الأمم المتحدة A/CN.9/WG.IV/WP.171

الجمعية العامة

Distr.: Limited
10 September 2021
Arabic
Original: English

**لجنة الأمم المتحدة للقانون التجاري الدولي**
**الفريق العامل الرابع (المعني بالتجارة الإلكترونية)**
**الدورة الثانية والستون**
فيينا، 22-26 تشرين الثاني/نوفمبر 2021

# مذكرة تفسيرية بشأن مشاريع الأحكام المتعلقة باستخدام إدارة الهوية وخدمات توفير الثقة والاعتراف بهما عبر الحدود

## مذكرة من الأمانة

المحتويات



290921 290921 V.21-06686 (A)

# أولا- مقدمة

1- طلب الفريق العامل إلى الأمانة في دورته الحادية والستين أن تقدم مشروع نصوص تفسيرية إلى جانب مشاريع الأحكام المنقحة لكي ينظر فيها الفريق العامل في دورته الثانية والستين. وترد تلك النصوص في المذكرة التفسيرية الواردة في المرفق.

2- وقد أَعدت الأمانة المذكرة التفسيرية لكي يدلي الفريق العامل بتعليقاته عليها ويعتمدها في نهاية المطاف. وهي تتضمن سجلاً لمداولات الفريق العامل، التي أُبلغت بها اللجنة، فضلاً عن معلومات سياقية إضافية تتعلق بولاية الفريق العامل. وهي تشير إلى مشاريع الأحكام الواردة في الوثيقة A/CN.9/WG.IV/WP.170 وسيجري تنقيحها لتجسد أي تعديلات على تلك الأحكام – وأي تعليقات – يتفق عليها الفريق العامل في دورته الثانية والستين. وقد تساعد المذكرة التفسيرية الفريق العامل أيضاً في وضع الصيغة النهائية لمشاريع الأحكام.

# المرفق

# مذكرة تفسيرية بشأن مشاريع الأحكام المتعلقة باستخدام إدارة الهوية وخدمات توفير الثقة والاعتراف بهما عبر الحدود

## أولا- مقدمة

### ألف- الغرض من هذه المذكرة التفسيرية

1- [يُستكمل النص لاحقاً]

### باء- الأهداف

2- شهدت السنوات العشرين الأخيرة نمواً مطرداً في قيمة النشاط التجاري عبر الإنترنت (أي في المعاملات الإلكترونية فيما بين الشركات وبين الشركات والمستهلكين وبين الشركات والحكومات). فقد نمت التجارة الإلكترونية العالمية من 64 مليار دولار في عام 1999 إلى 29 تريليون دولار في عام 2017.[(1)] ويتزامن هذا النمو مع زيادة وصول الأفراد والشركات إلى شبكة الإنترنت. فعلى سبيل المثال، ارتفعت نسبة الأسر التي تمتلك القدرة على الوصول إلى الإنترنت من 35 في المائة في عام 2002 إلى 83,6 في المائة في عام 2017.[(2)] وارتفعت تبعاً لذلك نسبة توافر خدمات الحكومة الإلكترونية (بما في ذلك الخدمات المتصلة بالتجارة)، والخدمات المصرفية الإلكترونية، والسداد الإلكتروني.

3- ويستند هذا النمو إلى الثقة – ويحتاج إلى دعمه بشعور من الثقة – في البيئة الإلكترونية. وتعد القدرة على تحديد هوية كل طرف على نحو موثوق، ولا سيما في غياب أي تعامل شخصي مسبق، من العناصر المهمة لهذه الثقة. وعلى مدى السنوات السابقة، اقتُرحت حلول متنوعة لمعالجة الحاجة إلى تحديد الهوية بواسطة الإنترنت. وقد أدى ذلك إلى تطوير مختلف النظم والطرائق والتكنولوجيات والأجهزة المستخدمة في إنشاء وإدارة الهويات الرقمية للأشخاص الطبيعيين والقانونيين. ولا تقتصر الاستفادة من معالجة الجوانب القانونية لإدارة الهوية على مستوى العالم على سد الفجوات بين هذه الحلول المختلفة، بل تشمل أيضاً تشجيع التشغيل المتبادل لنظم إدارة الهوية سواء من جانب الجهات الخاصة أم الحكومية.

4- وهناك عقبات تحول دون توسيع نطاق استخدام إدارة الهوية وخدمات توفير الثقة. وتشمل العقبات ذات الطابع القانوني ما يلي: (1) غياب التشريعات التي تعطي الأثر القانوني لإدارة الهوية وخدمات توفير الثقة؛ (2) اختلاف النُهُج القانونية إزاء إدارة الهوية، بما في ذلك القوانين القائمة على متطلبات تخص تكنولوجيات محددة؛ (3) التشريعات التي تشترط وجود مستندات هوية ورقية لإبرام المعاملات التجارية الإلكترونية؛ (4) غياب آليات الاعتراف القانوني عبر الحدود بإدارة الهوية وخدمات توفير الثقة.[(3)]

---

(1) UNCTAD, E-Commerce and Development Report 2001, UN DocUNCTAD/SDTE/ECB/1, p. 44; UNCTAD, Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries, UN DocUNCTAD/DER/2019, p. 15.

(2) ITU, ICT Statistics, Global ICT Developments, 2001–2018، متاح على الرابط التالي: www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx .

(3) A/CN.9/965، الفقرة 52.

5- والهدف الأساسي من [مشروع الصك] هو التغلب على هذه العقبات من خلال وضع قواعد قانونية موحدة. وتخدم هذه القواعد عدة أغراض: زيادة الكفاءة؛ وخفض تكاليف المعاملات؛ وتعزيز مستوى أمن المعاملات الإلكترونية واليقين القانوني فيها، ومن ثم إرساء الثقة؛ والمساهمة في سد الفجوة الرقمية من خلال إيجاد حلول متسقة.

6- وبالقيام بذلك يسهم [مشروع الصك] في تنفيذ أهداف التنمية المستدامة. وعلى وجه التحديد، أُقر في الهدف 16 بأهمية الهوية، حيث تدعو الغاية 9 منه إلى توفير هوية قانونية لجميع البشر. وتتحول هذه الدعوة في الاقتصاد الرقمي إلى الحق في امتلاك هوية رقمية. وسوف يعزز وجود إطار قانوني لإدارة الهوية وخدمات توفير الثقة التفعيل الآمن للهوية الرقمية. ومن خلال تعزيز الثقة في البيئة الإلكترونية، سيسهم هذا الإطار أيضاً في تحقيق التنمية المستدامة والإدماج الاجتماعي وفقاً للهدف 9 من أهداف التنمية المستدامة، الذي يتناول حفز الابتكار، من بين أمور أخرى.

## جيم- النطاق

7- [يستكمل النص لاحقاً.]

## دال- البنية

8- يتألف [مشروع الصك] من أربعة فصول تتناول على التوالي أحكاماً عامة، وإدارة الهوية، وخدمات توفير الثقة، والجوانب الدولية. وينطبق الفصلان الأول والرابع على إدارة الهوية وخدمات توفير الثقة، كلتيهما. علاوة على ذلك، توجد أوجه تشابه كبيرة في هيكل ومضمون الفصلين الثاني والثالث. ومن ثم، فإن تفسير حكم ما من أحكام الفصل الثاني قد ينطبق أيضاً على الحكم المناظر من الفصل الثالث، بقدر ما يتشابه الحكمان. وقد ينطبق هذا، على وجه الخصوص، على المواد 13 و14 و15 و22 و23 و24، فيما يتعلق بالمواد 5 و6 و7 و8 و10 و11 و12، على التوالي.

9- ويتضمن الفصل الأول تعاريف مصطلحات معينة مستخدمة في [مشروع الصك]؛ وتعيين نطاق الانطباق؛ وأحكاماً بشأن الاستخدام الطوعي لإدارة الهوية وخدمات توفير الثقة، بما في ذلك استخدام خدمات محددة؛ وأحكاماً بشأن العلاقة بين [مشروع الصك] والقوانين الأخرى، بما في ذلك اشتراطات تحديد أو استخدام خدمات بعينها من خدمات توفير الثقة؛ وأحكاماً بشأن التفسير المستقل لـ [مشروع الصك]، لأغراض من بينها سد الفجوات، في ضوء طبيعته الموحدة ومصدره الدولي.

10- ويحدد الفصل الثاني العناصر الأساسية للنظام القانوني المنطبق على إدارة الهوية، وهو ينص على التزامات أساسية معينة لمقدمي خدمات إدارة الهوية والمشتركين، ويضع قواعد بشأن مسؤولية مقدمي خدمات إدارة الهوية. وتنص المادة 5 على مبدأ الاعتراف القانوني بالتحديد الإلكتروني للهوية وعدم التمييز ضد إدارة الهوية. وتورد المادة 6 الالتزامات الأساسية لمقدمي خدمات إدارة الهوية؛ ومن هذا المنطلق، تحدد الخطوات الرئيسية في دورة حياة إدارة الهوية. وتتناول المادة 7 التزامات مقدم خدمات إدارة الهوية في حال وقوع خرق للبيانات، وهي تُستكمَل بالمادة 8، بشأن التزامات المشتركين في حال التلاعب بإثباتات الهوية. وتتضمن المادة 9 قاعدة للتكافؤ الوظيفي بين تحديد الهوية بدون اتصال عبر الإنترنت، وتحديد الهوية الإلكتروني الذي يتطلب استخدام طريقة موثوقة. وتقيَّم موثوقية الطريقة بالتقرير اللاحق للموثوقية استناداً إلى الظروف المذكورة في المادة 10، أو بالتعيين المسبق للموثوقية وفقاً للمادة 11. وعلاوة على ذلك، إذا أدت الطريقة وظيفتها بالفعل، فلا يلزم تقرير موثوقيتها. وأخيراً، تتناول المادة 12 مسؤولية مقدمي خدمات إدارة الهوية.

11- ويحدد الفصل الثالث العناصر الأساسية للنظام القانوني المنطبق على استخدام خدمات توفير الثقة. وتتضمن المادة 13 قاعدة عامة بشأن عدم التمييز ضد الآثار القانونية لخدمات توفير الثقة. وتحدد المادة 14 التزامات مقدمي خدمات توفير الثقة وتتناول المادة 15 التزامات المشتركين في خدمات توفير الثقة في حال وقوع تلاعب بخدمة توفير الثقة. وتوضح المواد من 16 إلى 21 الوظائف المطلوب أداؤها بواسطة خدمات محددة مسماة من خدمات توفير الثقة (التوقيعات الإلكترونية؛ والأختام الإلكترونية؛ وأختام الوقت الإلكترونية؛ والأرشفة الإلكترونية؛ وخدمات التوصيل المسجَّل الإلكتروني؛ والتوثُّق من المواقع الشبكية) والاشتراطات المرتبطة بها، بما في ذلك استخدام طريقة موثوق بها. وفي أغلب الأحوال، تصاغ الأحكام المتعلقة بخدمات إدارة توفير الثقة المسماة كقواعد للتكافؤ الوظيفي. ومع ذلك، بالنظر إلى أن خدمات توفير الثقة قد لا يكون لها مكافئ ورقي، فإنها لا تتطلب بالضرورة قاعدة للتكافؤ الوظيفي. وتنص المادة 22 على إرشادات بشأن التقرير اللاحق لموثوقية الطريقة المستخدمة في خدمة توفير الثقة، وتنص المادة 23 على تعيين الموثوقية مسبقاً. وأخيراً، تتضمن المادة 24 قواعد بشأن مسؤولية مقدمي خدمات توفير الثقة.

12- ويتناول الفصل الرابع تمكين الاعتراف عبر الحدود بإدارة الهوية وخدمات توفير الثقة، وهو أحد الأهداف الرئيسية [لمشروع الصك]. ولا ينظر [مشروع الصك] في إنشاء هيئة مخصصة للاعتراف القانوني بإدارة الهوية وخدمات توفير الثقة، ولكنه يتوخى عدة آليات تقوم على نهج لا مركزي. وإلى جانب المادتين 25 و26، تتصل الأحكام المخصصة الواردة في المواد 10 (3) و11 (4) و22 (3) و23 (4)، المتعلقة بعدم التمييز الجغرافي في تقرير موثوقية إدارة الهوية وخدمات توفير الثقة وفي تعيين خدمات إدارة الهوية وخدمات توفير الثقة الموثوقة، اتصالاً مباشراً بهذه المسألة. وقد تكون الاتفاقات التعاقدية ذات صلة أيضاً بتمكين استخدام إدارة الهوية وخدمات توفير الثقة عبر الحدود.

## هاء- معلومات أساسية

### 1- تاريخ الصياغة

13- [انظر الفقرات 4-20 من الوثيقة A/CN.9/WG.IV/WP.169].

14- [يُستكمل النص لاحقاً]

### 2- العلاقة بالنصوص السابقة للأونسيترال

15- لا تتضمن نصوص الأونسيترال السابقة أحكاماً بشأن خدمات توفير الثقة. إلا أنها تحتوي على قواعد للتكافؤ الوظيفي قد تكون ذات صلة ببعض خدمات توفير الثقة. وعلى وجه الخصوص، تنص المادة 7 من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (قانون التجارة الإلكترونية)، والمادة 6 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، والمادة 9 (3) من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية، والمادة 9 من قانون الأونسيترال النموذجي بشأن السجلات الإلكترونية القابلة للتحويل (قانون السجلات الإلكترونية)، على الاشتراطات التي يجب أن تمتثل لها التوقيعات الإلكترونية لكي تكون مكافئة وظيفياً للتوقيعات الورقية. وتستند المادة 16 من [مشروع الصك] إلى المادة 9 من قانون السجلات الإلكترونية. وبالمثل، تحدد المادة 10 من قانون التجارة الإلكترونية الاشتراطات المتعلقة بالتكافؤ الوظيفي للاحتفاظ بالمعلومات. وتستند المادة 19 من [مشروع الصك] إلى المادة 10 (1) من قانون التجارة الإلكترونية.

16- وتشير المواد من 16 إلى 21 من [مشروع الصك] إلى خدمات توفير الثقة التي تهدف إلى تقديم ضمانة لبعض سمات رسالة البيانات. إلا أن خدمات توفير الثقة المشمولة بتلك الأحكام لا تحظى جميعها

بمفاهيم ورقية مكافئة. وعلاوة على ذلك، قد لا يلزم استخدام خدمة من خدمات توفير الثقة المسماة في [مشروع الصك] لاستيفاء قواعد التكافؤ الوظيفي الواردة في نصوص الأونسيترال السابقة المذكورة.

## واو- المفاهيم والمبادئ الرئيسية

17- يوضح هذا القسم عدة مفاهيم ومبادئ رئيسية يرتكز عليها [مشروع الصك]. ويرد توضيح كذلك لمصطلحات معرَّفة مستخدمة في [مشروع الصك] في شرح المادة 1 أدناه، في حين ترد في الوثيقة A/CN.9/WG.IV/WP.150 قائمة أكثر اتساعاً من المصطلحات والمفاهيم ذات الصلة بإدارة الهوية وخدمات توفير الثقة التي جُمعَت على أساس التعاريف الواردة في النصوص القانونية والتقنية المتفق عليها دولياً. وحسبما هو مبين في تلك الوثيقة، قد تَستخدِم تلك النصوص مصطلحات معرَّفة مختلفة لنفس المفهوم أو قد تعرِّف نفس المصطلح بشكل مختلف.

