانات العمومية تبعات بشأن تلك الخدمة.

٢١- وقد حدد الفريق العامل بالفعل مسائل معينة ذات صلة بمناقشاته حول مسؤولية المشاركين في إدارة الهوية وخدمات توفير الثقة، أي الكيانات التي ينبغي تحميلها بالمسؤولية (المصْدِرون (جهات الإصدار) ومقدِّمو الخدمات والأطراف الأخرى)، مع الأخذ في الحسبان نظم المسؤولية الخاصة للكيانات العمومية؛ وإمكانية الحد من مسؤولية الأطراف الممتثلة للمقتضيات المحددة سلفا، والآليات القانونية المعنية بالحد من المسؤولية، مثل الإعفاء أو عكس عبء الإثبات؛ والاتفاقات التعاقدية على الحد من المسؤولية (A/CN.9/936، الفقرة ٨٥).

٢٢- وقد لا يسهل في بعض الحالات تحديد الجهة المسؤولة، مثلما هو الحال مع بيانات النعوت الموثوقة المقدَّمة من خدمات توفير الثقة، عند استخدام تكنولوجيا "الدفاتر الموزَّعة" في الختم الزمني (A/CN.9/936، الفقرة ٨٦). وقد تستخدم، في حالات أخرى، آلية للتأمين من أجل المعاملات التجارية يمكن في ظلها أن تدفع شركة التأمين تعويضاً عن الخطأ في استخدام مخطط التحديد الإلكتروني للهوية أو خدمات توفير الثقة. وتوجد آلية أخرى متاحة أيضاً تتوخى بطريقة مؤتمتة دفع تعويضات مقطوعة سلفا أو توقيع جزاءات محددة في حال استيفاء بعض الشروط.

١- إدارة الهوية

٢٣- تقضي المادة ٩ من لائحة الخدمات الإلكترونية بأن تُقدَّم، عند الإشعار بمخطط لإدارة الهوية، معلومات عن نظام المسؤولية المنطبق على مُصدر وسائل التحديد الإلكتروني للهوية والطرف الذي يسيِّر إجراءات الاستيقان.

٢٤- وتحمل المادة ١١ من لائحة الخدمات الإلكترونية الدولة العضو المقدِّمة للإشعار المسؤولية عن الأضرار التي تقع بسبب عدم وفائها بواجبها بشأن ضمان نسبة بيانات تحديد الهوية، التي تفرِّد كل شخص عن الآخر، إلى صاحبها بدقة وبشأن ضمان تيسير الاطلاع بالاتصال الحاسوبي المباشر على المعلومات المستخدمة في عملية الاستيقان من الهوية لتأكيد صحة بيانات تحديد هويته. كما أنها تحمل الطرف الذي يصدر وسائل للتحديد الإلكتروني للهوية (المصدر) المسؤولية عن الخسائر التي قد تنجم جراء عدم استخدامه وسائل للتحديد الإلكتروني لهوية كل شخص تفرد بيانات تحديد هويته عن غيره. وهي تحمِّل في نهاية المطاف الطرف الذي يسيِّر إجراءات الاستيقان المسؤولية عن عدم ضمان التطبيق الصحيح لإجراءات الاتصال الحاسوبي المباشر المستخدمة لتأكيد بيانات تحديد هوية الشخص.

٢٥- ولا تنطبق المادة ١١ من لائحة الخدمات الإلكترونية إلاَّ على المعاملات العابرة للحدود وتشترط أن يكون عدم الامتثال متعمداً أو ناتجاً عن الإهمال. وهي تطبق وفقاً لأحكام القانون الوطني المتعلقة بمسائل من قبيل تعريف الأضرار وتوزيع عبء الإثبات ودون مساس بأيِّ مسؤوليات إضافية ناشئة من القانون الوطني للأطراف المشاركة في المعاملات التي تستخدم نظام إدارة الهوية.

٢٦- وخلاصة القول إنَّ لائحة الخدمات الإلكترونية تقضي بمحاسبة المشاركين في مخطط إدارة الهوية عن عدم الوفاء ببعض الالتزامات المسماة إذا ما كان عدم الوفاء بها ناتج عن عمد أو إهمال وبشرط أن تكون المعاملة عابرة للحدود وعدم المساس بالمسؤوليات الإضافية الناشئة عن القانون الوطني.

