

Distr.: General  
21 February 2022  
Arabic  
Original: English



## 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

#### مذكرة من الأمانة

- 1- اختتم الفريق العامل الرابع (التجارة الإلكترونية) في دورته الثانية والستين (فيينا، 22-26 تشرين الثاني/نوفمبر 2021)، قراءته الثالثة لمشروع الأحكام بشأن استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود والمذكرة التفسيرية المتعلقة بها.
- 2- وفي تلك الدورة، طلب الفريق العامل إلى الأمانة أن تتفح مشاريع الأحكام والمذكرة التفسيرية لكي تجسد مداولاته وقراراته وأن تحيل النص المنقح إلى اللجنة، في شكل قانون نموذجي، من أجل النظر فيه في دورتها الخامسة والخمسين، في عام 2022. وطلب إلى الأمانة أيضاً تعميم النص المنقح على جميع الحكومات والمنظمات الدولية ذات الصلة من أجل التعليق عليه، وتجميع التعليقات الواردة لكي تنظر فيها اللجنة (A/CN.9/1087، الفقرة 11).
- 3- ويرد النموذج المنقح في المرفق الأول لهذه الوثيقة وترد المذكرة التفسيرية المنقحة في المرفق الثاني لهذه الوثيقة. وتدمج التقيحات مداولات الفريق العامل في دورته الثانية والستين حسبما وردت في الوثيقة A/CN.9/1087.



## المرفق الأول

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

## الفصل الأول - أحكام عامة

## المادة 1- التعاريف

لأغراض هذا القانون:

- (أ) "النعته" هو بند معلومات أو بيانات مقترن بشخص ما؛
- (ب) "رسالة البيانات" هي معلومات يتم توليدها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو مغناطيسية أو بصرية أو ما شابهها؛
- (ج) "تحديد الهوية إلكترونياً" ["التوثيق"]، في سياق خدمات إدارة الهوية، هو عملية تُستخدم لتوفير قدر كافٍ من الضمان في الربط بين الشخص والهوية؛
- (د) "الهوية" هي مجموعة من النعوت التي تتيح تمييز شخص بشكل متفرد ضمن سياق معين؛
- (هـ) "إثباتات الهوية" هي البيانات، أو الأشياء المادية التي قد توجد عليها البيانات، التي يمكن أن يقدمها شخص لتحديد هويته إلكترونياً؛
- (و) "خدمات إدارة الهوية" تعني خدمات لإدارة عمليات تدقيق الهوية أو التحديد الإلكتروني لها؛
- (ز) "مقدم خدمات إدارة الهوية" هو شخص يدخل في ترتيب لتقديم خدمات إدارة الهوية مع مشترك؛
- (ح) "نظام إدارة الهوية" هو مجموعة من الوظائف والقدرات اللازمة لإدارة عمليات تدقيق الهوية أو تحديدها إلكترونياً؛
- (ط) "تدقيق الهوية" هو عملية جمع ما يكفي من نعوت لتحديد وتأكيد هوية شخص ما في سياق معين والتحقق والتثبت من صحة تلك النعوت؛
- (ي) "الطرف المعوّل" هو شخص يتصرّف استناداً إلى النتيجة المترتبة على خدمات إدارة الهوية أو خدمات توفير الثقة؛
- (ك) "المشترك" هو الشخص الذي يدخل في ترتيب لتقديم خدمات إدارة الهوية أو خدمات توفير الثقة مع أحد مقدمي خدمات إدارة الهوية أو مقدمي خدمات توفير الثقة؛
- (ل) "خدمة توفير الثقة" هي خدمة إلكترونية تقدم ضماناً لبعض سمات رسالة البيانات وتشمل طرائق ووسائل إنشاء وإدارة التوقيعات الإلكترونية والأختام الإلكترونية وأختام الوقت الإلكترونية والتوثيق من المواقع الشبكية والأرشفة الإلكترونية وخدمات التوصيل المسجل الإلكتروني؛
- (م) "مقدم خدمات توفير الثقة" هو شخص يدخل في ترتيب لتقديم خدمة أو أكثر من خدمات توفير الثقة مع مشترك.

### المادة 2- نطاق الانطباق

- 1- ينطبق هذا القانون على استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود في سياق الأنشطة التجارية والخدمات ذات الصلة بالتبادل التجاري.
- 2- ليس في هذا القانون اشتراط يقضي بأن تحدّد هوية شخص ما.
- 3- ليس في هذا القانون ما يمس بأي اشتراط قانوني يقضي بأن تحدّد هوية شخص ما أو بأن تُستخدم إحدى خدمات توفير الثقة وفقاً لإجراء يحدده القانون أو ينص عليه.
- 4- فيما عدا ما هو منصوص عليه في هذا القانون، ليس في هذا القانون ما يمس بأن ينطبق على خدمات إدارة الهوية أو خدمات توفير الثقة أي قانون منطبق على حماية البيانات وخصوصيتها.

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

- 1- ليس في هذا القانون ما يلزم أي شخص باستخدام خدمة لإدارة الهوية أو خدمة لتوفير الثقة أو باستخدام خدمة محددة من خدمات إدارة الهوية أو من خدمات توفير الثقة دون موافقته.
- 2- لأغراض الفقرة 1، يمكن الاستدلال على الموافقة من خلال مسلك الشخص.

### المادة 4- التفسير

- 1- يراعى في تفسير هذا القانون مصدره الدولي وضرورة العمل على تطبيقه بشكل موحد والتزام حسن النية في التجارة الدولية.
- 2- المسائل المتعلقة بالأمر التي يحكمها هذا القانون ولا تسويها أحكامه صراحة تسوى وفقاً للمبادئ العامة التي يقوم عليها هذا القانون.

## الفصل الثاني- إدارة الهوية

### المادة 5- الاعتراف القانوني بإدارة الهوية

مع مراعاة الفقرة 3 من المادة 2، لا يجوز عدم منح التحديد الإلكتروني للهوية أثراً قانونياً أو نفي صحته أو وجوب نفاذه أو مقبوليته كدليل إثبات لمجرد ما يلي:

- (أ) أن تدقيق الهوية وتحديد الهوية إلكترونياً حدثاً في شكل إلكتروني؛ أو
- (ب) أن نظام إدارة الهوية ليس من النظم المعيّنة عملاً بالمادة 11.

### المادة 6- التزامات مقدمي خدمات إدارة الهوية

يتعين على مقدم خدمات إدارة الهوية القيام بما يلي، كحد أدنى:

- (أ) وضع قواعد وسياسات وممارسات تشغيلية مناسبة للغرض من نظام إدارة الهوية وتصميمه، بغية استيفاء الاشتراطات التالية، كحد أدنى:

'1' قيد الأشخاص بوسائل منها ما يلي:

أ- تسجيل النعوت وجمعها؛

- ب- تدقيق الهوية والتحقق منها؛
- ج- ربط إثباتات الهوية بالشخص؛
- 2' تحديث النعوت؛
- 3' إدارة إثباتات الهوية، بوسائل منها ما يلي:
- أ- إصدار الإثباتات وتسليمها وتفعيلها؛
- ب- تعليق الإثباتات وإلغاؤها وإعادة تفعيلها؛
- ج- تجديد الإثباتات وتبديلها؛
- 4' إدارة آليات التحديد الإلكتروني لهوية الأشخاص، بوسائل منها ما يلي:
- أ- إدارة عوامل تحديد الهوية إلكترونياً؛
- ب- إدارة آليات تحديد الهوية إلكترونياً؛
- (ب) التصرف وفقاً لقواعده وسياساته وممارساته التشغيلية ووفقاً لأي تأكيدات يقدمها بخصوصها؛
- (ج) ضمان إتاحة نظام إدارة الهوية بالاتصال الحاسوبي المباشر وتشغيله تشغيلاً صحيحاً؛
- (د) تسهيل اطلاع المشتركين والأطراف الثالثة على قواعده وسياساته وممارساته التشغيلية؛
- (هـ) توفير وسائل يكون الوصول إليها متيسراً بسهولة وتمكّن الطرف المعول من التأكد، عند الاقتضاء، مما يلي:
- 1' وجود أي قيد على الغرض أو القيمة التي يجوز أن تستخدم من أجلها خدمة إدارة الهوية؛
- 2' وجود أي قيد على نطاق أو مدى المسؤولية التي شرطها مقدم خدمات إدارة الهوية؛
- (و) توفير الوسائل التي يجوز أن يستخدمها المشترك لإبلاغ مقدم خدمات إدارة الهوية عن أي خرق أمني عملاً بالمادة 8، وإتاحتها للجمهور.

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

- 1- في حال وقوع خرق أمني لنظام إدارة الهوية أو مساس بسلامته من شأنه أن يؤثر تأثيراً كبيراً عليه، بما في ذلك النعوت المدارة داخله، يلتزم مقدم خدمات إدارة الهوية بما يلي، وفقاً للقانون:
- (أ) اتخاذ جميع التدابير المعقولة لاحتواء خرق النظام أو المساس بسلامته، بما في ذلك، عند الاقتضاء، تعليق الخدمة المتأثرة أو إلغاؤها أو إلغاء إثباتات الهوية المتأثرة؛
- (ب) معالجة خرق النظام أو المساس بسلامته؛
- (ج) الإبلاغ عن خرق النظام أو المساس بسلامته.
- 2- في حال أبلغ شخص مقدم خدمات إدارة الهوية بوقوع خرق أمني للنظام أو مساس بسلامته، يلتزم مقدم خدمات إدارة الهوية بما يلي:
- (أ) التحقيق في احتمال خرق النظام أو المساس بسلامته؛
- (ب) اتخاذ أي إجراء آخر مناسب بموجب الفقرة 1.

المادة 8- التزامات المشتركين

على المشترك أن يبلغ مقدم خدمات إدارة الهوية باستخدام الوسائل التي يتيحها مقدم خدمات إدارة الهوية عملاً بالمادة 6، أو باستخدام وسائل معقولة أخرى، في إحدى الحالتين التاليتين:

- (أ) إذا علم المشترك بوقوع تلاعب بإثباتات الهوية الخاصة به؛ أو  
 (ب) إذا كانت الملابس المعلوماتية للمشارك توحى بقوة باحتمال وقوع تلاعب بإثباتات الهوية الخاصة به.

المادة 9- تحديد هوية شخص باستخدام إدارة الهوية

رهنأً 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 لتحديد هوية الشخص إلكترونياً لذلك الغرض.

المادة 10- اشتراطات تقرير موثوقية خدمات إدارة الهوية

- 1- لأغراض المادة 9، تكون الطريقة كما يلي:
- (أ) موثقاً بها بقدر مناسب للغرض الذي تُستخدم من أجله خدمة إدارة الهوية؛ أو  
 (ب) أثبتت فعلياً أنها أدت الوظيفة المبيّنة في المادة 9.
- 2- لدى تقرير موثوقية الطريقة، تؤخذ في الاعتبار جميع الظروف ذات الصلة، بما قد يشمل ما يلي:
- (أ) امتثال مقدم خدمات إدارة الهوية للالتزامات الواردة في المادة 6؛  
 (ب) امتثال القواعد والسياسات والممارسات التشغيلية الخاصة بمقدم خدمات إدارة الهوية لأي معايير وإجراءات دولية منطبقة معترف بها ذات صلة بتقديم خدمات إدارة الثقة، بما في ذلك أطر مستوى الضمان، ولا سيما القواعد المتعلقة بما يلي:

- 1' الحوكمة؛  
 2' نشر الإشعارات ومعلومات المستخدمين؛  
 3' إدارة أمن المعلومات؛  
 4' حفظ السجلات؛  
 5' المرافق والموظفين؛  
 6' الضوابط التقنية؛  
 7' الإشراف والتدقيق؛  
 (ج) أي إجراءات للإشراف أو التصديق على نظم إدارة الهوية؛  
 (د) أي مستوى ذي صلة من موثوقية الطريقة المستخدمة؛  
 (هـ) الغرض من استخدام تحديد الهوية؛

- (و) أي اتفاق ذي صلة بين الطرفين، بما في ذلك أي قيود على غرض المعاملات التي يمكن استخدام خدمة إدارة الهوية من أجلها أو قيمة تلك المعاملات.
- 3- لدى تقرير موثوقية الطريقة، لا يعتد بما يلي:
- (أ) الموقع الجغرافي لمكان تقديم خدمات إدارة الهوية؛ أو
- (ب) الموقع الجغرافي لمكان عمل مقدم خدمات إدارة الهوية.
- 4- أي طريقة تستخدمها خدمة إدارة هوية معيّنة عملاً بالمادة 11 يُفترض أنها طريقة موثوقة.
- 5- لا تحد الفقرة 4 من قدرة أي شخص على القيام بأي مما يلي:
- (أ) إثبات موثوقية الطريقة بأية وسيلة أخرى؛ أو
- (ب) التبدل على عدم موثوقية أي من الطرائق التي تستخدمها خدمة من خدمات توفير الثقة المعيّنة عملاً بالمادة 11.

#### المادة 11- تعيين خدمات إدارة الهوية الموثوقة

- 1- [الجهات، من الأفراد أو الأجهزة أو السلطات، سواء أكانت جهات عامة أم خاصة، التي تقضي الولاية القضائية المشتركة بأنها مختصة،] أن تعين خدمات إدارة الهوية التي يُفترض أنها موثوقة.
- 2- على [الجهات، من الأفراد أو الأجهزة أو السلطات، سواء أكانت جهات عامة أم خاصة، التي تقضي الولاية القضائية المشتركة بأنها مختصة،] القيام بما يلي:
- (أ) مراعاة جميع الظروف ذات الصلة، ومنها العوامل المشار إليها في المادة 10، عند تعيين خدمات إدارة الهوية؛
- (ب) نشر قائمة بخدمات إدارة الهوية المعيّنة، بما في ذلك تفاصيل عن مقدمي تلك الخدمات.
- 3- يراعى في أي تعيين يُجرى عملاً بالفقرة 1 الانتساق مع المعايير والإجراءات الدولية المعترف بها ذات الصلة بتنفيذ عملية التعيين، بما في ذلك أطر مستوى الضمان.
- 4- لدى تعيين خدمات إدارة الهوية، لا يعتد بما يلي:
- (أ) الموقع الجغرافي لمكان تقديم خدمات إدارة الهوية؛ أو
- (ب) الموقع الجغرافي لمكان عمل مقدم خدمات إدارة الهوية.

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

- 1- يكون مقدّم خدمات إدارة الهوية مسؤولاً عما يتسبب فيه من خسارة للمشارك أو للطرف المعول نتيجة عدم الوفاء بالتزاماته بموجب المادتين 6 و7.
- 2- تطبّق الفقرة 1 وفقاً لقواعد المسؤولية المحددة بموجب القانون، مع عدم المساس بما يلي:
- (أ) أي أساس آخر للمسؤولية بموجب القانون، بما في ذلك المسؤولية عن عدم الامتثال للالتزامات التعاقدية؛ أو
- (ب) أي عواقب قانونية أخرى لعدم امتثال مقدم خدمات إدارة الهوية لالتزاماته بموجب هذا القانون.