### 1- مبادئ أساسية

18- يستند [مشروع الصك]، مثل نصوص الأونسيترال السابقة، إلى مبادئ استقلالية الأطراف، وحياد التكنولوجيا، والتكافؤ الوظيفي، وعدم التمييز ضد استخدام الوسائل الإلكترونية، رهناً بما قد يُدخَل عليه من تعديلات.[4] وعلى الرغم من أن [مشروع الصك] لا يحدد صراحة تلك المبادئ العامة، فإنها تشكل إطاراً للأحكام الرئيسية للنص. فعلى سبيل المثال، يتجسد مبدأ عدم التمييز، حسبما ينطبق على إدارة الهوية وخدمات توفير الثقة، في المادتين 5 و13 على التوالي، في حين استُرشِد بمبدأ التكافؤ الوظيفي في المادة 9 والمواد من 16 إلى 21.

19- ويَفترِض نهج التكافؤ الوظيفي وجود اشتراطات قانونية تنص بصورة مباشرة أو غير مباشرة على بعض الأنشطة المادية أو الورقية، مثل استخدام إثباتات ورقية لتحديد هوية شخص ما أو خطاب ورقي للتوثُّق من واقعة أو شيء ما. وهو يحلل بعد ذلك أغراض تلك الاشتراطات ووظائفها، بهدف تحديد سبل الوفاء بتلك الأغراض أو الوظائف بالوسائل الإلكترونية. إلا أنه مثلما يسرت التكنولوجيا الرقمية طائفة من الأنشطة التي لا تقابلها مكافئات ورقية، فإن بعض خدمات إدارة الهوية وخدمات توفير الثقة المشمولة بـ [مشروع الصك] قد لا يكون لها مكافئ ورقي.

### 2- إدارة الهوية

20- تحديد الهوية هو عملية تمييز شخص ما بالإحالة إلى معلومات متعلقة بذلك الشخص (أي النعوت). وتلك المعلومات يمكن جمعها أو ملاحظتها. ويتسم تحديد الهوية بأهمية خاصة في بناء الثقة في المعاملات التي تُجرى عبر الإنترنت. وينطوي تحديد الهوية، في جوهره، على التحقق من أن النعوت المجمعة أو الملاحظة تتطابق مع "هوية" سبق تحديدها للشخص الذي يجري تحديد هويته. وغالباً ما يجري تحديد الهوية بهذا المعنى استجابة لادعاء بامتلاك هوية معينة وتقديم نعوت للتحقق منها.

21- ووفقاً لذلك، بموجب [مشروع الصك]، تنطوي إدارة الهوية على مرحلتين متميزتين (أو طورين متميزين) - أولاً، إصدار إثباتات الهوية، أي البيانات التي يمكن تقديمها لتحديد الهوية إلكترونياً؛ وثانياً، تقديم تلك الإثباتات والتحقق منها بالوسائل الإلكترونية:

(أ) تشمل المرحلة الأولى من إدارة الهوية جمع النعوت التي تؤلف "الهوية التأسيسية" للشخص (أي النعوت التي تسجلها الأجهزة الحكومية في نظم التسجيل المدني وإحصاءات الأحوال المدنية للأشخاص

(4) A/CN.9/902، الفقرتان 52 و63.

الطبيعيين وفي السجلات التجارية للأشخاص الاعتباريين). ويمكن تقديم هذه النعوت في شكل إثباتات هوية صادرة عن الحكومة (مثل شهادة تسجيل) ومعتمدة من الهيئة المصدرة لها. وهذه العملية، التي يمكن إجراؤها "بدون اتصال عبر الإنترنت" استناداً إلى إثباتات مادية يقدمها الشخص بنفسه، تؤدي إلى إصدار إثباتات هوية للشخص؛

(ب) تشمل المرحلة الثانية من إدارة الهوية تقديم تلك الإثباتات بالوسائل الإلكترونية والتحقق بوسائل إلكترونية من أن الشخص الذي يقدم الإثباتات هو الشخص الذي صدرت له إثباتات الهوية في المرحلة الأولى.

22- وتُستخدَم نظم إدارة الهوية لإدارة عمليات تحديد الهوية المرتبطة بكل مرحلة من هاتين المرحلتين، وكذلك في إدارة النعوت التي تُجمَع وإثباتات الهوية التي تُصدَر والوسائل المستخدمة للتحقق منها. وقد تشمل نظم إدارة الهوية كياناً واحداً ينفذ كافة العمليات المتضمنة في كل مرحلة من مرحلتي إدارة الهوية، أو كيانات متعددة تقوم بتنفيذ هذه العمليات. وعلاوة على ذلك، قد تقدم بعض نظم إدارة الهوية "خدمات" مختلفة من خدمات إدارة الهوية وفقاً لاحتياجات الأطراف (أي الطرف الذي يسعى إلى تحديد هوية ما، والطرف الذي يسعى إلى تحديد هويته هو نفسه).

23- وتُستخدَم نظم إدارة الهوية لتقديم خدمات إدارة الهوية. ويجوز أن تتولى تشغيل نظم إدارة الهوية كيانات عامة أو خاصة وقد تقدم خدمات متعددة من خدمات إدارة الهوية. وفي الممارسة العملية، تناظِر نظم إدارة الهوية العامة عموماً خدمة واحدة لإدارة الهوية، في حين أن نظم إدارة الهوية الخاصة قد تناظر خدمات متعددة لإدارة الهوية بمستويات مختلفة من الموثوقية. ويوجد تصنيف آخر لنظم إدارة الهوية يتعلق بطابعها المركزي أو الموزع. ويتسم [مشروع الصك] بالحياد التكنولوجي والنموذجي، ويمكن تبعاً لذلك تطبيقه على جميع أنواع نظم وخدمات إدارة الهوية.

24- ويجوز لمقدمي خدمات إدارة الهوية والمشتركين والأطراف المعولين والكيانات المعنية الأخرى الاتفاق على العمل بموجب سياسات ومعايير وتقنيات متوافقة فيما بينهم، يُنَص عليها في قواعد النظام، حتى تكون إثباتات الهوية التي يقدمها كل واحد من مقدمي خدمات إدارة الهوية المشاركين مفهومةً وموثوقةً لجميع الأطراف المعولة المشاركة. ويمكن الإشارة إلى هذا الترتيب باسم "اتحاد الهويات"، وإلى قواعد النظام، التي تكون ذات طابع تعاقدي، باسم "إطار الثقة". وقد يساهم اتحاد الهويات في زيادة عدد المستخدمين والتطبيقات التي تشترك في خدمات إدارة الهوية نفسها، مما قد يساعد بدوره على احتواء التكاليف وضمان الاستدامة على المدى الطويل.

### 3- خدمات توفير الثقة

25- تتسم خدمات توفير الثقة هي الأخرى بأهمية بالغة في بناء الثقة في استخدام المعاملات الإلكترونية. وهي تُعنى، في جوهرها، بتوفير ضمانات لبعض سمات رسائل البيانات، مثل المصدر والسلامة ووقت معالجة إجراء معين فيما يخص البيانات. وعلى الرغم من أن [مشروع الصك] يحدد بعض خدمات توفير الثقة التي يشيع استخدامها، فإنه يعترف بأن هناك خدمات أخرى لتوفير الثقة قد تكون موجودة أو يمكن تطويرها في المستقبل.

26- ويُعنى مفهوم خدمة توفير الثقة في [مشروع الصك] بتقديم خدمة ما وليس بتلك الخدمة في حد ذاتها. فهو يُعنى، مثلاً، بالخدمات التي تدعم طرائق إنشاء التوقيع الإلكتروني وإدارته، وليس بالتوقيع الإلكتروني فقط.

### 4- تقرير الموثوقية

27- تماشياً مع نصوص الأونسيترال السابقة، تشير عدة أحكام من [مشروع الصك] إلى استخدام طريقة موثوقة. ويتوخى [مشروع الصك] آليتين لتقييم موثوقية الطريقة، كما يلي: تنص المادتان 10 و22 على قائمة

إرشادية بالعوامل المناسبة لتقرير مدى الموثوقية؛ وتنص المادتان 11 و23 على آلية لتعيين الطرائق الموثوقة. ويستند هذا النهج إلى المادتين 6 و7 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية.

28- وحين يجمع [مشروع الصك] بين تقرير الموثوقية وتعيين الطرائق الموثوقة، فإنه لا يحبذ آلية على أخرى، بل إنه يهدف إلى الجمع بين مزايا الآليتين مع تقليل عيوبهما إلى أدنى حد ممكن، وتمكين الأطراف في نهاية المطاف من اختيار الحل المفضل.

29- ولا تتضمن جميع نصوص الأونسيترال التي تتناول خدمات توفير الثقة أحكاماً تنص على الأخذ بنهجي التقرير المسبق واللاحق للموثوقية، كليهما. إلا أن نهجي التقرير المسبق واللاحق للموثوقية يُعتبران عموماً متوافقين ومتكاملين.

### (أ) التقرير اللاحق للموثوقية

30- لا يُلجأ إلى تقرير الموثوقية إلا في حالة المنازعة، أي بعد أن تكون الطريقة استُخدِمت (واقعة لاحقة). ومن هذا المنطلق، فإن [مشروع الصك] عموماً يمكِّن معاملات إدارة الهوية، ويقصر الحاجة إلى تقرير موثوقية الطريقة المستخدمة على حالات التنازع بشأن صحة المعاملة نتيجة عدم وجود هوية لطرف أو أكثر أو عدم كفاية تلك الهوية.

31- ويتميز نهج التقرير اللاحق للموثوقية بأنه يوفر للأطراف أقصى قدر من المرونة في اختيار التكنولوجيات والطرائق. وعلاوة على ذلك، يمكن إدارة هذا النهج لامركزياً وهو لا يستلزم إنشاء آلية مؤسسية، ومن ثم، يتجنب التكاليف المرتبطة بها.

32- ومن ناحية أخرى، يعيب نهج التقرير اللاحق للموثوقية أنه لا يعزز اليقين القانوني مقدماً، ومن ثم، فهو لا يتيح للأطراف إمكانية التنبؤ بصحة الطريقة المستخدمة، مما قد يعرضهم لمخاطر إضافية محتملة إذا ما اعتُبرت الطريقة المستخدمة غير موثوقة. وعلاوة على ذلك، فإنه يوكل أمر البت في تقرير موثوقية الطريقة لطرف ثالث، وهي عملية قد تستغرق وقتاً طويلاً وقد تتمخض عن قرارات غير متسقة.

### (ب) التعيين المسبق للخدمات الموثوقة

33- يجري تعيين الخدمات الموثوقة قبل استخدام الطريقة (مسبقاً)، مقابل قائمة بالشروط المحددة مسبقاً، وبعبارات عامة بدلاً من الإشارة إلى معاملة محددة. وينبغي ألا يؤدي إيراد الشروط الإضافية المحددة في [مشروع الصك] إلى فرض اشتراطات تخص تكنولوجيات محددة.

34- ولا يتعلق التعيين بأنواع عامة من خدمات إدارة الهوية وتوفير الثقة أو بجميع خدمات إدارة الهوية وتوفير الثقة التي يقدمها أحد مقدمي خدمات إدارة الهوية أو مقدمي خدمات توفير الثقة، بل بخدمة محددة يقدمها أحد مقدمي الخدمات بعينه.

35- وقد يوفر نهج التقرير المسبق للموثوقية مستوى أعلى من الوضوح وإمكانية التنبؤ بالأثر القانوني لخدمات إدارة الهوية وتوفير الثقة، بما في ذلك عند استخدامها عبر الحدود، مقارنة بنهج التقرير اللاحق للموثوقية. إلا أن إدارته ينبغي أن تتيح التكيف السريع مع التطور التكنولوجي لتجنب إعاقة الابتكار. عدا ذلك فإنه قد يميز ضد خدمات إدارة الهوية وخدمات توفير الثقة غير المعيَّنة، على الرغم من توافرها واعتمادها على طرائق موثوقة.

36- ويجب أن تحدد الولاية القضائية المشترعة الكيان المسؤول عن التعيين، الذي قد يكون هيئة عامة أو خاصة. ويجوز اعتماد الكيانات القائمة بالتعيين وفقاً للمعايير التقنية المطبقة على هيئات اعتماد المنتجات

والعمليات والخدمات. وثمة فائدة أيضاً للتصديق (بما في ذلك التصديق الذاتي) في تقييم الخدمات باستخدام معايير مبنية على النتائج، ومن ثم قد يكون ذا وجاهة فيما يخص تعيين تلك الخدمات.

37- وتتطلب الآلية المؤسسية اللازمة لتنفيذ نهج التقرير المسبق وجود آلية مخصصة للتعيين غالباً ما تدار مركزياً. وأي آلية من هذا القبيل تتضمن عناصر مختلفة مثل معايير تقييم الخدمات، وتفاصيل عملية التقييم التي تتخذ القرار، ومصادر التمويل. وقد تكون إدارة نظام الترخيص هذا معقدة ومكلفة، اعتماداً على عدة عوامل من بينها الترتيبات المؤسسية. ولهذا السبب، يفضل تطبيق التعيين على الخدمات التي توفر مستوى أعلى من الضمان والموثوقية، والتي تُستخدَم تبعاً لذلك في معاملات ذات قيمة أعلى. وفيما يتعلق بالولايات القضائية المشترعة التي تود أن تنفذ نهج التقرير المسبق، يَفترِض [مشروع الصك] مسبقاً وجود الآلية المؤسسية اللازمة ولا ينص على إنشائها أو إدارتها.

### 5- الجوانب الدولية

38- يعد التمكين القانوني للاعتراف عبر الحدود بإدارة الهوية وخدمات توفير الثقة أحد الأهداف الرئيسية لـ[مشروع الصك]. ويجري ذلك من خلال تطبيق مبادئ الحياد التكنولوجي وعدم التمييز ضد المنشأ الجغرافي. ويُسترشَد بهذه المبادئ في المواد 10 (3) و11 (4) و22 (3) و23 (4) من [مشروع الصك]. وعلاوة على ذلك، يتناول الفصل الرابع (المادتان 25 و26) تحديداً مسألة الاعتراف عبر الحدود.

39- ولا يشترط [مشروع الصك] وضع ترتيب مؤسسي رسمي للاعتراف القانوني عبر الحدود. إلا أن هناك أمثلة على هذه الترتيبات على الصعيدين الإقليمي والثنائي. ولعل الولايات القضائية المشترعة تود أن تستخدم [مشروع الصك] كنموذج لإقامة ترتيب مؤسسي مع الشركاء الدوليين، بما في ذلك في إطار اتفاق مخصص.

