الأمم المتحدة A/CN.9/1113/Add.1

الجمعية العامة

Distr.: General
14 June 2022
Arabic
Original: English/Spanish

لجنة الأمم المتحدة للقانون التجاري الدولي

الدورة الخامسة والخمسون

نيويورك، 27 حزيران/يونيه – 15 تموز/يوليه 2022

مشروع قانون نموذجي بشأن استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود

تجميع للتعليقات الواردة من الحكومات والمنظمات الدولية

المحتويات

الصفحة

ثانيا- تجميع التعليقات 2

واو- رابطة المصرفيين للتمويل والتجارة 2

زاي- دولة بوليفيا المتعددة القوميات 4

حاء- جمهورية إيران الإسلامية 5

طاء- بلغاريا 10

ياء- سنغافورة 11

010722 010722 V.22-03954 (A)

الرجاء إعادة استعمال الورق

ثانيا- تجميع التعليقات

واو- رابطة المصرفيين للتمويل والتجارة

[الأصل: بالإنكليزية]
[27 أيار/مايو 2022]

1- تقدر رابطة المصرفيين للتمويل والتجارة (الرابطة) هذه الفرصة التي أُتيحت لها للتعليق على الوثيقة المعنونة "مشروع قانون نموذجي بشأن استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود".

2- ورابطة المصرفيين للتمويل والتجارة هي رابطة دولية لقطاع الخدمات المالية تضم في عضويتها طائفة واسعة من المؤسسات المالية وشركات التكنولوجيا المالية من جميع أوساط المجتمع العالمي. ويضطلع أعضاء الرابطة البالغ عددهم قرابة 300 عضو، بوصفها منتدى عالميا للتحليل والمناقشة وأنشطة الدعوة في مجال الخدمات المالية الدولية، بقيادة الجهود الرامية إلى بناء توافق في الآراء بشأن الحفاظ على الطابع الآمن والفعال لسير عمل النظام المالي في جميع أنحاء العالم. وترى المؤسسات الأعضاء في الرابطة أن رقمنة عمليات تمويل التجارة الدولية هي أولوية رئيسية للقطاع، وأن إدارة الهوية عنصر بالغ الأهمية لإحراز تقدم في مجال الرقمنة.

3- وتمثل الحاجة إلى إنشاء إدارة للهوية قاسما مشتركا بين العديد من جوانب المعاملات المصرفية الدولية، بما في ذلك تمويل التجارة، وتمويل سلاسل التوريد، والمدفوعات، ومجالاتٍ متعلقة بالامتثال مثل "اعرف زبونك" (KYC) ومكافحة غسل الأموال. ومن ثمَّ، تعرب الرابطة عن دعمها الكامل لجهود الأونسيترال الرامية إلى صياغة مشروع القانون النموذجي.

4- ويهدف العديد من مسارات العمل في سياق المعاملات المصرفية العالمية إلى تزويد هذا النشاط بنظام إيكولوجي رقمي بالكامل. وتبشر الرقمنة بفوائد كثيرة. ومع ذلك، لا يمكن القول إن معدل الإنجاز والاعتماد في هذا المجال كان مرضيا حتى الآن. ومن الواضح أن الرقمنة لن تحدث فجأة بطريقة "الانفجار الكبير"، بل ستتحقق من خلال مبادرات تكميلية تسمح بإحراز تقدم ملموس.

5- والسوق بحاجة إلى قواعد واضحة لكي يتمكن من تعزيز الرقمنة في العمليات اليومية. وفي هذا الصدد، أطلقت غرفة التجارة الدولية ومصرف التنمية الآسيوي وحكومة سنغافورة المبادرة المعنونة "مبادرة المعايير الرقمية" التي تهدف إلى معالجة المسائل المتعلقة بالمعايير وقابلية المنصات للتشغيل المتبادل والعلاقات مع شركات التكنولوجيا المالية[(1)]. وفيما يتعلق بالدعم القانوني، وضعت الغرفة خريطة طريق لتشجيع الحكومات على اعتماد تشريعات محددة للأعمال التجارية الرقمية على النحو الذي يروج له قانون الأونسيترال النموذجي بشأن السجلات الإلكترونية القابلة للتحويل (قانون السجلات الإلكترونية)[(2)]. وتشارك الرابطة في الجهود الرامية إلى تشجيع اعتماد هذا القانون النموذجي عالميا. وبالإضافة إلى الإطار القانوني، يعمل القطاع على وضع معايير للتشغيل المتبادل. ففي آب/أغسطس 2020، أصدرت الرابطة المنشور المعنون Distributed Ledger Payment Commitment – Industry Best Practices (الالتزامات بالدفع باستخدام السجلات الموزعة – الممارسات التقنية الفضلى)[(3)] بغية توفير إرشادات للقطاع حول الالتزامات بالدفع القابلة للتشغيل المتبادل والمنفذة باستخدام السجلات الموزعة.

(1) مبادرة المعايير الرقمية التابعة لغرفة التجارة الدولية، آذار/مارس 2020.

(2) قانون الأونسيترال النموذجي بشأن السجلات الإلكترونية القابلة للتحويل، تموز/يوليه 2017.

(3) رابطة المصرفيين للتمويل والتجارة: الالتزامات بالدفع باستخدام السجلات الموزعة، أيار/مايو 2020.

6- ويوفر المشروع الحالي للقانون النموذجي الإطار العام لخدمات إدارة الهوية وتوفير الثقة؛ ولكنَّه يتجنب اتباع أي نهج ينطوي على أقل قدرٍ من الإلزام. فهو ينص صراحة على أنه يستند "مثل نصوص الأونسيترال السابقة، إلى مبادئ استقلالية الأطراف، وحياد التكنولوجيا، والتكافؤ الوظيفي، وعدم التمييز ضد استخدام الوسائل الإلكترونية، رهنا بما قد يُدخَل عليه من تعديلات. ويتيح مبدأ استقلالية الأطراف لأطراف العقد أن تختار القواعد المنطبقة مع حدود القانون الإلزامي. وهو يستند إلى الاعتراف بأن هذه الأطراف قد تكون الأقدر على تقرير أكثر القواعد ملاءمة للمعاملة المعنية".

7- ويتوخى مشروع القانون النموذجي أن تكون خدمات إدارة الهوية خاضعة لشروط تقرر مدى موثوقيتها، كما تقتضي المادة 10، ولكنه لا ينص على كيفية وضع إطار مستوى الضمان. ويؤكد مشروع القانون النموذجي أن البعد الدولي يُعدُّ أساسيا لاستخدام خدمات إدارة الهوية وتوفير الثقة، وبصورة أعم، لاستخدام الخدمات الإلكترونية. ومع ذلك، يؤكد النص أن هناك نوعين من العقبات، هما: '1' عدم التوافق التقني الذي يؤدي إلى تعذر إمكانية التشغيل المتبادل، و'2' العقبات القانونية التي تحول دون الاعتراف عبر الحدود.

8- ومن أجل توفير التوجيه فيما يتعلق بكيفية التغلب على هاتين العقبتين على وجه الخصوص، ستدعم الرابطة الإشارة المباشرة في مشروع القانون النموذجي إلى القدر الكبير من العمل الذي اضطلعت به المؤسسة العالمية لتحديد هوية الكيانات القانونية (GLEIF)[4] وما أحرزته من تقدم في تنفيذ النظام العالمي لتحديد هوية الكيانات القانونية (النظام العالمي لتحديد الهوية). والنظام العالمي لتحديد الهوية هو نظام معتمد من الناحية التنظيمية يوفر آلية للتحديد الإلكتروني لهوية الكيانات القانونية تحظى بالاعتراف والثقة عالميا. والنظام العالمي لتحديد الهوية هو معيار عالمي (ISO 17442) يربط بين المعلومات المرجعية الرئيسية التي تتيح تحديد هوية الكيانات القانونية على نحو واضح وفريد. وقد أنشأ مجلس تحقيق الاستقرار المالي المؤسسة العالمية تحديد هوية الكيانات القانونية، وهي مؤسسة سويسرية غير هادفة للربح، بناء على توصية من مجموعة العشرين في عام 2011. ويشرف على أنشطة المؤسسة 65 هيئة تنظيمية و19 مراقبا في لجنة الرقابة التنظيمية من أكثر من 50 بلدا.

9- ويمكن أن تعتبر البيانات المجمعة الخاصة بالنظام العالمي لتحديد الهوية، وهي بيانات متاحة للجمهور، دليلا عالميا يعزز الشفافية في السوق العالمية إلى حد بعيد. وهذا النظام العالمي منفعة عامة واسعة النطاق ينبغي أن يُستفاد منها من أجل ضمان التوافق التقني على الصعيدين الوطني والدولي.

10- ويهدف مشروع القانون النموذجي إلى مواءمة القواعد من خلال سن التشريعات. ومن شأن هذا النهج أن يؤدي إلى وضع عدد ضخم من المعايير التقنية الوطنية، مما يعني انتفاء القابلية للتشغيل المتبادل واستنزاف الموارد في محاولات تحليل البيانات غير المتجانسة وفهمها. ويمكن أن يؤدي استخدام عدد كبير من محدِّدات الهوية وما تستند إليه من معايير تقنية وطنية إلى إعاقة القدرة على تحديد هوية كل طرف من أطراف المعاملات الإلكترونية بطريقة موثوقة ومتجانسة وقابلة للمقارنة. ولذلك، ينبغي للأونسيترال، على الرغم من رغبتها في تجنب تفضيل أي تكنولوجيا بعينها والحفاظ على حيادها التكنولوجي، أن تدرس إدراج النظام العالمي لتحديد الهوية في مشروع النص باعتباره محدِّد الهوية الأساسي، وذلك بغية تيسير تحديد هوية الكيانات القانونية والتحقق منها عبر الحدود، إذ إن هذا النظام العالمي لتحديد الهوية ليس خيارا تكنولوجيا بل هو منفعة عامة، كما توخته مجموعة العشرين (G20) وأخرجه إلى الوجود مجلس تحقيق الاستقرار المالي.

