

Distr.: General
3 May 2016
Arabic
Original: English



لجنة الأمم المتحدة للقانون التجاري الدولي
الفريق العامل الرابع (المعني بالتجارة الإلكترونية)
الدورة التاسعة والأربعون
نيويورك، ٢٧ حزيران/يونيه - ١٥ تموز/يوليه ٢٠١٦

المسائل القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة مذكّرة من الأمانة

المحتويات

الصفحة	الفقرات	
٢	٥-١	أولاً- مقدمة
٣	٥٥-٦	ثانياً- المسائل القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة
٣	٣٠-٦	ألف- البيئة القانونية الحالية لإدارة الهوية وخدمات توفير الثقة
٩	٤٣-٣١	باء- تعزيز الثقة في استخدام إدارة الهوية وخدمات توفير الثقة
١١	٥٥-٤٤	جيم- المسائل ذات الصلة بالأعمال المقبلة



أولاً - مقدمة

١ - طلبت اللجنة، في دورتها الثامنة والأربعين، في عام ٢٠١٥، إلى الأمانة أن تطلع بأعمال تحضيرية بشأن إدارة شؤون الهوية وخدمات توفير الثقة بوسائل منها تنظيم ندوات واجتماعات لأفرقة خبراء، وذلك حتى يتسنى مناقشة تلك المواضيع مستقبلاً على مستوى الأفرقة العاملة، إثر العمل الراهن بشأن السجلات الإلكترونية القابلة للتحويل على أساس اقتراح مقدم إلى اللجنة كي تنظر فيه (A/CN.9/854).^(١)

٢ - وخلال الدورة، طلبت اللجنة إلى الأمانة أيضاً أن تعرض على الفريق العامل الرابع نتائج تلك الأعمال التحضيرية التماساً لتوصيات بشأن تحديد النطاق الدقيق للعمل ومنهجيته الممكنة وأولوياته لكي تنظر فيها اللجنة في دورتها التاسعة والأربعين.^(٢)

٣ - وتنفيذاً لذلك الطلب، نُظمت ندوة الأونسيترال بشأن المسائل القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة يومي ٢١ و٢٢ نيسان/أبريل ٢٠١٦ في فيينا. وإضافة إلى ذلك، شاركت الأمانة في مؤتمر بعنوان "مسائل مفتوحة بشأن التجارة الإلكترونية: الهوية الرقمية"، نظمتها جامعة بولونيا (١٠ حزيران/يونيه ٢٠١٥، بولونيا، إيطاليا)؛ وفي حلقة عمل بشأن "قوانين وسياسات إدارة الهوية على الصعيد الدولي"، اشتركت في تنظيمها رابطة المحامين الأمريكيين والبنك الدولي (واشنطن، الولايات المتحدة الأمريكية، ١٤ كانون الثاني/يناير ٢٠١٦)؛ وفي مؤتمر بشأن "إدارة الهوية وخدمات توفير الثقة منذ صدور اللائحة التنظيمية بشأن الخدمات الإلكترونية الخاصة بتحديد الهوية وتوفير الثقة في مجال المعاملات الإلكترونية في السوق الداخلية"، نظمتها جامعة نامور (نامور، بلجيكا، ١٨ آذار/مارس ٢٠١٦).^(٣)

٤ - وتقدم هذه المذكرة موجزا للمناقشات التي دارت خلال تلك الندوة، وخلال الاجتماعات الأخرى ذات الصلة. ويمكن الاطلاع على المواد المستخدمة في العروض الإيضاحية المقدمة في الندوة في موقع الأونسيترال الشبكي.^(٤)

(١) الوثائق الرسمية للجمعية العامة، الدورة السبعون، الملحق رقم ١٧ (A/70/17)، الفقرات ٣٥٤ و٣٥٥ و٣٥٨.

(٢) المرجع نفسه، الفقرة ٣٥٨.

(٣) نُشرت مداوات ذلك المؤتمر في: Hervé Jacquemin (Dir.), L'identification électronique et les services de confiance depuis le règlement eIDAS, Bruxelles, 2016.

(٤) يمكن الاطلاع على تلك المواد، معروضة بالشكل الذي قدمها به المتكلمون، في الموقع الشبكي التالي: www.uncitral.org/uncitral/en/commission/colloquia/idm2016-programme.html

٥- ولعل اللجنة تود أن تحيط علماً بأن وثيقة تتضمن لمحة عامة عن إدارة الهوية قد قُدمت إلى الفريق العامل الرابع (المعني بالتجارة الإلكترونية) في دورته السادسة والأربعين (A/CN.9/WG.IV/WP.120)، وبأن هناك اعتبارات إضافية ترد في وثيقة مقدّمة إلى الفريق العامل الثالث (المعني بتسوية المنازعات بالاتصال الحاسوبي المباشر) في دورته الثانية والثلاثين (A/CN.9/WG.III/WP.136). ويمكن أيضاً الاطلاع على تقرير عن ندوة سابقة حول التجارة الإلكترونية، شملت حلقة نقاش بشأن إدارة شؤون الهوية (الوثيقة A/CN.9/728، الفقرات ٩-٢٨).