٢٧- وتنص المادة ٢٨١ من القانون رقم ٢٠ لسنة ٢٠١٧ في بنن على محاسبة مشغل نظم إدارة الهوية عن الأضرار التي تلحق بمستخدمي مخططات إدارة الهوية إذا ما كانت ناشئة عن عمد أو إهمال.

٢٨- وتعفي المادة ١-٥٥٢ من قانون فيرجينيا للإدارة الإلكترونية للهوية مشغل إطار توفير الثقة في الهوية ومقدِّم خدمات الهوية من المسؤولية إذا ما التزما في إصدار مثبتات الهوية وإسناد نعوت الهوية وعلامات الثقة بها بمعايير إدارة الهوية التي يقرها وزير التكنولوجيا في كومنولث فيرجينيا وأيِّ اتفاق تعاقدي وأيِّ قواعد وسياسات محررة بشأن إطار توفير الثقة في الهوية الذي ينتمي إلى عضويته مقدِّم خدمات الهوية. وتُعرِّف المادة ١-٥٥٠ علامة الثقة بأنها شيء في صورة "ختم رسمي قابل للقراءة الآلية أو سمة استيقان أو شهادة أو رخصة أو شعار يمنحه مشغل خدمات توفير الثقة في الهوية لمقدِّمي خدمات الهوية المؤهلين المنتمين إلى إطاره الخاص بتوفير الثقة في الهوية للإقرار بأنَّ مقدِّم خدمات الهوية ممتثل للقواعد والسياسات المحررة لإطار توفير الثقة في الهوية".

٢٩- وخلاصة القول إنَّ قانون فيرجينيا للإدارة الإلكترونية للهوية يعفي من المسؤولية مشغلي أطر توفير الثقة في الهوية ومقدِّمي خدمات الهوية الممتثلين للمعايير التي تحددها هيئة عمومية والإقرارات التعاقدية وقواعد الاتحادات. ويجب التقيد بالمواصفات والمعايير الدنيا التي يحددها كومنولث فيرجينيا مع استخدام صلاحيات التصديق من جهة مستقلة من الأطراف الثالثة توفر استعراضات موضوعية ومتسقة وقابلة للمراجعة لمدى هذا التقيد بناء على معايير للتصديق محددة بدقة.(٤) ولا يسري هذا الإعفاء إذا ما ارتكب مشغل إطار توفير الثقة في الهوية أو مقدِّم خدمات الهوية فعلاً ما أو امتنع عن القيام بفعل ما نتيجة إهمال جسيم أو سوء سلوك متعمد.

٣٠- ولا تجيز المادة ١-٥٥٥ من قانون فيرجينيا للإدارة الإلكترونية للهوية تفسير أيِّ حكم في ذلك القانون أو أيِّ فعل أو إغفال لفعل على أنه بمثابة تنازل عن الحصانة السيادية لذلك الكيان العمومي.

٣١- ولعلَّ الفريق العامل يودُّ مناقشة مسألة تحديد ماهية الكائنات التي ينبغي إخضاعها للمساءلة والنظام الذي تجري مساءلتها وفقه وما إذا كان من الضروري استحداث نظام للمسؤولية خاص بالكيانات العمومية.

٣٢- ولعلَّ الفريق العامل يودُّ خلال مناقشة نظام المسؤولية أن ينظر فيما يلي: (أ) إمكانية الحد من مسؤولية الأطراف الممتثلة لمتطلبات محددة مسبقا كأن يكون ذلك مثلاً بالإعفاء أو بعكس عبء الإثبات؛ و(ب) ما إذا كان من الضروري ربط مستويات الضمان المختلفة بنظم مختلفة للمسؤولية؛ و(ج) إمكانية الحد من المسؤولية تعاقديًّا؛ و(د) ما إذا كان من الضروري النص على بيانات فوقية (وصفية) تصف نظام المسؤولية، بما يشمل أيَّ حد منها.

٢- خدمات توفير الثقة

٣٣- تجعل المادة ١٣ من لائحة الخدمات الإلكترونية مقدِّمي خدمات الثقة مسؤولين عما يتسببون فيه عن عمد أو إهمال من أضرار لأيِّ شخص طبيعي أو اعتباري نتيجة عدم الوفاء بالتزاماتهم المنصوص عليها في اللائحة، أي بعبارة أخرى أنَّ مقدِّم خدمات توفير الثقة الذي يفي بالتزاماته المنصوص عليها في اللائحة لا يعتبر مسؤولا.