11- وبالنظر إلى أن البيانات المرجعية الخاصة بالنظام العالمي لتحديد الهوية تتضمن بالفعل رقم التسجيل المحلي للكيان المعني، وعنوانه، وختم الوقت الذي يبين آخر تحديث للبيانات، ومعلومات بشأن خانات البيانات التي حُدِّثت، فإن هذا النظام ينطوي على إمكانية تعزيز توحيد البيانات الخاصة بكل كيان على المستوى العالمي.

(4) المؤسسة العالمية للتحديد هوية الكيانات القانونية (www.gleif.org).

12- ويسلِّم مشروع القانون النموذجي بالفعل بأن القواعد الموحدة يمكن أن تحسن الكفاءة بالتشجيع على قبول نتيجة تطبيق خدمات إدارة الهوية وتوفير الثقة على نطاق المنظومات؛ وخفض تكاليف المعاملات بتيسير الامتثال للشروط التنظيمية؛ وزيادة إمكانية التنبؤ واليقين القانونيين للمعاملات الإلكترونية على أساس معاملة المسائل معاملة موحدة، عبر قنوات من بينها آليات الاعتراف عبر الحدود؛ والمساهمة في سد الفجوة الرقمية من خلال إتاحة الحلول المشتركة بسهولة أكبر.

13- وفي حال وجود نهج متباينة، تشير المادة 27 إلى أن التعاون يمكن أن ييسر التوصل إلى اتفاق على تعاريف مشتركة للمعايير التقنية، بما في ذلك مستويات الضمان ومستويات الموثوقية. غير أن المصالح الوطنية المتنافسة قد تسبب اختناقات، وفي أحسن الأحوال تأخيرات، في التوصل إلى اتفاق على المعايير التقنية المطلوبة وغير ذلك من الأطر الأساسية لجودة البيانات. ومن شأن اضطلاع الأونسيترال بدور قيادي في اختيار النظام العالمي لتحديد الهوية بوصفه محدِّد الهوية السائد للكيانات القانونية أن يعجِّل بتنفيذ التحديد الإلكتروني للهوية عبر الحدود، وأن يستفيد من هذا النظام الذي أنشأته هيئات تنظيمية لمعالجة أوجه القصور في النظم الوطنية/الإقليمية/الخاصة لتحديد الهوية. ويوفر النظام العالمي لتحديد الهوية، بوصفه نظاما فعالا ثبتت جدواه، حلا قابلا للتشغيل المتبادل ومحايدا من الناحية التقنية.

14- وينطوي التحول الرقمي في المعاملات المصرفية العالمية على إمكانية خفض التكاليف وتحسين الكفاءة وتعزيز الضوابط التنظيمية، وعلى مخاطر أقل، ويتيح لأصحاب المصلحة فرصا للتعاون على صعيد الاقتصاد العالمي. ويعد إنشاء إدارة الهوية وتكييفها خطوة أولى حاسمة في عملية الرقمنة. والنظام العالمي لتحديد الهوية هو المعيار العالمي الوحيد لتحديد الهوية القانونية، ومن هذا المنطلق، تؤيد الرابطة إدراجه في نص مشروع القانون النموذجي.

زاي- دولة بوليفيا المتعددة القوميات

[الأصل: بالإسبانية]
[27 أيار/مايو 2022]

قدمت هيئة تنظيم الاتصالات والنقل في دولة بوليفيا المتعددة القوميات التعليقات والملاحظات التالية على مشروع القانون النموذجي للنظر فيها.

المادة 6- التزامات مقدمي خدمات إدارة الهوية

التعليق/الملاحظة:

يُوصى بإرساء التزام بضمان توافر نظام إلكتروني عبر الإنترنت للتحقق من الهوية الإلكترونية أو التوقيع الإلكتروني وتشغيله على نحو سليم، مما سيتيح التحقق من هوية الموقِّع وصحة سلسلة الثقة لدى جهة الاعتماد المأذون لها في بلد المنشأ.

المادة 16- التوقيعات الإلكترونية

التعليق/الملاحظة:

يُوصى بالنظر في إنشاء آلية لكشف أي تحوير في رسالة البيانات وضمان صحتها وسلامتها وعدم التنصل منها.

المادة 17- الأختام الإلكترونية

التعليق/الملاحظة:

ينبغي ضمان صحة رسالة البيانات وسلامتها وعدم التنصل منها وضمان صلاحيتها القانونية والإثباتية أيضاً، وفقا لأنظمة البلد الذي يوجد فيه مقر مقدم خدمات إدارة الهوية.

حاء- جمهورية إيران الإسلامية

[الأصل: بالإنكليزية]
[30 أيار/مايو 2022]

1- نطاق التطبيق

استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود

1- **المسألة:** عملا بولاية الأونسيترال المتمثلة في مواءمة القانون التجاري الدولي وتحديثه، وفي ضوء المهمة المسندة إلى الفريق العامل الرابع بإزالة الحواجز في مجال التجارة الإلكترونية الدولية، ترى جمهورية إيران الإسلامية أن نطاق انطباق القانون النموذجي شديد الاتساع ويلزم تقييده بحيث يقتصر فقط على المجال الدولي والظروف التي تنطوي على عنصر أجنبي. وبعبارة أخرى، بحسب فهمنا، في حالات استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها محليا، عندما لا تنطوي الحالة المعنية على أي عنصر أجنبي ويكون جميع المشاركين في دورة حياة خدمات إدارة الهوية وتوفير الثقة موجودين في نفس البلد، من المتوقع أن يكون القانون الوطني للدول هو من يحكم هذا الوضع وينظم شؤونها الداخلية.

الحل المقترح

2- يُوصى بتقييد نطاق القانون النموذجي بحيث يقتصر على استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود، وتوضيح أن هذا الصك لا يهدف إلى التدخل في البنى التحتية الوطنية المتعلقة بخدمات إدارة الهوية وتوفير الثقة في الدول الأعضاء، ولا إلى أن تكون له الأسبقية على القوانين الوطنية التي تحكم الشؤون الداخلية لتلك الدول. وفي الوقت نفسه، نلاحظ أنه لا يزال من الممكن أن يظل المجال مفتوحا أمام الولايات القضائية المشترِعة لتوسيع نطاق انطباق الصك بحيث يشمل شؤونها الداخلية، فقط إن أرادت ذلك.

الخدمات ذات الصلة بالتبادل التجاري

3- **المسألة:** فيما يتعلق بمصطلح "الخدمات ذات الصلة بالتبادل التجاري" الوارد في المادة 2، تجدر الإشارة إلى أنه على الرغم من الشرح الوارد في الفقرة 95 من الوثيقة التفسيرية، فإن هذا المصطلح، على حد فهمنا، لا يزال غامضا ولا يمكن للمستخدمين التعرُّف عليه بسهولة، وكذلك يمكن تفسيره على نحو أوسع نطاقا عما هو متوخى بموجب القانون النموذجي، أو يمكن أن يُوسَّع نطاقه توسيعا غير سليم بحيث يشمل جميع النظم النشطة في بلد ما في مجال خدمات إدارة الهوية وتوفير الثقة في حين أن هذه النظم لا تتصل بالضرورة بالتبادل التجاري.

الحل المقترح

4- يُوصـــى بأن يركز القانون النموذجي على الحالات التي تُصـــادَف في الأنشـــطة التجارية. ومع ذلك، يمكن أن توضـح المذكرة التفسـيرية أن "القانون النموذجي ليس فيه ما ينبغي أن يمنع دولة مشـترِعة من توسـيع نطاقه بحيث يشـمل اسـتخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود في سـياق الخدمات ذات الصلة بالتبادل التجاري".

2- صون سيادة الدول ونظامها العام

5- **المسألة:** يعرب وفدنا عن قلقه إزاء ما لهذا القانون النموذجي من آثار ضمنية على سيادة الدول التي يســتخدم مواطنوها أو الأعمال التجارية الموجودة فيها خدمات إدارة الهوية وتوفير الثقة عبر الحدود. ومن أجل فهم هذا الشـاغل، قد يكفي النظر إلى واقع السـوق من منظور البلدان النامية، وملاحظة كيف أصـبحت جميع القطاعات ذات الصـــلة في هذه البلدان واقعة تحت هيمنة شـــركات رقمية عالمية تقع مقراتها في عدد قليل من البلدان الرقمية الرائدة، وتقدم خدماتها للمشـتركين في جميع أنحاء العالم. وإضـافة إلى ذلك، فإن إشـراك مقدمي الخدمات الرقمية في مجال خدمات إدارة الهوية، في الوقت الذي لم تعهد لهم الحكومات المعنية بهذه المهمة من قبل، وخصـوصـا عندما تكون النعوت التي يجمعونها مرتبطة ارتباطا وثيقا بالهوية التأسـيسـية للأشـخاص، يمكن أن يكون أمرا غير منطقي ومن شـــأنه أن يؤدي إلى نتائج غير موثوقة، بل ويمكن أيضـــا أن يؤدي إلى التدخل في الوظائف السيادية المناطة بالدول بالنظر إلى ما تتمتع به من اختصاص حصري فيما يتعلق بكامل دورة حياة إدارة هوية مواطنيها. وينطوي ذلك أيضـــا على خطر فقدان البيانات والإضـــرار بالسـيادة التكنولوجية والســـيبرانية للبلدان النامية، وكذلك فقدان الحماية التي تكفلها القوانين الإلزامية المعمول بها في تلك البلدان لمواطنيها. وتصـبح العواقب الضـارة المترتبة على هذه الممارسـة أكثر وضـوحا إذا نظرنا إلى حالة التبعية التي تعاني منها البلدان النامية والضـــغوط الكبيرة التي تتعرض لها في محافل التجارة العالمية لاختيار نموذج الاقتصاد الرقمي العالمي السائد في عدد قليل من البلدان التي تقع فيها مقرات معظم الشركات الرقمية العملاقة. ولذلك، تعرب جمهورية إيران الإسلامية عن اعتقادها الراسخ بأنه إذا ما كان سيتاح للبلدان النامية أن تستفيد من عمل المنظمات الدولية، ينبغي لها أولا أن تكون قادرة على حماية سـيادتها ونظامها العام. وفي ضـوء ما تقدم، نعتقد أن أحكام القانون النموذجي بشـأن اسـتخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود تفتقر إلى إشارة صريحة إلى حماية سيادة الدول، والمساواة، وعدم التدخل في المسائل التي تقع حصرا ضمن الولاية القضائية الداخلية للدول.