40- ويمكن أن يساعد [مشروع الصك] أيضاً في تنفيذ أحكام الاعتراف القانوني المتبادل الواردة في اتفاقات التجارة الحرة أو في اتفاقات الاقتصاد الرقمي المخصصة.

## ثانيا- شرح المواد مادة فمادة

## ألف- الفصل الأول - أحكام عامة (المواد 1 إلى 4)

### 1- المادة 1- التعاريف

41- يتضمن الفصل الأول تعاريف المصطلحات المستخدمة في [مشروع الصك].[(5)]

*"النعت"*

42- "النعت" يعني بنداً من المعلومات أو البيانات المقترنة بشخص ما. وتشمل الأمثلة على نعوت الشخص الطبيعي الاسم والعنوان والعمر وعنوان البريد الإلكتروني، وكذلك بيانات مثل الحضور الشبكي للشخص والجهاز الذي يستعمله. وتشمل الأمثلة على نعوت الشخص الاعتباري اسم الشركة وعنوان مكتبها الرئيسي واسمها بالتسجيل والولاية القضائية التي يتبعها التسجيل. ويُستخدَم مفهوم النعت في تعريف الهوية.

(5) أُعدت قائمة بالمصطلحات والمفاهيم ذات الصلة بإدارة الهوية وخدمات توفير الثقة التي جُمعَت على أساس التعاريف الواردة في النصوص القانونية والتقنية المتفق عليها دولياً دعماً لتحضير [مشروع الصك]، وهي ترد في الوثيقة A/CN.9/WG.IV/WP.150.

43- وقد تحتوي النعوت على بيانات شخصية يخضع التعامل معها لقانون خصوصية البيانات وحمايتها. ولا يتناول [مشروع الصك] خصوصية البيانات وحمايتها ويحافظ صراحة على تطبيق ذلك القانون.

*المراجع*

A/CN.9/WG.IV/WP.150، الفقرة 13.

*"رسالة البيانات"*

44- يمكن الاطلاع على تعريف "رسالة البيانات" في جميع نصوص الأونسيترال الحالية المتعلقة بالتجارة الإلكترونية. ويعد هذا المصطلح النقطة المرجعية الرئيسية لتحديد اشتراطات خدمات توفير الثقة، بالنظر إلى أن نتيجة تطبيق خدمة توفير الثقة هي توفير ضمانات لسمات رسائل البيانات.

*المراجع*

الوثيقة A/CN.9/1045، الفقرة 40.

*"تحديد الهوية إلكترونياً" ["التوثُّق"]*

45- يشير مصطلح "تحديد الهوية إلكترونياً" إلى التحقق من الربط بين الهوية المزعومة وإثباتات الهوية المقدمة، وهي المرحلة الثانية من إدارة الهوية. ويُستخدم مصطلح "تحديد الهوية إلكترونياً" بدلاً من مصطلح "التوثُّق" لمعالجة الشواغل المتعلقة بتعدد معاني مصطلح "التوثُّق". وفي الاستخدام التقني، يشير مصطلح "التوثُّق" إلى تقديم أدلة على الهوية.

46- ويُستخدم مصطلح "تحديد الهوية" دون تحفظ بالمعنى غير التقني في المادة 9.

*المراجع*

A/CN.9/1005، الفقرات 13 و84-86 و92؛ A/CN.9/1045، الفقرتان 134 و136؛ A/CN.9/1051، الفقرة 67.

*"الهوية"*

47- يقع تعريف "الهوية" في صميم مفهوم إدارة الهوية وهو يشير إلى القدرة على تحديد الصفات المتفرِّدة التي تميِّز شخصاً طبيعياً أو اعتبارياً في سياق معين. وهو لذلك مفهوم متناسب مع السياق. ويُستمد هذا التعريف من التعريف الوارد في التوصية ITU-T X.1252، البند 6-40.

*المراجع*

A/CN.9/WG.IV/WP.150، الفقرة 31؛ A/CN.9/1005، الفقرة 108.

*"إثباتات الهوية"*

48- "إثباتات الهوية" هي البيانات، أو الأشياء المادية التي قد توجد عليها البيانات، المقدمة لتدقيق الهوية. ومن الأمثلة على إثباتات الهوية الرقمية أسماء المستخدمين والبطاقات الذكية وهوية الجوال والشهادات الرقمية وجوازات

السفر البيومترية وبطاقات الهوية الإلكترونية. ويمكن استخدام إثباتات الهوية ذات الشكل الإلكتروني بالاتصال الحاسوبي المباشر أو بدونه وفقاً لخصائص نظام إدارة الهوية. ويعد مصطلح "إثباتات الهوية" مرادفاً بوجه عام لمصطلح "وسائل تحديد الهوية إلكترونياً" المستخدم في التشريعات الإقليمية والوطنية (على سبيل المثال، في المادة 3 (2) من لائحة الاتحاد الأوروبي بشأن تحديد الهوية إلكترونياً وخدمات توفير الثقة (eIDAS)).

*المراجع*

A/CN.9/1005، الفقرة 110؛ A/CN.9/1045، الفقرة 137.

*"خدمات إدارة الهوية"*

49- يجسد تعريف "خدمات إدارة الهوية" مفهوم أن إدارة الهوية تتألف من مرحلتين (أو طورين) هما: "تدقيق الهوية" و"تحديد الهوية إلكترونياً". ويشير تعريف خدمات إدارة الهوية إلى الخدمات التي تتصل بإحدى المرحلتين أو كلتيهما، حيث إن استخدام حرف العطف "أو" في ذلك التعريف لا يحول دون الجمع بين الخيارين. وتوضح المادة 6 (أ)، المتعلقة بالالتزامات الأساسية لمقدمي خدمات إدارة الهوية، المراحل والخطوات المختلفة التي ينطوي عليها تقديم خدمات إدارة الهوية.

*المراجع*

A/CN.9/1005، الفقرتان 84 و109.

*"مقدم خدمات إدارة الهوية"*

50- مقدم خدمات إدارة الهوية هو الشخص الطبيعي أو الاعتباري الذي يقدم خدمات إدارة الهوية، عن طريق القيام بالوظائف المذكورة في المادة 6، مباشرة أو عن طريق متعاقدين من الباطن. إلا أن الوظائف المدرجة في تلك المادة قد لا تكون كلها مناسبة لجميع نظم إدارة الهوية، ولذلك فإن مقدم خدمات إدارة الهوية قد لا يحتاج إلى القيام بكل وظيفة مدرجة في القائمة.

*المراجع*

A/CN.9/971، الفقرة 97؛ A/CN.9/1005، الفقرة 111؛ A/CN.9/1045، الفقرة 88.

*"نظام إدارة الهوية"*

51- يوضح تعريف "نظام إدارة الهوية" النظام المستخدم للتعامل مع إدارة الهوية عن طريق إجراء تدقيق الهوية وتحديد الهوية إلكترونياً. وهو يشير إلى "الوظائف والقدرات" التي تتسق مع مصطلحات الاتحاد الدولي للاتصالات، أي التوصية ITU-T X.1252، البند 6-43. وخلافاً لتعريف "خدمات إدارة الهوية"، يشمل تعريف "نظام إدارة الهوية" بالضرورة المرحلتين كلتيهما، حتى وإن كان مقدمو خدمات إدارة الهوية مختلفين في كل مرحلة.

*المراجع*

A/CN.9/1005، الفقرة 112.

*"تدقيق الهوية"*

52- يشير مصطلح "تدقيق الهوية" إلى المرحلة الأولى من إدارة الهوية ويشمل القيد، وهي العملية التي يستخدمها مقدمو خدمات إدارة الهوية للتحقق من مزاعم الهوية التي يدَّعيها كيان ما قبل إصدار إثباتات الهوية لذلك الكيان. وهو يُستخدَم بدلاً من مصطلح "تحديد الهوية" لمعالجة الشواغل المتعلقة بالمعاني المتعددة لمصطلح "تحديد الهوية".

*المراجع*

A/CN.9/1005، الفقرة 84.

*"المشترك"*

53- يشير مصطلح "المشترِك" إلى الشخص الذي تُقدَّم إليه الخدمات ولا يشمل الأطراف المعولة. وهو يفترض مسبقاً وجود عقد بين مقدم الخدمة والمشترك. فعلى سبيل المثال، ينسحب تعريف "المشترك" على الشخص الذي يوقع بتوقيع إلكتروني.

*المراجع*

A/CN.9/1005، الفقرتان 43 و96؛ A/CN.9/1045، الفقرتان 18 و22.

*"خدمات توفير الثقة"*

54- يجمع تعريف "خدمات توفير الثقة" بين وصف تجريدي للوظيفة المطلوب أداؤها باستخدام خدمات توفير الثقة ينصب تركيزه على أي خدمة تُعنى بتوفير ضمانة لجودة البيانات مثل صحتها وأصالتها، وبين قائمة غير حصرية بخدمات توفير الثقة الواردة في [مشروع الصك]. واعتماد قوائم غير حصرية يتيح تطبيق القواعد العامة المتعلقة بخدمات توفير الثقة على أنواع خدمات توفير الثقة في المستقبل.

55- وتوضح الإشارة إلى "طرائق الإنشاء والإدارة" أن مفهوم "خدمة توفير الثقة" يشير إلى الخدمات المقدمة وليس إلى النتيجة المستمدة من استخدام تلك الخدمات. فخدمات توفير الثقة ليست، على سبيل المثال، التوقيع الإلكتروني نفسه (أي البيانات التي تحدد هوية الموقِّع وتشير إلى نيته فيما يخص المعلومات الواردة في رسالة البيانات الأساسية)، بل هي الخدمة التي تدعم التوقيع الإلكتروني (أي الخدمة التي توفر الطرائق اللازمة لتمكين الموقِّع من إنشاء التوقيع الإلكتروني وتوفر ضمانات بشأن أداء الوظائف المطلوبة من التوقيع الإلكتروني).

*المراجع*

A/CN.9/965، الفقرات 101-106؛ A/CN.9/971، الفقرتان 110 و111؛ A/CN.9/1005، الفقرات 14-18؛ A/CN.9/1051، الفقرات 35-40.

*"مقدم خدمات توفير الثقة"*

56- مقدم خدمات توفير الثقة هو شخص طبيعي أو اعتباري يقدم خدمات توفير الثقة. وأي مقدم لخدمات التصديق، بالمعنى المقصود في قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، يقدم مثالاً لمقدم

خدمات توفير الثقة فيما يخص التوقيعات الإلكترونية. وخلافاً لمقدمي خدمات إدارة الهوية (المادة 6)، لا يحدد [مشروع الصك] الوظائف التي يتعين على مقدمي خدمات توفير الثقة الاضطلاع بها.

57- ولا يقتضي [مشروع الصك] استخدام أحد مقدمي خدمات توفير الثقة من الأطراف الثالثة كشرط للاعتراف القانوني. وإذا لم يُستخدَم أحد مقدمي خدمات توفير الثقة من الأطراف الثالثة، يجوز لنفس الكيان أن يؤدي دور مقدم خدمات توفير الثقة ودور المشترك.

*المراجع*

[يستكمل النص لاحقاً.]

## 2- المادة 2- نطاق الانطباق

58- تحدد المادة 2 نطاق انطباق [مشروع الصك] بالإشارة إلى استخدام نظم إدارة الهوية وخدمات توفير الثقة في سياق الأنشطة التجارية والخدمات ذات الصلة بالتبادل التجاري والاعتراف بتلك النظم والخدمات عبر الحدود. ويهدف مصطلح "الخدمات ذات الصلة بالتبادل التجاري" إلى شمول المعاملات التي ترتبط ارتباطاً وثيقاً بالتبادل التجاري ولكنها ليست تجارية في طابعها. وقد تشمل هذه المعاملات كيانات عامة مثل السلطات الجمركية التي تشغِّل منفذاً واحداً لإجراءات الاستيراد والتصدير.

59- وبالنظر إلى أن استخدام إدارة الهوية وخدمات توفير الثقة له تبعات تتجاوز حدود المعاملات التجارية، فإنه يجوز للولايات القضائية المشترعة أن توسع نطاق [مشروع الصك] ليشمل جميع أنواع المعاملات.

60- وتماشياً مع المبدأ العام الذي ترتكز عليه نصوص الأونسيترال بشأن التجارة الإلكترونية الذي يحبذ تجنب إدخال التعديلات على القانون الموضوعي القائم أو تقليلها إلى أدنى حد، توضح الفقرة 2 (أ) أن [مشروع الصك] لا يطرح أي التزامات جديدة لتحديدها.

61- وتنفِّذ الفقرة 2 (ب) و(ج)، التي تشير إلى أن [مشروع الصك] لا يشترط استخدام أي خدمات إدارة هوية أو خدمات توفير ثقة محددة، مبادئ الحياد التكنولوجي، بما في ذلك ما يتعلق بحياد النماذج والنظم.

62- وتحتفظ الفقرة 3 بتلك الاشتراطات القانونية التي تقتضي استخدام إجراء معين لتحديد الهوية أو استخدام خدمة محددة من خدمات توفير الثقة. وتشمل هذه الاشتراطات، التي تكون تنظيمية عادة، على سبيل المثال، طلب وثيقة هوية محددة (مثل جواز السفر) أو وثيقة هوية ذات سمات معينة مناظرة للنعوت ذات الصلة (مثل بطاقة هوية تحمل صورة حاملها وتاريخ ميلاده). وقد تتطلب اشتراطات تحديد الهوية أيضاً أن يقوم شخص معين ذو وظائف محددة بتحديد الهوية. فحين يُسمَح بتحديد الهوية إلكترونياً، غالباً ما يطلب المنظمون المعنيون استخدام إجراء محدد لإدارة الهوية أو خدمة محددة من خدمات توفير الثقة من قبيل إثباتات الهوية الصادرة عن هيئة عامة.

63- وبالنظر إلى الطابع التمكيني لـ [مشروع الصك]، شأنه شأن قوانين الأونسيترال النموذجية القائمة، فإنه لا يؤثر على تطبيق أي قانون آخر على إدارة الهوية وخدمات توفير الثقة، من القوانين التي قد تنظم تلك الأنشطة أو بعض الجوانب الموضوعية للمعاملات التي تُجرى باستخدام إدارة الهوية وخدمات توفير الثقة. وتحدد الفقرة 4 ذلك المبدأ فيما يتعلق بقانون خصوصية البيانات وحمايتها، الذي يُذكَر تحديداً بسبب أهميته. ولا يشير الحكم إلى الخصوصية في سياقات أخرى.

*المراجع*

A/74/17، الفقرة 172؛ A/CN.9/936، الفقرة 52؛ A/CN.9/965، الفقرة 125؛ A/CN.9/971، الفقرة 23؛ الوثيقة A/CN.9/1005، الفقرة 115؛ A/CN.9/1045، الفقرات 76-78.

### 3- المادة 3- الاستخدام الطوعي لخدمات إدارة الهوية وتوفير الثقة

64- تشير المادة 3 إلى أن [مشروع الصك] لا يُلزِم أي شخص باستخدام خدمات إدارة الهوية أو توفير الثقة دون موافقته على استخدام خدمات إدارة الهوية أو توفير الثقة. إلا أنه يمكن الاستدلال على الموافقة من خلال مسلك الطرف، مثلاً، عندما يقرر استخدام برمجية محددة للتجارة الإلكترونية أو نظام محدد للخطابات الإلكترونية تدعمهما خدمات إدارة الهوية وتوفير الثقة.