- 3- بصرف النظر عن الفقرة 1، لا يكون مقدم خدمات إدارة الهوية مسؤولاً تجاه المشترك عن الخسارة الناجمة عن استخدام خدمة إدارة الهوية في الحالتين التاليتين:
- (أ) أن يكون ذلك الاستخدام قد تجاوز القيود المفروضة على غرض المعاملة التي تُستخدم من أجلها خدمة إدارة الهوية أو قيمة تلك المعاملات؛
- (ب) أن ترد تلك القيود في الترتيب المبرم بين مقدم خدمات إدارة الهوية والمستخدم.
- 4- بصرف النظر عن الفقرة 1، لا يكون مقدم خدمات إدارة الهوية مسؤولاً تجاه الطرف المعول عن الخسارة الناجمة عن استخدام خدمة إدارة الهوية في الحالتين التاليتين:
- (أ) أن يكون ذلك الاستخدام قد تجاوز القيود المفروضة على غرض المعاملة التي تُستخدم من أجلها خدمة إدارة الهوية أو قيمة تلك المعاملات؛
- (ب) أن يكون مقدم خدمات إدارة الهوية قد امتثل لالتزاماته بموجب الفقرة الفرعية (هـ) من المادة 6 فيما يتعلق بتلك المعاملة.

### الفصل الثالث - خدمات توفير الثقة

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

- لا يجوز عدم منح النتيجة المترتبة على استخدام خدمة توفير الثقة أثراً قانونياً أو نفي صحتها أو وجوب نفاذها أو مقبوليتها كدليل إثبات لمجرد ما يلي:
- (أ) أنها في شكل إلكتروني؛ أو
- (ب) أن خدمة توفير الثقة ليست من الخدمات المعيّنة عملاً بالمادة 23.

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

- 1- يلتزم مقدم خدمات توفير الثقة بما يلي، كحد أدنى:
- (أ) وضع قواعد وسياسات وممارسات تشغيلية، بما في ذلك خطة لضمان الاستمرارية في حالة إنهاء النشاط، مناسبة للغرض من خدمة توفير الثقة وتصميمها؛
- (ب) التصرف وفقاً لقواعده وسياساته وممارساته التشغيلية ووفقاً لأي تأكيدات يقدمها بخصوصها؛
- (ج) تسهيل اطلاع المشتركين والأطراف الثالثة على قواعده وسياساته وممارساته التشغيلية؛
- (د) توفير الوسائل التي يجوز أن يستخدمها المشترك لإبلاغ مقدم خدمات توفير الثقة عن أي خرق أمني عملاً بالمادة 15، وإتاحتها للجمهور؛
- (هـ) توفير وسائل يكون الوصول إليها متيسراً وتمكّن الطرف المعول من التأكد، عند الاقتضاء، مما يلي:

'1' وجود أي قيد على الغرض أو القيمة التي يجوز أن تستخدم من أجلها خدمة توفير الثقة؛

'2' وجود أي قيد على نطاق أو مدى المسؤولية التي شرطها مقدم خدمات توفير الثقة.

2- في حال وقوع خرق أمني لخدمة توفير الثقة أو مساس بسلامتها من شأنه أن يؤثر تأثيراً كبيراً عليها، يلتزم مقدم خدمات توفير الثقة بما يلي وفقاً للقانون:

- (أ) اتخاذ جميع التدابير المعقولة لاحتواء خرق الخدمة أو المساس بسلامتها، بما في ذلك، عند الاقتضاء، تعليق الخدمة المتأثرة أو إلغاؤها؛
- (ب) معالجة خرق النظام أو المساس بسلامته؛
- (ج) الإبلاغ عن خرق النظام أو المساس بسلامته.

#### المادة 15- التزامات المشتركين

على المشترك أن يبلغ مقدم خدمات توفير الثقة باستخدام الوسائل التي يتيحها مقدم خدمات توفير الثقة عملاً بالفقرة 1 من المادة 14، أو باستخدام وسائل معقولة أخرى، في إحدى الحالتين التاليتين:

- (أ) أن يعلم المشترك بوقوع تلاعب بالبيانات أو الوسائل التي يستخدمها المشترك من أجل الوصول إلى خدمة توفير الثقة واستخدامها؛ أو
- (ب) إذا كانت الملايسات المعلومة للمشارك توحى بقوة باحتمال وقوع ذلك التلاعب بخدمة توفير الثقة.

#### 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 من أجل ما يلي:

- (أ) تحديد هوية الشخص؛
- (ب) بيان نية الشخص فيما يتعلق بالمعلومات الواردة في رسالة البيانات.

#### المادة 17- الأختام الإلكترونية

حيثما يشترط القانون على شخص اعتباري وضع ختم، أو ينص على عواقب لعدم وجود ختم، يستوفى ذلك الاشتراط فيما يخص رسالة البيانات إذا استُخدمت طريقة من أجل ما يلي:

- (أ) توفير ضمانات للتأكد من منشأ رسالة البيانات؛
- (ب) اكتشاف أي تغيير في رسالة البيانات بعد وقت وتاريخ وضع الختم، بخلاف إضافة أي مصادقة وأي تغيير يطرأ في السياق المعتاد للإرسال والتخزين والعرض.

#### 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 من أجل ما يلي:

- (أ) بيان الوقت والتاريخ بوسائل منها الإشارة إلى منطقة التوقيت؛
- (ب) ربط ذلك الوقت والتاريخ برسالة البيانات.



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 من أجل ما يلي:

- (أ) تيسر الوصول إلى المعلومات الواردة في رسالة البيانات على نحو يتيح استخدامها لاحقاً؛
- (ب) بيان وقت وتاريخ الأرشفة وربط ذلك الوقت والتاريخ برسالة البيانات؛
- (ج) الاحتفاظ برسالة البيانات بالشكل الذي تم به توليدها أو إرسالها أو استلامها أو بأي شكل آخر يمكنه كشف أي تغيير في رسالة البيانات بعد ذلك الوقت والتاريخ، بخلاف إضافة أي مصادقة أو تغيير يطرأ في السياق المعتاد للإرسال والتخزين والعرض؛
- (د) الاحتفاظ بهذه المعلومات، إن وجدت، على نحو يتيح تحديد منشأ رسالة البيانات ووجهتها ووقت وتاريخ إرسالها أو استلامها.

المادة 20- خدمات التوصيل المسجل الإلكتروني

حيثما يشترط القانون توصيل وثائق أو سجلات أو معلومات بالبريد المسجل أو بخدمة مشابهة، أو ينص على عواقب لعدم توصيلها، يستوفى ذلك الاشتراط فيما يخص رسالة البيانات إذا استُخدمت طريقة من أجل ما يلي:

- (أ) بيان وقت وتاريخ استلام رسالة البيانات بغرض توصيلها، وبيان وقت وتاريخ توصيل رسالة البيانات؛
- (ب) اكتشاف أي تغيير في رسالة البيانات بعد وقت وتاريخ استلام رسالة البيانات بغرض توصيلها حتى وقت وتاريخ توصيلها، بخلاف إضافة أي مصادقة أو معلومات تقتضيها هذه المادة، وأي تغيير يطرأ في السياق المعتاد للإرسال والتخزين والعرض؛
- (ج) تحديد هوية المرسل والمستلم.

المادة 21- التوثيق من المواقع الشبكية

حيثما يشترط القانون التوثيق من المواقع الشبكية، أو ينص على عواقب لعدم التوثيق من المواقع الشبكية، يستوفى ذلك الاشتراط إذا استُخدمت طريقة من أجل ما يلي:

- (أ) تحديد هوية حائز اسم النطاق الخاص بالموقع الشبكي؛
- (ب) ربط ذلك الشخص بالموقع الشبكي.

المادة 22- اشتراطات تقرير موثوقية خدمات توفير الثقة

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

- (أ) موثقاً بها بقدر مناسب للغرض الذي تُستخدم من أجله خدمة توفير الثقة؛ أو
- (ب) أثبتت فعلياً أنها أدت الوظائف المبينة في المادة.

2- لدى تقرير موثوقية الطريقة، تؤخذ في الاعتبار جميع الظروف ذات الصلة، بما قد يشمل ما يلي:

- (أ) امتثال مقدم خدمات توفير الثقة للالتزامات الواردة في المادة 14؛
- (ب) امتثال القواعد والسياسات والممارسات التشغيلية الخاصة بمقدم خدمات توفير الثقة لأي معايير وإجراءات دولية منطبقة معترف بها ذات صلة بتقديم خدمات توفير الثقة؛
- (ج) أي مستوى ذي صلة من موثوقية الطريقة المستخدمة؛
- (د) أي معيار منطبق في القطاع المعني؛
- (هـ) أمن المعدات والبرمجيات؛
- (و) الموارد المالية والبشرية، بما في ذلك توافر الموجودات؛
- (ز) انتظام ونطاق عمليات المراجعة التي تتولاها هيئات مستقلة؛
- (ح) وجود إقرار من جهة الإشراف أو الاعتماد أو آلية طوعية بموثوقية الطريقة؛
- (ط) الغرض من استخدام خدمة توفير الثقة؛
- (ي) أي اتفاق ذي صلة بين الطرفين، بما في ذلك أي قيود على غرض المعاملات التي يمكن استخدام خدمة توفير الثقة من أجلها أو قيمة تلك المعاملات.

3- لدى تقرير موثوقية الطريقة، لا يعتد بما يلي:

- (أ) الموقع الجغرافي لمكان تقديم خدمة توفير الثقة؛ أو
- (ب) الموقع الجغرافي لمكان عمل مقدم خدمات توفير الثقة.
- 4- أي طريقة تستخدمها خدمة من خدمات توفير الثقة المعيّنة عملاً بالمادة 23 يُفترض أنها طريقة موثوقة.
- 5- لا تحد الفقرة 4 من قدرة أي شخص على القيام بأي مما يلي:
- (أ) إثبات موثوقية الطريقة بأية وسيلة أخرى؛ أو
- (ب) التدليل على عدم موثوقية أي من الطرائق التي تستخدمها خدمة من خدمات توفير الثقة المعيّنة عملاً بالمادة 23.

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

- 1- [الجهات، من الأفراد أو الأجهزة أو السلطات، سواء أكانت جهات عامة أم خاصة، التي تقضي الولاية القضائية المشتترعة بأنها مختصة،] أن تعين خدمات توفير الثقة التي يُفترض أنها موثوقة.
- 2- على [الجهات، من الأفراد أو الأجهزة أو السلطات، سواء أكانت جهات عامة أم خاصة، التي تقضي الولاية القضائية المشتترعة بأنها مختصة،] القيام بما يلي:
- (أ) مراعاة جميع الظروف ذات الصلة، ومنها العوامل الواردة في المادة 22، لدى تعيين خدمات توفير الثقة؛
- (ب) نشر قائمة بخدمات توفير الثقة المعيّنة، بما في ذلك تفاصيل عن مقدمي تلك الخدمات.
- 3- يراعى في أي تعيين يُجرى عملاً بالفقرة 1 الاتساق مع المعايير والإجراءات الدولية المعترف بها ذات الصلة بتنفيذ عملية التعيين.
- 4- لدى تعيين خدمة توفير الثقة، لا يُعتمد بما يلي:

(أ) الموقع الجغرافي لمكان تقديم خدمة توفير الثقة؛ أو

(ب) الموقع الجغرافي لمكان عمل مقدم خدمات توفير الثقة.

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

1- يكون مقدم خدمات توفير الثقة مسؤولاً عما يتسبب فيه من خسارة للمشارك أو للطرف المعول نتيجة عدم الوفاء بالتزاماته بموجب المادة 14.

2- تطبق الفقرة 1 وفقاً لقواعد المسؤولية المحددة بموجب القانون، مع عدم المساس بما يلي:

(أ) أي أساس آخر للمسؤولية بموجب القانون، بما في ذلك المسؤولية عن عدم الامتثال للالتزامات التعاقدية؛ أو

(ب) أي عواقب قانونية أخرى لعدم امتثال مقدم خدمات توفير الثقة لالتزاماته بموجب هذا القانون.

3- بصرف النظر عن الفقرة 1، لا يكون مقدم خدمات توفير الثقة مسؤولاً تجاه المشارك عن الخسارة الناجمة عن استخدام خدمة توفير الثقة في الحالتين التاليتين:

(أ) أن يكون ذلك الاستخدام قد تجاوز القيود المفروضة على غرض المعاملة التي تُستخدم من أجلها خدمة توفير الثقة أو قيمة تلك المعاملات؛

(ب) أن ترد تلك القيود في الترتيب المبرم بين مقدم خدمات توفير الثقة والمشارك.

4- بصرف النظر عن الفقرة 1، لا يكون مقدم خدمات توفير الثقة مسؤولاً تجاه الطرف المعول عن الخسارة الناجمة عن استخدام خدمة توفير الثقة في الحالتين التاليتين:

(أ) أن يكون ذلك الاستخدام قد تجاوز القيود المفروضة على غرض المعاملة التي تُستخدم من أجلها خدمة توفير الثقة أو قيمة تلك المعاملات؛

(ب) أن يكون مقدم خدمات توفير الثقة قد امتثل لالتزاماته بموجب الفقرة الفرعية (هـ) من المادة 14 فيما يتعلق بتلك المعاملة.

### الفصل الرابع - الجوانب الدولية

#### المادة 25- الاعتراف عبر الحدود بتحديد الهوية إلكترونياً

1- يكون لتحديد الهوية إلكترونياً الذي يُجرى خارج [الولاية القضائية المشتري] نفس الأثر القانوني في [الولاية القضائية المشتري] مثله مثل تحديد الهوية إلكترونياً الذي يُجرى داخل [الولاية القضائية المشتري] إذا كانت الطريقة التي يستخدمها نظام إدارة الهوية أو خدمة إدارة الهوية أو إثبات الهوية، حسب الاقتضاء، تتيح مستوى مكافئاً على الأقل من الموثوقية.

2- يعتد بالمعايير الدولية المعترف بها لدى تقرير ما إذا كان نظام إدارة الهوية أو خدمة إدارة الهوية أو إثبات للهوية، حسب الاقتضاء، يوفر مستوى مكافئاً على الأقل من الموثوقية.

3- لأغراض الفقرة 1، يفترض أن يوفر نظام إدارة الهوية أو خدمة إدارة الهوية أو إثبات الهوية مستوى مكافئاً على الأقل من الموثوقية إذا قررت [جهات، من الأفراد أو الأجهزة أو السلطات تسميها الولاية القضائية المشتري عملاً بالمادة 11] هذا التكافؤ، مع مراعاة الفقرة 2 من المادة 10.