٣٤- وعلاوةً على ذلك، تفترض المادة ١٣ افتراضاً قابلاً للدحض بشأن نية أو إهمال مقدِّم خدمات توفير الثقة المؤهل، بينما يقع عبء إثبات نية أو إهمال مقدِّم خدمات توفير الثقة غير المؤهل على الشخص الذي يدعي وقوع الضرر. ويهدف هذا الحكم إلى إشاعة الثقة بمقدِّم الخدمات المؤهل لدى مستعملي خدماته بالنظر إلى أنَّ هذا الافتراض ييسر التماس سبل الانتصاف في حالة وقوع الضرر. وتتيح المادة ١٣ في نهاية المطاف لمقدِّمي خدمات توفير الثقة إمكانية الحد من مسؤوليتهم بشرط إخطار مستهلكي خدماتهم مسبقا بتلك الحدود للمسؤولية وأن تعترف أطراف ثالثة بهذه الحدود.

(٤) Commonwealth of Virginia Identity Management Standards Advisory Council, *Guidance Document 5: Certification of Identity Trust Framework Operators* (draft), Section 7: Certification of Identity Trust Framework Operators.

٣٥- وتتضمن أحكام القانون النموذجي للتوقيعات الإلكترونية أحكاماً تعالج المسؤولية الناشئة من سلوك الموقِّع (المادة ٨) ومقدِّم خدمات التصديق (المادة ٩) والطرف المعوِّل (المادة ١١). وتحدد تلك الأحكام التزامات كل كيان يشارك في دورة حياة التوقيع الإلكتروني. ويتيح القانون لمقدِّمي خدمات التصديق إمكانية الحد من نطاق أو حجم مسؤوليتهم.

دال- آليات التعاون المؤسسي

٣٦- يمكن لآليات التعاون المؤسسي أن تساعد في تحقيق الاعتراف القانوني المتبادل وتوفير إمكانية التشغيل البيني لنظم إدارة الهوية وخدمات توفير الثقة. وقد يكون لهذه الآليات طابع الكيان الخاص أو العمومي.

٣٧- وتوفر المادة ١٢ من لائحة الخدمات الإلكترونية مثالاً لآليات التعاون المؤسسي حيث تشير إلى أنَّ على الدول الأعضاء أن تتعاون على تحقيق إمكانية التشغيل البيني لمخططات إدارة الهوية وتوفير الأمن لها. وقد يتألف هذا التعاون من تبادل للمعلومات والخبرات والممارسات الجيدة، ولا سيما فيما يتعلق بالمتطلبات التقنية لمستويات الضمان واستعراض مخططات إدارة الهوية من جانب الأقران وفحص التطورات ذات الصلة.

٣٨- ويوفر قانون تنفيذي للائحة الخدمات الإلكترونية[٥] تفاصيل إضافية عن تبادل المعلومات واستعراض الأقران، بما يشمل الإشارة إلى أنه لا يجوز للدول الأعضاء أن تقدم المعلومات المطلوبة إذا ما كان من شأن الكشف عنها المساس بمسائل تمس الأمن العام أو الأمن القومي أو الأسرار التجارية أو المهنية أو أسرار الشركات. كما أنه ينشئ شبكة تعاونية لتيسير ممارسة أنشطة التعاون. ومما يجدر بالذكر أيضاً أنَّ الإشعار باستعراض أيِّ مخطط لإدارة الهوية من جانب الأقران مسألة اختيارية، غير أنَّ محصلة هذه العملية يمكن أن توفر في الواقع العملي معلومات مهمة تتيح استبصار مدى إمكانية وفاء المخطط بالمعايير المطلوبة، ومن ثم، فهي خطوة مهمة في آلية الإشعار التي تكمن في صلب الهيكل المؤسسي للائحة الخدمات الإلكترونية.