65- ويرتبط مبدأ الاستخدام الطوعي لخدمات إدارة الهوية وتوفير الثقة بمبدأ استقلالية الأطراف، بالنظر إلى أن كلا المبدأين يستند إلى الإرادة. وقد لا تكون الموافقة على استخدام خدمات إدارة الهوية وتوفير الثقة متطابقة مع الموافقة على معاملة المعلومات الشخصية بموجب قانون خصوصية البيانات وحمايتها.

66- وتمنع المادة 3، التي تستند إلى المادة 8 (2) من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية، فرض أي التزام جديد باستخدام إدارة الهوية وخدمات توفير الثقة على المشترك وعلى مقدمي الخدمات وعلى الطرف المعول. ويتماشى ذلك مع القاعدة العامة التي تقضي بعدم إدخال أي تعديل على القانون الموضوعي.

67- وقد يكون هناك التزام باستخدام إدارة الهوية وخدمات توفير الثقة في قانون آخر. ويمكن فرض هذا الالتزام في المعاملات مع الكيانات العامة أو في المعاملات التي تنطوي على الامتثال لالتزامات تنظيمية.

*المراجع*

A/CN.9/965، الفقرتان 22 و110؛ A/CN.9/1005، الفقرة 116؛ A/CN.9/1045، الفقرة 79.

### 4- المادة 4- التفسير

68- تستند المادة 4 إلى أحكام موجودة في عدة معاهدات وقوانين نموذجية سابقة للأونسيترال، بما في ذلك الأحكام المتعلقة بالتجارة الإلكترونية (المادة 3 من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية؛ والمادة 4 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية؛ والمادة 5 من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية؛ والمادة 3 من قانون الأونسيترال النموذجي بشأن السجلات الإلكترونية القابلة للتحويل).

69- وتهدف الفقرة 1 إلى تعزيز الأخذ بتفسير موحد عبر الولايات القضائية المشترعة. وهي تفعل ذلك من خلال توجيه انتباه القضاة والهيئات القضائية الأخرى إلى أن التشريعات المحلية [لمشروع الصك] ينبغي تفسيرها في ضوء أصلها الدولي والحاجة إلى توحيد التطبيق. ولذلك، يشجَّع المحتكم إليهم على مراعاة القرارات الصادرة عن ولايات قضائية أجنبية عند البت في القضايا بغية المساهمة في توطيد الاتجاهات التفسيرية الموحدة عبر الوطنية.

70- وتهدف الفقرة 2 إلى الحفاظ على الاتساق في تفسير وتطبيق تشريعات [مشروع الصك] باشتراط أن تُسوَّى المسائل التي لا تسويها أحكامه صراحة وفقاً للمبادئ العامة التي يقوم عليها [مشروع الصك]، بدلاً من المبادئ الموجودة في القانون المحلي.

71- وعلى غرار سائر نصوص الأونسيترال التشريعية بشأن التجارة الإلكترونية، لا يحدد [مشروع الصك] صراحة المبادئ العامة التي يقوم عليها. فالنصوص التشريعية للأونسيترال بشأن التجارة الإلكترونية ترتكز عموماً على مبادئ عدم التمييز ضد استخدام الوسائل الإلكترونية، والحياد التكنولوجي، والتكافؤ الوظيفي، واستقلالية الأطراف، وقد استبينت وجاهة تلك المبادئ أيضاً فيما يخص [مشروع الصك]، رهناً بما يُدخل عليه من تعديلات. فعلى سبيل المثال، على الرغم من أن استقلالية الأطراف مبدأ أساسي من مبادئ القانون التجاري، فإن تطبيقها يخضع لقيود منصوص عليها في القانون الإلزامي، بما في ذلك أحكام [مشروع الصك] التي لا يجوز للأطراف أن تبطلها. وعلاوة على ذلك، حسبما ذكر أعلاه (الفقرة 20)، قد لا يُطبَّق مبدأ التكافؤ الوظيفي في حالة عدم وجود شرط يقتضي إثبات الهوية دون اتصال عبر الإنترنت.

*المراجع*

A/CN.9/936، الفقرتان 67 و72؛ A/CN.9/1005، الفقرتان 117 و118؛ A/CN.9/1051، الفقرات 53-56.

## باء- الفصل الثاني- إدارة الهوية (المواد 5 إلى 12)

### 1- المادة 5- الاعتراف القانوني بإدارة الهوية

72- تمنح المادة 5 اعترافاً قانونياً بإدارة الهوية بإيراد إشارة إلى أن الشكل الإلكتروني لتدقيق الهوية وتحديد الهوية إلكترونياً لا يمنع في حد ذاته أثرهما القانوني أو ينفي صحتهما أو وجوب نفاذهما أو مقبوليتهما كدليل إثبات. ومن ثم، فإن الفقرة 1 تنفذ المبدأ العام المتمثل في عدم التمييز ضد استخدام الوسائل الإلكترونية فيما يخص إدارة الهوية. وينطبق المبدأ بغض النظر عن وجود مكافئ دون اتصال عبر الإنترنت.

73- وتحظر المادة 5 التمييز ضد تحديد الهوية إلكترونياً الناتج عن عملية إدارة الهوية. ويشير عنوانها إلى "الاعتراف القانوني"، وليس إلى "عدم التمييز"، للحفاظ على الاتساق مع عنوان الأحكام المناظرة في نصوص الأونسيترال القائمة.

74- وتنص الفقرة الفرعية (ب) على أن كَوْن خدمة إدارة الهوية خدمة غير معيَّنة لا يحول دون الاعتراف بها قانونياً. وبعبارة أخرى، تمنح الفقرة الفرعية (ب) اعترافاً قانونياً متساوياً بخدمات إدارة الهوية المعينة وتلك غير المعينة، مما يكفل الحياد فيما يتعلق بالنهج المختار لتقييم الموثوقية. إلا أن الفقرة الفرعية (ب) لا توحي بأن أي خدمة من خدمات إدارة الهوية تَستخدِم طرائق موثوقة وتوفر تبعاً لذلك مستوى كافياً من الضمان لتحديد الهوية إلكترونياً: فمن أجل تحقيق تلك النتيجة، ينبغي تقييم موثوقية الطريقة المستخدمة وفقاً للمادتين 10 و11، حسب الحالة.

75- وتؤكد الإشارة إلى الفقرة 3 من المادة 2 في فاتحة المادة 5، أن المادة 5 لا تمس بأي شرط قانوني يقضي بأن تحدد هوية الشخص وفقاً لإجراء معين أو منصوص عليه في القانون. فالفقرة 3 من المادة 2 ليست شرطاً للمادة 5 فحسب، بل أيضاً لجميع الأحكام الأخرى في [مشروع الصك].

*المراجع*

A/CN.9/965، الفقرتان 107 و108؛ A/CN.9/1005، الفقرات 79-86؛ A/CN.9/1045، الفقرات 17 و82-84.

### 2- المادة 6- التزامات مقدمي خدمات إدارة الهوية

76- تنص المادة 6 على التزامات مقدمي خدمات إدارة الهوية. والالتزامات الواردة فيها هي الالتزامات الأساسية لمقدمي خدمات إدارة الهوية، التي يمكن استكمالها بالتزامات قانونية أو تعاقدية إضافية. وقد يجيز عدم تنفيذ هذه الالتزامات الاحتجاج بالمسؤولية وفقاً للمادة 12 ويؤثر على موثوقية خدمات إدارة الهوية، بما في ذلك الخدمات المعيَّنة.

77- وعلاوة على ذلك، تهدف المادة 6 إلى ضمان بقاء مقدم خدمات إدارة الهوية مسؤولاً عن كامل مجموعة خدمات إدارة الهوية التي تقدم إلى المشترك، وإن كان من الممكن أن تؤدَّى وظائف معينة بواسطة كيانات أخرى مثل المتعاقدين أو مقدمي خدمات إدارة الهوية المتفردين في نظم إدارة الهوية المتعددة الأطراف من القطاع الخاص. ولا تمنع المادة 6 مقدم خدمات إدارة الهوية من الاستعانة بمصادر خارجية في أداء أي من الوظائف، أو من توزيع المخاطر على المتعاقدين معه أو على شركاء الأعمال الآخرين.

78- وقد تختلف نظم إدارة الهوية اختلافاً كبيراً في غرضها وتصميمها، وفي الخدمات التي تقدمها. وفي المقابل، قد يعتمد تصميم نظام إدارة الهوية أيضاً على النموذج الذي يقع عليه الاختيار. وبناءً عليه، قد لا تنطبق جميع الالتزامات الواردة في المادة 6 على جميع مقدمي خدمات إدارة الهوية: بل إن تصميم نظام إدارة الهوية ونوع خدمات إدارة الهوية المقدمة سيحددان الالتزامات التي تنطبق على أحد مقدمي خدمات إدارة الهوية بعينه. وتتجسد هذه المرونة في مراعاة تصميم نظم إدارة الهوية في عبارة "مناسبة للغرض والتصميم".

79- وتوضَّح الالتزامات بطريقة محايدة تكنولوجياً بالنظر إلى أن تطبيق مبدأ الحياد التكنولوجي في سياق إدارة الهوية يستلزم متطلبات دنيا لنظم إدارة الهوية تتعلق بخصائص النظام وليس بتكنولوجيات محددة.

80- وفي الممارسة التجارية، عادة ما تخضع الوظائف الواردة في المادة 6 لقواعد تشغيل تعاقدية، لا سيما في الحالات التي يشارك فيها مقدمو خدمات إدارة هوية من القطاع الخاص. وتستند هذه القواعد، التي توفر توجيهات بشأن كيفية تنفيذ العمليات، إلى السياسات، وتنفَّذ من خلال الممارسات، وتُجسَّد في الاتفاقات التعاقدية. ويعترف الالتزام "بوضع قواعد وسياسات وممارسات تشغيلية" بتلك الممارسة التجارية. وبالنظر إلى أهميتها القانونية والعملية، يقتضي البند (د) تسهيل اطلاع المشتركين والأطراف الثالثة على القواعد والسياسات والممارسات التشغيلية.

81- وقد كُرس تقيُّد مقدم الخدمة بالتزاماته وبالتأكيدات التي يقدمها في المادة 9 (أ) من القانون النموذجي بشأن التوقيعات الإلكترونية، التي تفرض التزاماً على مقدِّم خدمات التصديق بأن "يتصرف وفقاً للتأكيدات التي يقدمها بخصوص سياساته وممارساته".

*المراجع*

A/CN.9/936، الفقرة 69؛ A/CN.9/1045، الفقرات 85-95.

### 3- المادة 7- التزامات مقدمي خدمات إدارة الهوية في حال خرق البيانات

82- تنص المادة 7 على التزامات أساسية لمقدمي خدمات إدارة الهوية في حال وقوع خرق للبيانات من شأنه أن يؤثر تأثيراً كبيراً على نظام إدارة الهوية. وتنطبق الالتزامات بموجب المادة 7 بغض النظر عن الغرض من نظام إدارة الهوية وتصميمه، ولا يمكن أن تختلف باختلاف العقد، بما في ذلك في القواعد التشغيلية. وقد تؤثر الخروق الأمنية على نظم إدارة الهوية وخدمات إدارة الهوية على السواء، وقد تؤثر أيضاً على النعوت التي تدار في نظام إدارة الهوية.

83- ويشير مفهوم "خرق البيانات" إلى أي خرق أمني يؤدي إلى التدمير العرضي أو غير القانوني لبيانات مرسلة أو مخزنة أو معالجة، أو فقدان تلك البيانات أو تغييرها أو كشفها دون إذن أو الوصول إليها. وقد يكون له تعريف في قانون خصوصية البيانات وحمايتها.

84- ويُستخدَم مفهوم "التأثير الكبير" في القوانين الإقليمية[6] والوطنية. وقد تساهم عدة عوامل في تقييم هذا التأثير. وتساعد استمارات الإبلاغ عن الخروق في تقييم التأثير من خلال توضيح مدة تلك الخروق ونوع البيانات المتأثرة والنسبة المئوية للمشتركين المتأثرين والمعلومات الأخرى ذات الصلة. وتتوفر أيضاً مبادئ توجيهية تقنية للإبلاغ عن الحوادث، فضلاً عن التقارير السنوية عن الحوادث الأمنية.

85- وتقر المادة 7 بأن اتخاذ تدابير بخلاف التعليق الكامل قد يكون ملائماً، فتُلزِم مقدم خدمات إدارة الهوية "باتخاذ جميع التدابير المعقولة" للتصدي للخرق الأمني واحتوائه.

86- وتنص الفقرة 1 (ج) على واجب الإبلاغ عن الخروق الأمنية، وهو أحد جوانب مبدأ الشفافية. وثمة أهمية لوجود آلية مناسبة للإبلاغ عن الخروق الأمنية لتحسين الأداء ورفع مستوى الثقة في خدمات إدارة الهوية وتوفير الثقة.

87- ويجوز تحديد جوانب معينة للالتزامات الواردة في المادة 7، مثل تحديد الأطراف التي يتعين إبلاغها بالخرق وتوقيت الإبلاغ ومضمونه والكشف عن الخرق وعن تفاصيله التقنية، في القانون الوطني وفي الاتفاقات التعاقدية وفي القواعد والسياسات والممارسات التشغيلية لمقدم خدمات إدارة الهوية.

88- وقد تتطابق الالتزامات المنصوص عليها في المادة 7 مع الالتزامات المقررة بموجب قانون خصوصية البيانات وحمايتها. وفي هذه الحالة، ينبغي تنفيذ جميع الإجراءات المذكورة، وليس مجرد الإخطار، وفقاً لقانون خصوصية البيانات وحمايتها المنطبق.

89- وتنطبق المادة 7 بالتزامن مع قانون خصوصية البيانات وحمايتها وكذلك أي قانون آخر ينطبق على الحادث المحدد. فعلى سبيل المثال، ينطوي الإبلاغ عن خرق البيانات على عناصر مشتركة مع الإبلاغ عن الخروق الأمنية، ولكن توجد بينهما أيضاً اختلافات كبيرة.

*المراجع*

A/CN.9/971، الفقرات 84-87؛ A/CN.9/1005، الفقرات 32-36 و94؛ A/CN.9/1045، الفقرات 96-101.

### 4- المادة 8- التزامات المشتركين

90- تحدد المادة 8 التزامات المشتركين فيما يتعلق بالإبلاغ بوقوع أو باحتمال وقوع تلاعب بإثباتات الهوية. وهذه الالتزامات تكمل التزامات مقدمي خدمات إدارة الهوية بتوفير وسيلة للإبلاغ بالخروق الأمنية (المادة 6 (هـ)) والتصدي للخروق الأمنية أو المساس بسلامة النظام (المادة 7).