المادة 26- الاعتراف عبر الحدود بنتيجة استخدام خدمات توفير الثقة

- 1- يكون للنتائج المستمدة من استخدام خدمات توفير الثقة المقدمّة خارج [الولاية القضائية المشتريّة] نفس الأثر القانوني الذي يكون في [الولاية القضائية المشتريّة] للنتيجة المستمدة من استخدام خدمات توفير الثقة المقدمة في [الولاية القضائية المشتريّة] إذا كانت الطريقة التي استخدمتها خدمات توفير الثقة تتيح مستوى مكافئاً على الأقل من الموثوقية.
- 2- يعتد بالمعايير الدولية المعترف بها لدى تقرير ما إذا كانت خدمة لتوفير الثقة تقدّم مستوى مكافئاً على الأقل من الموثوقية.
- 3- لأغراض الفقرة 1، يفترض أن توفر خدمة توفير الثقة مستوى مكافئاً على الأقل من الموثوقية إذا قررت [جهات، من الأفراد أو الأجهزة أو السلطات تسميها الولاية القضائية المشتريّة عملاً بالمادة 23] هذا التكافؤ، مع مراعاة الفقرة 2 من المادة 22.

المادة 27- التعاون

[يجوز للجهات، من الأفراد أو الأجهزة أو السلطات التي تقضي الولاية القضائية المشتريّة بأنها مختصة،] التعاون مع الكيانات الأجنبية من خلال تبادل المعلومات والخبرات والممارسات الجيدة المتعلقة بإدارة الهوية وخدمات توفير الثقة، وخصوصاً فيما يتعلق بما يلي:

- (أ) الاعتراف بالآثار القانونية لنظم إدارة الهوية وخدمات توفير الثقة الأجنبية، سواء من جانب واحد أو بالاتفاق المتبادل؛
- (ب) تعيين نظم إدارة الهوية وخدمات توفير الثقة؛
- (ج) بيان مستويات الضمان في نظم إدارة الهوية ومستويات موثوقية خدمات توفير الثقة.

## مذكرة تفسيرية لمشروع القانون النموذجي بشأن استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود

### أولاً - مقدمة

#### ألف - الغرض من هذه المذكرة التفسيرية

1- رأت لجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال)، عند إعداد واعتماد قانون الأونسيترال النموذجي بشأن استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود (يشار إليه فيما يلي باسم "القانون النموذجي")، أن القانون النموذجي سيكون أكثر فعالية في موامة التشريعات وتحديثها إذا كان مشفوعاً بمعلومات أساسية وتفسيرية.

2- وتهدف هذه المذكرة التفسيرية، المستمدة من الأعمال التحضيرية للقانون النموذجي، إلى مساعدة المهتمين باعتماد القانون النموذجي واستخدامه وتفسيره بشكل موحد، مثل مقرري السياسات والمشرعين والأكاديميين والممارسين والقضاة والمحكمين والمشغلين التجاريين ومستخدمي خدمات إدارة الهوية وخدمات توفير الثقة. فعلى سبيل المثال، يمكن لهذه المعلومات، في وقت التشريع، أن تساعد السلطات القضائية على تكييف القانون النموذجي بما يلائم احتياجاتها من حيث التفاعل بين أحكام القانون النموذجي والضوابط التنظيمية لخدمات إدارة الهوية وتوفير الثقة.

#### باء - الأهداف

3- في السنوات العشرين الأخيرة، شهد نمو مطرد في قيمة النشاط التجاري عبر الإنترنت (أي في المعاملات الإلكترونية فيما بين الشركات وبين الشركات والمستهلكين وبين الشركات والحكومات). ويصاحب هذا النمو، الذي تسارعت وتيرته بسبب الحاجة إلى التخفيف من آثار جائحة كوفيد-19<sup>(1)</sup>، زيادة مماثلة في معاملات البيانات وهو يستدعي وضع إطار قانوني وتقني ملائم.

4- ويستند نمو الأنشطة التجارية عبر الإنترنت 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. وأقر في الهدف 16 من أهداف التنمية المستدامة بأهمية الهوية، حيث تدعو الغاية 9 منه إلى توفير هوية قانونية لجميع البشر، بما في ذلك في صورة إلكترونية. وتتحول هذه الدعوة في الاقتصاد الرقمي إلى الحق في امتلاك هوية رقمية.

5- وعلى مدى السنوات السابقة، اقترحت حلول متنوعة لتلبية الحاجة إلى تحديد الهوية بواسطة الإنترنت. وقد أدى ذلك إلى تطوير 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.

(1) مؤتمر الأمم المتحدة للتجارة والتنمية (الأونكتاد)، تقرير الاقتصاد الرقمي: تدفقات البيانات عبر الحدود والتنمية: من تدفق البيانات لصالحهم، وثيقة من وثائق الأمم المتحدة UNCTAD/DER/2021، الصفحتان 16 و 17.

- 6- وثمة عنصر هام آخر من عناصر الثقة عبر الإنترنت هو القدرة على الاعتماد بقدر كاف من الثقة على نوعية البيانات، وهو ما تركز عليه عمليات تبادل البيانات. وقد برزت خدمات توفير الثقة، التي توفر تأكيدا لبعض سمات رسالة البيانات مثل مصدرها وسلامتها ووقت معالجه إجراء معين ذي صلة، كحلول لتوفير تلك الثقة.
- 7- وقد تكون العقوبات التي تحول دون توسيع نطاق استخدام إدارة الهوية وخدمات توفير الثقة ذات طابع مختلف. فعلى سبيل المثال، قد يكون الوصول إلى إدارة الهوية وخدمات توفير الثقة محدودا بسبب التكلفة ونقص الوعي والقيود التقنية. وتشمل العقوبات ذات الطابع القانوني ما يلي: (1) غياب التشريعات التي تعطي الأثر القانوني لإدارة الهوية وخدمات توفير الثقة؛ (2) اختلاف النهج 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<sup>(2)</sup>.
- 8- والهدف الأساسي من القانون النموذجي هو التغلب على هذه العقبات من خلال وضع قواعد قانونية موحدة تخدم عدة أغراض. فالقواعد الموحدة يمكن أن تحسن الكفاءة بالتشجيع على قبول نتيجة تطبيق خدمات إدارة الهوية وتوفير الثقة على نطاق المنظومات؛ وخفض تكاليف المعاملات بتيسير الامتثال للاشتراطات التنظيمية؛ وزيادة إمكانية التنبؤ واليقين القانونيين للمعاملات الإلكترونية على أساس معاملة المسائل معاملة مشتركة، عبر قنوات من بينها آليات الاعتراف عبر الحدود؛ والمساهمة في سد الفجوة الرقمية من خلال إتاحة الحلول المشتركة بسهولة أكبر.
- 9- وعلى وجه الخصوص، سوف يعزز وجود إطار قانوني لإدارة الهوية وخدمات توفير الثقة التعجيل الأمن للهوية الرقمية ومعاملات البيانات. 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

- 10- ينطبق القانون النموذجي على استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود في سياق الأنشطة التجارية والخدمات ذات الصلة بالتبادل التجاري. ويجوز للولايات القضائية المشترعة أن تقرر توسيع نطاق تطبيق القانون النموذجي ليشمل الأنشطة غير التجارية.
- 11- وقد يكون العديد من التشريعات المختلفة ذا صلة بتبادل البيانات. ولا يهدف القانون النموذجي إلى التأثير على تلك القوانين الموجودة، أي القانون المطبق على خصوصية البيانات وحمايتها. وهو لا يفرض أيضاً التزامات جديدة باستخدام خدمات إدارة الهوية وتوفير الثقة أو باستخدام أي خدمة بعينها لإدارة الهوية أو لتوفير الثقة، وهو لا يؤثر على أي من الاشتراطات الحالية (انظر الفقرات 102-104 أدناه).
- 12- وتنطبق أحكام القانون النموذجي المتعلقة بإدارة الهوية على تحديد هوية الأشخاص الطبيعيين والاعتباريين. وتنطبق الأحكام المتعلقة بخدمات توفير الثقة على جميع المعلومات التي تكون في شكل رسالة بيانات. وتنطبق كلتا المجموعتين من الأحكام بغض النظر عن الطابع الخاص أو العام لمقدم الخدمة والمشارك والطرف المعول.

## دال - البنية

- 13- يتألف القانون النموذجي 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، كليهما. علاوة على ذلك، توجد أوجه تشابه كبيرة في هيكل ومضمون الفصلين الثاني والثالث. ومن ثم، فإن تفسير حكم

(2) A/CN.9/965، الفقرة 52.

ما من الأحكام الواردة في الفصل الثاني قد يكون ذا صلة بالحكم 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.

14- ويتضمن الفصل الأول تعاريف مصطلحات معينة مستخدمة في القانون النموذجي؛ وتعيين نطاق الانطباق؛ وأحكاماً بشأن الاستخدام الطوعي لخدمات إدارة الهوية وتوفير الثقة، بما في ذلك استخدام خدمات محددة؛ وأحكاماً بشأن العلاقة بين القانون النموذجي والقوانين الأخرى، بما في ذلك اشتراطات تحديد أو استخدام خدمات بعينها من خدمات توفير الثقة؛ وأحكاماً بشأن التفسير المستقل للقانون النموذجي، لأغراض من بينها سد الفجوات، في ضوء طبيعته الموحدة ومصدره الدولي.

15- ويحدد الفصل الثاني العناصر الأساسية للنظام القانوني المنطبق على إدارة الهوية، وهو ينص على التزامات أساسية معينة لمقدمي خدمات إدارة الهوية والمشاركين، ويضع قواعد بشأن مسؤولية مقدمي خدمات إدارة الهوية. وتتص المادة 5 على مبدأ الاعتراف القانوني بإدارة الهوية وعدم التمييز ضد تحديد الهوية إلكترونياً. وتورد المادة 6 الالتزامات الأساسية لمقدمي خدمات إدارة الهوية؛ ومن هذا المنطلق، تحدد الالتزامات الجوهرية لمقدمي خدمات إدارة الهوية، التي تناظر العناصر الأساسية لنظم إدارة الهوية والخطوات الرئيسية في دورة حياة إدارة الهوية. وتتناول المادة 7 التزامات مقدم خدمات إدارة الهوية في حال وقوع خرق للبيانات، وهي تُستكمل 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. وتقيم 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.

16- 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 المسجل الإلكتروني؛ والتوثيق 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. وتتص المادة 22 على إرشادات بشأن التقرير اللاحق لموثوقية الطريقة المستخدمة في خدمة توفير الثقة، وتتص المادة 23 على تعيين الموثوقية مسبقاً. وأخيراً، تتضمن المادة 24 قواعد بشأن مسؤولية مقدمي خدمات توفير الثقة.

17- ويتناول الفصل الرابع تمكين الاعتراف عبر الحدود بإدارة الهوية وخدمات توفير الثقة، وهو أحد الأهداف الرئيسية للقانون النموذجي. ولا ينظر القانون النموذجي في إنشاء هيئة مخصصة للاعتراف القانوني بإدارة الهوية وخدمات توفير الثقة، ولكنه يتوخى عدة آليات تقوم على نهج لا مركزي. وإلى جانب المواد 25 و26 و27، ثمة وجهة للأحكام المخصصة الواردة في المواد 10 (3) و11 (4) و22 (3) و23 (4)، المتعلقة بعدم التمييز الجغرافي في تقرير موثوقية خدمات إدارة الهوية وتوفير الثقة وفي تعيين خدمات إدارة الهوية وتوفير الثقة الموثوقة. وقد تكون الاتفاقات التعاقدية أيضاً ذات أهمية في تمكين استخدام خدمات إدارة الهوية وتوفير الثقة عبر الحدود.

## هاء - معلومات أساسية

## 1- تاريخ الصياغة

18- يبنثق القانون النموذجي من طلب صاغته اللجنة في دورتها الثامنة والأربعين في عام 2015. وفي تلك الدورة، طلبت اللجنة إلى الأمانة أن تضطلع بأعمال تحضيرية بشأن الجوانب القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة، بوسائل منها تنظيم ندوات واجتماعات لأفرقة خبراء، وذلك حتى يتسنى مناقشة تلك المواضيع مستقبلا على مستوى الفريق العامل<sup>(3)</sup>، وأن تعرض على الفريق العامل الرابع نتائج تلك الأعمال التحضيرية التماسا لتوصيات بشأن تحديد النطاق الدقيق للعمل ومنهجياته الممكنة وأولوياته، لكي تنظر فيها اللجنة<sup>(4)</sup>.

19- واستجابة لهذا الطلب، عُرضت على اللجنة في دورتها التاسعة والأربعين في عام 2016 مذكرة من الأمانة بشأن المسائل القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة (A/CN.9/891) تضمنت ملخصا للمناقشات التي جرت أثناء ندوة الأونسيرال بشأن المسائل القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة، والتي عُقدت في فيينا، يومي 21 و22 نيسان/أبريل 2016<sup>(5)</sup>. واتفقت اللجنة على أنه ينبغي استبقاء مسألة إدارة الهوية وخدمات توفير الثقة في جدول أعمال الفريق العامل<sup>(6)</sup>.

20- وعقد الفريق العامل، بناء على ولاية أسندتها إليه اللجنة، مناقشات أولية حول هذا الموضوع في دورته الرابعة والخمسين (فيينا، 31 تشرين الأول/أكتوبر - 4 تشرين الثاني/نوفمبر 2016). واتفق الفريق العامل على أن أعماله المقبلة بشأن إدارة الهوية وخدمات توفير الثقة ينبغي أن تقتصر على استخدام نُظم إدارة الهوية لأغراض تجارية، وأنه ينبغي النظر بعين الاعتبار إلى مقدمي خدمات إدارة الهوية من القطاع العام والقطاع الخاص، على السواء. واتفق الفريق العامل أيضا على أنه يمكن الاضطلاع بالأعمال المتعلقة بإدارة الهوية قبل الأعمال المتعلقة بخدمات توفير الثقة، إلا أن أعمال تحديد وتعريف المصطلحات ذات الصلة بكل من إدارة الهوية وخدمات توفير الثقة ينبغي الاضطلاع بها على نحو متزامن، وذلك بالنظر إلى العلاقة الوثيقة بين الموضوعين. وأتفق كذلك على أنه ينبغي التركيز على نُظم إدارة الهوية المتعددة الأطراف وعلى تحديد هوية الأشخاص الطبيعيين والاعتباريين، وعلى أن الفريق العامل ينبغي أن يواصل أعماله بزيادة توضيح أهداف المشروع وتحديد نطاقه واستبانة المبادئ العامة المنطبقة وصوغ التعاريف اللازمة (A/CN.9/897، الفقرات 118-120 و122).

21- وتماشيا مع ما اتخذته الفريق العامل من قرارات سابقة، ناقش الفريق العامل في دورته الخامسة والخمسين (نيويورك، 24-28 نيسان/أبريل 2017)، جملة مواضيع منها أهداف العمل المزمع الاضطلاع به بشأن إدارة الهوية وخدمات توفير الثقة، والمبادئ العامة لذلك العمل ونطاقه (A/CN.9/902، الفقرات 29-85).