٣٩- ويمكن تحقيق نوع مختلف من التعاون بين نظم إدارة الهوية من خلال اتحاد نظم إدارة الهوية، ويتيح ذلك النموذج، بأسلوب متفق عليه ويخضع لإدارة دقيقة، معلومات الهوية المحققة لدى أحد نظم إدارة الهوية إلى أطراف متعددين داخل نظام مختلف لإدارة الهوية يحتاجون تلك المعلومات من أجل أغراض مختلفة (انظر أيضاً الوثيقة A/CN.9/WG.IV/WP.153، الفقرة ٤٧). ويحقق اتحاد نظم إدارة الهوية إمكانية التشغيل البيني بين جميع المشاركين باستخدام إطار تقني وقانوني مشترك تحدده مجموعة من القواعد الخاصة بتلك النظم. ومن ثم، يمكن للاتحاد أن يساهم في زيادة عدد المستخدمين المشاركين والتطبيقات المشاركة وأن يحتوي التكاليف المتعلقة بإدارة الهوية. ورغم أنَّ هذه الاتحادات تنهض على اتفاقات تعاقدية، فإنَّ وجود أحكام تشريعية يمكن

(٥) قرار المفوضية التنفيذي ٢٩٦/٢٠١٥ المؤرخ ٢٤ شباط/فبراير ٢٠١٥ بشأن تحديد ترتيبات إجرائية للتعاون بين الدول الأعضاء في مجال التحديد الإلكتروني للهوية.

أن يساهم في تعزيز تلك الاتحادات (انظر، على سبيل المثال، استخدام علامات الثقة في قانون فيرجينيا للإدارة الإلكترونية للهوية في الفقرة ٢٨ أعلاه).

هاء- الشفافية

٤٠- اعتبر الفريق العامل أنَّ لمبدأ الشفافية أهمية في مناقشاته المقبلة بشأن إدارة الهوية وخدمات توفير الثقة (A/CN.9/936، الفقرة ٨). وسلط الضوء، في ذلك السياق، على واجبين متعلقين بذلك المبدأ، هما واجب الإفصاح عن خدمات إدارة الهوية وتوفير الثقة المقدَّمة ونوعيتها؛ وواجب الإبلاغ عن الخروقات الأمنية.

٤١- وفيما يتعلق بالخدمات المقدَّمة ونوعيتها، يجدر بالملاحظة أنَّ مقدِّمي خدمات الهوية وتوفير الثقة المشاركين في الاتحادات أو الذين يحصلون على تصديق على خدماتهم بشكل آخر يفصحون عن قدر كبير من المعلومات. ويمكن تحديد واجبات دنيا للإفصاح من أجل مقدِّمي الخدمات الآخرين، فالمادة ٩ (١) من القانون النموذجي للتوقيعات الإلكترونية تتضمن مثلاً قائمة بالمعلومات التي ينبغي لمقدِّمي خدمات التصديق الإفصاح عنها للأطراف المعولة.

٤٢- وفيما يتعلق بواجب الإبلاغ عن الخروقات الأمنية، أُشير إلى أنَّ الإبلاغ عن الخروقات الأمنية يتضمن عناصر مشتركة مع الإبلاغ عن انتهاك سرية البيانات، وإن كانت توجد بينهما أيضاً اختلافات كبيرة. وأُشير إلى وجود أمثلة مفيدة لآليات تتجاوز مهامها مجرد الإبلاغ في حال حدوث خروقات أمنية (A/CN.9/936، الفقرة ٨٩). ولعلَّ من الاعتبارات الإضافية في هذا الشأن إمكانية استخدام المعلومات الاستخبارية المتعلقة بالتهديدات السيبرانية من أجل التخفيف من المخاطر.

٤٣- وتوجب المادة ١٠ من لائحة الخدمات الإلكترونية على الدول الأعضاء الإبلاغ عن الخروقات أو الانتهاكات التي قد تؤثر على مخطط الاستيقان عبر الحدود. وينبغي للدولة العضو المعنية أيضاً أن تبادر دون إبطاء إلى تعليق أو رفض عملية الاستيقان المنتهكة أو أجزائها التي تعرضت للانتهاك.

٤٤- وتلزم المادة ١٩ (٢) من لائحة الخدمات الإلكترونية مقدِّمي خدمات توفير الثقة بالمثل بإبلاغ الجهات المشرفة عليهم وأيِّ هيئات أخرى معنية، مثل الجهات المعنية بحماية البيانات، بأيِّ خرق أمني أو مساس بسلامة النظام من شأنه أن يؤثر تأثيرا خطيرا على خدمات توفير الثقة المقدَّمة أو على البيانات الشخصية الموجودة بها. وينبغي الإبلاغ عن هذه الحوادث دون تأخير لا مبرر له وبما لا يتجاوز بأيِّ حال ٢٤ ساعة من وقت العلم بوقوعها.