91- وينشأ التزام المشترك في حالة خرق البيانات في حالة تعرض إثباتات الهوية للتلاعب، أو في وجود احتمال مثبت بحدوث تلاعب بها. وتبعاً لذلك، تختلف هذه الواقعة عن الواقعة الذي تحدد التزامات مقدمي

(6) المادة 19 (2) من لائحة الاتحاد الأوروبي رقم 2014/910 الصادرة عن البرلمان الأوروبي والمجلس في 23 تموز/يوليه 2014 بشأن تحديد الهوية إلكترونياً وخدمات توفير الثقة فيما يخص المعاملات الإلكترونية في السوق الداخلية، والتي ألغت التوجيه 1999/93/EC (eIDAS Regulation).

خدمات إدارة الهوية في حال خرق البيانات، وهو وقوع خرق أمني للنظام أو مساس بسلامته من شأنه أن يؤثر تأثيراً كبيراً على خدمة إدارة الهوية.

92- وتهدف الإشارة إلى احتمال وقوع تلاعب بإثباتات الهوية إلى ضمان عدم فرض توقعات كبيرة على نحو غير معقول على المشتركين من حيث ما لهم من خبرة تقنية. ولا ينشأ الالتزام بالإبلاغ إلا في حال وجود ملابسات معلومة للمستعمِل تثير شكوكا مبرَّرة بشأن ما إذا كانت إثباتات الهوية تعمل بشكل ملائم.

93- ويجوز أن يتضمن العقد المبرم بين المشترك ومقدم خدمات إدارة الهوية التزامات إضافية للمشترك. وقد يتضمن ذلك العقد أيضاً معلومات إضافية عن سبل الامتثال للالتزام بالإبلاغ الوارد في المادة 8.

94- وتشير الإشارة إلى "استخدام وسائل معقولة أخرى" إلى أن المشترك ليس محدداً باستخدام قنوات الإبلاغ التي يوفرها مقدم خدمات إدارة الهوية.

95- ويشير مفهوم "التلاعب بإثباتات الهوية" إلى حالات الوصول غير المأذون به إلى إثباتات الهوية.

96- وتهدف الفقرة (ب) إلى تناول الحالات التي لا يكون فيها المشترك على علم فعلي بوقوع تلاعب ولكن لديه أسباب للاعتقاد باحتمال حدوث ذلك. وهي مستوحاة من المادة 8 (1) (ب) '2' من القانون النموذجي بشأن التوقيعات الإلكترونية، التي تتضمن التزامات مماثلة على الموقِّع.

*المراجع*

A/CN.9/936، الفقرة 68؛ A/CN.9/971، الفقرات 88-96؛ A/CN.9/1005، الفقرات 37-43 و95 و96؛ A/CN.9/1045، الفقرات 102-105.

## 5- المادة 9- تحديد هوية شخص باستخدام إدارة الهوية

97- في نصوص الأونسيترال المتعلقة بالتجارة الإلكترونية، تحدد قواعد التكافؤ الوظيفي الشروط التي يجب أن تستوفيها السجلات أو الطرائق أو العمليات الإلكترونية للوفاء بشرط قانوني يوجب توافر مستندات ورقية. وتنص المادة 9 على قاعدة للتكافؤ الوظيفي للحالات التي يشترط فيها القانون تحديد الهوية، أو التي يتفق فيها الأطراف على تحديد هويتهم. وبالنظر إلى أن الهدف من هذا الحكم هو وضع شروط للتكافؤ بين تحديد الهوية بالاتصال الحاسوبي المباشر وبدونه، فإن المادة 9 لا تنطبق إلا إذا وُجِد مكافئ لتحديد الهوية بدون اتصال عبر الإنترنت. ومع ذلك، تشكل المادة 9 أحد الأحكام الأساسية لإنشاء نظام قانوني لإدارة الهوية.

98- وتماشياً مع المبادئ الراسخة في نصوص الأونسيترال، تكمل قاعدة التكافؤ الوظيفي هذه قاعدة الاعتراف القانوني المنصوص عليها في المادة 5. ولكن على الرغم من أن المادة 5 تنطبق على جميع أشكال تحديد الهوية إلكترونياً، بصرف النظر عن وجود مكافئ لتحديد الهوية دون اتصال عبر الإنترنت، فإن الهدف من المادة 9 هو تقرير تحديد الهوية إلكترونياً باعتباره مكافئاً وظيفياً لتحديد الهوية دون اتصال عبر الإنترنت، ومن ثم، لا تُفعَّل المادة 9 إلا بإيراد إشارة إلى مكافئ ورقي.

99- وتشير المادة إلى استخدام خدمات إدارة الهوية، للإشارة إلى أن اشتراطات التكافؤ تُستوفى باستخدام إثباتات الهوية، مقابل استخدام نظم إدارة الهوية أو الهوية نفسها.

100- والمادة 9 لا تمس باشتراطات تحديد الهوية وفقاً لإجراء بعينه أو طريقة بعينها، وفق ما تنص عليه المادة 2 (3). وقد تتعلق تلك الاشتراطات بالامتثال التنظيمي، مثل تلك التي تحددها اللوائح المصرفية ولوائح مكافحة غسل الأموال (انظر الفقرة 62 أعلاه).

101- ويمكن استخدام التحديد الإلكتروني للهوية لاستيفاء شرط التحقق من نعوت محددة في هوية شخص ما، مثل العمر أو مكان الإقامة، حسبما يقتضيه التحديد المادي للهوية. وفي هذا الصدد، بالنظر إلى أن مفهوم "الهوية" يعرف بالإشارة إلى "السياق"، الذي يحدد بدوره النعوت المطلوبة لتحديد الهوية، فإن التحديد الناجح لهوية الشخص استناداً إلى المادة 9 يشمل التحقق من النعوت المطلوبة. وتتجسد الحاجة إلى التحقق من النعوت ذات الصلة أيضاً في عبارة "لذلك الغرض". ولا تتناول الأحكام المتعلقة بالموثوقية الواردة في المادة 10 مسألة التحقق من نعوت محددة، لأن تلك الأحكام تتعلق بالعمليات المتصلة بإدارة إثباتات الهوية وليس بالنعوت الواردة في إثباتات الهوية.

102- وتشير المواد 9 ومن 16 إلى 21 من [مشروع الصك] إلى حالات يَشترِط فيها القانون اتخاذ إجراء أو ينص على عواقب لعدم اتخاذ إجراء. وقد وُضعَت هذه الصيغة، المستخدمة في المادة 9 من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية، لاستيعاب قواعد التكافؤ الوظيفي في الحالات التي لا يشترط فيها القانون اتخاذ إجراءات معينة ولكنه يرتب عواقب قانونية على اتخاذها، وهي تشمل أيضاً الحالات التي يصرح فيها القانون باتخاذ إجراءات معينة (انظر المادة 9 من القانون النموذجي بشأن السجلات الإلكترونية القابلة للتحويل).

*المراجع*

A/CN.9/965، الفقرات 62-85؛ A/CN.9/971، الفقرات 24-49؛ A/CN.9/1005، الفقرات 97-100؛ A/CN.9/1045، الفقرات 106-117؛ A/CN.9/1051، الفقرات 42-44.

## 6- المادة 10- اشتراطات تقرير موثوقية خدمات إدارة الهوية

103- تقدم المادة 10 إرشادات بشأن تقرير موثوقية الطريقة المستخدمة لتحديد الهوية في المادة 9 بعد أن تكون الطريقة قد استُخدمَت (نهج التقرير اللاحق).

104- وتطبق الفقرة 1 (أ) نهج التقرير اللاحق بالإشارة إلى استخدام طريقة "موثوق بها بقدر مناسب للغرض الذي تُستخدَم من أجله خدمة إدارة الهوية". ويجسد هذا الحكم الفهم بأن الموثوقية مفهوم نسبي. ومع ذلك، وخلافاً لبعض خدمات توفير الثقة التي قد تؤدي وظائف متعددة، يؤدي التحديد الإلكتروني للهوية وظيفة واحدة، وهي تحديد الهوية على نحو موثوق بالوسائل الإلكترونية. ويمكن أداء هذه الوظيفة لأغراض مختلفة، يرتبط كل منها بمستوى مختلف من الموثوقية.

105- وتتضمن الفقرة 1 (ب) بنداً يهدف إلى الحيلولة دون رفض خدمة إدارة الهوية حين تكون قد أدت وظيفتها فعلياً. ويحدث الرفض عندما يعلن كيان ما عدم أداء إجراء ما. ولكي تُفعَّل الآلية الواردة في الفقرة 1 (ب)، يجب أن تكون الطريقة، سواء كانت موثوقة أم لا، قد أدت وظيفة تحديد الهوية فعلياً، أي ربط الشخص الذي يلتمس تحديد الهوية بإثباتات الهوية. ويستند هذا الحكم إلى المادة 9 (3) (ب) '2' من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية.

106- وتتضمن الفقرة 2 قائمة بالظروف، الموصوفة بعبارات محايدة تكنولوجياً، التي قد تكون ذات صلة بتقرير الموثوقية بواسطة المحتكم إليه. وبالنظر إلى أن القائمة توضيحية وليست حصرية، فقد تكون هناك ظروف إضافية ذات صلة. وعلاوة على ذلك، قد لا تكون جميع الظروف المذكورة ذات صلة في جميع الحالات التي يتعين فيها تقرير الموثوقية. وعلى وجه الخصوص، قد تتباين أهمية اتفاق الأطراف تبايناً كبيراً تبعاً لمستوى الاعتراف الذي تمنحه الولاية القضائية المعنية لاستقلالية الأطراف في مجال تحديد الهوية.

وإضـــافة إلى ذلك، قد لا تؤثر الاتفاقات التعاقدية على الأطراف الثالثة، ومن ثم لن تكون هذه الظروف ذات صلة عندما يتعلق الأمر بأطراف ثالثة.

107- وتنص الفقرة 3 على أن مكان تقديم خدمة إدارة الهوية ومكان عمل مقدم خدمات إدارة الهوية لا يعتد بهما في حد ذاتهما لدى تقرير الموثوقية. ويهدف هذا الحكم إلى تيســـير الاعتراف عبر الحدود بخدمات إدارة الهوية وهو مســتوحى من المادة 12 (1) من قانون الأونسـيترال النموذجي بشـأن التوقيعات الإلكترونية، التي ترســـي قاعدة عامة بعدم التمييز في تحديد المفعول القانوني للشـــهادة أو التوقيع الإلكتروني. وللاطلاع على مناقشـات بشـأن التفاعل بين المادتين 12 (1) و12 (2) من القانون النموذجي بشـأن التوقيعات الإلكترونية، انظر الوثيقة A/CN.9/483، الفقرات 28-36.

108- ووفقاً للفقرة 4، يترتب على تعيين خدمة موثوقة من خدمات إدارة الهوية وفقاً للمادة 11 افتراضٌ بموثوقية الطرائق التي تســـتخدمها خدمة إدارة الهوية المعيَّنة. وهذا هو التمييز الوحيد بين خدمات إدارة الهوية المعيَّنة وغير المعيَّنة. وعلاوة على ذلك، وفقاً للفقرة 5 (ب)، يجوز دحض افتراض الموثوقية الذي يُعلَّق على التعيين.

109- وتوضـح الفقرة 5 العلاقة بين المادتين 10 و11 بالنص على أن وجود آلية للتعيين لا يسـتبعد تطبيق التقرير اللاحق لموثوقية الطريقة. وهذا الحكم مستلهم من المادة 6 (4) من قانون الأونسـيترال النموذجي بشـأن التوقيعات الإلكترونية.

### (أ) إطار مستوى الضمان

110- تشـير المادة 10 والمادة 11 إلى مفهوم "مسـتوى الضـمان" أو الأطر المماثلة المسـماة بخلاف ذلك. ويوفر مستوى الضـمان توجيهات للأطراف المعولة بشأن درجة الثقة التي قد تضـعها في عمليات تدقيق الهوية وتحديد الهوية إلكترونياً، وما إذا كانت تلك العمليات ملائمة لأغراض محددة. ولا يحدد [مشـــروع الصـــك] مستويات الضمان ولا يشترط تعريفها أو استخدامها.

111- وتتوخى أطر الضـــمان مســـتويات مختلفة من الضـــمانات المرتبطة بالاشـــتراطات المختلفة. وبعبارة أخرى، توضـح أطر مسـتويات الضـمان الاشـتراطات التي يجب أن تسـتوفيها نظم وخدمات إدارة الهوية لتوفير مسـتوى معين من الضـمان في موثوقيتها. وينبغي توضـيح مسـتويات الضـمانات بعبارات عامة للحفاظ على الحياد التكنولوجي.

112- وفي المقابل، يمكن صـياغة اشـتراط توفير مسـتوى معين من الضـمان لموثوقية الهويات المسـتخدمة بإيراد إشـارة إلى المسـتويات المبينة في إطار مسـتوى الضـمان. ويمكن عندئذ حصـر النظم والخدمات المحددة لإدارة الهوية مقابل الاشـتراطات التي يقتضـيها مسـتوى الضـمان المطلوب. والمطابقة الناجحة بين خدمة إدارة الهوية والاشـتراطات المقترنة بذلك المسـتوى من الضـمان تؤدي إلى إمكانية اسـتخدام خدمة إدارة الهوية تلك، لذلك النوع من المعاملة تحديداً.

### (ب) التصديق والإشراف

113- تذكر المادة 10 من ضـمن الظروف التي يحتمل أن تكون ذات صـلة، وجود "إجراءات للإشـراف أو التصـديق فيما يتعلق بخدمة إدارة الهوية"، إن وجدت. وقد يسـاعد التصـديق والإشـراف بشـكل كبير في ترسـيخ الثقة في مقدمي خدمات إدارة الهوية وخدماتهم، لأغراض من بينها تقرير موثوقية الطريقة المســـتخدمة، لأنهما (أي التصـديق والإشـراف) يرتبطان بمسـتوى معين من الموضـوعية في تقييم موثوقية الطريقة المسـتخدمة. وقد

سبق الإقرار بذلك في المادة 12 (أ) '6' من القانون النموذجي بشأن السجلات الإلكترونية القابلة للتحويل وفي المادة 10 (و) من القانون النموذجي بشأن التوقيعات الإلكترونية.

114- وتشمل خيارات التصديق: التصديق الذاتي، والتصديق بواسطة طرف ثالث مستقل، والتصديق بواسطة طرف ثالث مستقل معتمد، والتصديق بواسطة كيان عام. ويتأثر اختيار الشكل الأنسب للتصديق بنوع الخدمة المعنية وتكلفتها ومستوى الضمان المنشود. ففي سياق المعاملات بين المنشآت التجارية، ينبغي أن يكون بوسع شركاء الأعمال انتقاء الخيار الأنسب لاحتياجاتهم، مع التسليم بأن كل خيار ستترتب عليه آثار مختلفة.

115- وقد يُعتبر وجود آلية إشرافية لنظم وخدمات إدارة الهوية أمراً مفيداً أو حتى ضرورياً لإرساء الثقة في إدارة الهوية. غير أن إنشاء هيئة إشرافية تترتب عليه آثار إدارية ومالية قد تكون باهظة التكلفة. ولا يوجب [مشروع الصك] إنشاء نظام إشرافي أو ييسر ذلك.