22- وأكدت اللجنة مجددا الولاية التي أسندت للفريق العامل (انظر الفقرة 19 أعلاه) في دورتها الخمسين، في عام 2017، وطلبت إلى الأمانة أن تنظر في دعوة فريق من الخبراء إلى الانعقاد. ودعيت الدول والمنظمات الدولية إلى تبادل خبراتها<sup>(7)</sup>. ووفقا لذلك، عقدت الأمانة اجتماعا لفريق من الخبراء بشأن الجوانب القانونية المتعلقة بإدارة الهوية وخدمات توفير الثقة في فيينا يومي 23 و24 تشرين الثاني/نوفمبر 2017.

23- واستنادا أيضا إلى نتائج اجتماع فريق الخبراء، حدد الفريق العامل، في دورته السادسة والخمسين (نيويورك، 16-20 نيسان/أبريل 2018)، المواضيع التالية باعتبارها ذات صلة بمناقشته للجوانب القانونية

(3) الوثائق الرسمية للجمعية العامة، الدورة السبعون، الملحق رقم 17 (A/70/17)، الفقرات 354 و355 و358.

(4) المرجع نفسه، الفقرة 358.

(5) المرجع نفسه، الدورة الحادية والسبعون، الملحق رقم 17 (A/71/17)، الفقرة 228.

(6) المرجع نفسه، الفقرتان 235 و236.

(7) المرجع نفسه، الدورة الثانية والسبعون، الملحق رقم 17 (A/72/17)، الفقرة 127.



لإدارة الهوية وخدمات توفير الثقة: نطاق العمل؛ المبادئ العامة؛ التعاريف؛ متطلبات وآليات الاعتراف المتبادل؛ اعتماد نُظُم إدارة الهوية وخدمات توفير الثقة؛ مستويات الضمان في إدارة الهوية وخدمات توفير الثقة؛ المسؤولية؛ آليات التعاون المؤسسي؛ الشفافية؛ الالتزامات بشأن الهوية؛ الاحتفاظ بالبيانات؛ الإشراف على مقدمي الخدمات (A/CN.9/936، الفقرات 61-94).

24- وطلبت اللجنة إلى الفريق العامل، في دورتها الحادية والخمسين في عام 2018، بناء على توصيته (A/CN.9/936، الفقرة 95)، الاضطلاع بأعمال بهدف إعداد نص يرمي إلى تيسير الاعتراف عبر الحدود بإدارة الهوية وخدمات توفير الثقة، استناداً إلى المبادئ والمسائل التي استبانها الفريق العامل (انظر الفقرة 23 أعلاه)<sup>(8)</sup>.

25- وبناء على ذلك، واصل الفريق العامل نظره في المسائل التي استبانها (A/CN.9/965، الفقرات 10-129) في دورته السابعة والخمسين (فيينا، 19-23 تشرين الثاني/نوفمبر 2018).

26- وقُدِّمت أول مجموعة من مشاريع أحكام بشأن الاعتراف عبر الحدود بإدارة الهوية وخدمات توفير الثقة (A/CN.9/WG.IV/WP.157) مصحوبة بملاحظات توضيحية (A/CN.9/WG.IV/WP.158) للنظر فيها في دورة الفريق العامل الثامنة والخمسين (نيويورك، 8-12 نيسان/أبريل 2019). ونظر الفريق العامل في مشاريع الأحكام المتعلقة بنطاق انطباق نُظُم إدارة الهوية وخدمات توفير الثقة والاعتراف بتلك النُظُم والخدمات ومدى موثوقيتها، وأنواع خدمات توفير الثقة المشمولة، والالتزامات ومسؤوليات مقدمي خدمات إدارة الهوية وخدمات توفير الثقة (A/CN.9/971، الفقرات 13-153).

27- وفي تلك الدورة، طلب الفريق العامل إلى الأمانة أن تعد، بالتشاور مع الخبراء، مقترحات محددة بشأن المسائل المتعلقة بموثوقية نظم إدارة الهوية (A/CN.9/971، الفقرة 67). وتلبية لهذا الطلب، عقدت الأمانة اجتماعاً لفريق من الخبراء في فيينا يومي 22 و23 تموز/يوليه 2019 لمناقشة المعايير والإجراءات التي توّهل نُظُم إدارة الهوية للاعتراف القانوني بها، وكذلك سائر المسائل المشمولة في مشاريع الأحكام، ولا سيما موثوقية نُظُم إدارة الهوية، والالتزامات ومسؤوليات مقدمي خدمات إدارة الهوية.

28- وأعربت اللجنة عن ارتياحها للتقدم الذي أحرزه الفريق العامل في دورته الثانية والخمسين، في عام 2019<sup>(9)</sup>. وأشارت أيضاً إلى أنه ينبغي للفريق العامل أن يعمل على إعداد صك قابل للتطبيق على كلٍّ من الاستعمال الداخلي والاستعمال العابر للحدود لخدمات إدارة الهوية وتوفير الثقة، وأنَّ حصيلته هذا العمل لها تداعيات على مسائل خارجة عن نطاق المعاملات التجارية<sup>(10)</sup>.

29- ونظر الفريق العامل في مجموعة منقحة من مشاريع الأحكام (A/CN.9/WG.IV/WP.160)، تضمنت نتائج مشاورات الأمانة مع الخبراء (انظر الفقرة 27 أعلاه)، في دورته التاسعة والخمسين (فيينا، 25-29 تشرين الثاني/نوفمبر 2019). وأجرى الفريق العامل قراءة كاملة لمشاريع الأحكام، مع التركيز على الأحكام المتعلقة بخدمات توفير الثقة (A/CN.9/1005، الفقرات 10-122). وأجرى أيضاً مناقشات أولية بشأن شكل الصك، أعرب في إطارها عن تفضيل قوي لأن يتخذ الصك شكل قانون نموذجي وليس اتفاقية (المرجع نفسه، الفقرة 123).

30- وأعربت اللجنة عن ارتياحها للتقدم الذي أحرزه الفريق العامل في دورته الثالثة والخمسين، في عام 2020<sup>(11)</sup>.

(8) المرجع نفسه، الدورة الثالثة والسبعون، الملحق رقم 17 (A/73/17)، الفقرة 159.

(9) المرجع نفسه، الدورة الرابعة والسبعون، الملحق رقم 17 (A/74/17)، الفقرة 175.

(10) المرجع نفسه، الفقرة 172.

(11) المرجع نفسه، الدورة الخامسة والسبعون، الملحق رقم 17 (A/75/17)، الجزء الثاني، الفقرتان 41 و51 (د).

- 31- وعُرضت على الفريق العامل مجموعة ثانية منقحة من مشاريع الأحكام (A/CN.9/WG.IV/WP.162)، فأجرى قراءة كاملة لتلك الأحكام (A/CN.9/1045، الفقرات 16-138) في دورته الستين (فيينا، 19-23 تشرين الأول/أكتوبر 2020). واتفق أيضاً على إمكانية عقد مشاورات غير رسمية لمناقشة المواضيع العالقة.
- 32- وعُقدت مشاورات غير رسمية عن بُعد مع المندوبين والمراقبين في الفترة من 15 إلى 17 آذار/مارس 2021 لمناقشة المسؤولية، وعلاقة مشاريع الأحكام بنصوص الأونسيترال القائمة، والاعتراف عبر الحدود، والتعاريف وغيرها من المسائل المتعلقة بالمصطلحات.
- 33- وأبلغ الفريق العامل بنتائج المشاورات غير الرسمية في دورته الحادية والستين (نيويورك، 6-9 نيسان/أبريل 2021). ونظراً للقيود الناشئة عن الشكل الهجين للدورة (بما في ذلك ضيق أوقات الاجتماعات)، ركزت اللجنة مداولاتها، لدى نظرها في مجموعة ثالثة منقحة من مشاريع الأحكام (A/CN.9/WG.IV/WP.167)، على المسائل التي نوقشت أثناء المشاورات (A/CN.9/1051، الفقرات 13-67).
- 34- وأبلغت اللجنة، في دورتها الرابعة والخمسين في عام 2021، بأن الفريق العامل أحرز تقدماً كبيراً نحو إكمال الصك، رغم ضيق أوقات الاجتماعات. وأعربت اللجنة عن ارتياحها وشجعت الفريق العامل على إنجاز عمله وتقديمه إلى اللجنة للنظر فيه في دورتها الخامسة والخمسين في عام 2022<sup>(12)</sup>.
- 35- وأجرى الفريق العامل في دورته الثانية والستين (فيينا، 22-26 تشرين الثاني/نوفمبر 2021) قراءة أخرى لمشاريع الأحكام (A/CN.9/1087، الفقرات 12-114) على أساس مجموعة منقحة (A/CN.9/WG.IV/WP.170) مصحوبة بمذكرة تفسيرية (A/CN.9/WG.IV/WP.171). وطلب الفريق العامل إلى الأمانة أن تتفح مشاريع الأحكام والمذكرة التفسيرية لكي تجسد مداولاته وقراراته وأن تحيل النص المنقح إلى اللجنة، في شكل قانون نموذجي، من أجل النظر فيه في دورتها الخامسة والخمسين. وطلب إلى الأمانة تعميم النص المنقح على جميع الحكومات والمنظمات الدولية ذات الصلة من أجل التعليق عليه، وتجميع التعليقات الواردة لكي تنتظر فيها اللجنة (A/CN.9/1087، الفقرة 11).
- 36- [يُستكمل النص لاحقاً]

## 2- العلاقة بالنصوص السابقة للأونسيترال

- 37- ليس في نصوص الأونسيترال السابقة حكم بشأن خدمات توفير الثقة. إلا أن تلك النصوص تحدد قواعد للتكافؤ الوظيفي قد تكون ذات صلة ببعض خدمات توفير الثقة. فالمادة 7 من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (قانون التجارة الإلكترونية)<sup>(13)</sup>، والمادة 6 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية (قانون التوقيعات الإلكترونية)<sup>(14)</sup>، والمادة 9 (3) من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية<sup>(15)</sup>، والمادة 9 من القانون النموذجي بشأن السجلات الإلكترونية القابلة للتحويل (قانون السجلات الإلكترونية)<sup>(16)</sup>، تنص على الاشتراطات التي يجب أن تمتثل لها التوقيعات الإلكترونية لكي تكون مكافئة وظيفياً للتوقيعات الورقية. وتتشرط تلك الأحكام تحديد هوية الموقع،

(12) المرجع نفسه، النورة السادسة والسبعون، الملحق رقم 17 (A/76/17)، الفصل التاسع.

(13) قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع لسنة 1996 ومع المادة 5 مكرراً الإضافية، بصيغتها المعتمدة في عام 1998 (1999)، منشورات الأمم المتحدة، رقم المبيع A.99.V.4.

(14) قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية ودليل اشتراكه (2002)، منشورات الأمم المتحدة، رقم المبيع A.02.V.8.

(15) United Nations, Treaty Series, vol. 2898, p. 3.

(16) قانون الأونسيترال النموذجي بشأن السجلات الإلكترونية القابلة للتحويل (2018)، منشورات الأمم المتحدة، رقم المبيع A.17.V.5.

وهو ما قد ينطوي على استخدام تحديد الهوية إلكترونياً، وبوجه أعم، على استخدام إدارة الهوية. وتستند المادة 16 من القانون النموذجي إلى المادة 9 من قانون السجلات الإلكترونية.

38- وبالمثل، تحدد المادة 10 من قانون التجارة الإلكترونية الإشتراطات المتعلقة بالتكافؤ الوظيفي للاحتفاظ بالمعلومات، وتستند المادة 19 من القانون النموذجي إلى المادة 10 (1) من قانون التجارة الإلكترونية. أما أحكام الأونسيترال الأخرى التي استخدمت كمصادر لمواد القانون النموذجي فتُحدّد في التعليق على المادة المقابلة. إلا أنه قد لا يلزم استخدام خدمة من خدمات توفير الثقة المسماة في القانون النموذجي لاستيفاء قواعد التكافؤ الوظيفي الواردة في نصوص الأونسيترال السابقة.

39- وقد نوقشت بالتفصيل عدة مسائل ذات صلة بالقانون النموذجي، مثل تقييم الوثوقية، والمسؤولية، وآليات الاعتراف عبر الحدود، في وثيقة توجيهية بشأن استخدام التوقيعات الإلكترونية على الصعيد الدولي<sup>(17)</sup>.

## واو- المفاهيم والمبادئ الرئيسية

40- يوضح هذا القسم عدة مفاهيم ومبادئ رئيسية يركز عليها القانون النموذجي. ويرد توضيح كذلك لمصطلحات معرّفة مستخدمة في القانون النموذجي في شرح المادة 1 أدناه، في حين ترد في الوثيقة [A/CN.9/WG.IV/WP.150](#) قائمة أوسع من المصطلحات والمفاهيم ذات الصلة بخدمات إدارة الهوية وتوفير الثقة التي جُمعت على أساس التعاريف الواردة في النصوص القانونية والتقنية المتفق عليها دولياً. وحسبما هو مبين في تلك الوثيقة، قد تُستخدم تلك النصوص مصطلحات معرّفة مختلفة لنفس المفهوم أو قد تعرّف نفس المصطلح بشكل مختلف.

### 1- مبادئ أساسية

41- يستند القانون النموذجي، مثل نصوص الأونسيترال السابقة، إلى مبادئ استقلالية الأطراف، وحياد التكنولوجيا، والتكافؤ الوظيفي، وعدم التمييز ضد استخدام الوسائل الإلكترونية، رهناً بما قد يُدخّل عليه من تعديلات<sup>(18)</sup>.

42- 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.

43- ويكفل مبدأ عدم التمييز، الذي ورد للمرة الأولى في المادة 5 من قانون التجارة الإلكترونية والمعروف أيضاً باسم مبدأ الاعتراف القانوني، ألا ينقي عن المعلومات أثرها القانوني أو صحتها أو قابليتها للإنفاذ لمجرد أنها في شكل إلكتروني.

44- ويكفل مبدأ الحياد التكنولوجي ألا يفرض القانون أو يحبذ استخدام أي تكنولوجيا أو طريقة محددة، مما يجعل القوانين تتحوط للمستقبل. والحياد التكنولوجي ضروري لتحقيق قابلية التشغيل المتبادل، وهو ما يمكن فعلياً من تدفق البيانات. والركيزة القانونية التي يقوم عليها هذا المبدأ هي التعريف الواسع لـ"رسالة البيانات"، الذي ورد للمرة الأولى في المادة 2 (أ) من قانون التجارة الإلكترونية، والذي يهدف إلى استيعاب جميع التكنولوجيات القائمة والمقبلة.

45- ويحدد مبدأ التكافؤ الوظيفي المعايير التي تعتبر بموجبها المعاملات الإلكترونية مستوفية لشروط الشكل المنطبقة على الوثائق الورقية، مثل أن تكون الوثيقة مكتوبة أو أصلية أو موقعة. وهو يفترض وجود اشتراطات

(17) أمانة الأونسيترال، تعزيز الثقة بالتجارة الإلكترونية: المسائل القانونية الخاصة باستخدام طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي (2007)، منشورات الأمم المتحدة، رقم المبيع A.09.V.4.