ثانياً- المسائل القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة

ألف- البيئة القانونية الحالية لإدارة الهوية وخدمات توفير الثقة

٦- إن إدارة الهوية الإلكترونية مسألة أساسية من أجل استخدام الوسائل الإلكترونية. فكثيراً ما يندرج ضمن الشواغل الأساسية التحقق من هويات أطراف بعينين، مثل تحديد هوية من يسعى إلى الوصول إلى قاعدة بيانات على الإنترنت تحتوي على معلومات حساسة، ومن يحاول تحويل أموال من حساب ما بالاتصال الحاسوبي المباشر، ومن وقع عقداً إلكترونياً، ومن أذن عن بعد بشحن منتج معين، ومن يسعى إلى الوصول إلى خدمات حكومية بالاتصال الحاسوبي المباشر، ومن أرسل بريداً إلكترونياً. ومن الناحية الوظيفية، ترمي إدارة الهوية إلى الإجابة على السؤالين الأساسيين التاليين: "من أو ما الذي يسعى إلى إثبات الهوية؟" و"ما مدى موثوقية إثبات الهوية؟" في بيئة إلكترونية.^(٥)

٧- وتجدر الإشارة في هذا الصدد إلى أن التحقق بطريقة موثوقة من هوية طرف بعيد في بيئة إلكترونية يختلف بالضرورة عن التحقق بطريقة جديدة بالثقة من هوية طرف حاضر في بيئة مادية. فعلى سبيل المثال، يمكن أن تُستخدم إدارة الهوية عن بعد وعلى نحو متزامن في تطبيقات متعددة، بينما لا يمكن ذلك في حالة الوسائل التقليدية لتحديد الهوية.

٨- وقد استُخدمت وثائق الهوية الورقية على مدى قرون لتحديد هوية الأشخاص الطبيعيين، ووضعت ممارسات راسخة حتى يعرف مستخدمو تلك الوثائق موثوقيتها كأدوات لتحديد الهوية وكذلك المخاطر المرتبطة باستخدامها. وفي المقابل، بالنظر لكون إدارة الهوية عملية جديدة نسبياً تتطلب وجود ارتباط بين معلومات الهوية الإلكترونية وشخص ليس

(٥) الوثيقة A/CN.9/WG.IV/WP.120، الفقرتان ٦ و ٨.

موجوداً شخصياً، فإن الممارسات التجارية ذات الصلة لا تزال غير راسخة تماماً وتباين المخاطر من تقييم إلى آخر. ومن ثم فإن تعزيز الثقة في استخدام نظم إدارة الهوية يتطلب توضيح جملة أمور، منها مختلف الجوانب التقنية والقانونية، بما في ذلك المسائل المتعلقة بالمسؤولية.

٩- وقد يكون لإدارة الهوية، بالنظر إلى اتساع نطاق أهميتها، تأثير على الإدماج الثقافي والسياسي والاجتماعي والاقتصادي.^(٦) ولإدارة الهوية انعكاسات عدة على أهداف التنمية المستدامة، حيث إنها ترتبط ارتباطاً مباشراً بالهدف ١٦-٩ (بشأن توفير هوية قانونية للجميع)، بما في ذلك تسجيل الموالييد، بحلول عام ٢٠٣٠)، وتضطلع بدور العامل المساعد لتحقيق عدد من الأهداف الأخرى مثل الهدف ١-٤ (بشأن ضمان حصول الفقراء على الموارد الاقتصادية، بما في ذلك التملك والتمويل)، والهدف ١٠-ج (بشأن خفض تكاليف التحويلات المالية)، والهدف ١٦-٥ (بشأن الحد من الفساد).

١٠- ويتطلب الانتقال المستمر صوب الاقتصادات المدعومة بالإنترنت والقائمة على البيانات استخدام إدارة الهوية في استخدامات تجارية واجتماعية متعددة. ويقترح واضعو السياسات اعتماد نماذج إدارة الهوية القائمة على المستخدم حيث يتاح للمستخدمين الاختيار بين وثائق إثبات الهوية التي يعتمون استخدامها ومستوى موثوقية تلك الوثائق.^(٧)

١١- وفي البيئة القانونية الحالية، تخضع نظم إدارة الهوية وخدمات توفير الثقة للمتطلبات الواردة في القوانين التي جرت صياغتها لأغراض أخرى، من ناحية (مثل القانون المدني والتجاري؛ وقوانين الخصوصية)، وللاتفاقات التعاقدية (التي كثيراً ما يشار إليها بقواعد النظام أو بأطر توفير الثقة ("system rules" أو "scheme rules" أو "trust frameworks"))، التي تهدف إلى ضمان الأداء السليم وموثوقية النظام من خلال تحديد التزامات الأطراف، من ناحية أخرى.

١٢- وعلى الرغم من أن معظم الولايات القضائية في العالم تعتمد قوانين بشأن المعاملات الإلكترونية والتوقيعات الإلكترونية كثيراً ما تتضمن أحكاماً ذات صلة بإدارة الهوية

(٦) انظر بصفة عامة الورقة الصادرة عن البنك الدولي بعنوان "Identification for Development" في الموقع الشبكي: <http://www.worldbank.org/en/programs/id4d>.