116- وتوجد نهوج مختلفة فيما يتعلق بإشراك السلطات العامة في التصديق والإشراف، وهو قرار سياساتي يخص الولاية القضائية المشترعة. ويستند النهج المتبع في [مشروع الصك] إلى الحياد النموذجي، ولا تستبعد الإشارات إلى التصديق والإشراف نظم التصديق الذاتي. فحين تكون الكيانات العامة جهات تصديق أو إشراف ومقدِّمة لخدمات إدارة الهوية في الوقت نفسه، يمكن فصل مهام التصديق والإشراف عن تقديم خدمات إدارة الهوية.

117- وفي بعض الحالات، مثل الحالات التي تُستخدَم فيها أنواع معينة من تكنولوجيا الدفاتر الموزَّعة، قد لا يكون أي حل يفترض مسبقاً وجود هيئة مركزية للتصديق أو الاعتماد أو الإشراف مناسباً بسبب التحديات التي يطرحها تحديد الكيان الذي يمكنه طلب التصديق، والكيان المطلوب تقييمه، والكيان المسؤول عن اتخاذ الإجراءات التصحيحية وإجراءات الإنفاذ، ضمن أمور أخرى.

*المراجع*

A/CN.9/965، الفقرات 40-55 و112-115؛ A/CN.9/971، الفقرات 50-61؛ A/CN.9/1005، الفقرة 101؛ A/CN.9/1045، الفقرات 118-124؛ A/CN.9/1051، الفقرات 47-49؛ A/CN.9/WG.IV/WP.153، الفقرتان 74 و75.

## 7- المادة 11- تعيين نظم [وخدمات] إدارة الهوية الموثوقة

118- تكمل المادة 11 المادة 10 بتوفير إمكانية تعيين نظم [وخدمات] إدارة الهوية. وبعبارة أدق، فهي تورد الشروط التي يجب أن تستوفيها نظم [أو خدمات] إدارة الهوية حتى تُدرج في قائمة نظم [وخدمات] إدارة الهوية المعيَّنة.

119- ويستند تعيين نظم [وخدمات] إدارة الهوية التي تستخدم طرائق موثوقة إلى جميع الظروف ذات الصلة، بما في ذلك تلك الواردة في المادة 10 المتعلقة بتقرير موثوقية الطريقة. والإشارة إلى الظروف المذكورة في المادة 10 تكفل قدراً من الاتساق بين الطرائق التي تعيَّن موثوقيتها مسبقاً والطرائق التي تعيَّن موثوقيتها لاحقاً. وعلاوة على ذلك، يراعى في أي تعيين "الاتساقُ مع المعايير والإجراءات الدولية المعترف بها ذات الصلة بتنفيذ عملية التعيين" من أجل تعزيز الاعتراف القانوني عبر الحدود وقابلية التشغيل المتبادل.

120- وثمة أهمية حاسمة للمعلومات المتعلقة بنظم [وخدمات] إدارة الهوية المعيَّنة لإعلام المشتركين المحتملين بوجودها. فالكيان القائم بالتعيين عليه التزام بنشر قائمة بنظم [وخدمات] إدارة الهوية المعيَّنة، بما في ذلك تفاصيل مقدم خدمة إدارة الهوية، على موقعه الشبكي مثلاً، أو إعلام الجمهور بوسيلة أخرى بالتعيين.

ويُسلَّم أيضاً في المعايير التقنية المستخدمة على نطاق واسع بأهمية هذه القوائم لضمان الشفافية في تعيين خدمات إدارة الهوية، في سياقات من بينها السياق العابر للحدود.

121- وتشير الفقرة 2 (أ) إلى المعايير والإجراءات ذات الصلة بتقرير الموثوقية، وهي تهدف إلى ضمان مستوى معين من الاتساق في نتائج تقييمات التقرير المسبق واللاحق للموثوقية. ومن ناحية أخرى، تشير الفقرة 3 صراحة إلى المعايير والإجراءات ذات الصلة بالتعيين، مثل تقييم الامتثال وعمليات المراجعة، التي يتميز بها نهج التقرير المسبق على وجه الخصوص.

122- ومثل الفقرة 10 (3)، تنص الفقرة 4 على أن مكان تقديم نظم [أو خدمات] إدارة الهوية ومكان عمل مقدم خدمات إدارة الهوية لا يعتد بهما في حد ذاتهما لدى تعيين خدمة موثوقة. ومن ثم، تستند الفقرة 4 أيضاً إلى المادة 12 (1) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، التي ترسي قاعدة عامة متعلقة بعدم التمييز في تحديد المفعول القانوني للشهادة أو التوقيع الإلكتروني. ومن الناحية العملية، يسمح هذا الحكم لمقدم خدمات إدارة الهوية الأجنبي بطلب تعيين نظام [أو خدمات] إدارة الهوية من السلطة المختصة في الولاية القضائية المشترعة، على النحو المبين أيضاً في المادة 25 (3).

*المراجع*

A/CN.9/965، الفقرات 40-55؛ A/CN.9/971، الفقرات 68-76؛ A/CN.9/1005، الفقرتان 102 و105؛ A/CN.9/1045، الفقرات 125-129.

## 8- المادة 12- مسؤولية مقدمي خدمات إدارة الهوية

123- قد يكون لنظام المسؤولية القانونية تأثير مهم في تعزيز استخدام إدارة الهوية وخدمات توفير الثقة، وهو أحد العناصر الأساسية لـ[مشروع الصك]. وتنص المادة 12 على نظام مسؤولية واحد لمقدمي خدمات إدارة الهوية تجاه المشتركين على أساس مبدأ أن يكون مقدم خدمات إدارة الهوية مسؤولاً عن عواقب عدم تقديم الخدمات وفقاً لما يقتضيه القانون وما يُتفَق عليه في العقد.

124- وتستند المادة 12 إلى ثلاثة عناصر هي: (أ) أنها لا تمس بتطبيق القانون الإلزامي، بما في ذلك الواجبات الإلزامية لمقدم خدمات إدارة الهوية بموجب [مشروع الصك]؛ (ب) أنها تحدد مسؤولية مقدم خدمات إدارة الهوية عن الإخلال بواجباته الإلزامية بصرف النظر عما إذا كانت تلك الواجبات لها أيضاً أساس تعاقدي؛ (ج) أنها تقر بإمكانية الحد من المسؤولية في ظل شروط معينة.

125- وطبيعة المسؤولية بموجب المادة 12 طبيعة قانونية، وهي منفصلة، من هذا المنطلق، عن المسؤولية بموجب قانون العقود. ويتمثل هدفها في الاعتراف بإمكانية مساءلة مقدم الخدمات عن عدم الامتثال لالتزاماته المقررة بموجب [مشروع الصك] بغض النظر عما إذا كان لتلك الالتزامات أيضا أساس تعاقدي. وينطبق هذا الحكم بغض النظر عن الطبيعة العامة أو الخاصة لمقدم خدمات إدارة الهوية.

126- وقد تنشأ مسؤولية مقدمي خدمات إدارة الهوية من استخدام خدمات إدارة الهوية المعيَّنة وغير المعيَّنة. إلا أنها ليست مسؤولية مطلقة. فعلى سبيل المثال، قد لا يكون مقدم خدمات إدارة الهوية مسؤولاً تجاه المشترك إذا كان سبب الخسارة هو استخدام إثباتات هوية كان المشترك يعلم وقتها، أو كان من واجبه أن يعلم، أنها إثباتات هوية متلاعب بها.

127- وتُترَك المسائل المتعلقة بالمسؤولية التي لم تعالج في المادة 12 للقانون المنطبق خارج نطاق مشاريع الأحكام. وتشمل تلك المسائل مستوى العناية ودرجة الخطأ، وعبء الإثبات، وتحديد حجم الأضرار والتعويض، وما إلى ذلك.

128- وتقر المادة 12 بإمكانية الحد من المسؤولية في ظل شروط معينة، وهي وجود قيود مفروضة على غرض المعاملات التي استُخدمَت خدمة إدارة الهوية من أجلها أو قيمة تلك المعاملات، وأن يكون المشترك قد أُبلغ بهذه القيود.

129- وقد تكون القيود المفروضة على المسؤولية ضرورية لاحتواء تكلفة التأمين، ضمن أمور أخرى. ويتم الاتفاق على حدود المسؤولية في العقد المبرم بين مقدم الخدمة والمشترك. ومن الناحية العملية، تجسَّد هذه الممارسات عادة في القواعد والسياسات والممارسات التشغيلية لمقدم الخدمة.

130- ويحدد القانون المنطبق مدى قدرة مقدم خدمات إدارة الهوية على الحد من مسؤوليته. ولا يمس [مشروع الصك] بتطبيق أي قانون يقيد حق مقدم الخدمة في الحد من مسؤوليته أو وضع شروط لهذه القيود.

131- ولا تهدف الفقرة 3 (ب) إلى استحداث التزام جديد بالإبلاغ، ولكنها تشير إلى أن الحكم لا يراد به أن يبطل اشتراطات أكثر صرامة تخص الإبلاغ بموجب القانون المنطبق. وسيحدد ذلك القانون أي اشتراط منطبق فيما يخص الإبلاغ، مثل الإخطار أو الموافقة الصريحة.

132- ولا تتناول المادة 12 سوى مسؤولية مقدمي خدمات إدارة الهوية تجاه المشتركين. ولأي طرف ثالث مُني بخسارة ناجمة عن استخدام خدمات إدارة الهوية أن يلتمس التعويض بموجب قواعد المسؤولية القائمة إما ضد مقدم الخدمة أو ضد المشترك. وفي الحالة الأخيرة، يمكن للمشترك عندئذ أن يقدم مطالبة ضد مقدم خدمات إدارة الهوية.

133- ولا تحد المادة 12 من قدرة مقدم الخدمة على الحد من المسؤولية تجاه الأطراف الثالثة بموجب قانون آخر. وتقتضي المادة 6 (د) من مقدم الخدمة أن يسهل اطلاع الأطراف الثالثة أيضاً على قواعده وسياساته وممارساته التشغيلية. إلا أن [مشروع الصك] لا يشترط تحديداً على مقدم الخدمة إبلاغ الأطراف الثالثة المعولة بحدود المسؤولية لأن التحديد المسبق لتلك الأطراف الثالثة قد يكون صعباً.

134- وتنطبق المادة 12 على مقدمي خدمات إدارة الهوية بغض النظر عن طبيعتهم العامة أو الخاصة. وقد تحتاج الولاية القضائية المشترعة إلى تكييف هذا الحكم مع أي قاعدة خاصة بشأن مسؤولية الكيانات العامة. ولا تنطبق المادة 12 على الكيانات العامة التي تؤدي وظائف إشرافية وتدير السجلات المدنية وإحصاءات الأحوال المدنية التي قد توفر إثباتات للهوية التأسيسية.

*المراجع*

A/CN.9/936، الفقرات 83-86؛ A/CN.9/965، الفقرات 116-118؛ A/CN.9/971، الفقرات 98-107؛ A/CN.9/1005، الفقرة 76؛ A/CN.9/1045، الفقرتان 130 و131؛ A/CN.9/1051، الفقرات 13-29.

## جيم- الفصل الثالث- خدمات توفير الثقة (المواد 13 إلى 24)

### 1- المادة 13- الاعتراف القانوني بخدمات توفير الثقة

135- تنص المادة 13 على قاعدة عامة بشأن عدم التمييز ضد النتيجة المستمدة من استخدام خدمة توفير الثقة، وهي ضمان صحة سمات معينة لرسالة البيانات. وتتماشى الإشارة إلى النتيجة المستمدة من استخدام

خدمة توفير الثقة مع النهج المتبع في المادة 5، الذي يعطي اعترافاً قانونياً بتحديد الهوية إلكترونياً نتيجة لاستخدام إدارة الهوية.

136- وتنطبق المادة 13 على خدمات توفير الثقة بصرف النظر عما إذا كانت مسماة في [مشروع الصك] وهي تطبق بشكل مستقل عن وجود قاعدة للتكافؤ الوظيفي.

*المراجع*

A/CN.9/971، الفقرات 112-115؛ A/CN.9/1005، الفقرات 19-26؛ A/CN.9/1045، الفقرتان 16 و17.

### 2- المادة 14- التزامات مقدمي خدمات توفير الثقة

137- تحدد المادة 14 الالتزامات الأساسية لمقدمي خدمات توفير الثقة بغض النظر عما إذا كانت خدمة توفير الثقة مسماة أم لا. ويجوز للاتفاقات التعاقدية أن تنص تحديداً على هذه الالتزامات الأساسية وتكملها، ولكن لا يجوز أن تحيد عنها. وهذا النهج شبيه بالنهج المعتمد في المادتين 6 و7 بشأن التزامات مقدمي خدمات إدارة الهوية.

138- وتقر الإشارة إلى كون القواعد والسياسات والممارسات التشغيلية "مناسبة للغرض من خدمة توفير الثقة وتصميمها" بأن التزامات مقدمي خدمات توفير الثقة تتباين في ضوء التنوع في تصميم كل خدمة من خدمات توفير الثقة وتصميمها.

139- ويجسد الالتزام بتسهيل اطلاع الأطراف الثالثة أيضاً على السياسات والممارسات، الممارسة القائمة التي تعترف بأن هذه المعلومات لها أهميتها لدى الطرف المعوِّل في تقرير ما إذا كان سيقبل النتيجة المستمدة من استخدام خدمة توفير الثقة، بما يتماشى مع مبدأ الاستخدام الطوعي لخدمات توفير الثقة (المادتان 2 (2) (ج) و3 (1)).

140- وعادة ما تُجسَّد القيود المفروضة على غرض المعاملات التي تُستخدَم خدمة توفير الثقة من أجلها أو قيمة تلك المعاملات في القواعد التشغيلية التي تحكم خدمة توفير الثقة، التي تشمل أيضاً سياسات وممارسات مقدم خدمات توفير الثقة. ولذلك، تهدف الفقرة 1 (ج) أيضاً إلى الوفاء بواجب الشفافية تجاه الأطراف الثالثة فيما يتعلق بالقيود التعاقدية المنطبقة. ويوجد حكم مماثل في المادة 9 (1) (د) '2' من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية.

*المراجع*

A/CN.9/971، الفقرتان 152 و153؛ A/CN.9/1005، الفقرات 28-36 و73؛ A/CN.9/1045، الفقرات 18-21 و57.

### 3- المادة 15- التزامات المشتركين

141- تحدد المادة 15 التزامات المشتركين في حالة وقوع تلاعب بخدمة توفير الثقة. ولا يحدد [مشروع الصك] التزامات إضافية للمشتركين فيما يتعلق باستخدام خدمات توفير الثقة. ويمكن الاطلاع على مثال على هذه الالتزامات في المادة 8 (1) (أ) و(ج) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية.