(18) [A/CN.9/902](#)، الفقرتان 52 و63.

قانونية تنص بصورة مباشرة أو غير مباشرة على بعض الأنشطة المادية أو الورقية، مثل استخدام إثباتات ورقية لتحديد هوية شخص ما. وهو يحل بعد ذلك أغراض تلك الاشتراطات ووظائفها، بهدف تحديد سبل الوفاء بتلك الأغراض أو الوظائف بالوسائل الإلكترونية.

46- وعلى الرغم من أن القانون النموذجي لا يحدد صراحة تلك المبادئ العامة، فإنها تشكل إطاراً للأحكام الرئيسية للنص. ويرد مبدأ استقلالية الأطراف في المادة 3، ويتجسد مبدأ عدم التمييز، حسبما ينطبق على خدمات إدارة الهوية وتوفير الثقة، في المادتين 5 و13 على التوالي. وعلاوة على ذلك، استُرشِد بمبدأ التكافؤ الوظيفي في المادة 9، المتعلقة بتحديد الهوية إلكترونياً، والمواد 16-21 المتعلقة بخدمات توفير الثقة المعينة. إلا أن بعض خدمات توفير الثقة المشمولة بالقانون النموذجي قد لا يكون لها مكافئ ورقي، ولذلك لن ينطبق مبدأ التكافؤ الوظيفي عليها.

## 2- إدارة الهوية

47- تحديد الهوية هو عملية تمييز شخص ما عن الآخرين بالإحالة إلى معلومات متعلقة بذلك الشخص (أي النعوت). وتلك المعلومات يمكن جمعها أو ملاحظتها. وينطوي تحديد الهوية على التحقق من أن النعوت المجمع أو الملاحظة تتطابق مع "هوية" سبق تحديدها للشخص الذي يجري تحديد هويته. وغالباً ما يجري تحديد الهوية بهذا المعنى استجابة لادعاء شخص ما بامتلاك هوية معينة وتقديم نعوت للتحقق منها.

48- ووفقاً لذلك، بموجب القانون النموذجي، 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 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 تُقدّم إثباتاته هو الشخص الذي صدرت له إثباتات الهوية في المرحلة الأولى.

49- وتُستخدم نظم إدارة الهوية لإدارة عمليات تحديد الهوية المرتبطة بكل مرحلة من المرحلتين، وكذلك في إدارة النعوت التي تُجمع وإثباتات الهوية التي تُصدّر 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. علاوة على ذلك، قد يوفر نظام إدارة الهوية خدمات مختلفة من خدمات إدارة الهوية. ويجوز للأطراف (أي الطرف الذي يسعى إلى تحديد هوية ما، والطرف الذي يسعى إلى تحديد هويته هو نفسه) أن تختار خدمة تحديد الهوية الملائمة حسب الحاجة.

50- ويجوز أن تتولى تشغيل نظم إدارة الهوية كيانات عامة أو خاصة. وفي الممارسة العملية، تناظر 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. وتطبيقاً لمبدأ حياد التكنولوجيا (انظر الفقرة 44 أعلاه)، لا يفترض القانون النموذجي مسبقاً استخدام أي تكنولوجيا أو نموذج، ويمكن تبعاً لذلك تطبيقه على جميع أنواع نظم وخدمات إدارة الهوية.

51- ويجوز لمقدمي خدمات إدارة الهوية والمشاركين والأطراف المعولنين والكيانات المعنية الأخرى الاتفاق على العمل بموجب سياسات ومعايير وتقنيات متوافقة فيما بينهم، يُنص عليها في قواعد النظام، حتى تكون إثباتات الهوية التي يقدمها كل واحد من مقدمي خدمات إدارة الهوية المشاركين مفهومة وموثوقة لجميع الأطراف المعولة المشاركة. ويمكن الإشارة إلى هذا الترتيب باسم "اتحاد الهويات"، وإلى قواعد النظام، التي تكون ذات طابع تعاقدية، باسم "إطار الثقة". وقد يساهم اتحاد الهويات في زيادة عدد المستخدمين والتطبيقات التي تشترك في خدمات إدارة الهوية نفسها، مما قد يخفض التكاليف ويضمن، من ثم، الاستدامة على المدى الطويل.

### 3- خدمات توفير الثقة

52- خدمات توفير الثقة عبارة عن خدمات عبر الإنترنت توفر ضمانات لبعض سمات رسائل البيانات، مثل المصدر والسلامة ووقت معالجة إجراء معين فيما يخص البيانات. وضمان جودة البيانات أمر بالغ الأهمية لإرساء الثقة في عمليات تبادل البيانات التي تشكل العمود الفقري للتجارة الرقمية. ويحدد القانون النموذجي بعض خدمات توفير الثقة التي يشجع استخدامها ويعترف بأن هناك خدمات أخرى لتوفير الثقة قد تكون موجودة أو يمكن تطويرها في المستقبل.

53- ويُعنى مفهوم خدمة توفير الثقة في القانون النموذجي بتقديم خدمة ما وليس بالخدمة في حد ذاتها. فعلى سبيل المثال، يمكن وضع توقيع إلكتروني باستخدام خدمة تستخدم طرائق إنشاء التوقيع الإلكتروني وإدارته. وتقاديا للشك، يحدد كل حكم من أحكام القانون النموذجي ما إذا كان معنيا بالطرائق المستخدمة في تقديم خدمة التوقيع الإلكتروني، أو بالتوقيع الإلكتروني الذي ينتج عن تطبيق تلك الخدمة.

### 4- تقييم الموثوقية

54- تماشياً مع نصوص الأونسيترال السابقة، تشير عدة أحكام من القانون النموذجي إلى استخدام طريقة موثوقة لتقديم خدمات إدارة الهوية وتوفير الثقة. ويتوخى القانون النموذجي 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.

#### (أ) التعيين المسبق للموثوقية

55- يشترط أحد النهج المحتملة لتقييم موثوقية طريقة ما أن يُجرى ذلك التقييم قبل استخدام الطريقة (مسبقاً)، مقابل قائمة بالشروط المحددة مسبقاً، وبعبارة عامة بدلاً من الإشارة إلى معاملة محددة. ويشير القانون النموذجي إلى هذا النهج بوصفه تعييناً للموثوقية، ويورد في المادتين 11 (المنطبقة على خدمات إدارة الهوية) و23 (المنطبقة على خدمات توفير الثقة) اشتراطات ذلك التعيين، التي تشمل نفس الظروف ذات الصلة بتقرير الموثوقية.

56- ولا يتعلق موضوع 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.

57- 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. إلا أن إدارته تقتض مسبقاً وجود آلية مؤسسية، أي كيان مختص بإدارة عملية التعيين.

58- ويجب على الولاية القضائية المشتري التي تود أن تنفذ النهج المسبق أن تحدد 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 للتصديق (بما في ذلك التصديق الذاتي) في تقييم الخدمات باستخدام معايير مبنية على النتائج، ومن ثم قد يكون ذا وجهة فيما يخص تعيين تلك الخدمات.

59- ويفترض القانون النموذجي مسبقاً وجود الآلية المؤسسية اللازمة لتنفيذ نهج التقرير المسبق ولكنه لا ينص على إنشائها أو إدارتها. وأي آلية من هذا القبيل تتضمن عناصر مختلفة مثل معايير تقييم الخدمات، وتفصيل 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 تُستخدم تبعاً لذلك في معاملات ذات قيمة أعلى.

60- وينبغي أن تتكيف الآلية المخصصة للتعيين مع التطور التكنولوجي بسرعة لتجنب إعاقة الابتكار. عدا ذلك فإنه قد يميز ضد خدمات إدارة الهوية وتوفير الثقة التي لم تعين، على الرغم من توافرها واعتمادها على طرائق موثوقة. وعلاوة على ذلك، ينبغي ألا يؤدي إيراد الشروط الإضافية للتعيين إلى فرض اشتراطات تخص تكنولوجيات محددة.

### (ب) التقرير اللاحق للموثوقية

61- وثمة نهج آخر محتمل لتقييم موثوقية طريقة ما يؤجل هذا التقييم إلى اللحظة التي تنشأ فيها منازعة بشأن الموثوقية. ولذلك، لا يُجرى التقييم إلا بعد أن تكون الطريقة استُخدمت (واقعة لاحقة). ويشير القانون النموذجي إلى هذا النهج باسم تقرير الموثوقية، وترد في المادتين 10 (المنطقة على خدمات إدارة الهوية) و22 (المنطقة على خدمات توفير الثقة) اشتراطات ذلك التقرير، شاملة قائمة غير حصرية بالظروف ذات الصلة.

62- ويمكن نهج التقرير المسبق للموثوقية عموماً إجراء معاملات إدارة الهوية دون عمل تقييم مسبق للموثوقية ويقصر الحاجة إلى تقييم الموثوقية على حالات المنازعة الفعلية. وهو يوفر أيضاً أقصى قدر من المرونة للأطراف في اختيار التكنولوجيات والطرائق. وعلاوة على ذلك، يمكن إدارة هذا النهج لامركزياً وهو لا يستلزم إنشاء آلية مؤسسية، ومن ثم، يتجنب التكاليف المرتبطة بها.

63- ومن ناحية أخرى، قد لا يوفر نهج التقرير اللاحق للموثوقية مستوى أعلى من إمكانية التنبؤ بصحة الطريقة المستخدمة قبل أن تُستخدم فعلياً، مما يعرض الأطراف لخطر احتمال أن تعتبر الطريقة غير موثوقة. وعلاوة على ذلك، فإنه يوكل أمر البت في تقرير موثوقية الطريقة لطرف ثالث، وهي عملية قد تستغرق وقتاً طويلاً وقد تتخض عن قرارات غير متسقة.

### (ج) النهج المشترك

64- يجمع القانون النموذجي بين تقرير الموثوقية وتعيين الطرائق الموثوقة، مما يتيح الاعتراف بأي خدمة من خدمات إدارة الهوية وخدمات توفير الثقة، إلا أنه يوفر أيضاً توجيهات بشأن خدمات إدارة الهوية وتوفير الثقة التي تقدم درجة أعلى من الاطمئنان إلى موثوقيتها (نهج "ذو شعبتين"). ومن هذا المنطلق، لا يحبذ القانون النموذجي آلية على أخرى، بل إنه يهدف إلى الجمع بين مزاي الآليتين مع تقليل عيوبهما إلى أدنى حد ممكن، وإلى تمكين الحل المفضل للأطراف في نهاية المطاف.

65- ولا تتضمن جميع نصوص الأونسيترال أحكاماً تنص على الأخذ بنهجي التقرير المسبق واللاحق للموثوقية، كليهما. إلا أن نهجي التقرير المسبق واللاحق للموثوقية يُعتبران عموماً متوافقين ومتكاملين. ويستند النهج المشترك المعتمد في القانون النموذجي إلى المادتين 6 و7 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية.

## 5- المسائل المتعلقة بالمسؤولية

66- قد يكون لنظام المسؤولية القانونية تأثير مهم في تعزيز استخدام خدمات إدارة الهوية وتوفير الثقة، وهو أحد العناصر الأساسية للقانون النموذجي. ومن الناحية التاريخية، اعتمد المشرعون حلولاً مختلفة، تتراوح بين عدم وجود نظام مكرس بشأن المسؤولية وبين اعتماد أحكام تتناول معايير السلوك وقواعد المسؤولية المنطبقة على مقدمي الخدمات فقط، أو على جميع الأطراف المعنية (مقدمو الخدمات والمشترون والأطراف المعولة)<sup>(19)</sup>. وقد اعتمد النهج الأخير في قانون التوقيعات الإلكترونية<sup>(20)</sup>.

67- وتُخصّص المسؤولية فيما يتعلق بخدمات إدارة الهوية وتوفير الثقة بالأساس عن طريق اتفاقات تعاقدية أو بموجب نظام أساسي. وقد يفضل اتباع النهج الأخير لضمان عدم استبعاد أحكام معينة تعاقدية. وعلاوة على ذلك، يجوز تطبيق قواعد قانونية أيضاً في حالة عدم وجود اتفاق تعاقدية، أي فيما يتعلق بالأطراف المعولة.

68- وتتص المادتان 12 و 24 على نظام مسؤولية موحد لمقدمي الخدمات تجاه المشتركين والأطراف المعولة على أساس مبدأ أن يكون مقدم الخدمات مسؤولاً عن عواقب عدم تقديم خدماته وفقاً لما يقتضيه القانون. وبناء عليه، ترسي المادتان 12 و 24 أساساً قانونياً للمسؤولية يعمل جنباً إلى جنب مع المسؤولية التعاقدية وغير التعاقدية. وعلاوة على ذلك، يسمح القانون النموذجي لمقدمي الخدمات بوضع حدود للمسؤولية فيما يتعلق بالمشاركين والأطراف المعولة، على حد سواء.

69- ولا يتناول القانون النموذجي درجة الخطأ اللازمة لكي تستوجب المسؤولية ولا نوع ومقدار التعويضات التي يمكن تحصيلها<sup>(21)</sup>. ولذلك تنطبق القواعد العادية للولاية القضائية المشتتة على هذه المسائل إذا لم تعتمد في وقت سن القانون النموذجي قاعدة خاصة منطبقة على إدارة الهوية وخدمات توفير الثقة.

## 6- الجوانب الدولية

70- يعد البعد الدولي أساسياً لاستخدام خدمات إدارة الهوية وتوفير الثقة، وبصورة أعم، لاستخدام المعاملات الإلكترونية. إلا أن ذلك الاستخدام قد يعوقه نوعان من العقبات هما: عدم التوافق التقني الذي يؤدي إلى تعذر إمكانية التشغيل المتبادل، والعقبات القانونية التي تحول دون الاعتراف عبر الحدود<sup>(22)</sup>.

71- وقد تنشأ عقبات قانونية من جراء وجود نهج وطنية متضاربة، لا سيما حين يُلزم القانون بالأخذ بتكنولوجيا أو طريقة أو منتجات معينة أو بحبذها. وفي هذه الحالة، قد تعوق الاشتراطات القانونية الداخلية الاعتراف بأنواع خدمات إدارة الهوية وتوفير الثقة التي لا تمثل لتلك الاشتراطات. وعلاوة على ذلك، فإن ما يستجد من معايير تقنية وطنية - وهو أمر قد يحدث أيضاً في إطار النهج "ذي الشعبتين"، حين تُربط تلك المعايير بقرائن قانونية - قد يوجد خليطاً من الاشتراطات التي تأتي أيضاً بأثر يعوق الاستخدام عبر الحدود.