(٧) OECD, Digital Identity Management: Enabling Innovation and Trust in the Internet Economy, Paris, 2011, pp. 7 ff.

وخدمات توفير الثقة،^(٨) لا يوجد سوى عدد محدود من القوانين التي تتناول تحديداً استخدام إدارة الهوية وخدمات توفير الثقة.^(٩) وقد تلبى أحكام تشريعية إضافية احتياجات صناعات محدّدة، مثل احتياجات القطاع المصرفي وخدمات المدفوعات.^(١٠)

١٣ - وقد أبدت عدة دول اهتماماً بإعداد تشريعات بشأن إدارة الهوية أو شرعت في ذلك. وتستند تلك المبادرات إلى نهج ومفاهيم مختلفة. ولذلك فهناك حاجة واضحة وقوية وعاجلة إلى توفير إرشادات للمشرّعين من أجل اقتراح الخيارات المستصوبة والحيلولة دون عدم الاتساق.

نطاق نظم إدارة الهوية

١٤ - يُستخدم حالياً عدد من النماذج المختلفة لإدارة الهوية للاضطلاع بعدة وظائف قد تنطوي على تفاوت كبير من حيث متطلباتها والغرض منها. وحيث إنّ نظم إدارة الهوية قد تنطوي على أنواع مختلفة من التطبيقات والخدمات والمستخدمين، فمن المهم ألا يقتصر تحليلها القانوني على أنواع معيّنة من المعاملات، مثل المعاملات التجارية. وتنطبق اعتبارات مماثلة على خدمات توفير الثقة.

١٥ - وقد تُستخدم نظم إدارة الهوية لتحديد هوية الأشخاص الطبيعيين والاعتباريين وكذلك الأشياء المادية والرقمية. بيد أنّ تلك الكيانات لا تحظى جميعاً بالقدر نفسه من الاهتمام في سياق دراسة المسائل القانونية المتصلة بإدارة الهوية. فيبدو أنّ العمل بشأن الجوانب القانونية لتحديد هوية الأشياء يتطلب مزيداً من الاهتمام على وجه الخصوص. وفي هذا الصدد، تجدر الإشارة إلى أنّ بعض التكنولوجيات (مثل علامات التعرف بالترددات اللاسلكية أو غيرها من التكنولوجيات غير التلامسية) قد تكون أنسب من غيرها للتعرف على الأشياء، ومن ثم قد توفر أمثلة على حالات استخدامها يمكن أن تكون مفيدة لبدء ذلك التحليل.

(٨) للاطلاع على لمحة عامة عن الحالة الراهنة للتشريعات المتعلقة بالمعاملات الإلكترونية والتوقيعات

الإلكترونية، انظر UNCTAD Global Cyberlaw Tracker في الموقع الشبكي

http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx

(٩) على سبيل المثال، اللائحة رقم ٩١٠/٢٠١٤ الصادرة عن البرلمان الأوروبي والمجلس في ٢٣ تموز/يوليه ٢٠١٤

بشأن خدمات التعرف وتوفير الثقة فيما يتعلق بالمعاملات الإلكترونية في السوق الداخلية؛ وقانون فيرجينيا لإدارة الهوية الإلكترونية لسنة ٢٠١٥ (مشروع القانون رقم ٨١٤ المقدم إلى مجلس الشيوخ).

(١٠) انظر الأحكام ذات الصلة الواردة في التوجيه ٢٣٦٦/٢٠١٥ الصادر عن البرلمان الأوروبي والمجلس بتاريخ

٢٥ تشرين الثاني/نوفمبر ٢٠١٥ بشأن خدمات الدفع في السوق الداخلية.

١٦ - وعادة ما يضطلع المستخدمون التجاريون لإدارة الهوية بتحليل للفوائد والتكاليف المرتبطة بالتكنولوجيات والأساليب المستخدمة لتصريف الأعمال، مما يتطلب قدراً كبيراً من المرونة. وعلاوة على ذلك، فإن هؤلاء المستخدمين يلزمهم الوضوح وقابلية التنبؤ بشأن توزيع الالتزامات والمسؤوليات ذات الصلة بين الأطراف المعنية. وقد لا تنطبق نفس الاعتبارات بالضرورة في حالة استخدام نظم إدارة الهوية من أجل تقديم الخدمات العامة.

١٧ - ويجوز تصنيف نظم إدارة الهوية بأساليب شتى، كأن تصنف لأغراض "تجارية" أو "حكومية" وكنظم "مركزية" أو "لامركزية". ويشير تصنيف آخر إلى نظم إدارة الهوية التي توفر هويات تأسيسية أو أساسية، أي خصائص للتعريف بالهوية لا تتغير عادة، مثل الاسم عند الميلاد أو تاريخ الميلاد اللذين يُفترض أن يكونا متعددي الأغراض؛ وإلى نظم إدارة الهوية التي توفر هويات وظيفية، أي خصائص تعريفية تصدر لغرض محدد.