٤٥- وتوفر المادة ٨ (١) (ب) من القانون النموذجي للتوقيعات الإلكترونية آلية اختيارية للإبلاغ يمكن للموقع استخدامها في حال المساس بسرية البيانات المنشئة لتوقيعه أو وجود احتمالات كبيرة بوقوع ذلك.

٤٦- ومن الصيغ الممكنة للإلزام بالإبلاغ عن الخروقات الأمنية ما يلي:

> على مقدِّمي خدمات الهوية وخدمات توفير الثقة، بمجرد علمهم بوقوع أيِّ خرق أمني أو مساس بسلامة النظام من شأنه أن يؤثر تأثيراً [كبيراً] على الخدمات أو مثبتات الهوية

أو عمليات الاستيقان المقدَّمة أو على البيانات الشخصية المحفوظة فيها، أن يبلغوا [جهة الإشراف][الأشخاص المضارين من الزبائن والأطراف المعوِّلة] بذلك دون أيِّ تأخير [وبما لا يتجاوز بأيِّ حال من الأحوال ... يوما من تاريخ علمه بذلك].

ويعلق مقدِّم خدمات الهوية وتوفير الثقة الخدمات المتأثرة [حتى ...] إذا كان الخرق الأمني أو المساس بسلامة النظام كبيراً.

وعلى مستعمل خدمات الهوية وتوفير الثقة أن يبلغ مقدِّم الخدمات في حال علمه بالمساس بسرية مثبتات هويته أو عمليات الاستيقان أو بيانات إنشاء خدمة توفير الثقة أو عندما توحي الملابسات المعروفة له بوجود احتمالات كبيرة بالمساس بسرية مثبتات هويته أو عمليات الاستيقان أو بيانات إنشاء خدمة توفير الثقة.

٤٧- ويتضمن مشروع الحكم عبارات اختيارية لوضع حدود زمنية يتعين الإبلاغ خلالها وتحديد الأطراف التي يجب إبلاغها وتحديد مستوى الأثر على الخدمات أو مثبتات الهوية أو البيانات الشخصية الذي يصبح عنده الإبلاغ واجباً. ومن الممكن أيضاً النص على وجوب تعليق نظام إدارة الهوية وخدمات توفير الثقة إلى حين احتواء الخرق أو المساس بالسلامة، أو يمكن بدلاً من ذلك النص على إخضاع النظام لعملية تصديق جديدة أو لإجراء مماثل.

واو- الاحتفاظ بالبيانات

٤٨- سبق أن شدد الفريق العامل على أهمية الاتساق بين نظم الاحتفاظ بالبيانات وإمكانية تشغيلها تشغيلا بينيًّا (A/CN.9/936، الفقرة ٩١). وسلط الضوء آنذاك على ملمحين على الأقل لهذا الموضوع يمكن أن تكون لهما أهمية في ذلك الشأن، أولهما متعلق بحماية البيانات والثاني يشير إلى تخزين البيانات وأرشفتها.

٤٩- وحماية البيانات موضوع قد يثير مسائل معقدة بشدة. وتماشيا مع حرص الأونسيترال على ألاَّ تمس نصوصها التمكينية في مجال التجارة الإلكترونية بالقوانين الموضوعية كمبدأ عام لها (انظر الوثيقة A/CN.9/WG.IV/WP.153، الفقرة ٤٨)، لعلَّ الفريق العامل يودُّ أن يؤكد أنَّ القوانين المتعلقة بحماية البيانات والمسائل ذات الصلة، مثل الخصوصية، ينبغي أن تظل واجبة التطبيق بأكملها وأن ينظر فيما إذا كان من المفيد إضافة أيِّ مواصفات أو إيضاحات أخرى.

٥٠- وتخزين الوثائق وأرشفتها مسألة يمكن القيام بها باستخدام وسائل إلكترونية، كما سبق أن أشارت المادة ١٠ من القانون النموذجي للتجارة الإلكترونية، التي تحدد متطلبات التكافؤ الوظيفي بين رسائل البيانات والوثائق الورقية فيما يتعلق بالاحتفاظ بها. وتنشأ الالتزامات بحفظ الوثائق من القانون الموضوعي وهي متصلة بالوقت اللازم لاستنفاد مختلف الإجراءات.