6- ويضاهي ذلك أهمية الحفاظ على النظام العام للدول المشترِعة. ففي الوقت الحاضر، أصبحت تدفقات البيانات عبر الحدود وقدرة مقدمي الخدمات الأجانب على الوصـــول إلى بيانات مواطني البلدان الأخرى والشـــركات الموجودة فيها شـــاغلا رئيســـيا من الشـــواغل المتعلقة بالنظام العام في العديد من الدول النامية. وعلى خلاف نصـوص الأونسـيترال السـابقة (مثل المواد 6 و7 و8 و11 و12 و15 و17 من القانون النموذجي بشـأن التجارة الإلكترونية)، لا يوجد إجراء متاح بمقتضـى هذا القانون النموذجي للحد من نطاق الصـك أو آثار أيٍّ من مواده عند الاقتضـاء، وخصـوصـا لأغراض النظام العام للدول المشـترِعة. ونرى أنه لما كان تطبيق هذا القانون النموذجي قد ينطوي على مســـائل مختلفة تتعلق بالنظام العام من المتوخى تركها لكل دولة على حدة، فإنه ينبغي إتاحة قدر من المرونة بغية تمكين محاكم الدولة المشترِعة أو السلطات المسؤولة عن تطبيق القانون النموذجي من منع الآثار القانونية المترتبة على اســـتخدام الخدمات الأجنبية لإدارة الهوية أو توفير الثقة، أو إبطال تلك الآثار، بالاستناد إلى أسباب إلزامية، بما في ذلك النظام العام لتلك الدولة.

الحلول المقترحة

7- من الضروري أن يوضح هذا الصك صراحة أن القانون النموذجي ينبغي أن يُنفَّذ على نحو يحترم مبادئ سيادة الدول والمساواة وعدم التدخل في الشؤون الداخلية للدول الأخرى. وإضافة إلى ذلك، لا ينبغي لهذا الصك أن يأذن لمقدمي خدمات إدارة الهوية/توفير الثقة الأجانب بالاضطلاع بالمهام ذات الطابع السيادي التي تقع تحت الاختصاص الحصري للدول وفقا لقوانينها الداخلية. وبالمثل، من المتوقع أن يُشار إلى ذلك في القسم واو من المذكرة التفسيرية بوصفه مبدأ عاما ومفهوما رئيسيا.

8- ومن أجل الاستجابة للشواغل المتعلقة بالنظام العام، وتماشيا مع الموقف الذي اتخذته الأونسيترال من قبل في نصوصها السابقة، من المستصوب النظر في ثلاثة خيارات:

أولا: إدراج بعض الأحكام في القانون النموذجي التي تسمح للولايات القضائية المشترِعة باستبعاد تطبيق مواد معينة من هذا الصك أو آثار تلك المواد في الحالات التي تتعارض فيها مع النظام العام لتلك الولايات القضائية (هناك عدة سوابق تفيد بذلك في نصوص الأونسيترال السابقة).

ثانيا: من الممكن إتاحة قدر من المرونة في صياغة بعض المواد بغية تقييد نطاق تطبيقها المطلق. ومن ذلك مثلا إضافة عبارة إلى الفقرة الفرعية 3 من المادتين 10 و22 يكون نصها على غرار ما يلي: "لدى تقرير موثوقية الطريقة، وما لم ترَ الجهة المختصة ضرورة لغير ذلك، لا يعتد بما يلي...:". وعلى نفس المنوال، يمكن تعديل الفقرة الفرعية 4 من المادتين 11 و23 ليصبح نصها على غرار ما يلي: "لدى تعيين خدمات إدارة الهوية، وما لم ترَ [الجهات، من الأفراد أو الأجهزة أو السلطات، سواء أكانت جهات عامة أم خاصة، التي تقضي الولاية القضائية المشترِعة بأنها مختصة،] ضرورة لغير ذلك، لا يعتد بما يلي:...". وإضافة إلى ذلك، من شأن الاستعاضة عن كلمة "يكون" في عبارة "يكون لتحديد..." الواردة في المادتين 25 و26 بعبارة "يمكن أن يكون..." أن يوفر المرونة في صياغة المواد المذكورة بغرض الاستجابة للشواغل المتعلقة بالنظام العام، وكذلك يبدو منطقيا أكثر في ضوء عدم وضوح المعايير الدولية المعترف بها المذكورة في المادتين 25 (2) و26 (2).

ثالثا: إذا تعذر الأخذ بالخيارين المذكورين أعلاه، سيكون من المفيد توفير قاعدة عامة بمقتضى القانون النموذجي تشير إلى الاستثناءات المستندة إلى النظام العام وتترك التفاصيل لكل ولاية قضائية مشترِعة لتحديدها في تشريعاتها.

3- القانون الإلزامي الغالب

9- المسألة: في الوقت الحاضر، يعرض مقدمو خدمات إدارة الهوية/توفير الثقة خدماتهم على مواطنين وشركات في دول أخرى. وفي حين أن هذه الظاهرة حتمية وتمثل عنصرا لا غنى عنه في التجارة الإلكترونية العالمية، ينبغي اتخاذ تدابير احترازية من أجل ضمان امتثال مقدمي الخدمات للقوانين الإلزامية الغالبة ذات الصلة التي لا يجوز الحيد عنها.

10- وتدرك جمهورية إيران الإسلامية أن هذا الصك لا يمس بتطبيق أي قانون إلزامي قد يتداخل مع نطاق أحكامه، وتدرك أيضا أنه لا يُقصد من القانون النموذجي أن يتدخل في تطبيق قواعد القانون الدولي الخاص. ومع ذلك، نحن نعتقد اعتقادا راسخا بأن هناك حاجة إلى إدراج حكم محدد في هذا الصك بشأن إنفاذ القانون الإلزامي للبلد الذي تُقدَّم فيه أو تُوجَّه إليه خدمات إدارة الهوية أو توفير الثقة. وهناك أسباب عديدة لاتباع هذا النهج. ويتعلق السبب الأول بقدرة مقدمي الخدمات على الوصول إلى بيانات المواطنين والشركات والمنظمات في البلد المعني. وبالنظر إلى أن البيانات مورد قيّم قد يقع، في حالة الخدمات التي تتجاوز نطاق الحدود الإقليمية، في أيدي مقدمي الخدمات الأجانب، نعتقد أن أصحاب البيانات سيكونون في أفضل وضع إذا أُخضعت بياناتهم

لنظام الحماية والقانون الإلزامي المطبقين في البلد الذي تُقدَّم فيه أو تُوجَّه إليه الخدمة. والسبب الثاني هو عدم وجود قاعدة واضحة بمقتضى القانون الدولي الخاص تحدد القانون المنطبق والقواعد الإلزامية الغالبة بشأن حماية مستخدمي خدمات التجارة الإلكترونية. ويبدو أن هناك توافقا عاما في الآراء على القانون المنطبق بشأن حماية المستهلكين في سياق عقود المستهلكين، إلا أن بعض الغموض قد ينشأ فيما يتصل بحماية المشتركين في سياق العقود المبرمة مع مقدمي الخدمات الرقمية، وهي عقود قد لا تندرج ضمن نطاق قانون حماية المستهلك. ويتعلق السبب الثالث بما تنطوي عليه العقود المبرمة بين المشتركين ومقدمي الخدمات من اختلال في موازين القوى. ففي كثير من الأحيان، يكون المشتركون في مواقف غير متكافئة عندما يتعلق الأمر بإبرام عقد في بيئة رقمية والموافقة على القواعد والسياسات والممارسات التشغيلية المنظِّمة له. ونرى أن الشروط المدرجة في العقود المبرمة بين المشتركين ومقدمي الخدمات هي في معظمها شروط لا يجري التفاوض عليها، وعادة ما تتضمن بنودا بشأن القانون المنطبق أو اختيار المحكمة مؤاتية أكثر لمقدمي الخدمات على حساب المشتركين. ومن شأن عدم إدراج أي إشارة في القانون النموذجي إلى قانون البلد الذي تُقدَّم فيه أو تُوجَّه إليه الخدمة، أو النص على إنفاذ ذلك القانون، أن يترك المشتركين دون الحماية اللازمة التي يستحقونها.