142- وتنص المادة 15 على التزامات المشتركين في حال وقوع تلاعب بخدمة توفير الثقة، في حين تنص المادة 14 (2) على التزامات مقدمي خدمات توفير الثقة في حال وقوع خرق للبيانات. ويشير مفهوم "التلاعب بخدمة توفير الثقة" إلى حالات الوصول غير المأذون به إلى خدمة توفير الثقة. وبناءً عليه، تفترض المادة 15

مسبقاً وقوع حادث يؤثر في موثوقية خدمة توفير الثقة، في حين تفترض المادة 14 مسبقاً وقوع خرق أمني لخدمة توفير الثقة أو مساس بسلامتها من شأنه أن يؤثر تأثيراً كبيراً عليها.

143- ويورد عادة العقد المبرم بين مقدم خدمات توفير الثقة والمشترك تفاصيل عن سبل الامتثال للالتزامات الواردة في المادة 15. وعادة ما تشير هذه الاتفاقات التعاقدية إلى سياسات وممارسات مقدم خدمات توفير الثقة.

144- ولا يتضمن [مشروع الصك] قواعد للمسؤولية خاصة بالمشتركين. ولذلك، فإن مسؤولية المشترك تتقرر بالأحكام التعاقدية، التي قد تحدد التزامات إضافية للمشتركين، وبقواعد المسؤولية العامة.

145- وخلافاً لأحكام معينة وردت في نصوص الأونسيترال السابقة (انظر المادة 11 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية)، لا تنص المادة 15 على التزامات الأطراف الثالثة التي يمكن أن تكون مسؤولة بموجب قانون آخر.

*المراجع*

A/CN.9/1005، الفقرات 37-43؛ A/CN.9/1045، الفقرات 22-26.

### 4- المادة 16- التوقيعات الإلكترونية

146- تتناول المادة 16 التوقيعات الإلكترونية. وتتضمن كافة النصوص التشريعية للأونسيترال بشأن التجارة الإلكترونية أحكاماً بشأن استخدام التوقيعات الإلكترونية يمكن للأشخاص الطبيعيين أو الاعتباريين، على السواء، الأخذ بها. وصياغة المادة 16 مستلهمة من صياغة المادة 9 من قانون الأونسيترال النموذجي بشأن السجلات الإلكترونية القابلة للتحويل، التي تأخذ بدورها في الاعتبار صيغة المادة 9 (3) من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية.

147- ويُستوفى اشتراط التوقيع الورقي إذا استخدمت طريقة لتحديد هوية الموقّع على رسالة البيانات وبيان نية الموقّع فيما يتعلق برسالة البيانات الموقَّعة. وتنطبق الإشارة إلى استخدام طريقة "فيما يتعلق بالمعلومات الواردة في رسالة البيانات" على تحديد هوية الشخص وعلى بيان نية الشخص، كليهما.

148- ويجوز استخدام التوقيعات الإلكترونية لتحقيق أغراض متنوعة مثل تحديد مُنشئ رسالة ما وارتباطه بمحتواها. وتتوافر عدة تكنولوجيات وطرائق لاستيفاء اشتراطات التوقيع الإلكتروني. ففي سياق تجاري، يجوز للأطراف أن تحدد التكنولوجيا والطريقة الأكثر ملاءمة للتوقيع الإلكتروني في ضوء التكاليف ومستوى الضمان المطلوب وتوزيع المخاطر وغير ذلك من الاعتبارات. وقد ناقشت نصوص الأونسيترال السابقة بتعمق أغراض التوقيعات الإلكترونية وطرائقها (دليل الاشتراع الخاص بقانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، الفقرات 29-62؛ وتعزيز الثقة، الفقرات 24-66).

*المراجع*

A/CN.9/971، الفقرات 116-119؛ A/CN.9/1005، الفقرات 44-51؛ A/CN.9/1045، الفقرة 34؛ A/CN.9/1051، الفقرة 50.

### 5- المادة 17- الأختام الإلكترونية

149- توفر الأختام الإلكترونية ضمانات للتأكد من منشأ وسلامة رسالة البيانات التي تنشأ من شخص اعتباري. فهي تجمع عملياً بين وظيفة التوقيع الإلكتروني العام فيما يتعلق بالمنشأ، ووظيفة أنواع معينة من

التوقيعات، التي تستند عادة إلى استخدام مفاتيح التشفير، فيما يتعلق بالسلامة. ويُجسَّد وجود هذه التوقيعات الإلكترونية في المادة 6 (3) (د) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية. وبناءً عليه، يستند شرح الاشتراط المتعلق بالسلامة الوارد في المادة 17 إلى المادة 6 (3) (د) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية.

150- والمادة 17 مستوحاة من التشريعات الإقليمية، التي تنص على أن "الأختام الإلكترونية يمكن أن تُستخدَم للتوثُّق من أي موجود رقمي من موجودات الشخص الاعتباري، مثل شفرات البرامج الحاسوبية أو الخوادم، بالإضافة إلى التوثُّق من الوثيقة الصادرة عن الشخص الاعتباري". (لائحة الاتحاد الأوروبي بشأن تحديد الهوية إلكترونياً وخدمات توفير الثقة فيما يخص المعاملات الإلكترونية في السوق الداخلية (eIDAS)، البند 65).

151- ويتحقق التأكد من منشأ رسالة البيانات عن طريق تحديد مصدرها، الذي يتطلب بدوره تحديد هوية الشخص الاعتباري منشئ رسالة البيانات. والطريقة المستخدمة لتحديد هوية الشخص الاعتباري الذي يضع الختم هي نفسها المستخدمة لتحديد هوية الموقّع، وعادة ما اشتُرِعَت أحكام الأونسيترال بشأن التوقيعات الإلكترونية لتنطبق على الأشخاص الطبيعيين والقانونيين على السواء.

152- وعلاوة على ذلك، تشترط الأحكام الواردة في نصوص الأونسيترال السلامة لتحقيق التكافؤ الوظيفي مع المفهوم الورقي "للأصل". وعلى وجه الخصوص، تشير المادة 6 (3) (د) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية إلى مفهوم "السلامة" إذا كان الغرض من الاشتراط القانوني للتوقيع هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع.

153- وفي ضوء ما سبق، من الممكن ألا تميز الولايات القضائية التي اشترعت بالفعل أحكام الأونسيترال بشأن التوقيعات الإلكترونية التي توفر ضمانات بشأن السلامة، بين الوظائف المطلوب أداؤها باستخدام التوقيع الإلكتروني وتلك المطلوب أداؤها باستخدام الختم الإلكتروني. وهذا قد يجسد أيضاً الممارسة التجارية المتمثلة في استخدام طرائق هجينة تجمع بين الأختام الإلكترونية والتوقيعات الإلكترونية.

*السلامة*

154- السلامة عنصر أساسي من عناصر الأختام الإلكترونية والأرشفة الإلكترونية، ويجوز أن تكون عنصراً اختيارياً في خدمات توفير الثقة الأخرى. وفي نصوص الأونسيترال السابقة، تعد السلامة شرطاً لتحقيق التكافؤ الوظيفي مع المفهوم الورقي "للأصل" (المادة 8 من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية). وتُستوحى المادتان 17 و19 من المادة 8 (3) من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية من حيث الاشتراطات المتعلقة بالتأكد من السلامة.

*المراجع*

A/CN.9/971، الفقرات 124-128؛ A/CN.9/1005، الفقرات 52-54 و58؛ A/CN.9/1045، الفقرات 35 و36 و56-58.

### 6- المادة 18- أختام الوقت الإلكترونية

155- توفر أختام الوقت الإلكترونية دليلاً على تاريخ ووقت وضع الختم على البيانات. وفي العادة، يرتب القانون عواقب على احتمال تعذر إثبات تاريخ ووقت حدوث واقعة معينة بمستوى كاف من الثقة. فعلى سبيل المثال، قد يلزم إثبات تاريخ إبرام عقد ما حتى تتمكن أطراف ثالثة من الطعن فيه.

156- وعادة ما توضع أختام الوقت فيما يتعلق بإجراءات معينة مثل إنشاء سجل إلكتروني في شكله النهائي، والتوقيع، وإرسال الخطابات الإلكترونية وتلقيها، وما إلى ذلك. ويمكن استيفاء اشتراط تحديد منطقة التوقيت بالإشارة إلى التوقيت العالمي المنسق (UTC)، جوازاً وليس إلزاماً.

157- وتتضمن المادة 18 إشارة إلى "البيانات" إلى جانب "الوثائق والسجلات والمعلومات". وتهدف هذه الإشارة إلى شمول الحالات التي تُربط فيها أختام الوقت ببيانات لا ترد في وثيقة أو سجل، وليست مقدمة بشكل منظم كمعلومات.

*المراجع*

A/CN.9/971، الفقرات 129-134؛ A/CN.9/1005، الفقرة 55.

## 7- المادة 19- الأرشفة الإلكترونية

158- تتناول المادة 19 خدمات الأرشفة الإلكترونية التي توفر اليقين القانوني بشأن صحة السجلات الإلكترونية المحتفظ بها. وتوفر الطريقة المستخدمة للأرشفة الإلكترونية ضمانات بشأن سلامة السجلات الإلكترونية المحفوظة في الأرشيف وكذلك تاريخ ووقت الحفظ. وعلاوة على ذلك، ينبغي أن تتوافر إمكانية الاطلاع على المعلومات المحفوظة في الأرشيف وفقاً لشرط التكافؤ الوظيفي مع المفهوم الورقي "للكتابة" (المادة 6 (1) من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية).

159- والمادة 19 مستلهمة من مواد من بينها المادة 10 من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، التي تتناول الاحتفاظ برسائل البيانات. إلا أن المادة 10 من ذلك القانون تشير إلى "الاحتفاظ" برسائل البيانات لأنها تعنى باستيفاء الشرط القانوني الورقي الذي يقضي بالاحتفاظ بالوثائق، في حين أن المادة 19 تشير إلى "الأرشفة" لأنها تتناول وفاء خدمة توفير الثقة المقدَّمة بذلك الشرط (أي الأرشفة الإلكترونية).

160- ولا يلزم أن تكون رسائل البيانات المؤرشفة قد أُرسلَت أو تُلقيت، ويجوز للمنشئ أن يحتفظ بها.

161- وقد يتطلب تناقل رسائل البيانات والاحتفاظ بها، لأسباب فنية، إدخال إضافات وتعديلات على رسالة البيانات لا تغير من سلامتها. ويسمح بهذه الإضافات والتعديلات ما دام محتوى رسالة البيانات يبقى مكتملاً ودون تغيير. وعلى وجه الخصوص، تستوعب الفقرة (أ) '2' نقل الملفات وتغييرات الشكل التي تمثل جزءاً من الممارسات العادية في سياق الاحتفاظ بالبيانات. وتستند صياغتها إلى المادة 8 (3) (أ) من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية.

162- ولا تتناول المادة 19 مسألة ما إذا كان ينبغي أن تكون السجلات الإلكترونية المحفوظة قابلة للنقل بحيث يمكن الوصول إليها على الرغم من التقادم التكنولوجي. وتتحقق تلك النتيجة بتطبيق مبدأ الحياد التكنولوجي واشتراطات التكافؤ الوظيفي على مفهوم "السلامة"، حتى يتسنى، عندما يُشترط تقديم المعلومات، أن تكون تلك المعلومات قابلة للعرض على الشخص الذي يتعين أن تُقدم إليه (المادة 8 (1) (ب) من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية).

*المراجع*

A/CN.9/971، الفقرات 135-138؛ A/CN.9/1005، الفقرات 56-61؛ A/CN.9/1045، الفقرات 37-41.

### 8- المادة 20- خدمات التوصيل المسجَّل الإلكتروني

163- توفر المادة 20 ضمانة لإرسال خطاب إلكتروني بواسطة المرسِل ولتلقي المرسَل إليه له، ولوقت حدوث الإرسال والاستلام، وسلامة البيانات المتبادلة، وهوية المرسل والمتلقي.

164- وخدمات التوصيل المسجل الإلكتروني هي مكافئ خدمات البريد المسجل، حيث إن نوعي الخدمة كليهما يُستخدم لإثبات تناقل الخطابات. ولضمان أمن وخصوصية المراسلات الإلكترونية، ينبغي تحديد هوية المتلقي قبل منحه حق الوصول إلى الخطاب الإلكتروني.

165- ولا تشير المادة 20 إلى مفاهيم مستخدمة في نصوص الأونسيترال السابقة مثل "الإرسال" و"التلقي" (انظر المادة 10 من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية) لأنها صيغت بالتركيز على التكافؤ الوظيفي بين خدمات البريد المسجل وخدمات التوصيل المسجَّل الإلكتروني بدلاً من المفاهيم الكامنة وراءها.

*المراجع*

A/CN.9/971، الفقرات 139-141؛ A/CN.9/1005، الفقرات 62-64؛ A/CN.9/1045، الفقرات 42-44.

### 9- المادة 21- التوثُّق من المواقع الشبكية

166- تتناول المادة 21 التوثُّق من المواقع الشبكية، التي تتمثل وظيفتها الأساسية في ربط الموقع الشبكي بالشخص الذي خُصص أو رُخص له اسم النطاق لإثبات جدارة الموقع الشبكي بالثقة. ومن ثم، يتألف التوثُّق من المواقع الشبكية من عنصرين هما: تحديد هوية حائز اسم النطاق الخاص بالموقع الشبكي، وربط ذلك الشخص بالموقع الشبكي. ولا يهدف التوثُّق من المواقع الشبكية إلى تحديد هوية الموقع الشبكي.

167- والمادة 21 ليست قاعدة للتكافؤ الوظيفي بالنظر إلى أن أي موقع شبكي لا وجود له إلا في شكل إلكتروني، ومن ثم فإن التوثُّق من المواقع الشبكية ليس له مكافئ بدون اتصال عبر الإنترنت.

168- ويشير مصطلح "حائز اسم النطاق" إلى الأشخاص الذين خَصَّصت لهم جهة تسجيل أسماء النطاقات اسم النطاق أو رخصت لهم استخدامه. ولا يلزم أن يكون هذا الشخص "مالك" الموقع الشبكي أو مزود المحتوى أو المشغل الخاص به.

169- وقد يلزم وجود ضمانات إضافية في الحالات التي يُستخدَم فيها اسم نطاق ما لمنصة تستضيف صفحات شبكية ينشئها ويديرها أشخاص مختلفون. فعلى سبيل المثال، قد يحتاج مشغل المنصة إلى تحديد هوية الأشخاص وفقاً لإجراء معين للحفاظ على التوثُّق من الموقع الشبكي.

*المراجع*

A/CN.9/971، الفقرات 142-144؛ A/CN.9/1005، الفقرتان 65 و66؛ A/CN.9/1045، الفقرتان 47 و48.

### 10- المادة 22- اشتراطات تقرير موثوقية خدمات توفير الثقة

170- تتضمن المادة 22 قائمة غير حصرية بالظروف التي قد تكون ذات وجاهة في تقرير موثوقية الطريقة المستخدمة وفقاً لنهج التقرير اللاحق للموثوقية. والقائمة مستوحاة من قوائم واردة في المادة 10 من قانون

الأونسيترال النموذجي بشأن التوقيعات الإلكترونية وفي المادة 12 من قانون الأونسيترال النموذجي بشأن السجلات الإلكترونية القابلة للتحويل.