٥١- ويمكن أن يكون توفير خدمات تخزين البيانات وأرشفتها موضوعا لخدمة مخصصة لذلك الغرض من خدمات توفير الثقة (انظر أدناه الفقرتين ٦٤ و٦٥). ولعلَّ الفريق العامل يودُّ أن يناقش في إطار بحث إطار التشغيل البيني لخدمات توفير الثقة المسائل المتعلقة بإمكانية نقل الخدمات الإلكترونية.

زاي- الإشراف على مقدِّمي الخدمات

٥٢- في حال ما إذا رأى الفريق العامل أنَّ من المناسب معالجة مخططات إدارة الهوية ونظم خدمات توفير الثقة بدلا من المعاملات ذات الصلة (انظر الوثيقة A/CN.9/WG.IV/WP.153، الفقرات ٥٧-٥٩)، فقد يكون من المفيد أو حتى من الضروري إنشاء هيئة إشرافية من أجل إشاعة الثقة في مقدِّمي الخدمات وفي الخدمات التي يقدمونها. غير أنَّ إنشاء هيئة من هذا القبيل قد تترتب عليه عدة تبعات إدارية ومالية. وقد تساعد بعض الآليات البديلة أو المكملة في هذا الشأن، مثل التصديق من طرف ثالث، على تحقيق الغايات المنشودة من مقدِّمي خدمات الإشراف مع الوفر في التكاليف ذات الصلة.

٥٣- ويحدد القانون في ولايتي فيرجينيا وفيرمونت سلطة تشرف على مقدِّمي خدمات الهوية للهيئات العمومية. كما أنَّ المادة ٩٧ من القانون رقم ٧ لسنة ٢٠١٧ في توغو تعهد إلى هيئة التصديق الوطنية بوظائف إشرافية على مقدِّمي خدمات توفير الثقة. ووفقاً للمادة ٢٨٣ من القانون رقم ٢٠ لسنة ٢٠١٧ في بنن، تعين سلطة عمومية مقدِّمي خدمات الهوية. وآلية الإشراف على خدمات إدارة الهوية وتوفير خدمات الهوية محددة ضمنا أيضاً في مخطط الإشعار الذي تنص عليه لائحة الخدمات الإلكترونية.

٥٤- وفيما يتعلق بمقدِّمي خدمات توفير الثقة، يعطي عدد من القوانين هيئة إشرافية الصلاحية لمنح صفة الأهلية أو للإشراف على كيفية قيام الجهات من الأطراف الثالثة بمنح تلك الصفة. وتنص لائحة الخدمات الإلكترونية على أن تعين الدول الأعضاء هيئة وطنية مختصة للإشراف على مقدِّمي خدمات توفير الثقة.

٥٥- ويشير القانون النموذجي للتوقيعات الإلكترونية إلى الهيئات الإشرافية باعتبارها خيارا في ضوء مبدأ الحياد الذي ينتهجه إزاء النماذج المختلفة، ذلك أنَّ إدراج حكم ملزم بإنشاء هيئات إشرافية يمكن أن يُفهم على أنه يمنع من الأخذ بنموذج سوقي قائم على التنظيم الذاتي لهيئات توفير الثقة.

حاء- مسائل محددة بشأن خدمات توفير الثقة

٥٦- تتصل معالجة المسائل القانونية المتعلقة بخدمات توفير الثقة اتصالاً وثيقاً بالمسائل القانونية المتعلقة بإدارة الهوية. ولذا سيقت تعليقات على خدمات توفير الثقة في سياق مناقشة المسائل المتعلقة بمبدأ التكافؤ الوظيفي (A/CN.9/WG.IV/WP.153، الفقرتان ٣٦ و٣٧)، والاعتراف القانوني (A/CN.9/WG.IV/WP.153، الفقرات ٩٣-٩٨)، ومستويات الضمان (الفقرات ١٧-١٩ أعلاه)، والمسؤولية (الفقرات ٣٣-٣٥ أعلاه) في إطار إدارة الهوية.

٥٧- غير أنَّ المعالجة القانونية لخدمات توفير الثقة قد تثير أيضاً تحديات خاصة. ومن المسائل الجوهرية في هذا الشأن اختلاف كل خدمة من خدمات توفير الثقة عن الأخرى، مما يجعلها تثير مجموعة مختلفة من المسائل التي يتعين النظر فيها. وهناك أيضاً تساؤل حول ما إذا كانت المعالجة القانونية لخدمات توفير الثقة سوف تتطلب النظر في إعداد قائمة مفتوحة بتلك الخدمات على

أساس تعريف مشترك لماهية ذلك النوع من الخدمات أو سوف تستلزم بدلا من ذلك تحديد قواعد عامة تنطبق على جميع خدمات توفير الثقة وقواعد محددة تنطبق على كل خدمة منها.