الحلول المقترحة

11- يتطلب إيجاد ضمانات وحلول ملائمة للاستجابة للشواغل المذكورة أعلاه مزيدا من التعاون الدولي والحوار بشأن السياسات، بمشاركة كاملة من البلدان النامية التي غالبا ما تكون متلقية للخدمات العابرة للحدود. ومع ذلك، نعرض فيما يلي بعض اقتراحاتنا:

- ينبغي أن يكون اشتراط "امتثال القواعد والسياسات والممارسات التشغيلية الخاصة بمقدم خدمات إدارة الهوية/توفير الثقة للقانون الإلزامي المعمول به في المكان الذي تُقدَّم فيه أو تُوجَّه إليه خدماتهم" التزاما يدرج في المادتين 6 و14 ويتعين على مقدمي خدمات إدارة الهوية/توفير الثقة الامتثال له، وكذلك عنصرا ينبغي النظر فيه فيما يتصل بكل من تحديد موثوقية الطريقة (لاحقا) في المادتين 10 (2) و22 (2)، وتعيين الخدمات الموثوقة (مسبقا) في المادتين 11 (2) (أ) و23 (2) (أ)، ومعيارا يُطبَّق على الطلبات المتعلقة بمنح الأثر القانوني في تقديم الخدمات عبر الحدود في المادتين 25 و26.

- ولأغراض إنفاذ القانون الإلزامي المعمول به في المكان الذي تُقدَّم فيه أو تُوجَّه إليه الخدمة، ستكون هناك حاجة إلى فرض التزامات أخرى على مقدمي الخدمات في المادتين 6 و14 يمكن تناولها بمزيد من التفصيل في الفقرتين 113 و175 من المذكرة التفسيرية. ومن ذلك مثلا تعاون مقدمي الخدمات مع سلطات إنفاذ القانون في البلد الذي تُقدَّم فيه أو تُوجَّه إليه الخدمة (مثلا في المسائل المتعلقة بحماية البيانات أو الحالات التي يمكن أن تؤدي إلى نشوء مسؤولية تقصيرية أو جنائية، بما في ذلك الوقاية من الجرائم أو التحقيق في الجرائم أو كشفها أو ملاحقة مرتكبيها قضائيا)، وتحقيقا لهذه الغاية، إنشاء مكاتب محلية أو تعيين ممثلين في ذلك البلد، وتعديل شروط الخدمات والسياسات المطبقة لدى مقدمي الخدمات وفقا للقانون الإلزامي المعمول به في المكان الذي تُقدَّم فيه أو تُوجَّه إليه الخدمات وما إلى ذلك. ونعتقد أن الإخلال بهذه الالتزامات ينبغي أن يكون أساسا لمسؤولية مقدمي خدمات إدارة الهوية/توفير الثقة بموجب المادتين 12 و24.

- ومن شأن الامتثال للالتزامات المذكورة أعلاه أن ييسر تحقيق هدف الاعتراف المتبادل الوارد في المادتين 25 و26. ومن ثمَّ، سيكون من المستصوب للغاية أن توفِّر الولايات القضائية المشترعة، من خلال تبادل المعلومات المشار إليه في المادة 27، معلومات بشأن ما تطبقه من شروط قانونية إلزامية. ويمكن لهذه المعلومات أن تمكِّن مقدمي الخدمات الأجانب الراغبين في تقديم خدماتهم خارج

الحدود الإقليمية من تعديل شروط خدماتهم وسياساتهم بحيث تمتثل مسبقا للأنظمة ذات الصلة. ويمكن إدراج مزيد من التفاصيل بشأن هذا التعاون في الفقرة 234 من المذكرة التفسيرية.

4- الاستخدام الطوعي لخدمات إدارة الهوية وتوفير الثقة

12- **المسألة:** تعرب جمهورية إيران الإسلامية عن قلقها إزاء الاستدلال على موافقة شخص ما من خلال مسلكه، المشار إليه في المادة 3 (2) من القانون النموذجي. فعلى الرغم من أن هذه قاعدة راسخة بموجب نصوص الأونسيترال السابقة، يراودنا شعور قوي بأنها ستكون غير منصفة للأشخاص الذين لديهم معرفة ضعيفة بالتكنولوجيا، ولا يدركون بالضرورة أنهم، باشتراكهم في خدمة ما أو استخدامهم لبرمجية محددة للتجارة الإلكترونية، يسمحون باستخدام خدمات إدارة الهوية أو توفير الثقة التي تدعمها تلك البرمجيات. وإضافة إلى ذلك، يمكن أن يؤدي هذا الوضع إلى مزيد من الآثار السلبية إذا أخذنا في الاعتبار أن المشتركين، عند إبرام العقود الرقمية، يفعلون ذلك على أساس "القبول أو الرفض"، وكذلك عند قبولهم الأعمى أحيانا للأحكام والشروط المنصوص عليها ضدهم، التي تحدد الحالات التي يمكن بموجبها افتراض موافقتهم على الأحكام والشروط التعاقدية. ونود أن نلفت انتباه اللجنة إلى أن المستهلكين الأوروبيين يتمتعون بالحماية من الشروط التعاقدية الموحدة المجحفة بموجب توجيه صادر عن الاتحاد الأوروبي بشأن شروط التعاقد المجحفة (93/13/EEC)، ولكن يبدو لنا أنه لا توجد تشريعات واسعة النطاق لهذا الغرض في البلدان غير الأوروبية.

الحل المقترح

13- نود أن نقترح إتاحة بعض المرونة فيما يتعلق بالاستدلال على موافقة الشخص على استخدام خدمة إدارة الهوية/توفير الثقة من خلال مسلكه، وأن نشدد على أن هذه الموافقة الضمنية ينبغي أن تُحدَّد بطريقة أوضح وأكثر قابلية للتنبؤ بها. ومن ثمَّ، سيكون من المفيد للدول الأعضاء أن تناقش ذلك بمزيد من التفصيل وأن تضع حلولا بشأن كيفية الوفاء بهذا الاشتراط بصورة أفضل فيما يتعلق بالعقود المبرمة في البيئة الرقمية. ونرى أنه سيكون من المفيد أن تتخذ هذه الموافقة الضمنية من قِبل الأطراف شكل افتراض يمكن دحضه بعد ذلك في مرحلة لاحقة.

5- الأرشفة الإلكترونية

14- **المسألة:** نحن ندرك أن القانون النموذجي لا يمس بالقانون المنطبق على خصوصية البيانات وحمايتها. ومع ذلك، وبالنظر إلى أن هذا المجال من القانون وثيق الصلة بالموضوع في حالة الأرشفة الإلكترونية، نعتقد أن هناك حاجة إلى التشديد في المادة 19 على أنه ينبغي إيلاء الاعتبار الواجب، فيما يتعلق بالأرشفة الإلكترونية، للقانون الإلزامي بشأن خصوصية البيانات وحمايتها. وفيما يتعلق بالقانون الإلزامي المتصل بهذه الحالة، ينبغي أن يولى الاهتمام للمهام التي يضطلع بها مقدمو خدمات إدارة الهوية/توفير الثقة عبر الحدود واعتمادهم الوثيق على بيانات مواطني البلدان الأخرى والشركات والمنظمات الموجودة فيها. وبالنظر إلى أن نقل هذه البيانات عبر الحدود يشكل شاغلا رئيسيا من الشواغل المتعلقة بالنظام العام، وقد يحرم المشتركين من نظام حماية البيانات الذي يحق لهم التمتع به، نعتقد أنه ينبغي أن يُتاح بموجب هذا القانون النموذجي المجال الكافي لمنح الأثر القانوني لقانون حماية البيانات المعمول به في البلد الذي تُقدَّم فيه أو تُوجَّه إليه الخدمة، وأن يتلقى المشتركون هذه الخدمة في ذلك المكان. وتود جمهورية إيران الإسلامية أن تلفت انتباه اللجنة إلى أن الجهات موضوع البيانات في أوروبا محمية بنطاق الانطباق الإقليمي الواسع للائحة الاتحاد الأوروبي التنظيمية العامة لحماية البيانات، ولكن قد لا تتوافر في أماكن أخرى، خاصة في بلدان العالم الثالث،

مثل هذه اللائحة الواسعة النطاق، التي تعد ملزمة لمقدمي الخدمات الأجانب ويمكن أن تجبرهم على احترام قانون الحماية المعمول به في المكان الذي تُقدَّم فيه أو تُوجَّه إليه خدماتهم.

الحلول المقترحة

15- التشديد صراحة في المادة 19 على أنه: "ينبغي أن يخضع الاحتفاظ بالوثائق أو السجلات أو المعلومات الواردة في المادة 19 لضمانات ملائمة فيما يتعلق بقانون خصوصية البيانات وحمايتها". وبغية الاستجابة للشاغل الثاني المذكور أعلاه، نقترح إدراج فقرة بهذا المعنى مفادها أن الأرشفة الإلكترونية لن تحرم المشتركين في خدمات إدارة الهوية/توفير الثقة عبر الحدود من نظام حماية البيانات الذي يحق لهم التمتع به بمقتضى القانون المعمول به في المكان الذي تُقدَّم فيه أو تُوجَّه إليه الخدمة.

6- العناصر الناقصة

16- من أجل إعداد نص أكثر شمولا من نواح كثيرة، ينبغي النظر في إدراج بعض العناصر الناقصة في القانون النموذجي. ومن ذلك مثلا تعريف مصطلحات "مستوى الضمان" و"مستوى الموثوقية" و"الطرف المعوِّل" الواردة في المادة 1، ووصفٌ لحقوق الطرف المعوِّل والتزاماته، وكذلك يلزم اتباع نهج صريح وأكثر شمولا إزاء حقوق المشتركين.