72- ويعد التمكين القانوني للاعتراف بخدمات إدارة الهوية وتوفير الثقة عبر الحدود أحد الأهداف الرئيسية للقانون النموذجي. ويجري ذلك من خلال تطبيق مبادئ الحياد التكنولوجي وعدم التمييز ضد المنشأ

(19) تعزيز الثقة بالتجارة الإلكترونية، الفقرة 175.

(20) للاطلاع على التفاصيل، انظر قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، الملاحظة التوضيحية، الفقرات 77-81.

(21) فيما يتعلق بهذه المسائل، انظر تعزيز الثقة بالتجارة الإلكترونية، الفقرات 177-193 (أساس المسؤولية: الإهمال العادي والإهمال المفترض والمسؤولية المطلقة) والفقرات 194-201 (الأطراف التي يحق لها المطالبة بتعويضات عن الأضرار، ومقدار التعويضات التي يمكن أن تحصلها عن الأضرار).

(22) تعزيز الثقة بالتجارة الإلكترونية، الفقرات 137-152.

الجغرافي<sup>(23)</sup>، التي تسترشد بها المواد 10 (3) و 11 (4) و 22 (3) و 23 (4) من القانون النموذجي. وعلاوة على ذلك، يتناول الفصل الرابع تحديداً مسائل الاعتراف عبر الحدود. ونتيجة لذلك، لا يثني القانون النموذجي عن اعتماد تشريعات تخص تكنولوجيات محددة فحسب، بل يشجع أيضاً على وضع معايير تقنية قابلة للتشغيل المتبادل، بما في ذلك من خلال التعاون.

73- ويتجاوز القانون النموذجي، تماشياً مع النهج المعتمد في نصوص الأونسيترال الموجودة من قبل، مجرد الإشارة إلى مكان المنشأ بوصفه عاملاً ذا صلة لمنح الاعتراف القانوني لخدمات إدارة الهوية وتوفير الثقة الأجنبية. وبصورة أدق، يشترط القانون النموذجي التقرير اللاحق لموثوقية خدمات إدارة الهوية وتوفير الثقة الأجنبية على أساس نفس الظروف المقررة لما يماثلها من خدمات إدارة الهوية وتوفير الثقة المحلية. وهو ينص أيضاً على آليات لتعيين موثوقية خدمات إدارة الهوية وتوفير الثقة الأجنبية على أساس نفس الظروف المقررة لما يماثلها من خدمات إدارة الهوية وتوفير الثقة المحلية. وباختصار، ينبغي أن تحدد الموثوقية التقنية، وليس مكان المنشأ، ما إذا كان الاعتراف القانوني سيُمنح.

74- ولا يشترط القانون النموذجي وضع ترتيب مؤسسي رسمي للاعتراف القانوني عبر الحدود. إلا أن هناك أمثلة على هذه الترتيبات على الصعيدين الإقليمي والثنائي. ولعل الولايات القضائية المشتعبة تود أن تستخدم القانون النموذجي كنموذج لإقامة ترتيب مؤسسي مع الشركاء الدوليين، بما في ذلك في إطار اتفاق مخصص.

75- وتتضمن الفصول المتعلقة بالتجارة الإلكترونية في اتفاقات التجارة الحرة عادةً أحكاماً بشأن التوقيعات الإلكترونية أو غيرها من أشكال تحديد الهوية إلكترونياً، التي يشار إليها أحياناً كثيرة باسم "طرائق التوثيق"، كما أنها تشترط بصورة متزايدة الاعتراف المتبادل بطرائق تحديد الهوية إلكترونياً. وعلاوة على ذلك، تتضمن اتفاقات الاقتصاد الرقمي وحدة مخصصة للهوية الرقمية تهدف إلى تمكين التشغيل المتبادل عبر الحدود. وقد يساعد اشتراع القانون النموذجي في تنفيذ تلك الأحكام الواردة في اتفاقات التجارة الحرة والاقتصاد الرقمي.

## ثانياً - شرح المواد مادة مادة

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

#### 1- المادة 1- التعاريف

76- يتضمن الفصل الأول تعاريف المصطلحات المستخدمة في القانون النموذجي.

"النعته"

77- "النعته" 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 النعته في تعريف الهوية.

78- وقد تحتوي النعوت على بيانات شخصية يخضع التعامل معها لقانون خصوصية البيانات وحمايتها. ولا يتناول القانون النموذجي خصوصية البيانات وحمايتها ويحافظ صراحة على تطبيق ذلك القانون.

(23) حُدد بالفعل حياض التكنولوجيا والأخذ بنهج غير تمييزي إزاء التوقيعات والخدمات الأجنبية باعتبارهما مبدئين يرتكز عليهما توافق ناشئ في الآراء بشأن الآليات القانونية للاعتراف بالتوقيعات الإلكترونية عبر الحدود في الوثيقة المعنونة تعزيز الثقة بالتجارة الإلكترونية، الفقرة 149.



## المراجع

A/CN.9/WG.IV/WP.150، الفقرة 13.

## "رسالة البيانات"

79- يمكن الاطلاع على تعريف "رسالة البيانات" في جميع نصوص الأونسيترال الحالية المتعلقة بالتجارة الإلكترونية، حيث يستخدم لتنفيذ مبدأ حياد التكنولوجيا (انظر الفقرة 44 أعلاه). 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

A/CN.9/1045، الفقرة 40.

## "تحديد الهوية إلكترونياً" ["التوثيق"]

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

81- وقد يكون الكشف عن اسم الشخص الطبيعي أو الاعتباري غير ضروري لاستيفاء اشتراطات تحديد الهوية إلكترونياً حين يكون التحقق من نعوت أخرى كافياً. ويتمشى ذلك مع النهج المعتمد في نصوص الأونسيترال الموجودة من قبل، أي قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، الذي ينص على أنه "لأغراض تعريف التوقيع الإلكتروني" بموجب القانون النموذجي، يمكن أن تكون عبارة "تعيين الهوية" أو مع نطاقاً من مجرد تحديد اسم الموقع<sup>(24)</sup>.

82- 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"

83- يقع تعريف "الهوية" في صميم مفهوم إدارة الهوية وهو يشير إلى القدرة على تحديد الصفات المتفرّدة التي تميّز 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.

(24) قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، ملاحظة توضيحية، الفقرة 117.

*"إثباتات الهوية"*

84- "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 الأجهزة النقالة والشهادات الرقمية وجوازات السفر البيومترية وبطاقات الهوية الإلكترونية. ويمكن استخدام إثباتات الهوية ذات الشكل الإلكتروني بالاتصال عبر الإنترنت 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))<sup>(25)</sup>.

*المراجع*

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

*"خدمات إدارة الهوية"*

85- 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 كليهما، 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؛ A/CN.9/1087، الفقرة 19.

*"مقدم خدمات إدارة الهوية"*

86- 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. والإشارة إلى وجود ترتيب مع مشترك تدكر بأن مقدم خدمات إدارة الهوية مسؤول عن كامل مجموعة الخدمات المقدمة، بغض النظر عما إذا كانت الوظائف ذات الصلة تنفذ مباشرة أو عن طريق التعاقد مع أطراف ثالثة.

*المراجع*

A/CN.9/971، الفقرة 97؛ A/CN.9/1005، الفقرة 111؛ A/CN.9/1045، الفقرة 88؛ A/CN.9/1087، الفقرة 22.

(25) 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 ("eIDAS Regulation") 1999/93/EC.

*"نظام إدارة الهوية"*

87- 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 كليهما، حتى وإن كان مقدمو خدمات إدارة الهوية مختلفين في كل مرحلة.

*المراجع*

A/CN.9/1005، الفقرة 112؛ A/CN.9/1087، الفقرة 19.

*"تدقيق الهوية"*

88- 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 يدّعيها كيان ما قبل إصدار إثباتات الهوية لذلك الكيان. وقد يكون الكيان شخصاً طبيعياً أو اعتبارياً. ويُستخدم مصطلح "تدقيق الهوية" بدلاً من مصطلح "تحديد الهوية" لمعالجة الشواغل المتعلقة بالمعاني المتعددة لمصطلح "تحديد الهوية".

*المراجع*

A/CN.9/1005، الفقرة 84.

*"الطرف المعوّل"*

89- يشير مصطلح "الطرف المعوّل" إلى شخص طبيعي أو اعتباري يتصرّف فعلياً استناداً إلى النتيجة المترتبة على خدمات إدارة الهوية أو خدمات توفير الثقة. فعلى سبيل المثال، يكون الطرف المعوّل شخصاً يتصرف بناءً على توقيع إلكتروني وليس على خدمة توفير الثقة المستخدمة في إنشاء التوقيع الإلكتروني. ويستند هذا التعريف إلى التعريف الوارد في المادة 2 (و) من قانون الأونسيرال النموذجي بشأن التوقيعات الإلكترونية.

*المراجع*

A/CN.9/1087، الفقرتان 55 و72.

*"المشترك"*

90- يشير مصطلح "المشترك" إلى الشخص الذي تُقدّم إليه الخدمات ولا يشمل الأطراف المعولة. وهو يفترض مسبقاً وجود علاقة بين مقدم الخدمة والمشارك قد تكون تعاقدية أو ذات طبيعة أخرى (على سبيل المثال، بمقتضى القانون). 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؛ A/CN.9/1087، الفقرة 23.

*"خدمات توفير الثقة"*

- 91- يجمع تعريف "خدمات توفير الثقة" بين وصف تجريدي للوظيفة المطلوب أداؤها باستخدام خدمات توفير الثقة ينصب تركيزه على أي خدمة تُعنى بتوفير ضمانات لجودة البيانات مثل صحتها وأصالتها، وبين قائمة غير حصرية بخدمات توفير الثقة الواردة في القانون النموذجي. واعتماد قوائم غير حصرية يتيح تطبيق القواعد العامة المتعلقة بخدمات توفير الثقة على أنواع خدمات توفير الثقة في المستقبل.
- 92- 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 الموقع 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 الموقع من إنشاء التوقيع الإلكتروني وتوفير 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"*

- 93- 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 مثلاً لمقدم خدمات توفير الثقة فيما يخص التوقيعات الإلكترونية. وخلافاً لمقدمي خدمات إدارة الهوية (المادة 6)، لا يحدد القانون النموذجي الوظائف التي يتعين على مقدمي خدمات توفير الثقة الاضطلاع بها. والإشارة إلى وجود ترتيب مع مشترك تذكر بأن مقدم خدمات توفير الثقة مسؤول عن كامل مجموعة الخدمات المقدمة، بغض النظر عما إذا كانت الوظائف ذات الصلة تنفذ مباشرة أو عن الطريق التعاقد مع أطراف ثالثة.
- 94- ولا يقتضي القانون النموذجي استخدام أحد مقدمي خدمات توفير الثقة من الأطراف الثالثة كشرط للاعتراف القانوني. وإذا لم يُستخدم أحد مقدمي خدمات توفير الثقة من الأطراف الثالثة، يجوز لنفس الكيان أن يؤدي دور مقدم خدمات توفير الثقة ودور المشترك.

*المراجع*

- A/CN.9/1087، الفقرة 22.

**2- المادة 2- نطاق الانطباق**

- 95- تحدد المادة 2 نطاق انطباق القانون النموذجي بالإشارة إلى استخدام خدمات إدارة الهوية وتوفير 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 تشغل منفذاً واحداً لإجراءات الاستيراد والتصدير.

96- وبالنظر إلى أن استخدام خدمات إدارة الهوية وتوفير الثقة له تبعات تتجاوز حدود المعاملات التجارية، فإنه يجوز للولايات القضائية المشترعة أن توسع نطاق القانون النموذجي ليشمل جميع أنواع المعاملات الإلكترونية التي تنطوي على أعمال تجارية أو حكومية أو مستهلكين.

97- وتماشياً مع المبدأ العام الذي تركز عليه نصوص الأونسيترال بشأن التجارة الإلكترونية الذي يحذّر تجنب إدخال التعديلات على القانون الموضوعي القائم أو تقليدها إلى أدنى حد، توضح الفقرة 2 (أ) أن القانون النموذجي لا يطرح أي التزامات جديدة لتحديد هوية.

98- وتحفظ 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 يُسمح بتحديد الهوية إلكترونياً، غالباً ما يطلب المنظّمون استخدام إجراء محدد لإدارة الهوية أو خدمة محددة من خدمات توفير الثقة من قبيل إثباتات الهوية الصادرة عن هيئة عامة.

99- وبالنظر إلى الطابع التمكيني للقانون النموذجي، شأنه شأن نصوص الأونسيترال التشريعية بشأن التجارة الإلكترونية القائمة، فإنه لا يؤثر على تطبيق أي قانون آخر على خدمات إدارة الهوية وتوفير 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 يُذكر 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؛ A/CN.9/1087، الفقرة 27.

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

100- تشير المادة 3 إلى أن القانون النموذجي لا يلزم 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 تدعمها خدمات إدارة الهوية وتوفير الثقة.

101- 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 بالضرورة مع الموافقة على معاملة المعلومات الشخصية بموجب قانون خصوصية البيانات وحمايتها.

102- 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 خدمات إدارة الهوية وتوفير الثقة على المشترك وعلى مقدمي الخدمات وعلى الطرف المعول. ويتماشى ذلك مع القاعدة العامة التي تقتضي بعدم إدخال أي تعديل على القانون الموضوعي.

103- علاوة على ذلك، تنفد المادة 3، بإيراد إشارة إلى أن القانون النموذجي لا يشترط استخدام أي خدمات محددة لإدارة الهوية أو لتوفير الثقة، مبادئ الحياد التكنولوجي، بما في ذلك ما يتعلق بحياد النماذج والنظم.

104- وقد يكون هناك التزام في قانون آخر باستخدام خدمات إدارة الهوية وتوفير الثقة، أو خدمة محددة من خدمات إدارة الهوية أو توفير الثقة. ويمكن فرض هذا الالتزام، مثلاً، 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؛ A/CN.9/1087، الفقرة 28.

#### 4- المادة 4- التفسير

105- 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).

106- وتهدف الفقرة 1 إلى تعزيز الأخذ بتفسير موحد عبر الولايات القضائية المشتعبة من خلال توجيه انتباه القضاة والهيئات القضائية الأخرى إلى أن التشريعات المحلية للقانون النموذجي ينبغي تفسيرها في ضوء أصلها الدولي والحاجة إلى توحيد التطبيق. ولذلك، يشجّع المحكم إليهم على مراعاة القرارات الصادرة عن ولايات قضائية أجنبية عند البت في القضايا بغية المساهمة في توحيد الاتجاهات التفسيرية الموحدة عبر الوطنية.

107- وتهدف الفقرة 2 إلى الحفاظ على الاتساق في تفسير وتطبيق تشريعات القانون النموذجي باشتراط أن تُسوّى المسائل التي لا تسويها أحكامه صراحة وفقاً للمبادئ العامة التي يقوم عليها القانون النموذجي، بدلاً من المبادئ الموجودة في القانون المحلي.