٥٨- وقد يكون من الممكن، بالإضافة إلى ذلك، الإشارة إلى أحكام للتكافؤ الوظيفي لوصف الوظائف الواجب النهوض بها لدى استخدام كل خدمة من خدمات توفير الثقة على نحو قريب من أحكام الأونسيترال بشأن التوقيعات الإلكترونية والاحتفاظ بالمستندات (انظر الوثيقة A/CN.9/WG.IV/WP.153، الفقرة ٣٦). ومما قد يساعد على النظر في هذا الاقتراح كثرة التشريعات القائمة في مجال التوقيعات الإلكترونية[٦] ووفرة الخبرات المكتسبة من تطبيقها.

٥٩- وتقدم لائحة الخدمات الإلكترونية نموذجا لتشريع شامل بشأن خدمات توفير الثقة. وهي تتضمن أحكاماً عامة عن بعض الجوانب، مثل المسؤولية وعبء الإثبات (المادة ١٣؛ انظر الفقرات ٢٣-٢٦ أعلاه)، والإشراف (المادة ١٧؛ انظر الفقرة ٥٣ أعلاه)، والمتطلبات الأمنية (المادة ١٩؛ انظر الفقرة ٤٤ أعلاه بشأن واجب الإبلاغ عن الخروقات الأمنية أو فقدان البيانات).

٦٠- وتتضمن لائحة الخدمات الإلكترونية بابا محددا منطبقا على جميع الخدمات المؤهلة لتوفير الثقة. ويمكن التعرف على الخدمات المؤهلة لتوفير الثقة بسبب إدراجها في قوائم النظم الموثوقة التي تتعهدها الدول الأعضاء في الاتحاد الأوروبي. ولعلَّ الفريق العامل يودُّ، في ذلك الصدد، أن ينظر فيما إذا كان من الضروري التمييز بين خدمات توفير الثقة بناء على مستوى الضمان المقترن بكل منها، وأن يحدد، في تلك الحالة، الآلية المؤسسية التي ينبغي أن تستخدم للتمييز بين خدمات توفير الثقة.

٦١- كما أنَّ لائحة الخدمات الإلكترونية تتضمن أحكاماً محددة بشأن خدمات توفير الثقة التالية: التوقيعات الإلكترونية؛ الأختام الإلكترونية؛ خدمات التوصيل المسجل الإلكتروني؛ الاستيقان من الموقع الشبكي.[٧] ويمكن توصيل كل خدمة من خدمات توفير الثقة باستخدام شكل يستوفي الشروط المطلوبة، كما يمكن توصيل التوقيعات الإلكترونية والأختام الإلكترونية باستخدام أشكال متقدمة.

٦٢- ويتضمن القانون رقم 045-2009/AN في بوركينا فاسو باباً بشأن الأحكام الواجبة التطبيق على جميع مقدِّمي خدمات توفير الثقة والأحكام المتعلقة بكيفية اعتماد خدماتهم، وهو أمر مهم لاعتبارهم مؤهلين للقيام بتلك الخدمات. كما يتضمن ذلك القانون أحكاماً معينة بشأن الشهادات الإلكترونية والأرشفة الإلكترونية والأختام الزمنية الإلكترونية وخدمات التوصيل المسجل الإلكتروني المستوفية للشروط. وهو يتضمن أيضاً فصلاً مخصَّصاً للتوقيعات الإلكترونية.

٦٣- ويتضمن القانون رقم ٢٠ لسنة ٢٠١٧ في بنن جزءاً عامًّا منطبقاً على جميع مقدِّمي خدمات توفير الثقة وأحكاماً محددة بشأن خدمات توفير الثقة التالية: التوقيعات الإلكترونية؛ الأختام الإلكترونية؛ الأختام الزمنية الإلكترونية؛ الأرشفة الإلكترونية.