طاء- بلغاريا

[الأصل: بالإنكليزية]
[8 حزيران/يونيه 2022]

1- يستند القانون الوطني البلغاري وقانون الاتحاد الأوروبي بشأن خدمات التحديد الإلكتروني للهوية وتوفير الثقة (التوثُّق) إلى لائحة الاتحاد الأوروبي رقم 2014/910 بشأن خدمات تحديد الهوية إلكترونيا وتوفير الثقة في السوق الداخلية وخدمات توفير الثقة في سياق المعاملات الإلكترونية، التي ألغت توجيه الاتحاد الأوروبي رقم 93/1999. وصلاحيات لجنة التنظيم البلغارية محددة بموجب المادة 32 من القانون بشأن الوثائق الإلكترونية وخدمات التوثق الإلكترونية، التي تنص على أن لجنة التنظيم هي السلطة الإشرافية الوطنية في مجال خدمات التوثق الإلكترونية، وهي المسؤولة عن تنفيذ أحكام لائحة الاتحاد الأوروبي المذكورة.

2- وترسي لائحة الاتحاد الأوروبي رقم 2014/910 إطارا قانونيا مشتركا لاستخدام خدمات التوثق في الدول الأعضاء في الاتحاد الأوروبي، في حين تنظم المادة 14 من اللائحة الاعتراف بخدمات التوثق الناشئة في دولة خارج الاتحاد. ويجوز الاعتراف بهذه الخدمات في حال إبرام اتفاق بين الاتحاد الأوروبي ودولة ثالثة معنية أو منظمة دولية، وفقا للمادة 218 من المعاهدة المنظِّمة لعمل الاتحاد الأوروبي.

3- وفي ضوء ما تقدم، ترى لجنة التنظيم البلغارية أن مشروع القانون النموذجي المقدم الذي أعدته الأونسيترال يحقق الأهداف والمبادئ الرئيسية المبينة في لائحة الاتحاد الأوروبي رقم 2014/910.

ياء - سنغافورة

[الأصل: بالإنكليزية]
[13 حزيران/يونيه 2022]

1- تعرب سنغافورة عن تقديرها للفريق العامل الرابع لما اضطلع به من أعمال متعلقة بمشروع القانون النموذجي بشأن استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود.

2- ونود أن نلفت انتباه اللجنة إلى ثلاثة جوانب من مشروع القانون النموذجي (بصيغته الواردة في الوثيقة A/CN.9/1112) تستحق دراسة متأنية، على النحو الموجز أدناه.

(أ) يتعلق الجانب الأول بضرورة القيام بما يلي:

'1' تبيان العلاقة بين المادة 9 والمادة 10 (1) (المتعلقة بخدمات إدارة الهوية) بقدر أكبر من الوضوح عن طريق إدراج عبارة "وفقا للمادة 10 (1)" في المادة 9، بحيث يصبح نص العبارة الواردة في المادة 9 على غرار ما يلي: "*عندما تُستخدم طريقة، وفقا للمادة 10 (1)، لتحديد هوية الشخص إلكترونيا لذلك الغرض*"؛

'2' تبيان العلاقات بين كل من المواد من 16 إلى 21 والمادة 22 (1) (المتعلقة بخدمات توفير الثقة) بقدر أكبر من الوضوح عن طريق إدراج عبارة "وفقا للمادة 22 (1)" في كل مادة من المواد من 16 إلى 21، بحيث يكون نص العبارات المعنية الواردة في المواد من 16 إلى 21 على غرار ما يلي: "*إذا استُخدمت طريقة، وفقا للمادة 22 (1)، من أجل ما يلي...*".

(انظر المناقشة المفصَّلة الواردة في الفقرتين 3 و4 أدناه)

(ب) يتعلق الجانب الثاني بأهمية الاحتفاظ بـ"شروط الأمان" المبينة في المادة 10 (1) (ب) (المتعلقة بموثوقية خدمات إدارة الهوية) والمادة 22 (1) (ب) (المتعلقة بموثوقية خدمات توفير الثقة). وتسعى شروط الأمان المذكورة، التي تحاكي الشروط الواردة في المادة 9 (3) (ب) '2' من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية (2007) (اتفاقية الخطابات الإلكترونية)[5] والمادة 12 (ب) من قانون الأونسيترال النموذجي بشأن السجلات الإلكترونية القابلة للتحويل (2017) (اتفاقية السجلات الإلكترونية)، إلى تجنب الطعون القانونية الزائفة (أي التي تستند إلى أن الطريقة المستخدمة لم تكن موثوقة بالقدر المناسب من الناحية النظرية)، عن طريق النص على أن الطريقة تعتبر قد استوفت الشرط الوارد في المادة 9 أو المواد من 16 إلى 21 إذا أثبتت فعليا، بحد ذاتها أو مقترنة بأدلة إضافية، أنها أدت الوظيفة المبينة في المادة 9 أو الوظائف ذات الصلة المبينة في المواد من 16 إلى 21 (أي الموثوقية الفعلية). ونرى أن المادتين 10 (1) (ب) و22 (1) (ب) توفران ضمانات حاسمة الأهمية ضد هذه الطعون الزائفة، وينبغي الإبقاء عليهما بنفس الصيغة. وإضافة إلى ذلك، من شأن حذف (أو نقل) المادتين 10 (1) (ب) و22 (1) (ب) أن يجعل مشروع القانون النموذجي غير متسق مع اتفاقية الخطابات الإلكترونية وقانون السجلات الإلكترونية. وفي هذه الحالة، سيتعين على اللجنة أن (أ) تكوّن رأيا بشأن ما ينبغي أن تفعله الدول الأطراف في اتفاقية الخطابات الإلكترونية أو التي اشترعت قانون السجلات الإلكترونية من أجل معالجة عدم الاتساق المذكور؛ (ب) البت فيما إذا كانت اللجنة ستواصل توصية الدول التي تنظر في الانضمام إلى اتفاقية الخطابات

(5) على غرار الطريقة التي تحدد بها المادة 10 (1) شروط تقرير موثوقية الطريقة المستخدمة لتحديد الهوية إلكترونيا، تحدد المادة 9 (3) (ب) من اتفاقية الخطابات الإلكترونية شروط تقرير موثوقية الطريقة المستخدمة لإنشاء توقيع إلكتروني.

الإلكترونية أو في اشتراع قانون السجلات الإلكترونية (بما يشمل الأحكام غير المتسقة) بتلك الاتفاقية أو بذلك القانون النموذجي. ونقترح إدخال تعديلات على الفقرتين 142 و143 من مشروع المذكرة التفسيرية بغية تبيان الغرض من مشروع المادة 10 (1) (ب) وأثرها بصورة أدق.

(انظر المناقشة المفصَّلة الواردة في الفقرات 5 إلى 16 أدناه)

(ج) يتعلق الجانب الثالث بعبارة "مستوى مكافئا على الأقل من الموثوقية" الواردة في المادتين 25 و26. ونرى أن اشتراط التكافؤ الدقيق في الموثوقية كشرط للاعتراف المتبادل بخدمة أجنبية لإدارة الهوية أو توفير الثقة أمر غير قابل للتطبيق. إذ لا يمكن تحديد مستويات الموثوقية بدقة متناهية، ومن المحتم أن يؤدي اشتراط التكافؤ الدقيق إلى إثارة صعوبات عملية في الاعتراف عبر الحدود. وستكون عبارة "مستوى مكافئا جوهريا أو أعلى من الموثوقية"[(6)] أكثر ملاءمة في السياق المتعدد الأطراف.

(انظر المناقشة المفصَّلة الواردة في الفقرات 17 إلى 19 أدناه)

أولا- العلاقة بين المادة 9 والمادة 10 (1)، والعلاقة بين المواد من 16 إلى 21 والمادة 22 (1)

3- تتشكل بنية القانون النموذجي على النحو التالي:

(أ) تحدد المادة 9 قاعدة التكافؤ الوظيفي الخاصة بتحديد هوية الشخص الذي يستخدم خدمات إدارة الهوية، في حين تحدد المادة 10 (1) شروط الموثوقية التي يجب أن تمتثل لها طريقة تحديد الهوية الواردة في المادة 9.

(ب) بالمثل، تنص المواد من 16 إلى 21 على قواعد التكافؤ الوظيفي الخاصة بالتوقيعات الإلكترونية (المادة 16)، والأختام الإلكترونية (المادة 17)، وأختام الوقت الإلكترونية (المادة 18)، والأرشفة الإلكترونية (المادة 19)، وخدمات التوصيل المسجَّل الإلكتروني (المادة 20)، والتوثُّق من المواقع الشبكية (المادة 21)، في حين تبين المادة 22 (1) شروط الموثوقية التي يجب أن تمتثل لها كل طريقة من الطرق المذكورة في المواد من 16 إلى 21.

4- ونرى أنه ينبغي توضيح العلاقة بين المادة 9 والمادة 10 (1)، وبين كل مادة من المواد من 16 إلى 21 والمادة 22 (1)، عن طريق إدراج عبارة "*وفقا للمادة 10 (1)*،" مباشرة بعد عبارة "*عندما تُستخدم طريقة*،" الواردة في المادة 9، وبإدراج عبارة "*وفقا للمادة 22 (1)*،"مباشرة بعد عبارة "*إذا استُخدمت طريقة*،" الواردة في كل مادة من المواد 16 إلى 21. ومن شأن ذلك أن يوضح أن هذا الشرط يُستوفى إذا استُخدمت طريقة ما، وفقا للمادة 10 (1) أو المادة 22 (1)، لتأدية هذه الوظائف، وذلك بغية تجنب ما قد يوحي بأن *أي* طريقة ستكون كافية. وترد الصيغ المنقحة لتلك المواد في التذييل أدناه.

ثانيا- المادتان 10 (1) (ب) و22 (1) (ب)

ألف- منع الطعون القانونية الزائفة

5- تنص المادة 10 (1) من مشروع القانون النموذجي على ما يلي:

المادة 10- اشتراطات تقرير موثوقية خدمات إدارة الهوية

(6) نُظر في هذا المصطلح خلال دورة الفريق العامل الثالثة والستين.