١٨ - وعلى الرغم من أن الضرورة التجارية لإدارة الهوية هي أحد المحركات الرئيسية لنظم إدارة الهوية على المستوى العالمي، فينبغي عدم الاستهانة بأهمية النظم الحكومية لإدارة الهوية. وتجدر الإشارة إلى أن سجلات التسجيل المدني والإحصاءات الحيوية تضطلع تقليدياً بعدد من الوظائف المتصلة بإدارة الهوية في العالم المادي. وكانت الحكومات تتولى إدارة هذه السجلات، ولا سيما في القرنين الماضيين. وعادة ما تقوم الحكومات، عند الاضطلاع بالوظائف المتعلقة بالتسجيل المدني والإحصاءات الحيوية، بالحد من مسؤوليتها تمشياً مع النظام القانوني المنطبق على الأنشطة الحكومية، وبالتحقق من موثوقية المعلومات الواردة في السجل استناداً إلى آليات قانونية أخرى (مثل أحكام القانون الجنائي بشأن تقديم أو اختلاق معلومات مزيفة بشأن الهوية).

١٩ - وقد تطورت الممارسات التجارية المتعلقة بتحديد هوية الأطراف على مر القرون على أساس معلومات الهوية المتاحة من سجل التسجيل المدني والإحصاءات الحيوية وغيره من السجلات وما يرتبط بذلك من إطار قانوني. وحتى الآن، تضطلع سجلات التسجيل المدني والإحصاءات الحيوية بدور مهم في توفير المعلومات المستخدمة في إدارة الهوية. وعلى وجه الخصوص، قد تُستخدم سجلات التسجيل المدني والإحصاءات الحيوية كأساس لما يسمى "الوثائق الاستصدارية" التي تعتمد عليها النظم التجارية في تحديد هوية الأشخاص الطبيعيين والاعتباريين.

٢٠ - وإضافة إلى ذلك، قد تكون النظم الحكومية لإدارة الهوية مصممة كامتدادات وتحسينات لسجلات التسجيل المدني والإحصاءات الحيوية التقليدية. وقد تشدد هذه النظم على الأمن وسمات أخرى ذات صلة باستخدامها الرئيسي المعتمزم. وعلاوة على ذلك، وتمشياً مع النهج التقليدي

لمشغلي سجلات التسجيل المدني والإحصاءات الحيوية، فإنَّ مقدّمها لا يعملون بالضرورة في إطار نظام قائم على المسؤولية الكاملة في حالة عدم أداء خدماتها أو أدائها بصفة جزئية.

٢١- وقد تعتمد الوثائق التجارية لإثبات الهوية الصادرة لأغراض مختلفة على نفس وثيقة الهوية الرئيسية. بيد أنَّ وثائق إثبات الهوية المختلفة تلك قد تنطوي على مستويات متباينة من الموثوقية، وهي تُستخدم بطرائق وتكنولوجيات مختلفة. ومن ثم، فإنَّ التحليل القانوني للعلاقة بين مختلف وثائق إثبات الهوية ووثيقة الهوية الاستصدارية الرئيسية تتطلب دراسة متأنية.

٢٢- ويتضح من الاعتبارات المذكورة أعلاه عدم وجود نموذج أو حل وحيد فيما يتعلق بإدارة الهوية. بل على العكس من ذلك، فإنَّ هناك العديد من نظم إدارة الهوية ذات الأغراض المختلفة المعمول بها على نحو متزامن. وبالمثل، فإنَّ التزامات ومسؤوليات الأطراف المشاركة في نظم إدارة الهوية قد تتباين من نظام إلى آخر. بيد أنَّ ذلك لا يمنع إمكانية تحديد العناصر المشتركة واعتبارها أساساً لتعزيز عناصر قابلية التشغيل التبادلي القانوني.

التفاعل وقابلية التشغيل التبادلي بين نظم إدارة الهوية

٢٣- كثيراً ما تكون نظم إدارة الهوية جامعة. ووفقاً لهذا النموذج، فإنَّ معلومات الهوية التي يتحقق منها أحد الكيانات تتاح، بطريقة متفق عليها وخاضعة للإدارة، لأطراف متعددة تحتاج إلى هذه المعلومات التعريفية للأغراض المختلفة.^(١١) وتحقق النظم الجامعة لإدارة الهوية إمكانية التشغيل التبادلي بين المشاركين فيها باستخدام إطار تقني وقانوني مشترك تحدده مجموعة من قواعد النظام. ويسهم الطابع الجامع لنظام إدارة الهوية في زيادة عدد المستخدمين والتطبيقات، وقد يساعد على احتواء التكاليف المتصلة بإدارة الهوية.

٢٤- بيد أنه في الوقت الراهن، تعمل معظم نظم إدارة الهوية بطريقة مستقلة من دون تفاعل أو بقدر ضئيل منه. والحواجز التي تعترض هذا التفاعل تقنية وقانونية. وعلى وجه الخصوص، قد تتسم القواعد القانونية المنطبقة على نظم إدارة الهوية بقدر كبير من التفاوت. بيد أنَّ قيمة نظام إدارة الهوية تتناسب مع عدد الأطراف التي تستخدمه وعدد التطبيقات التي يمكن استخدامه فيها وتنوع تلك التطبيقات. ومن ثم، ينبغي، في الظروف المثالية، أن تتفاعل النظم المختلفة لإدارة الهوية تفاعلاً سلساً بحيث لا تنفذ قابلية التشغيل التبادلي التقني فحسب، بل يخدم أيضاً أغراض الاعتراف المتبادل القانوني (يشار إليه باسم "قابلية التشغيل التبادلي القانوني").