---

(٦) يشير مَرْقَب الأونكتاد العالمي للقوانين السيبرانية إلى أنَّ ١٤٥ دولة، أو ٧٨ في المائة من مجموع الدول، قد اعتمدت قوانين بشأن المعاملات الإلكترونية تشمل بوجه عام أحكاما بشأن التوقيعات الإلكترونية.

(٧) يمكن الاطلاع على تعريف لخدمات توفير الثقة تلك في الوثيقة A/CN.9/WG.IV/WP.150.

٦٤- وتوضح المادة ٣٠١ من ذلك القانون أنَّ "الأرشفة الإلكترونية تكفل الاستيقان من الوثائق والبيانات والمعلومات المخزنة على ذلك النحو وتضمن سلامتها". ويتضمن القانون المذكور أيضاً حكماً بشأن التكافؤ الوظيفي مماثل للمادة ١٠ من القانون النموذجي للتجارة الإلكترونية.

٦٥- وتوضح المادة ٣٠٢ من القانون رقم ٢٠ لسنة ٢٠١٧ في بنن كذلك أنَّ الغرض من الأرشفة الإلكترونية هو المحافظة على الوثائق والبيانات والمعلومات من أجل استخدامها لاحقاً، وأنَّ البيانات ذات الصلة ينبغي هيكلتها وفهرستها وتخزينها على نحو يسمح بالمحافظة عليها ونقلها (انظر أيضاً الفقرة ٥١ أعلاه). وينبغي تيسير الوصول إلى البيانات بغض النظر عن مستوى التطور التكنولوجي. وينطبق هذا الحكم على الوثائق الإلكترونية المنشأ والوثائق الورقية المنشأ وصورها الرقمية اللاحقة.

٦٦- ويتضمن القانون رقم ٧ لسنة ٢٠١٧ في توغو أيضاً باباً للأحكام المنطبقة على مقدِّمي خدمات توفير الثقة، بما يشمل إجراءات الحصول على صفة مقدِّم خدمات مؤهل. كما ينص ذلك القانون على أحكام محددة بشأن الشهادات الإلكترونية والأرشفة الإلكترونية والأختام الزمنية الإلكترونية وخدمات التوصيل المسجل الإلكتروني. وهو يخصص فصلاً أيضاً للتوقيعات الإلكترونية.

٦٧- والمرسوم رقم 2018-062/PR في توغو يكمل قانونها رقم ٧ لسنة ٢٠١٧، ويحدد الواجبات المشتركة بين جميع مقدِّمي خدمات توفير الثقة، وتتصل هذه الواجبات بأمن البيانات وسريتها والمسؤولية والموارد المالية وإمكانية الوصول إلى البيانات وحماية البيانات والشفافية وإدارة المخاطر. وهو يتضمن، علاوة على ذلك، أحكاماً تتصل بكل خدمة من خدمات توفير الثقة يُعرِّفها القانون رقم ٧ لسنة ٢٠١٧.

٦٨- ومن الخدمات الإضافية في مجال توفير الثقة التي حدِّدت، ولكنها لم تعالج بعينها معالجة تشريعية، حسابات الضمان الإلكترونية والإثبات الإلكتروني للوجود، وهذا النوع الأخير من الخدمات خضع للمناقشة في سياق الوصايا الإلكترونية.(٨)

٦٩- ولعل الفريق العامل يودُّ النظر فيما إذا كان من الضروري استخدام آلية واحدة أو آليات مختلفة في المعالجة القانونية لموضوعي إدارة الهوية وخدمات توفير الثقة. ولعله يودُّ النظر كذلك فيما إذا كانت المعالجة القانونية لخدمات توفير الثقة تقتضي النظر في وضع قائمة مفتوحة لهذه الخدمات على أساس تعريف مشترك لماهية "خدمات توفير الثقة" أو تتطلب بدلا من ذلك وضع قواعد عامة منطبقة على جميع خدمات توفير الثقة وقواعد خاصة منطبقة على كل منها. ولعلَّ الفريق العامل يودُّ أيضاً أن ينظر فيما إذا كان من الضروري وضع قواعد للتكافؤ الوظيفي من أجل كل خدمة من خدمات توفير الثقة وما إذا كان ينبغي أيضاً الإشارة إلى مستويات للضمان في سياق خدمات توفير الثقة.

---

(٨) انظر، على سبيل المثال، المادة ٨ من مشروع قانون الوصايا الإلكترونية الذي أعده المؤتمر الوطني للمفوضين المعنيين بتوحيد قوانين الولايات.