1- لأغراض المادة 9، تكون الطريقة كما يلي:

(أ) موثوقا بها بقدر مناسب للغرض الذي تُستخدم من أجله خدمة إدارة الهوية؛ أو

(ب) أثبتت فعليا أنها أدت الوظيفة المبينة في المادة 9.

6- وتنص المادة 22 (1) من مشروع القانون النموذجي، التي لها بنية مماثلة، على ما يلي:

المادة 22- اشتراطات تقرير موثوقية خدمات توفير الثقة

1- لأغراض المواد من 16 إلى 21، تكون الطريقة كما يلي:

(أ) موثوقا بها بقدر مناسب للغرض الذي تُستخدم من أجله خدمة توفير الثقة؛ أو

(ب) أثبتت فعليا أنها أدت الوظائف المبينة في المادة.

7- وترد "شروط الأمان" المعنية في المادتين 10 (1) (ب) و22 (1) (ب). وهي تعكس المادة 9 (3) (ب) '2' من اتفاقية الخطابات الإلكترونية والمادة 12 (ب) من قانون السجلات الإلكترونية وتخدم نفس الغرض – أي منع الطعون القانونية الزائفة في الصلاحية.

(أ) تنص المادة 9 (3) من اتفاقية الخطابات الإلكترونية، التي تتضمن قاعدة التكافؤ الوظيفي الخاصة بالتوقيعات الإلكترونية، على ما يلي:

3- حيثما يشترط القانون أن يكون الخطاب أو العقد ممهورا بتوقيع طرف ما، أو ينص على عواقب لعدم وجود توقيع، يُستوفى ذلك الاشتراط فيما يخص الخطاب الإلكتروني إذا:

(أ) استُخدمت طريقة ما لتعيين هوية الطرف المعني وتبيين نية ذلك الطرف فيما يخص المعلومات الواردة في الخطاب الإلكتروني؛

(ب) وكانت الطريقة المستخدمة:

'1' موثوق بها بقدر مناسب للغرض الذي أُنشئ الخطاب الإلكتروني أو أُرسل من أجله، في ضوء كل الملابسات، بما فيها أي اتفاق ذي صلة؛ أو

'2' قد أثبتت فعليا، بحد ذاتها أو مقترنة بأدلة إضافية، أنها أوفت بالوظائف المذكورة في الفقرة الفرعية (أ) أعلاه.

وتتمثل المشكلة التي صيغت المادة 9 (3) (ب) '2' من اتفاقية الخطابات الإلكترونية بغية معالجتها في الخطر الذي تمثله الطعون القانونية الزائفة في صحة التوقيعات الإلكترونية، ليس على أساس أن الموقِّع المفترض لم يوقِّع، أو على أساس أن الوثيقة التي وقَّعها قد تم تحويرها، وإنما فقط على أساس أن طريقة التوقيع التي استُخدمت لم تكن موثوقة *بالقدر المناسب* في الملابسات المحيطة (أي أن الموثوقية من حيث المبدأ/النظرية ليست مناسبة في هذه الملابسات)[(7)]. وتمكِّن المادة 9 (3) (ب) '2' من دحض هذه الطعون

(7) يرد شرح ذلك بالتفصيل في الفقرة 164 من المذكرة التفسيرية لاتفاقية الخطابات الإلكترونية (المستنسخة أدناه):

"164 - بيد أن الأونسيترال اعتبرت أن الاتفاقية ينبغي ألا تتيح لطرف من الأطراف التذرع "باختبار الموثوقية" للتنصل من توقيعه في الحالات التي يكون من الممكن فيها إثبات الهوية والنية الفعليتين للطرف المعني. واشتراط أن يكون التوقيع الإلكتروني "موثوقا به بقدر مناسب" لا ينبغي أن يفضي بالمحكمة أو الهيئة القضائية إلى إبطال العقد برمته على أساس أنّ التوقيع الإلكتروني ليس موثوقا به ***بقدر مناسب***، إذا لم يكن هناك نزاع بشأن هوية الشخص الموقّع أو بشأن التوقيع ذاته، أي لم يكن هناك تساؤل بشأن صحة التوقيع الإلكتروني. ومثل هذه النتيجة ستكون مؤسفة جدا لأنها ستتيح لأحد أطراف المعاملة التي تشترط التوقيع محاولة الإفلات من التزاماته بإنكاره

القانونية الزائفة عن طريق إثبات أن الطريقة التي اســـتُخدمت قد أدت الوظائف المبينة في المادة 9 (3) (أ)، أي بإثبات أن الطريقة التي استُخدمت موثوقة *فعليا*.

(ب) تتضمن المادة 12 (ب) من قانون السجلات الإلكترونية "شرط أمان" مماثل للسبب نفسه[8].

8- وتجدر الإشـــارة أولا إلى أن عبارة "*موثوقة بقدر مناســـب*" مُســـتخدمة في المادتين 10 (1) (أ) و22 (1) (أ) لأن مدى ملاءمة موثوقية الطريقة التي اســتُخدمت يتوقف على الغرض الذي تُســتخدم من أجله الخدمة المعنية، مع مراعاة جميع الظروف ذات الصــلة التي قد تشــمل الظروف المذكورة في المادتين 10 (2) و22 (2). ومن الظروف ذات الأهمية الخاصــة وجود أي اتفاق بين الطرفين بشــأن الطريقة التي ســتُســتخدم. وبعبارة أخرى، يتوقف مدى ملاءمة الطريقة التي اســتُخدمت في معاملة معينة على ظروف تلك المعاملة، وتشــير المادتان 10 (1) (أ) و22 (1) (أ) إلى مستوى نسبي من الموثوقية، وليس إلى مستوى واحد متجانس منها.

9- وعلى غرار المادة 9 (3) (ب) '2' من اتفاقية الخطابات الإلكترونية والمادة 12 (ب) من قانون الســجلات الإلكترونية، تســعى المادتان 10 (1) (ب) و22 (1) (ب) إلى تجنب الطعون القانونية الزائفة التي تســتند إلى مدى ملاءمة موثوقية الطريقة المســتخدمة من الناحية النظرية (*الموثوقية النظرية*)، وذلك بالنص على أن الطريقة تعتبر قد اســـتوفت المادة 9 أو المواد من 16 إلى 21 إذا أثبتت فعليا، بحد ذاتها أو مقترنة بأدلة إضافية، أنها أدت الوظيفة المبينة في المادة (*الموثوقية الفعلية*).

10- ومن شــأن حذف المادتين 10 (1) (ب) و22 (1) (ب) أن يفتح الباب أمام الطعون القانونية الزائفة. وهذا أمر غير مرغوب فيه.

(أ) وفي غياب المادة 10 (1) (ب)، يمكن أن تتشـــجع الجهات الفاعلة الانتهازية (مثل طرف في معاملة تنطوي على تحديد الهوية إلكترونيا يرغب في التنصل من التزاماته، أو حتى طرف ثالث له مصلحة في إبطال صــحة الهوية الإلكترونية) على الطعن في صــحة تحديد الهوية الناتج – ليس على أساس أن تحديد الهوية لم يحدث، ولكن على أســـاس (فارغ) مفاده أن طريقة التحديد الإلكتروني للهوية المســـتخدمة لم تكن "***موثوقة بالقدر المناسب***" في الظروف المحيطة؛

صحة توقيعه (أو توقيع الطرف الآخر) – ليس على أساس أن الموقّع المفترض لم يوقّع، أو أن الوثيقة التي وقّعها قد تم تحويرها، وإنما فقط على أســـاس أن طريقة التوقيع التي اســـتُخدمت **لم تكن "*موثوقة بقدر مناســـب*"** في الملابســـات المحيطة. ولتفادي هذه الحالات، تقر الفقرة 3 (ب) '2' صــحة طريقة التوقيع – بغض النظر عن موثوقيتها من حيث المبدأ – كلما ثبت فعليا أنها عينت هوية الموقّع وبيّنت نيته فيما يخص المعلومات الواردة في الخطاب الإلكتروني".

[الخط العريض للتأكيد]

(8) انظر الفقرتين 136 و137 من المذكرة الإيضــاحية لقانون الأونســيترال النموذجي بشــأن الســجلات الإلكترونية القابلة للتحويل (المستنسخة أدناه):

"136 - تكفل الفقرة الفرعية (ب) "بندا للأمان" يرمي إلى ***منع المنازعات القضــائية الفارغة، وذلك بإقرار صــحة الأســاليب التي أثبتت في الواقع أنها تؤدي وظائفها بغض النظر عن خضــوعها لأي تقييم لموثوقيتها***. وتشـــير هذه الفقرة الفرعية إلى إنجاز الوظيفة في الحالة المحددة قيد النـــزاع، ولا ترمي إلى التنبؤ بموثوقية الطريقة في المستقبل من واقع أدائها في السابق. ويمكن إعمال هذا الحكم فيما يتعلق بأي من الوظائف المطلوب أداؤها باســـتخدام الســـجلات الإلكترونية القابلة للتحويل. ترد آلية مماثلة في الفقرة 3 (ب) '2' من المادة 9 من اتفاقية الخطابات الإلكترونية بشأن التعادل الوظيفي للتوقيعات الإلكترونية.

137- ولما كانت الطريقة المســتخدمة قد أدت الوظيفة المطلوبة بالفعل، فإن هذا، من الناحية العملية، ***ســوف يحول دون إثارة أي مناقشة بشأن تقييم موثوقيتها وفقا للفقرة الفرعية (أ)***".