(١١) A/CN.9/WG.IV/ WP.120، الفقرة ١٠.

٢٥- وبما أن الطابع الجامع وحده قد لا يعالج جميع المسائل التي تطرحها نظم إدارة الهوية، فإن هذه النظم سوف تستفيد من مواءمة الإطار القانوني. أمّا مسألة ما إذا كان الطابع الجامع لنظم إدارة الهوية بهذا المعنى يطرح تحديات قانونية محدّدة، فهي مسألة تتطلب مزيداً من التحقيق.

٢٦- وهناك تحديات إضافية قد تعترض قابلية التشغيل التبادلي التقني والقانوني على المستوى الإقليمي، حيث قد توجد اتجاهات محدّدة وحيث قد تكون القدرات والموارد المتاحة غير كافية.

٢٧- وهناك عدد من المنظمات التي تهدف إلى تطوير نظم إدارة الهوية وتوسيع نطاق استخدامها^(١٢) ويتطلب ذلك الهدف مزيجاً من القرارات المتعلقة بالسياسات والتطورات التقنية والأحكام القانونية. ومن الممكن أن تسهم قطعية القواعد القانونية المنطبقة وقابلية التنبؤ بها - وكذلك المواءمة بينها، قدر الإمكان - إسهاماً كبيراً في إزالة الحواجز التي تعترض استخدام إدارة الهوية عبر النظم والحدود الوطنية.

خدمات توفير الثقة

٢٨- تشمل خدمات توفير الثقة عدداً من الخدمات المختلفة التي ترمي إلى تعزيز الثقة في المعاملات الإلكترونية، بما في ذلك، على سبيل المثال لا الحصر: المحفوظات الرقمية؛ وختم الوقت؛ والتوقيعات التي تثبت منشأ الرسالة وسلامتها؛ والإشعار بالاستلام؛ وضمان الوجود في مرحلة زمنية معيّنة؛ والأختام الرقمية؛ والتوثيق من العنوان الإلكتروني (عناوين الموارد الموحّدة مثلاً) وحسابات الضمان.

٢٩- وتتضمن نصوص الأونسيرال المتعلقة بالتجارة الإلكترونية عدداً من الأحكام المتصلة بخدمات توفير الثقة، مثل الأحكام المتعلقة بالتوقيعات الإلكترونية، وسلامة رسائل البيانات، وحفظ رسائل البيانات، وإسناد رسائل البيانات. ونظراً لاعتماد تلك النصوص على نطاق واسع في العالم^(١٣) فإن هناك بالفعل قدراً كبيراً من القوانين الموحدة في هذا المجال.

(١٢) انظر الفقرة ٥ من الوثيقة A/CN.9/WG.IV/WP.120 للاطلاع على قائمة بأسماء عدة منظمات تعمل في هذا المجال.

(١٣) للاطلاع على حالة اعتماد نصوص الأونسيرال بشأن التجارة الإلكترونية، انظر http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce.html.

٣٠- وقد تكون هناك عناصر مشتركة بين خدمات توفير الثقة وخدمات إدارة الهوية. ومع ذلك، توجد بينها أيضاً اختلافات كبيرة، ولا سيما في ضوء الوظيفة المتوخاة من استخدام كل خدمة من خدمات توفير الثقة. ولم يتضح بعد ما إذا كان من المجدي والمستصوب النظر بشكل مشترك في الجوانب القانونية لإدارة الهوية وخدمات توفير الثقة.

باء- تعزيز الثقة في استخدام إدارة الهوية وخدمات توفير الثقة

٣١- إنَّ ضمان الثقة في تشغيل نظم إدارة الهوية وخدمات توفير الثقة أمر أساسي من أجل تعزيز استخدامهما (انظر الفقرات ٦-٨ أعلاه). والثقة يمكن تعريفها بأنها "الإيمان الراسخ بموثوقية شيء ما"^(٤) وهي من ثم رأي يؤثر على السلوك والاستعداد للاعتماد. وفي حالة إدارة الهوية وخدمات توفير الثقة، فإنَّ الثقة هي الرأي بشأن موثوقية الخدمة المقدَّمة.

٣٢- وفي المقابل، يمكن تعريف الموثوقية بأنها "نوعية الأداء الجيد على نحو متسق"^(٥) وهي نتيجة لعملية وليست منتجاً.

٣٣- وبشكل غياب الوضوح بشأن مسؤولية الأطراف حاجزاً رئيسياً أمام تعزيز الثقة في استخدام خدمات إدارة الهوية وتوفير الثقة. ويتعين على الأطراف أن تكون قادرة على أن تقيم بوضوح الحقوق والالتزامات وعلى أن توزع المخاطر. وفي الوقت الراهن، يمكن توضيح هذين المصطلحين في الاتفاقات التعاقدية (الواردة بكثرة في قواعد النظام) التي قد يتسم مضمونها بقدر كبير من التفاوت. وعلاوة على ذلك، قد يوزع القانون المسؤولية، ربما على أساس القواعد العامة، في غياب أيِّ اتفاق، أو قد يتجاوز أيضاً تلك الاتفاقات. والأحكام المتعلقة بحدود المسؤولية المنصوص عليها في القانون وفي الشروط التعاقدية مهمة أيضاً لتعريف توزيع المخاطر. ويتسم بأهمية ماثلة توافر التأمين التجاري لتغطية المخاطر المرتبطة باستخدام إدارة الهوية وخدمات توفير الثقة.