108- وعلى غرار سائر نصوص الأونسيترال التشريعية بشأن التجارة الإلكترونية، لا يحدد القانون النموذجي صراحة المبادئ العامة التي يقوم عليها. فالنصوص التشريعية للأونسيترال بشأن التجارة الإلكترونية تركز عموماً على مبادئ عدم التمييز ضد استخدام الوسائل الإلكترونية، والحياد التكنولوجي، والتكافؤ الوظيفي، واستقلالية الأطراف، وقد استبينت وجهة تلك المبادئ أيضاً فيما يخص القانون النموذجي، رهناً بما يُدخل عليه من تعديلات (انظر الفقرات 41-45 أعلاه). 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 القانون النموذجي التي لا يجوز للأطراف أن تبطلها. وعلاوة على ذلك، حسبما ذكر أعلاه (الفقرة 46)، قد لا يُطبّق 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

109- 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 صحتها أو وجود نفاذهما أو مقبوليتهما كدليل إثبات. ومن ثم، فهي 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.

110- 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.

111- وتنص الفقرة الفرعية (ب) على أن كَوْن خدمة إدارة الهوية خدمة غير معيّنة 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 توجي بأن أي خدمة من خدمات إدارة الهوية تستخدم 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.

112- وتؤكد الإشارة إلى الفقرة 3 من المادة 2 في فاتحة المادة 5 أن المادة 5 لا تمس بأي شرط قانوني يقضي بأن تحدّد 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 القانون النموذجي.

### 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

113- تنص المادة 6 على التزامات مقدمي خدمات إدارة الهوية. والالتزامات الواردة فيها هي الالتزامات الأساسية لمقدمي خدمات إدارة الهوية، التي يمكن استكمالها بالالتزامات قانونية أو تعاقدية إضافية. وتشير عبارة "كحد أدنى" الواردة في فاتحة المادة 6 إلى أنه لا يجوز لمقدم خدمات إدارة الهوية أن يحدد عن أداء هذه الالتزامات الأساسية وأنه يظل مسؤولاً تجاه المشتركين والأطراف المعولة أيضاً عندما يستعين بمتعاقدين في تقديم الخدمات. وقد يجيز عدم تنفيذ هذه الالتزامات الاحتجاج بالمسؤولية وفقاً للمادة 12 ويؤثر على موثوقية خدمات إدارة الهوية، بما في ذلك الخدمات المعيّنة.

114- وتوضّح الالتزامات الواردة في المادة 6 بطريقة محايدة تكنولوجياً بالنظر إلى أن تطبيق مبدأ الحياد التكنولوجي في سياق إدارة الهوية يستلزم متطلبات دنيا لنظم إدارة الهوية تتعلق بخصوصائص النظام وليس بتكنولوجيات محددة.

115- 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 تؤدي وظائف معينة بواسطة

كيانات أخرى مثل المتعاقدين أو مقدمي خدمات إدارة الهوية المتفردين في نظم إدارة الهوية المتعددة الأطراف من القطاع الخاص. وبناء عليه، تشير عبارة "كحد أدنى" الواردة في الفقرة الفرعية (أ) إلى أن مقدم خدمات إدارة الهوية ملزم بوضع قواعد وسياسات وممارسات تتناول اشتراطات أداء المهام المقررة. 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.

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

117- 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".

118- 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، وتنقذ من خلال الممارسات، وتُجسّد 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. وتهدف الإشارة إلى تيسير الاطلاع، الواردة أيضاً في البند (هـ)، إلى تسهيل الاطلاع على المعلومات للأطراف، مثل المنشآت الصغرى أو الصغيرة، التي قد تكون أقل دراية بالمسائل التقنية.

119- ويحدد البند (هـ) الالتزامات التي يجب أن يستوفيه مقدمو خدمات إدارة الهوية للحد من مسؤوليتهم تجاه الأطراف المعولة، مما يكمل المادة 12. وتهدف هذه الآلية إلى منع الصعوبات الناشئة عن اشتراط تحديد هوية جميع الأطراف المعولة المحتملة قبل تعويلها فعلاً.

120- وبالمثل، يكمل البند (و) المادة 8، بتحديد الالتزامات التي يجب أن يفي بها مقدمو خدمات إدارة الهوية فيما يتعلق بالالتزام المشترك بالإبلاغ عن الخروقات الأمنية.

### المراجع

A/CN.9/936، الفقرة 69؛ A/CN.9/1045، الفقرات 85-95؛ A/CN.9/1087، الفقرات 30-33 و55 و61.

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

121- 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. وتتنطبق 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 الخروقات الأمنية على نظم إدارة الهوية وخدمات إدارة الهوية على السواء، وقد تؤثر أيضاً على النعوت التي تدار في نظام إدارة الهوية.



122- 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 أيضا في قانون خصوصية البيانات وحمايتها.

123- ويُستخدَم مفهوم "التأثير الكبير" في القوانين الإقليمية<sup>(26)</sup> والوطنية. وقد تساهم عدة عوامل في تقييم هذا التأثير. وقد تساعد استمارات الإبلاغ عن الخروق في تقييم التأثير من خلال توضيح مدة تلك الخروق ونوع البيانات المتأثرة والنسبة المئوية للمشاركين المتأثرين والمعلومات الأخرى ذات الصلة. وتتوفر أيضاً مبادئ توجيهية تقنية للإبلاغ عن الحوادث، فضلاً عن التقارير السنوية عن الحوادث الأمنية التي تصدرها السلطات المعنية بخصوصية البيانات وحمايتها.

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

125- وتتص 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.

126- وتطبق 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.

127- 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 قوانين أخرى - أي قانون خصوصية البيانات وحمايتها - وفي الاتفاقات التعاقدية وفي القواعد والسياسات والممارسات التشغيلية لمقدم خدمات إدارة الهوية. وفي هذه الحالة، ينبغي تنفيذ جميع الإجراءات المذكورة، وليس مجرد الإخطار، وفقاً للقانون المنطبق.

#### المراجع

A/CN.9/971، الفقرات 84-87؛ A/CN.9/1005، الفقرات 32-36 و94؛ A/CN.9/1045، الفقرات 96-101؛ A/CN.9/1087، الفقرة 35.

#### 4- المادة 8- التزامات المشتركين

128- 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 بالخرق الأمنية (المادة 6 (و)) والتصدي للخرق الأمنية أو المساس بسلامة النظام (المادة 7).

129- 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 التي تحدد التزامات مقدمي 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. وعدم امتثال المشترك لالتزاماته بموجب المادة 8 لا يعفي بالضرورة مقدم خدمات إدارة الهوية من المسؤولية.

(26) المادة 19 (2) من لائحة الاتحاد الأوروبي بشأن تحديد الهوية إلكترونياً وخدمات توفير الثقة (eIDAS).

- 130- ويجوز أن يتضمن العقد المبرم بين المشترك ومقدم خدمات إدارة الهوية التزامات إضافية للمشارك. وقد يتضمن ذلك العقد أيضاً معلومات إضافية عن سبل الامتثال للالتزام بالإبلاغ الوارد في المادة 8.
- 131- وتشير الإشارة إلى "استخدام وسائل معقولة أخرى" إلى أن المشارك ليس محددًا باستخدام قنوات الإبلاغ التي يوفرها مقدم خدمات إدارة الهوية. ويشير مفهوم "التلاعب بإثباتات الهوية" إلى حالات الوصول غير المأذون به إلى إثباتات الهوية.
- 132- وتهدف الفقرة (ب) إلى تناول الحالات التي لا يكون فيها المشارك 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 الموقع، وتهدف إلى ضمان عدم فرض توقعات كبيرة على نحو غير معقول على المشاركين من حيث ما لهم من خبرة تقنية. ولا ينشأ الالتزام بالإبلاغ إلا في حال وجود ملايسات معلومة للمستعمل تثير شكوكاً مبررة بشأن ما إذا كانت إثباتات الهوية تعمل بشكل ملائم.

### المراجع

- A/CN.9/936، الفقرة 68؛ A/CN.9/971، الفقرات 88-96؛ A/CN.9/1005، الفقرات 37-43 و 95 و 96؛  
A/CN.9/1045، الفقرات 102-105؛ A/CN.9/1087، الفقرتان 36 و 37.

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

- 133- في نصوص الأونسيترال المتعلقة بالتجارة الإلكترونية، تحدد قواعد التكافؤ الوظيفي الشروط التي يجب أن تستوفيها السجلات أو الطرائق أو العمليات الإلكترونية للوفاء بشرط قانوني بوجود توافر مستندات ورقية. وتتص 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 عبر الإنترنت وبدونه، فإن المادة 9 لا تنطبق إلا إذا وُجد مكافئ لتحديد الهوية بدون اتصال عبر الإنترنت. ومع ذلك، تشكل المادة 9 أحد الأحكام الأساسية لإنشاء نظام قانوني لإدارة الهوية.
- 134- ويجب أن تتمثل الطريقة المستخدمة للوفاء بالقاعدة الواردة في المادة 9 للفقرة 1 من المادة 10، أي أن تكون موثوقاً بها بقدر مناسب للغرض الذي تُستخدم من أجله خدمة إدارة الهوية أو أثبتت فعلياً أنها أدت الوظيفة المنشودة من خلال استخدام الطريقة.
- 135- 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 تُفَعّل المادة 9 إلا بإيراد إشارة إلى مكافئ وظيفي.
- 136- وتشير المادة 9 إلى استخدام خدمات إدارة الهوية، للإشارة إلى أن اشتراطات التكافؤ تُستوفى باستخدام إثباتات الهوية، مقابل استخدام نظم إدارة الهوية أو الهوية نفسها.
- 137- 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 98 أعلاه).

138- 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.

139- وتشير المواد 9 ومن 16 إلى 21 من القانون النموذجي إلى حالات يشترط فيها القانون اتخاذ إجراء أو ينص على عواقب لعدم اتخاذ إجراء. وقد وُضعت 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 يصرح بها ويرتب عواقب قانونية على اتخاذها.

### 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؛ A/CN.9/1087، الفقرة 38.

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

140- تقدم المادة 10 إرشادات بشأن تقرير موثوقية الطريقة المستخدمة لتحديد الهوية في المادة 9 بعد أن تكون الطريقة قد استُخدمت (نهج التقرير اللاحق). وهو يشير إلى الطريقة المستخدمة في خدمة إدارة الهوية وليس إلى الطريقة المستخدمة في نظام إدارة الهوية، لأن نظاماً واحداً لإدارة الهوية يمكنه أن يدعم خدمات متعددة لإدارة الهوية تستخدم طرائق ذات مستويات مختلفة من الموثوقية.

141- وتطبق الفقرة 1 (أ) نهج التقرير اللاحق بالإشارة إلى استخدام طريقة "موثوق بها بقدر مناسب للغرض الذي تُستخدم 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.

142- 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 تُفعل 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 يلتزم بتحديد الهوية بإثباتات الهوية. ويستند هذا الحكم إلى المادة 9 (3) (ب) '2' من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية.

143- ويشترط القانون النموذجي عموماً 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 أنه يمكن، بموجب القانون النموذجي، تحديد الهوية واقعياً أو باستخدام طريقة موثوقة. وبعبارة أخرى، يستتبع تحقيق تحديد الهوية واقعياً الحاجة إلى التأكد من موثوقية الطريقة المستخدمة.

144- وتتضمن الفقرة 2 قائمة بالظروف، الموصوفة بعبارات محايدة تكنولوجياً، التي قد تكون ذات صلة بتقرير الموثوقية بواسطة المحكم 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. وإضافة إلى ذلك، قد لا تؤثر الاتفاقات التعاقدية على الأطراف الثالثة، ومن ثم لن تكون هذه الظروف ذات صلة عندما يتعلق الأمر بأطراف ثالثة.

145- وتتص 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 تيسير الاعتراف بخدمات إدارة الهوية عبر الحدود وهو مستوحى من المادة 12 (1) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، التي ترسي قاعدة عامة بعدم التمييز في تحديد الأثر القانوني للشهادة أو التوقيع الإلكتروني<sup>(27)</sup>.

146- ووفقاً للفقرة 4، يترتب على تعيين خدمة موثوقة من خدمات إدارة الهوية بموجب المادة 11 افتراضاً بموثوقية الطرائق التي تستخدمها خدمة إدارة الهوية المعيّنة. وهذا هو التمييز الوحيد بين خدمات إدارة الهوية المعيّنة وغير المعيّنة. وعلاوة على ذلك، وفقاً للفقرة الفرعية 5 (ب)، يجوز دحض افتراض الموثوقية الذي يُعَلَّق على التعيين.

147- وتوضح الفقرة 5 العلاقة بين المادتين 10 و 11 بالنص على أن وجود آلية للتعين لا يستبعد تطبيق التقرير اللاحق لموثوقية الطريقة. وهذا الحكم مستلهم من المادة 6 (4) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية.

#### (أ) إطار مستوى الضمان

148- تشير المادة 10 والمادة 11 إلى مفهوم "أطر مستوى الضمان" أو الأطر المماثلة المسماة بخلاف ذلك. ويوفر إطار مستوى الضمان توجيهات للأطراف المعولة بشأن درجة الثقة التي قد تضعها في عمليات تدقيق الهوية وتحديد الهوية إلكترونياً، وما إذا كانت تلك العمليات ملائمة لأغراض محددة. ولا يحدد القانون النموذجي مستويات الضمان ولا يشترط تعريفها أو استخدامها.

149- وتتوخى أطر الضمان مستويات مختلفة من الضمانات المرتبطة بالاشتراطات المختلفة. وبعبارة أخرى، توضح أطر مستويات الضمان الاشتراطات التي يجب أن تستوفيها نظم وخدمات إدارة الهوية لتوفير مستوى معين من الضمان في موثوقيتها. وينبغي توضيح مستويات الضمانات بعبارات عامة للحفاظ على الحياد التكنولوجي.

150- ويمكن استخدام أطر الضمان لتلبية حاجة السوق إلى التوجيه بشأن مدى جدارة خدمة إدارة الهوية المقدمّة بالثقة. ويمكن اعتبار مقدم خدمات إدارة الهوية الذي لا يدرج أي إشارة إلى مستويات الضمان في قواعده وسياساته وممارساته التشغيلية أنه يقدم خدمات بأقل مستوى من الضمان. إلا أنه ربما لم يُتَقَّ بعد على تعريف مقبول عالمياً لإطار مستوى الضمان، وقد يتعين استخدام تعاريف وطنية أو إقليمية مختلفة.

151- وفي المقابل، يمكن صياغة اشتراط توفير مستوى معين من الضمان لموثوقية الهويات المستخدمة بإيراد إشارة إلى المستويات المبينة في إطار مستوى الضمان. ويمكن عندئذ حصر النظم والخدمات المحددة لإدارة الهوية مقابل الاشتراطات التي يقتضيها مستوى الضمان المطلوب. والمطابقة الناجحة بين خدمة إدارة

(27) للاطلاع على مناقشات بشأن التفاعل بين المادتين 12 (1) و 12 (2) من القانون النموذجي بشأن التوقيعات الإلكترونية، انظر الوثيقة A/CN.9/483، الفقرات 28-36.