[الخط العريض للتأكيد]

(ب) وينطبق التحليل نفسه في سياق خدمات الثقة. فإذا أخذنا التوقيعات الإلكترونية كمثال، سنجد أنه في غياب المادة 22 (1) (ب)، يمكن أن يتشجع أحد أطراف معاملة استُخدم فيها توقيع إلكتروني على محاولة التنصل من التزاماته عن طريق إنكار صحة توقيعه (أو توقيع الطرف الآخر) – ليس على أساس أن الموقِّع المفترض لم يوقِّع، أو أن الوثيقة التي وقعها قد تم تحويرها، وإنما فقط على أساس (فارغ) مفاده أن طريقة التوقيع التي استُخدمت لم تكن "*موثوقة بالقدر المناسب*" في الظروف المحيطة. ويمكن أيضا أن يتشجع طرف ثالث له مصلحة في إبطال المعاملة على محاولة القيام بذلك.

11- وقد يقال جدلا إن المادتين 10 (1) (أ) و22 (1) (أ) وحدهما كافيتان لتجنب النتائج غير المرغوبة الموصوفة أعلاه – لأن المحكمة أو الهيئة القضائية يمكن أن ترفض الطعون القانونية الانتهازية عن طريق التوصل إلى استنتاج لاحق مفاده أن الطريقة التي استُخدمت في المعاملة كانت "*موثوقة بالقدر المناسب*" للغرض الذي استُخدمت من أجله الخدمة، على النحو المبين في المادة 9 (تحديد الهوية) أو المواد من 16 إلى 21 (خدمات الثقة). بيد أننا نرى أن هذا النهج ينطوي على مشكلتين، تتمثل الأولى في أنه حتى لو رُفضت الطعون القانونية الانتهازية في نهاية المطاف، فإن هذه الطعون القانونية لا تزال تمثل دعاوى قضائية لا ضرورة لها في سياق معاملات التجارة الإلكترونية. وهذا أمر غير مرغوب فيه.

12- أما المشكلة الثانية والأهم فهي أنه من شأن حذف شروط الأمان الواردة في المادتين 10 (1) (ب) و22 (1) (ب)، ومن ثمَّ تعريض جميع المعاملات الإلكترونية التي تُجرى بموجب التشريعات الداخلية المشترِعة للقانون النموذجي لخطر تقديم طعون قانونية زائفة قد تنطوي على تحديد الهوية إلكترونيا (المادة 9)، أو التوقيعات الإلكترونية (المادة 16)، أو الأختام الإلكترونية (المادة 17)، أو أختام الوقت الإلكترونية (المادة 18)، أو الأرشفة الإلكترونية (المادة 19)، أو التوصيل المسجَّل الإلكتروني (المادة 20)، أو التوثُّق من المواقع الشبكية (المادة 21)، أن يؤدي إلى عدم اليقين في المعاملات التجارية الرضائية. ويمكن توضيح ذلك بالمثال التالي:

(أ) لنفترض أنه في عام 2023 (عندما يكون القانون النموذجي قد اشتُرع كقانون داخلي في بعض الولايات القضائية)، اتفق طرفان على توقيع عقد ما باستخدام توقيع رقمي يستند إلى خوارزمية بعثرة مأمونة بمستوى بعثرة قدره 256 بِتًّا (SHA2-256) (أي التي تولِّد تشفيرا قدره 256 بِتًّا)؛

(ب) ولا يوجد نزاع على أن الطرفين قد وقَّعا العقد. ولم يُزعم أيضا أن العقد قد تم تحويره بأي شكل من الأشكال؛

(ج) ولكن في غياب شرط الأمان، سيكون الباب مفتوحا أمام الطرف ألف (الذي يريد مثلا التنصل من العقد الذي وقعه مع الطرف باء لأنه اكتشف أن الصفقة خاسرة) للطعن في صحة التوقيعات الرقمية المستخدمة في توقيع العقد بادعاء أن خوارزمية البعثرة لم تكن "*موثوقة بالقدر المناسب*"، لأنه كان يجب استخدام خوارزمية بعثرة مأمونة بمستوى بعثرة قدره 512 بِتًّا (SHA3-512) وليس بمستوى 256 بِتًّا، الذي لا يعد مستوى موثوقا بقدر مناسب.

ومن شأن هذا الوضع أن يكون مؤسفا. ونرى أنه في حين يتمتع معيار "*موثوقا بها بقدر مناسب*" بالقدر الكافي من المرونة، من الضروري التصدي لخطر الطعون القانونية المستندة إلى الملاءمة النظرية لموثوقية الطريقة المستخدمة. ومن أجل توفير اليقين للأعمال التجارية، نرى أن من غير المناسب الاعتماد فقط على معيار "*موثوقا بها بقدر مناسب*". فكيف يمكن للأعمال التجارية (مثل الطرف باء في مثالنا أعلاه) أن تثق في أن المعاملات الإلكترونية التي تجريها في عام 2023 لن تكون معرَّضة للطعون القانونية الزائفة في المستقبل؟ وتهدف شروط الأمان، بصيغتها الواردة في المادتين 10 (1) (ب) و22 (1) (ب) من مشروع القانون النموذجي، إلى الحيلولة دون ذلك.

باء- الحفاظ على اتساق مشروع القانون النموذجي مع اتفاقية الخطابات الإلكترونية وقانون السجلات الإلكترونية

13- من شأن الإبقاء على المادتين 10 (1) (ب) و22 (1) (ب) بصيغتهما الحالية أن يحافظ على اتساق مشروع القانون النموذجي مع اتفاقية الخطابات الإلكترونية التي تعد أحدث صك للأونسيترال بشأن المعاملات الإلكترونية. ومن المهم للغاية أن يظل مشروع القانون النموذجي متسقا مع المادة 9 (3) (ب) '2' من اتفاقية الخطابات الإلكترونية، إذ أن العديد من الدول (بما في ذلك سنغافورة) أطراف في اتفاقية الخطابات الإلكترونية، ومن ثمَّ، لا يمكنها اشتراع أي قوانين تتعارض معها. وهناك أيضا دول ليست أطرافا في اتفاقية الخطابات الإلكترونية، ولكنَّها اشترعت قوانين بشأن المعاملات الإلكترونية بالاستناد إلى الاتفاقية، بما يشمل شرط الأمان[9]. ومن شأن حذف المادتين 10 (1) (ب) و22 (1) (ب) (وخصوصا المادة 22 (1) (ب)) أن يؤدي إلى عدم اتساق مشروع القانون النموذجي مع المادة 9 (3) (ب) '2' من اتفاقية الخطابات الإلكترونية. ومن شأن ذلك أيضا أن يكون مبعث قلق للدول التي ستنضم إلى الاتفاقية في المستقبل.

14- وكذلك ستكون الدول التي اشترعت قانون السجلات الإلكترونية كقانون داخلي أو تعتزم اشتراعه قلِقة من حذف المادتين 10 (1) (ب) و22 (1) (ب) من مشروع القانون النموذجي لأنه سيؤدي إلى عدم اتساق مشروع القانون النموذجي مع قانون السجلات الإلكترونية.

15- وفي حال عدم الإبقاء على المادتين 10 (1) (ب) و22 (1) (ب) بصيغتهما الحالية، سيتعين على اللجنة (أ) تكوين رأي بشأن ما ينبغي أن تفعله الدول الأطراف في اتفاقية الخطابات الإلكترونية أو التي اشترعت قانون السجلات الإلكترونية من أجل معالجة عدم الاتساق المذكور؛ (ب) البت فيما إذا كانت اللجنة ستواصل توصية الدول التي تنظر في الانضمام إلى اتفاقية الخطابات الإلكترونية أو في اشتراع قانون السجلات الإلكترونية (بما يشمل الأحكام غير المتسقة) بتلك الاتفاقية أو بذلك القانون النموذجي.

جيم- تعديلات على مشروع المذكرة التفسيرية من أجل توضيح الغرض من المادتين 10 (1) (ب) و22 (1) (ب)

16- تماشيا مع الفهم الصحيح للغرض من "شرط الأمان" الوارد في المادتين 10 (1) (ب) و22 (1) (ب)، ينبغي تعديل الفقرتين 142 و143 من مشروع المذكرة التفسيرية ليصبح نصهما على غرار ما يلي:

142- وتتضمن الفقرة 1 (ب) بندا يهدف إلى الحيلولة دون رفض خدمة إدارة الهوية حين تكون قد أدت وظيفتها فعليا. ويحدث الرفض عندما يعلن كيان ما عدم أداء إجراء ما. ولكي تُفعَّل الآلية الواردة في الفقرة 1 (ب)، يجب أن تكون الطريقة، سواء كانت **<u>موثوقة بقدر مناسب</u>** أم لا، قد أدت وظيفة تحديد الهوية فعليا، أي ربط الشخص الذي يلتمس تحديد الهوية بإثباتات الهوية. ويستند هذا

---

(9) على سبيل المثال، صيغت المادة 10 (ب) '2' من قانون المعاملات الإلكترونية الأسترالي لسنة 1999 على غرار المادة 9 (3) (ب) '2' من اتفاقية الخطابات الإلكترونية. وتنص المادة 10 (ب) '2' من القانون الأسترالي المذكور على ما يلي:

عندما يُشترط، بموجب أحد قوانين الكمنولث، وجود توقيع من شخص ما، يُعد ذلك الاشتراط قد استوفي فيما يتعلق بالمعاملة الإلكترونية إذا:

(أ) استُخدمت، في جميع الحالات، طريقة ما لتعيين هوية الشخص المعني وتبيين نية ذلك الشخص فيما يخص المعلومات المرسَلة؛

(ب) وكانت الطريقة المستخدمة، في جميع الحالات:

'1' موثوق بها بقدر مناسب للغرض الذي أُنشئ الخطاب الإلكتروني أو أُرسل من أجله، في ضوء كل الظروف، بما فيها أي اتفاق ذي صلة؛ أو

'2' ***قد أثبتت فعليا، بحد ذاتها أو مقترنة بأدلة إضافية، أنها أوفت بالوظائف المذكورة في الفقرة (أ)...***

[الخط العريض للتأكيد]

الحكم إلى المادة 9 (3) (ب) '2' من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية.