٣٤- ومن الأهمية بمكان أن تركز التدابير التشريعية والأحكام التعاقدية الرامية إلى تعزيز الثقة على نتائج العملية، مثل توفير خدمات موثوقة، بدلاً من فرض عمليات محدَّدة، وهو ما قد ينتهك حياد التكنولوجيا أو حياد نظام الهوية. ولذلك نتاجه العملية المهمة، مثلاً من خلال ضمان ألاَّ تحول القواعد دون استخدام إدارة الهوية مع أيِّ تكنولوجيا أو وسيلة محدَّدة، من قبيل الأجهزة النقالة. وبالمثل، قد تشير المتطلبات التشريعية المرتبطة بالموثوقية إلى

(٤) Oxford English Dictionary Online, "Trust", sub 1 (١٤)

(٥) Oxford English Dictionary Online, "Reliability", sub 1 (١٥)

المعايير التقنية؛ بيد أنه لا بد من توحّي الحذر لتفادي محاباة أيّ تكنولوجيا أو أسلوب أو عملية، أو منع القدرة على التكيف مع التغيير.

٣٥- وعلى وجه التحديد، يمكن للقانون أن يعزز الثقة في موثوقية نظم إدارة الهوية وخدمات توفير الثقة من خلال مكافأة امتثال بعض المتطلبات المرتبطة بموثوقية النظام أو الخدمة.

٣٦- وعلى وجه الخصوص، قد يربط القانون قرائن قانونية باستخدام نظم إدارة الهوية أو خدمات توفير الثقة التي تستوفي شروطاً معيّنة. وقد تؤدي تلك القرائن إلى تحويل عبء الإثبات بشأن المنشأ والسلامة ووقت الإرسال والاستلام، وما إلى ذلك، عندما تُستخدم المعاملات الإلكترونية. بمساعدة نظم إدارة الهوية أو خدمات توفير الثقة التي تتسم بامتثال المتطلبات. وللأطراف حرية اختيار ما إذا كانت تلك النظم والخدمات مهمة ومفيدة بالنسبة إلى عملياتها التجارية بما يحقق المرونة المرجوة.

٣٧- وبدلاً من ذلك، قد ينص القانون على إرساء مسؤولية بعض الأطراف المشاركة في نظم إدارة الهوية وخدمات توفير الثقة أو استبعاد تلك المسؤولية ما دامت الأطراف تمتثل للمتطلبات المنصوص عليها في التشريعات أو الاتفاقات التعاقدية. وقد ينص القانون أيضاً على عدم جواز أن تؤدي الاتفاقات التعاقدية إلى الانتقاص من المسؤولية عن الإهمال الجسيم أو سوء التصرف المتعمد أو تغيير تلك المسؤولية.

٣٨- ومن بين الفوائد المهمة المتأتية عن التوصل إلى فهم أوضح لالتزامات الأطراف المختلفة في نظام الهوية وتوزيع مخاطر المسؤولية فيما بينها تحسّين تقييم احتياجات الأمن السيبراني، مما يسمح بدوره بتوزيع أكثر كفاءة للموارد ذات الصلة بما يتماشى مع الاحتياجات الفعلية للأطراف.

استخدام إدارة الهوية وخدمات توفير الثقة عبر الحدود

٣٩- إنّهية بيئة قانونية تمكينية من أجل استخدام إدارة الهوية وخدمات توفير الثقة تستوجب المراعاة الكاملة أيضاً للجوانب العابرة للحدود لذلك الاستخدام. وقد تشكل هذه الجوانب تحديات إضافية في غياب إطار قانوني موحد لتعزيز الاعتراف المتبادل بالمركز القانوني لنظم إدارة الهوية وخدمات توفير الثقة. وينبغي، لدى التعامل مع هذه الجوانب، إيلاء الاعتبار الواجب للأحكام المتعلقة بالاعتراف القانوني المتبادل بطرائق التوثيق الواردة في الصكوك الدولية مثل اتفاقات التجارة الحرة.^(١٦)

(١٦) انظر، مثلاً، المادة ١٤-٦ من اتفاق شراكة المحيط الهادئ.

٤٠ - وفي الوقت الراهن، قد يتحقق الاعتراف القانوني عبر الحدود على أساس اتفاقات خاصة تنص تعاقدياً على شروط الخدمة وكذلك المواصفات التقنية.^(١٧) بيد أن هذا النموذج يخضع للقيود المفروضة على حرية التعاقد المنصوص عليها في القانون الوطني المنطبق ولا ينطبق على الأطراف غير الملزمة تعاقدياً.