171- وعلى غرار مفهوم الطريقة الموثوقة المستخدمة لخدمات إدارة الهوية (انظر الفقرة 104 أعلاه)، يعد مفهوم الطريقة الموثوقة المستخدمة في خدمات توفير الثقة مفهوماً نسبياً ويختلف باختلاف الغرض المطلوب أداؤه. ويجسَّد الطابع النسبي للموثوقية في الفقرة 1 (أ)، أي في عبارة "موثوق بها بقدر مناسب"، التي تهدف، وفقاً لاستخدام الأونسيترال الراسخ، إلى تجسيد مختلف استخدامات خدمات توفير الثقة على نحو أفضل، وكذلك في الإشارة إلى "الغرض الذي تستخدم من أجله خدمة توفير الثقة".

*مستويات الموثوقية*

172- يميز قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية وعدد من القوانين الوطنية المتعلقة بالتوقيعات الإلكترونية بين خدمات توفير الثقة على أساس مستوى الموثوقية التي توفرها. وعلى وجه التحديد، ترتب هذه القوانين آثاراً قانونية أكبر على التوقيعات الإلكترونية التي تفي بمتطلبات معينة ومن ثم يُعتبر أنها توفر مستوى أعلى من الموثوقية. وعلاوة على ذلك، قد تقتضي بعض القوانين ألا تعيَّن توقيعات إلكترونية إلا التي توفر مستوى أعلى من الموثوقية. ولم يُتبع هذا النهج في [مشروع الصك] ويمكن تعيين خدمات توفير الثقة بغض النظر عن مستوى الموثوقية التي تقدمها.

173- وبالنظر إلى أن إثباتات الهوية التي توفر مستوى عالياً من الضمان قد تُستخدم من أجل خدمات توفير ثقة ذات مستويات مختلفة من الموثوقية، فإنه لا يوجد ارتباط مباشر بين مستوى ضمان خدمة إدارة الهوية ومستوى موثوقية خدمة توفير الثقة.

*المراجع*

A/CN.9/965، الفقرة 106؛ A/CN.9/971، الفقرتان 120 و121؛ A/CN.9/1005، الفقرات 67 و68 و73؛ A/CN.9/1045، الفقرات 18-21 و27-29 و52-57 و61؛ A/CN.9/1051، الفقرتان 45 و46.

## 11- المادة 23- تعيين خدمات توفير الثقة الموثوقة

174- تكمِّل المادة 23 المادة 22 بإتاحة تعيين خدمات توفير الثقة وفقاً لنهج التقرير المسبق للموثوقية. وبعبارة أدق، فهي تورد الشروط التي يجب أن تستوفيها خدمة إدارة الهوية حتى تُدرَج في قائمة خدمات إدارة الهوية المعيَّنة التي يُفتَرَض أنها موثوقة لأغراض المواد من 16 إلى 21.

175- وتركز المادة 23 على تعيين خدمات توفير الثقة، على أساس أن عملية تعيين خدمات توفير الثقة تنطوي بالضرورة على تقييم لتلك الطرائق. وعلى غرار تعيين خدمات إدارة الهوية، لا يخص تعيين خدمات توفير الثقة التي يُفتَرَض أنها تستخدم طرائق موثوقة الأنواع العامة من خدمات توفير الثقة أو جميع خدمات توفير الثقة التي يقدمها أحد مقدمي خدمات توفير الثقة بعينه، بل إنه يخص خدمة محددة من خدمات توفير الثقة يقدمها مقدِّم خدمات محدد.

176- وبالنظر إلى أن الأثر القانوني الوحيد للتعيين هو افتراض موثوقية الطريقة المستخدمة، فإن استخدام خدمات توفير الثقة التي جرى تعيينها، ولكنها فقدت هذا التعيين، يمنع الطرف المعني من الاستفادة من هذا الافتراض، ولكنه لا يؤثر على تقرير موثوقية الطريقة.

177- وتُلزِم المادة 23 السلطة القائمة بالتعيين بأن تنشر قائمة بخدمات توفير الثقة المعيَّنة، بما في ذلك تفاصيل عن مقدمي تلك الخدمات. والغرض من هذا الالتزام هو تعزيز الشفافية وإعلام المشتركين المحتملين في خدمة توفير الثقة. ولعل الولايات القضائية المشترعة تود النظر في سبل لتجميع تلك القوائم بحيث تتوافر المعلومات للاطلاع عليها في مستودع مركزي يتجاوز حدود الولاية الوطنية، على غرار الأمثلة الإقليمية القائمة.

*المراجع*

A/CN.9/971، الفقرات 150-152؛ A/CN.9/1005، الفقرات 69-73؛ A/CN.9/1045، الفقرات 30-33 و58-61.

### 12- المادة 24- مسؤولية مقدمي خدمات توفير الثقة

178- كمبدأ عام، ينبغي تحميل مقدِّمي خدمات توفير الثقة المسؤولية عن عواقب عدم تقديم الخدمات على النحو المتفق عليه أو على أي نحو آخر يقتضيه القانون. وتتضافر عدة عوامل، من بينها نوع خدمة توفير الثقة المقدَّمة، لتقرير مدى تلك المسؤولية. وفيما يتعلق بالأحكام الأخرى من [مشروع الصك]، فإن المادة 24 لا تؤثر على المسؤولية عن عدم الامتثال للالتزامات الناشئة خارج [مشروع الصك].

179- وفي حالات معينة، قد يكون تحديد مقدم خدمات توفير الثقة صعباً أو مستحيلاً (مثل خدمات أختام الوقت المستخدمة بالاقتران مع تكنولوجيا الدفاتر الموزَّعة)، ومن ثم، قد يتعذر تخصيص المسؤولية. وفي هذه الحالات، يمكن للنظام أن يوفر سبلاً أخرى لإرساء الثقة في استخدام خدمة توفير الثقة.

180- وفيما يتعلق بنصوص الأونسيترال السابقة، يتضمن قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية أحكاماً تتناول العواقب القانونية الناشئة عن سلوك الموقّع (المادة 8) ومقدِّم خدمة التصديق (المادة 9) والطرف المعوِّل (المادة 11). وتحدِّد هذه الأحكام التزامات كل كيان يشارك في دورة حياة التوقيع الإلكتروني. وعلاوة على ذلك، يسلِّم قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية بإمكانية أن يحد مقدمو خدمات التصديق من نطاق أو مدى مسؤوليتهم.

*المراجع*

A/CN.9/1005، الفقرات 74-76؛ A/CN.9/1045، الفقرات 62-66.

## دال- الفصل الرابع- الجوانب الدولية (المادتان 25 و26)

### 1- المادة 25- الاعتراف القانوني عبر الحدود

181- تنص المادة 25 على نظام للاعتراف القانوني عبر الحدود بإدارة الهوية وخدمات توفير الثقة يقوم على المعاملة القانونية المتماثلة لنظم إدارة الهوية وإثباتات الهوية وخدمات إدارة الهوية وخدمات توفير الثقة، المحلية والأجنبية. وهو يقوم على مبدأ عدم التمييز ضد المنشأ الجغرافي.

182- ويتمثل أحد أهداف المادة 25 في الحد من حاجة مقدمي الخدمات إلى تقديم طلب لاقتناء صفة الخدمات المعيَّنة في ولايات قضائية متعددة بموجب المادة 23. وقد يكون ذلك مفيداً بشكل خاص في الولايات القضائية التي تعتمد على استخدام معايير تقنية وطنية قد لا تكون، في حد ذاتها، مطابقة للمعايير التقنية الأجنبية. وقد يكون للاعتراف المتبادل بالتصديق، حيثما يكون متاحاً، دور هام في تنفيذ هذا الحكم.

183- وتشمل الإشارة إلى "مستوى الموثوقية" في المادة 25 مفهوم مستوى الضمان، وهو مصطلح فني لتقييم خدمات إدارة الهوية، ومفهوم مستوى الموثوقية، وهو مصطلح فني لتقييم خدمات توفير الثقة. وقد يكون هذان المفهومان بدورهما مهمين لتقرير موثوقية خدمة ما أو لتعيين خدمة موثوقة وفقاً للفصلين الثاني والثالث.

184- ولا يضع [مشروع الصك] مجموعة مشتركة من مستويات ضمان نظم إدارة الهوية ومستويات موثوقية خدمات توفير الثقة بسبب التحديات التي تعترض الاتفاق على تعاريف مقبولة عالمياً. وعلاوة على ذلك، توجد قوانين وممارسات تجارية مختلفة في وضع تلك التعاريف عبر الولايات القضائية، ولا سيما فيما يتعلق بدور السلطات المركزية إزاء دور الاتفاقات التعاقدية.

185- ومن ناحية أخرى، فإن تحديد مستوى ضمان خدمة إدارة الهوية ومستوى موثوقية خدمة توفير الثقة عملية تستغرق وقتاً طويلاً وتستهلك موارد كثيفة، وقد لا تتوافر لدى جميع الولايات القضائية موارد كافية. وقد تستفيد تلك الولايات القضائية بشكل خاص من إمكانية الاعتراف بخدمات إدارة الهوية وتوفير الثقة الأجنبية بالاعتماد على عمليات تقرير الموثوقية والتعيينات الأجنبية.

186- وتهدف الإشارة إلى "نظم إدارة الهوية أو خدمات إدارة الهوية أو إثباتات الهوية، حسب الاقتضاء"، إلى شمول جميع الجوانب الممكنة ذات الصلة بالاعتراف عبر الحدود. ومن الناحية العملية، قد يكون من الأفضل التركيز على كل خدمة من خدمات إدارة الهوية على حدة لتجنب الاعتراف بأن جميع خدمات إدارة الهوية التي يدعمها نظام لإدارة الهوية موثوقة بنفس القدر، وإن وجد احتمال بأن تكون واحدة أو أكثر ذات مستوى أقل من الموثوقية. وإضافة إلى ذلك، ينبغي للاعتراف بإثباتات الهوية أن يتجنب إثباتات إدارة الهوية التي بقيت دون تغيير على الرغم من وقوع تلاعب في خدمة إدارة الهوية المستخدمة لإصدارها.

187- وقد يقتضي الاعتراف بخدمات إدارة الهوية وتوفير الثقة الأجنبية من مقدم الخدمة أن يعدِّل شروط خدماته. فعلى سبيل المثال، قد يؤثر القانون الإلزامي للولاية القضائية المعترفة على قدرة مقدم الخدمة على الحد من المسؤولية.

188- وتقدم الفقرة 1 بديلين بشأن تكافؤ المستوى المطلوب من الموثوقية. ويشترط الأول مستوى مكافئاً على الأقل من الموثوقية؛ ويشترط الثاني أن توفر مستوى مكافئاً جوهرياً من الموثوقية. وتشمل الإشارة إلى "مستوى مكافئ على الأقل من الموثوقية" مستويات من الموثوقية أعلى من المستوى المطلوب.

189- ويهدف مفهوم "مستوى موثوقية مكافئ جوهرياً" إلى استيعاب الحالات التي لا يوجد فيها اتساق تام بين الولايات القضائية المختلفة بشأن تعريف مستوى الموثوقية، وهو وضع محتمل نظراً لعدم وجود تعاريف متفق عليها عالمياً لمستويات محددة من الموثوقية. وثمة شاغل آخر قد يعالجه هذا المفهوم يتعلق بالعقبات المحتملة في سبيل التجارة التي تنشأ عن الإلزام بالامتثال لاشتراطات تقنية صارمة.

190- وإذا كانت النظم أو الخدمات أو إثباتات الهوية توفر مستوى مكافئاً جوهرياً من الموثوقية، فإن موثوقيتها التي تتقرر بتطبيق الظروف الواردة في المادتين 10 و22 ستكون مكافئة هي الأخرى. وتشمل عبارة "مستوى مكافئ على الأقل من الموثوقية" مستويات من الموثوقية أعلى من المستوى المطلوب. ومفهوم "مستوى موثوقية مكافئ جوهرياً" مستمد من المادة 12 (2) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية.

191- وتوضح الفقرة 3 كذلك كيف يمكن لسلطات التعيين أن تعيِّن خدمات إدارة الهوية وتوفير الثقة الأجنبية. وهي تتوسع في تبيان الآليات المنصوص عليها في المادتين 11 (4) و23 (4)، اللتين تنصان على عدم التمييز الجغرافي في عملية التعيين، وذلك باستحداث إمكانية تعويل سلطة التعيين التابعة للولاية القضائية المشترعة على التعيين الذي تقوم به سلطة تعيين أجنبية لخدمات إدارة الهوية وتوفير الثقة.

192- ويمكن للولاية القضائية المشترعة، عند اعتماد اللوائح التنفيذية، أن تقرر ما إذا كان ينبغي تطبيق الفقرة 3 في شكل اعتراف تلقائي (على سبيل المثال، أن تحظى تلقائياً خدمات إدارة الهوية وتوفير الثقة التي تعينها السلطة الأجنبية بمركز قانوني بوصفها خدمات معيَّنة في الولاية المشترعة)، أو في شكل افتراض (على سبيل المثال، أن تُفترض في الولاية القضائية المشترعة موثوقية خدمات إدارة الهوية وتوفير الثقة التي تعينها السلطة الأجنبية، ولكن لا يكون لها مركز قانوني بوصفها خدمات معيَّنة في تلك الولاية القضائية دون أن تتخذ سلطة التعيين إجراءات أخرى في هذا الصدد).

193- ويمكن للآليات القائمة على المادة 25 (3) أن تحل محل الترتيبات القائمة على إبرام اتفاقات مخصصة للاعتراف المتبادل بين الهيئات الإشرافية.

*المراجع*

A/CN.9/936، الفقرات 75-77؛ A/CN.9/1005، الفقرة 120؛ A/CN.9/1045، الفقرات 67-74؛ A/CN.9/1051، الفقرات 57-66.

### 2- المادة 26- التعاون

194- قد تسهم آليات التعاون المؤسسي مساهمة كبيرة في تحقيق الاعتراف القانوني المتبادل وإمكانية التشغيل التقني المتبادل لنظم إدارة الهوية وخدمات توفير الثقة. وتوجد هذه الآليات بأشكال مختلفة وقد تكون ذات طابع خاص أو عام. وقد يتمثل التعاون في تبادل المعلومات والخبرات والممارسات الجيدة، وبخاصة فيما يتعلق بالاشتراطات الفنية، بما في ذلك مستويات الضمان ومستويات الموثوقية.

195- وعلاوة على ذلك، قد تيسر المادة 26 وضع تعاريف مشتركة للمعايير التقنية، بما في ذلك مستويات الضمان ومستويات الموثوقية، لدعم تقرير التكافؤ.

*المراجع*

A/CN.9/965، الفقرتان 119 و120؛ A/CN.9/1005، الفقرة 122؛ A/CN.9/1045، الفقرة 75؛ A/CN.9/WG.IV/WP.153، الفقرات 95-98.