ويشترط القانون النموذجي عموما استخدام طرائق موثوقة، ولا تهدف الفقرة 1 (ب) إلى التشجيع على استخدام طرائق غير موثوقة، أو إلى تأييد استخدام تلك الطرائق. بل إنه يقر بأن الوظيفة (وهي تحديد الهوية، في حالة المادة 9)، والموثوقية، من منظور تقني، سمتان مستقلتان، وهو **يوضح ينص على** أنه **يمكن** بموجب القانون النموذجي **تكون الطريقة موثوقة بالقدر المناسب للغرض الذي تُستخدم من أجله خدمة إدارة الهوية، أو قد يثبت أنها أدت وظيفة تحديد الهوية فعلياً أو باستخدام طريقة موثوقة**. وبعبارة أخرى، يستبق **الدليل على** تحقيق تحديد الهوية فعليا الحاجة إلى التأكد من **مناسبة** موثوقية الطريقة المستخدمة.

ثالثا- المادتان 25 و26

17- تتضمن المادتان 25 و26 أحكاما تيسر الاعتراف عبر الحدود بخدمات إدارة الهوية وتوفير الثقة على التوالي. ومن أجل الاعتراف المتبادل بتحديد الهوية إلكترونيا والنتائج المستمدة من استخدام خدمة توفير الثقة المقدَّمة خارج الولاية القضائية المشترِعة، يشترط مشروعا المادتين 25 و26 حاليا أن توفر الطريقة التي تستخدمها خدمة إدارة الهوية ونظيرتها التي تستخدمها خدمة توفير الثقة على التوالي "*مستوى مكافئا على الأقل من الموثوقية*".

18- ونحن نرى أن معيار العتبة "مستوى مكافئا على الأقل من الموثوقية" إشكالي لأنه يعمل في اتجاه واحد، ولن يكون صالحا في سياق متعدد الأطراف تشترع فيه دول مختلفة عديدة القانون النموذجي نفسه. وإضافة إلى ذلك، فإن مستوى موثوقية الطريقة المستخدمة، الذي يتوقف على عوامل قانونية وتقنية وعملية، هو معيار نوعي وليس معيارا كميا. وهذا يعني أنه سيكون من الصعب جدا على دولة تسعى إلى الحصول على الاعتراف المتبادل بخدماتها (الدولة ألف) أن توائم مستوى موثوقية خدماتها لكي يطابق تماما نفس مستوى موثوقية الخدمات بموجب قوانين الدولة المعترِفة (الدولة باء). ومن شأن ذلك أن يثير المزيد من المشاكل. وندعو اللجنة إلى النظر في السيناريو الافتراضي التالي:

(أ) لنفترض أن الدولة ألف ترغب في الحصول على اعتراف بخدمة إدارة الهوية الخاصة بها، التي يُشار إلى ما توفره من مستويات الموثوقية/الضمان باسم "المستوى 1"، في الدولة باء. و"المستوى 1" في الدولة ألف مكافئ جوهريا لأعلى مستويات الموثوقية/الضمان في الدولة باء، الذي يُشار إليه على أنه مستوى "مرتفع". ولكن نظرا لأن قوانين الدولة باء فيما يتعلق بالاعتراف المتبادل تشترط أن يكون مستوى الموثوقية/الضمان الذي توفره خدمة ما مكافئا تماما أو أعلى لما تطبقه محليا، لن يتسنى في الدولة باء منح الاعتراف المتبادل بخدمة إدارة الهوية المقدمة من الدولة ألف، ما لم تعدِّل الدولة ألف معاييرها القانونية والتقنية بحيث يصبح مستوى الموثوقية/الضمان المشار إليه باسم "المستوى 1" مماثلا تماما أو أعلى من المستوى "المرتفع" في الدولة باء.

(ب) ولدى القيام بذلك، من المرجح أن يكون مستوى الموثوقية/الضمان المعزز المشار إليه باسم "المستوى 1" الخاص بالدولة ألف أعلى من مستوى الموثوقية/الضمان "المرتفع" لدى الدولة باء (بما أن قياس الموثوقية ليس علما دقيقا، من المرجح أن تسعى الدولة ألف، لدى قيامها برفع مستوى الموثوقية/الضمان من أجل ضمان الاعتراف الناجح عبر الحدود، إلى كفالة أن يكون مستوى الموثوقية/الضمان المعزز المشار إليه باسم "المستوى 1" أعلى).

(ج) ونتيجة للتعديلات التي تدخلها الدولة ألف، سوف تتيح خدمة إدارة الهوية التي توفر "المستوى 1" في الدولة ألف لاحقا "*مستوى مكافئا على الأقل من الموثوقية*" لمستوى الموثوقية/الضمان الذي

تتيحه خدمة إدارة الهوية التي توفر مستوى الموثوقية/الضمان "المرتفع" في الدولة باء، مما سيمكِّن من الاعتراف المتبادل في الدولة باء بخدمة إدارة الهوية المذكورة بوصفها تتيح مستوى "مرتفعا". بيد أن هذا يعني في المقابل أن خدمة إدارة الهوية التي توفر المستوى "المرتفع" في الدولة باء لن تحصل على الاعتراف بموجب قوانين الدولة ألف بوصفها مكافئة لـ "المستوى 1"، لأن المستوى "المرتفع" في الدولة باء سيعتبر الآن أقل في الموثوقية/الضمان مقارنة بـ "المستوى 1" في الدولة ألف (على الرغم من أنه ربما يكون مكافئا له جوهريا).

19- وهذا وضع غير مرغوب، ومن شأنه أن يجعل الاعتراف المتبادل عبر الحدود من المستحيل تقريبا. ومن شأنه أيضا أن يجعل الاعتراف عبر الحدود على أساس متعدد الأطراف بين ولايات قضائية متعددة أقل قابلية للتطبيق. وفي ظل هذه الظروف، سيكون من الأنسب أن تستخدم المادتان 25 و26 معيار "*مستوى مكافئا جوهريا أو أعلى من الموثوقية*". ومن شأن اشتراط "*مستوى مكافئا جوهريا أو أعلى من الموثوقية*" أن يسمح بمنح الاعتراف عبر الحدود في الاتجاهين بين ولايتين قضائيتين دون اشتراط التكافؤ الدقيق. وسيمكِّن ذلك من الاعتراف المتبادل بخدمات الدولة ألف التي توفر "المستوى 1" وخدمات الدولة باء التي توفر المستوى "المرتفع"، ما دام كلاهما يوفر مستوى مكافئا جوهريا من الموثوقية/الضمان.

التذييل

المادة 9- تحديد هوية شخص باستخدام إدارة الهوية

رهنا بالفقرة 3 من المادة 2، حيثما يشترط القانون تحديد هوية شخص ما لغرض محدد، أو ينص على عواقب لعدم تحديد الهوية، يُستوفى ذلك الاشتراط فيما يتعلق بخدمات إدارة الهوية عندما تُستخدم طريقة، **وفقا للمادة 10 (1)**، لتحديد هوية الشخص إلكترونيا لذلك الغرض.

المادة 16- التوقيعات الإلكترونية

حيثما يشترط القانون توقيع شخص ما، أو ينص على عواقب لعدم وجود توقيع، يستوفى ذلك الاشتراط فيما يخص رسالة البيانات إذا استُخدمت طريقة، **وفقا للمادة 22 (1)**، من أجل ما يلي: [...]

المادة 17- الأختام الإلكترونية

حيثما يشترط القانون على شخص اعتباري وضع ختم، أو ينص على عواقب لعدم وجود ختم، يُستوفى ذلك الاشتراط فيما يخص رسالة البيانات إذا استُخدمت طريقة، **وفقا للمادة 22 (1)**، من أجل ما يلي: [...]

المادة 18- أختام الوقت الإلكترونية

حيثما يشترط القانون ربط وثائق أو سجلات أو معلومات أو بيانات بوقت وتاريخ، أو ينص على عواقب لعدم وجود وقت وتاريخ، يستوفى ذلك الاشتراط فيما يخص رسالة البيانات إذا استُخدمت طريقة، **وفقا للمادة 22 (1)**، من أجل ما يلي: [...]

المادة 19- الأرشفة الإلكترونية

حيثما يشترط القانون الاحتفاظ بوثائق أو سجلات أو معلومات، أو ينص على عواقب لعدم الاحتفاظ بها، يستوفى ذلك الاشتراط فيما يخص رسالة البيانات إذا استُخدمت طريقة، **وفقا للمادة 22 (1)**، من أجل ما يلي: [...]

المادة 20- خدمات التوصيل المسجَّل الإلكتروني

حيثما يشترط القانون الاحتفاظ بوثائق أو سجلات أو معلومات، أو ينص على عواقب لعدم الاحتفاظ بها، يستوفى ذلك الاشتراط فيما يخص رسالة البيانات إذا استُخدمت طريقة، **وفقا للمادة 22 (1)**، من أجل ما يلي: [...]

المادة 21- التوثُّق من المواقع الشبكية

حيثما يشترط القانون التوثق من المواقع الشبكية، أو ينص على عواقب لعدم التوثق من المواقع الشبكية، يستوفى ذلك الاشتراط إذا استُخدمت طريقة، **وفقا للمادة 22 (1)**، من أجل ما يلي: [...]