٤١ - وقد يرتقي نهج آخر تجاه الاعتراف القانوني عبر الحدود بنظم إدارة الهوية وخدمات توفير الثقة إنشاء نظام مركزي للاعتماد يجري تقييمه تُحدد نتيجته الوضع القانوني للنظام أو الخدمة ويكون ملزماً للدول المشاركة. ويُجرى تقييم مدى مطابقة النظم والخدمات قبل استخدامها الفعلي ووفقاً لفئات عامة. وقد يكون هذا النموذج مفيداً بوجه خاص عند تطبيقه في إطار التكامل الاقتصادي الإقليمي على اعتبار أن الدول التي تسعى إلى تحقيق ذلك التكامل يكون لديها الحافز للانضمام إليه.

٤٢ - بيد أن ثمة احتمالاً آخر يرتقي إعداد أحكام قانونية موحدة لتحقيق الاعتراف عبر الحدود، ويُفضّل أن يكون ذلك على أساس متعدد الأطراف. وفي تلك الحالة، لن يمكن إجراء تقييم الموثوقية إلا في حالة التزاع الفعلي وعلى أساس كل حالة على حدة.^(١٨)

٤٣ - ويرتبط أحد الاعتبارات المهمة بالحاجة إلى نص قانوني موحد للتفاعل مع قواعد القانون الدولي الخاص. وقد يتطلب تحليل ذلك التفاعل اهتماماً خاصاً.

جيم - المسائل ذات الصلة بالأعمال المقبلة

٤٤ - يرحب مختلف أصحاب المصلحة بقرار الأونسيرال الاضطلاع بأعمال بشأن الجوانب القانونية لاستخدام نظم إدارة الهوية وخدمات توفير الثقة، ويقترحون أن تتولى الأونسيرال إعداد أحكام تهدف إلى توفير توجيهات تشريعية محددة. ومن شأن النتيجة أن تعزز ثقة الأطراف في استخدام نظم إدارة الهوية وخدمات توفير الثقة وأن تنمي قابلية التشغيل التبادلي القانوني بين نظم إدارة الهوية. ومن شأن منتج العمل هذا أن يسد الفجوة الحالية بين التشريعات العامة والقواعد الخاصة بالنظم، من ناحية، ويضمن الاتساق في التشريعات المقبلة، من ناحية أخرى.

(١٧) هذا النموذج يستخدمه التحالف الآسيوي بشأن التجارة الإلكترونية.

(١٨) هذا النهج معتمد في الفقرة ٣ من المادة ٩ من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية.

٤٥- ويبدو من المهم بشكل خاص، لدى الاضطلاع بالأعمال المقبلة، ضمان التنسيق مع المنظمات ذات الصلة التي تتناول الجوانب القانونية والتقنية لنظم إدارة الهوية وخدمات توفير الثقة. وسيتيح ذلك تركيز الممارسات على قضايا محددة، انطلاقاً من الخبرات والمعارف القائمة وكذلك إبراز العناصر المشتركة بين القوانين الحالية والمرتبقة.

٤٦- وفيما يتعلق بشكل العمل المستقبلي للأونسيترال، بينما قد يُرتأى إعداد تشريع نموذجي يُسنُّ على الصعيد الوطني، قد يكون إعداد نص دولي أنسب لإدراج الجوانب العابرة للحدود. ويمكن لنصوص غير تشريعية، من قبيل الأحكام التعاقدية النموذجية، أن تعالج مسائل معيَّنة على نحو كاف. ويمكن صياغة نصوص متداخلة.

٤٧- وفيما يتعلق بمضمون الأحكام بشأن نظم إدارة الهوية وخدمات توفير الثقة، فإنَّ المبادئ العامة التي تقوم عليها نصوص الأونسيترال بشأن استخدام الخطابات الإلكترونية (الحياد التكنولوجي، وعدم التمييز بين الخطابات الإلكترونية، والتكافؤ الوظيفي) وغيرها من المبادئ العامة للقانون التجاري الموحد، مثل حرية التعاقد، لها أهميتها من أجل تحديد الإطار القانوني لاستخدام نظم إدارة الهوية وخدمات توفير الثقة.

٤٨- وعلاوة على ذلك، فإنَّ للعديد من الأحكام الواردة في نصوص الأونسيترال بشأن التجارة الإلكترونية (مثل الأحكام الخاصة بالتوقيعات الإلكترونية والمحفوظات) وفي نصوص أخرى معيَّنة^(١٩) صلة مباشرة بنظم إدارة الهوية وخدمات توفير الثقة ويمكن أن توفر توجيهات مفيدة. وقد يكون إجراء تحليل دقيق لتلك النصوص مفيداً لإعداد عمل الأونسيترال في المستقبل في هذا المجال.

٤٩- وفي هذا الصدد، يبدو أنَّ زيادة توضيح العلاقة بين نظم إدارة الهوية وخدمات توفير الثقة، من جهة، والتوقيعات الإلكترونية، من جهة أخرى، مفيدة بوجه خاص. ومن العناصر التي يجب مراعاتها في ذلك التحليل أنَّ التوقيعات الإلكترونية تستوجب وجود عنصر من عناصر الهوية. مما يتيح للأطراف التعويل على التوقيع بالتحقق من هوية الموقع على نحو موثوق. ويرتبط عنصر آخر من العناصر التي ينبغي مراعاتها باستخدام أنواع معيَّنة من التوقيعات الإلكترونية في تقديم خدمات توفير الثقة.

(١٩) على سبيل المثال، الفقرة ٢ من المادة ٥ من قانون الأونسيترال النموذجي للتحويلات الدائنة الدولية، ١٩٩٢.

٥٠ - ومن الممكن أن يكون إعداد تعاريف لأهم المصطلحات ذات الصلة المستخدمة فيما يتعلق بإدارة الهوية وخدمات توفير الثقة مفيداً لتوضيح المفاهيم المختلفة وضمان الفهم الموحد لها. ولدى القيام بذلك، لا بد من مراعاة المعايير التقنية وما تنطوي عليه من تعاريف.^(٢٠)

٥١ - وفي ضوء الاعتبارات الواردة أعلاه، يبدو من المفضل أن يشمل نطاق هذا المشروع التشريعي جميع أنواع نظم إدارة الهوية وخدمات توفير الثقة، بصرف النظر عن طبيعة المقدم والغرض أو الوظيفة أو الاستخدام المقصود الرئيسي. ويبدو من المستصوب أيضاً أن يراعي هذا المشروع جميع الكيانات الممكنة التي يمكن تحديدها من قبل نظام إدارة الهوية وجميع الأدوار الممكنة. وأخيراً، ينبغي أن يعالج المشروع استخدام نظم إدارة الهوية وكذلك المعاملات بين نظم إدارة الهوية.

٥٢ - وفيما يتعلق بمواضيع محددة، تبدو المسائل التالية من المسائل الأساسية التي ينبغي مناقشتها فيما يتعلق بإدارة الهوية: حقوق الأطراف والتزاماتها؛ والموثوقية في مختلف خطوات دورة إدارة الهوية؛ وعواقب الموثوقية على المسؤولية؛ وقواعد النظام وغيرها من الاتفاقات التعاقدية (مثل اتفاقات مستوى الخدمة)؛ والاعتراف القانوني المتبادل والمسائل الأخرى المتصلة بقابلية التشغيل التبادلي القانوني.

٥٣ - ويرتبط جانب مهم من جوانب إدارة الهوية بالخصوصية وحماية البيانات. وقد تفاوتت التهجس السياسية إزاء هذا الموضوع المعقد تفاوتاً كبيراً وهناك العديد من المبادرات التي تهدف إلى التوفيق بينها. وعلى الصعيد العملي، تعترف التشريعات القائمة بشأن إدارة الهوية بوجود قانون محدد بشأن الخصوصية وتنص على تطبيقه. وفي ظل هذه الخلفية، وبالنظر إلى أن العمل المتعلق بنظم إدارة الهوية وخدمات توفير الثقة ينبغي ألا يمتد إلى مسائل خارج ولاية الأونسيترال،^(٢١) فمن المشكوك فيه أن تتمكن الأونسيترال من التعامل بكفاءة مع تلك المسائل بالتفصيل في المرحلة الراهنة.

٥٤ - ويرتبط جانب آخر يستحق المزيد من التحليل باستخدام نظم إدارة الهوية وخدمات توفير الثقة في الحوسبة السحابية. والخدمات السحابية يمكن استخدامها لتوفير إدارة الهوية (الهوية كخدمة). وعلاوة على ذلك، فإن إدارة الهوية (في شكل التوثيق المتعدد العوامل مثلاً) يشجع استخدامها للحصول على الخدمات السحابية، وبخاصة لكفالة امتثال متطلبات

(٢٠) انظر الوثيقتين ISO/IEC 24760-1:2011 و ISO/IEC 24760-2:2015 للاطلاع على أمثلة على تعاريف ذات صلة بإدارة الهوية.

(٢١) الوثائق الرسمية للجمعية العامة، الدورة السبعون، الملحق رقم ١٧ (A/70/17)، الفقرة ٣٥٥.

الخصوصية وغيرها من المتطلبات التنظيمية. ومع ذلك، يلزم إجراء المزيد من التحقيقات من أجل توضيح ما إذا كانت تلك الاستخدامات تنطوي على مسائل قانونية محددة.

٥٥- وفيما يتعلق بأساليب العمل، يبدو من المستصوب بصفة خاصة تعزيز المشاركة الواسعة من جانب جميع المناطق في عمل الأونسيرال في المستقبل بغية إجراء تقييم أفضل للحالة الراهنة لتنظيم إدارة الهوية وخدمات توفير الثقة وكذلك التعرف على الاتجاهات الإقليمية المحددة.^(٢٢) ومن بين الأدوات الممكنة للقيام بذلك توزيع الدراسات الاستقصائية. ويمكن القيام بذلك أيضاً عن طريق التعاون والتنسيق مع المنظمات الإقليمية ذات الصلة، مثل المنظمة العربية لتكنولوجيات الاتصال والمعلومات.^(٢٣)

(٢٢) للمزيد من المعلومات عن الدول الأعضاء في رابطة أمم جنوب شرق آسيا، انظر Electronic Transactions Development Agency, Intra-ASEAN Secure Transactions Framework Final Report, Bangkok, July 2014.

(٢٣) يمكن تحديداً أن تشمل ولاية الفريق العامل الثالث للمنظمة العربية لتكنولوجيات الاتصال والمعلومات (المصادقة الإلكترونية والأمن السيرياني) إدارة الهوية.