الهوية والاشتراطات المقترنة بذلك المستوى من الضمان تؤدي إلى إمكانية استخدام خدمة إدارة الهوية تلك، لذلك النوع من المعاملة تحديداً.

## (ب) التصديق والإشراف

152- تذكر المادة 10 من ضمن الظروف التي يحتمل أن تكون ذات صلة، وجود "إجراءات للإشراف أو التصديق فيما يتعلق بخدمة إدارة الهوية"، إن وجدت. وقد يساعد التصديق والإشراف بشكل كبير في ترسيخ الثقة في مقدمي خدمات إدارة الهوية وخدماتهم، لأغراض من بينها تقرير موثوقية الطريقة المستخدمة، لأنهما (أي التصديق والإشراف) يرتبطان بمستوى معين من الموضوعية في تقييم موثوقية الطريقة المستخدمة. 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.

153- وتشمل خيارات 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 ستترب عليه آثار مختلفة.

154- 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.

155- وتوجد نهج مختلفة فيما يتعلق بإشراك السلطات العامة في التصديق والإشراف، وهو قرار سياساتي يخص الولاية القضائية المشترعة. فحين تكون الكيانات العامة جهات تصديق أو إشراف ومقدمة لخدمات إدارة الهوية في الوقت نفسه، يمكن فصل مهام التصديق والإشراف عن تقديم خدمات إدارة الهوية.

156- ولا يوجب القانون النموذجي إنشاء نظام إشرافي أو يبسر ذلك. ويستند النهج المتبع في القانون النموذجي إلى الحياد النموذجي، ولا تستبعد الإشارات إلى التصديق والإشراف نظم التصديق الذاتي.

157- وفي بعض الحالات، مثل الحالات التي تُستخدم فيها أنواع معينة من تكنولوجيا الدفاتر الموزعة، 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.9/1087، الفقرات 42-46 و105 و106؛ A/CN.9/WG.IV/WP.153، الفقرتان 74 و75.

## 7- المادة 11- تعيين خدمات إدارة الهوية الموثوقة

158- تكمل المادة 11 المادة 10 بتوفير إمكانية تعيين خدمات إدارة الهوية. وبعبارة أدق، فهي تورد الشروط التي يجب أن تستوفيها خدمة إدارة الهوية حتى تُدرج في قائمة خدمات إدارة الهوية المعيّنة. وتشير المادة 11، شأنها شأن المادة 10، إلى الطريقة المستخدمة في خدمة إدارة الهوية، وليس إلى الطريقة المستخدمة في نظام

إدارة الهوية، لأن نظاماً واحداً لإدارة الهوية يمكنه أن يدعم خدمات متعددة لإدارة الهوية لديها مستويات مختلفة من الموثوقية، ومن ثم، قد يكون معيّنًا أو غير معيّن.

159- ويستند تعيين خدمات 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 قدرًا من الاتساق بين الطرائق التي تعيّن موثوقيتها مسبقاً والطرائق التي تعيّن موثوقيتها لاحقاً. وعلاوة على ذلك، يراعى في أي تعيين "الاتساق مع المعايير والإجراءات الدولية المعترف بها ذات الصلة بتنفيذ عملية التعيين" من أجل تعزيز الاعتراف القانوني عبر الحدود وقابلية التشغيل المتبادل.

160- وثمة أهمية بالغة لنشر المعلومات المتعلقة بخدمات إدارة الهوية المعيّنة لإعلام المشتركين المحتملين بوجودها. فالكيان القائم بالتعيين عليه التزام بنشر قائمة بخدمات إدارة الهوية المعيّنة، بما في ذلك تفاصيل مقدم خدمة إدارة الهوية، على موقعه الشبكي مثلاً. ويُسلّم 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. ويجوز استخدام طرائق أخرى لإعلام الجمهور بخدمات إدارة الهوية المعينة، ولكن تلك الطرائق ينبغي أن تكون مكتملة لعملية نشر القائمة بدلاً من أن تحل محلها.

161- 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.

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

## 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؛ A/CN.9/1087، الفقرات 47-49.

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

163- تحدد المادة 12، حسبما أشير إليه (الفقرة 68 أعلاه)، نظاماً موحداً للمسؤولية يستند إلى مبدأ أن يكون مقدم خدمات إدارة الهوية مسؤولاً عن عواقب عدم تقديم الخدمات للمشاركين والأطراف المعولة. ويتمثل هدفها في الاعتراف بإمكانية مساءلة مقدم الخدمات عن عدم الامتثال لالتزاماته المقررة بموجب القانون النموذجي بغض النظر عما إذا كان لتلك الالتزامات أساس تعاقدية. وينطبق هذا الحكم بغض النظر عن الطبيعة العامة أو الخاصة لمقدم خدمات إدارة الهوية.

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

165- وطبيعة المسؤولية بموجب المادة 12 طبيعة قانونية، وهي تطبق، من هذا المنطلق، جنباً إلى جنب مع المسؤولية التعاقدية وغير التعاقدية. وبناء عليه، فإن تطبيق الأحكام المتعلقة بالمسؤولية التعاقدية وغير التعاقدية ذات الصلة بمقدمي خدمات إدارة الهوية والمنصوص عليها في القانون الداخلي لا يتأثر بالمادة 12، حسبما هو مبين في الفقرة 2 (أ).

166- وقد تنشأ مسؤولية مقدمي خدمات إدارة الهوية من استخدام خدمات إدارة الهوية المعيّنة وغير المعيّنة. 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.

167- وتترك 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.

168- وتقر المادة 12 بإمكانية الحد من المسؤولية في ظل شروط معينة. وقد تكون القيود المفروضة على المسؤولية ضرورية لاحتواء تكلفة التأمين، ضمن أمور أخرى، وهي تجسّد عادة في القواعد والسياسات والممارسات التشغيلية لمقدم الخدمة. وتقر المادة 12 أيضاً بقيام مقدمي خدمات إدارة الهوية، في الممارسة العملية، بالحد من مسؤوليتهم بشكل مختلف تبعاً للطرف المعني (أي ما إذا كان مشتركاً أو طرفاً معوّلاً) ولنوع الخدمة (مثلاً، حسب ارتفاع أو انخفاض قيم المعاملات). وهي لا تؤثر على قدرة مقدم خدمات إدارة الهوية على الاعتماد على قوانين أخرى من أجل تفعيل حد أقصى للمسؤولية ما دام يمثل لالتزاماته بموجب القانون النموذجي، بما فيها الالتزامات ذات الصلة بالحد من المسؤولية.

169- وفيما يتعلق بالمشترك، تسمح الفقرة 3 بالحد من مسؤولية مقدم خدمات إدارة الهوية بموجب شرطين. أولاً، أن يتجاوز استخدام خدمة إدارة الهوية القيود المفروضة على الغرض من المعاملة أو قيمتها وعلى حجم المسؤولية المنطبق على المعاملة التي تستخدم خدمة إدارة الهوية من أجلها. وثانياً، أن ترد تلك القيود في الترتيب المبرم بين مقدم خدمات إدارة الهوية والمشترك. وتماشياً مع تعريف "المشارك"، تهدف الإشارة إلى "الترتيب" إلى استيعاب جميع أنواع العلاقات القائمة بين مقدم خدمات إدارة الهوية والمشترك، ذات الطبيعة التعاقدية أو غيرها.

170- وبالمثل، تسمح الفقرة 4 بالحد من مسؤولية مقدم خدمات إدارة الهوية تجاه الطرف المعول بموجب شرطين. أولاً، أن يتجاوز استخدام خدمة إدارة الهوية القيود المفروضة على الغرض من المعاملة أو قيمتها وعلى حجم المسؤولية المنطبق على المعاملة التي تستخدم خدمة إدارة الهوية من أجلها. ثانياً، أن يمثل مقدم خدمات إدارة الهوية لالتزاماته بموجب المادة 6 (هـ) المتعلقة بتسهيل اطلاع الأطراف المعولة على القيود المفروضة على المعاملة المحددة.

171- ولا تتناول المادة 12 سوى مسؤولية مقدمي خدمات إدارة الهوية تجاه المشتركين والأطراف المعولة. ولأي طرف آخر 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 للمشارك عندئذ أن يقدم مطالبة ضد مقدم خدمات إدارة الهوية.

172- وتطبق 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؛  
A/CN.9/1087، الفقرات 52-73.

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

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

173- 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.

174- وتطبق المادة 13 على خدمات توفير الثقة بصرف النظر عما إذا كانت مسماة في القانون النموذجي 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

175- تحدد المادة 14 الالتزامات الأساسية لمقدمي خدمات توفير الثقة بغض النظر عما إذا كانت خدمة توفير الثقة المقدمة 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. وعلى غرار المادة 7 (1)، تنفذ جميع الالتزامات الواردة في المادة 14 (2) وفقاً للقانون المنطبق، إن وجد.

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

177- ويجسد الالتزام بتسهيل اطلاع الأطراف الثالثة أيضاً على السياسات والممارسات، الممارسة القائمة التي تعترف بأن هذه المعلومات لها أهميتها لدى الطرف المعول في تقرير ما إذا كان سيقبل النتيجة المستمدة من استخدام خدمة توفير الثقة، بما يتماشى مع مبدأ الاستخدام الطوعي لخدمات توفير الثقة (المادة 3 (1)).

178- وتنشئ الفقرة الفرعية (1) (هـ) آلية لإعلام الأطراف المعولة بالقيود المفروضة على الغرض الذي يجوز أن تستخدم خدمة توفير الثقة من أجله أو قيمتها، وبالقيود المفروضة على نطاق المسؤولية أو مداها، على غرار ما ورد في المادة 6 (هـ) وبما يكمل المادة 24.

179- وتنص الفقرة 2 على التزامات مقدمي خدمات توفير الثقة في حال خرق البيانات. وهي تفترض مسبقاً وقوع خرق أمني للنظام أو مساس بسلامته من شأنه أن يؤثر تأثيراً كبيراً على خدمة توفير الثقة.



## المراجع

A/CN.9/971، الفقرتان 152 و153؛ A/CN.9/1005، الفقرات 28-36 و73؛ A/CN.9/1045، الفقرات 18-21 و57؛ A/CN.9/1087، الفقرات 74-76.

## 3- المادة 15- التزامات المشتركين

180- تحدد المادة 15 التزامات المشتركين في حالة وقوع تلاعب بخدمة توفير الثقة. ويشير مفهوم "التلاعب بخدمة توفير الثقة" إلى حالات الوصول غير المأذون به إلى خدمة توفير الثقة، وهو يفترض مسبقاً وقوع حادث يؤثر في موثوقية خدمة توفير الثقة.

181- وتتعرف المادة 15 بأنه من غير المرجح أن يعلم المشترك فوراً بالمسائل التي تؤثر على خدمة توفير الثقة ككل، ولكنه قد يكون على علم بوقوع تلاعب بالمعلومات المرئية وقد يكون على علم بالمخاطر التي قد تمس بمعلومات غير مرئية مباشرةً للمشتري، مثل المفتاح الخاص. ولهذا السبب، فإن الفقرتين (أ) و(ب) لهما هدفان مختلفان.

182- ويورد عادة العقد المبرم بين مقدم خدمات توفير الثقة والمشتري تفاصيل عن سبل الامتثال للالتزامات الواردة في المادة 15. وعادة ما تشير هذه الاتفاقات التعاقدية إلى القواعد والسياسات والممارسات التشغيلية لمقدم خدمات توفير الثقة.

183- ولا يحدد القانون النموذجي التزامات إضافية للمشتري 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.

184- ولا يتضمن القانون النموذجي قواعد للمسؤولية خاصة بالمشتريين. ولذلك، فإن مسؤولية المشتري تقرر بالأحكام التعاقدية، التي قد تحدد التزامات إضافية للمشتريين، وبقواعد المسؤولية العامة.

185- وخلافاً للمادة 11 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، لا تنص المادة 15 على التزامات الأطراف المعولة التي يمكن أن تكون مسؤولة بموجب قانون آخر.

## المراجع

A/CN.9/1005، الفقرات 37-43؛ A/CN.9/1045، الفقرات 22-26؛ A/CN.9/1087، الفقرتان 77 و78.

## 4- المادة 16- التوقيعات الإلكترونية

186- تتناول المادة 16 التوقيعات الإلكترونية. وتتضمن كافة النصوص التشريعية للأونسيترال بشأن التجارة الإلكترونية أحكاماً بشأن استخدام التوقيعات الإلكترونية يُمكن للأشخاص الطبيعيين أو الاعتباريين، على السواء، الأخذ بها<sup>(28)</sup>. وصياغة المادة 16 مستلهمة من صياغة المادة 9 من قانون الأونسيترال النموذجي بشأن السجلات الإلكترونية القابلة للتحويل، التي تأخذ دورها في الاعتبار صيغة المادة 9 (3) من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية، وهي تترسي الاشتراطات بشأن التكافؤ الوظيفي بين التوقيعات اليدوية والتوقيعات الإلكترونية. وبناءً عليه، ينبغي تفسير مصطلح "تحديد الهوية" الوارد في المادة 16 بما يتماشى مع المعنى المستقر في أحكام الأونسيترال المماثلة واشتراطاتها.

(28) انظر أيضاً بشكل عام وثيقة تعزيز الثقة بالتجارة الإلكترونية.

- 187- ويُستوفى اشتراط التوقيع الورقي إذا استخدمت طريقة لتحديد هوية الموقع على رسالة البيانات وبيان نية الموقع فيما يتعلق برسالة البيانات الموقعة. وتطبق الإشارة إلى استخدام طريقة "فيما يتعلق بالمعلومات الواردة في رسالة البيانات" على تحديد هوية الشخص وعلى بيان نية الشخص، كليهما.
- 188- 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<sup>(29)</sup>.

### 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؛ A/CN.9/1087، الفقرات 82-84.

### 5- المادة 17- الأختام الإلكترونية

- 189- 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. ويُجسّد 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.

- 190- والمادة 17 مستوحاة من التشريعات الإقليمية، التي تنص على أن "الأختام الإلكترونية يمكن أن تُستخدم للتوثق من أي موجود رقمي من موجودات الشخص الاعتباري، مثل شهادات البرامج الحاسوبية أو الخوادم، بالإضافة إلى التوثق 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).

- 191- 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 الموقع، وعادة ما اشترعت أحكام الأونسيترال بشأن التوقيعات الإلكترونية لتطبق على الأشخاص الطبيعيين والاعتباريين على السواء.

- 192- 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.

- 193- 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

(29) قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، دليل الاشتراع، الفقرات 29-62؛ تعزيز الثقة بالتجارة الإلكترونية، الفقرات 24-66.

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

194- 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؛ A/CN.9/1087، الفقرتان 85 و86.

### 6- المادة 18- أختام الوقت الإلكترونية

195- 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 كافٍ من الثقة. فعلى سبيل المثال، قد يلزم إثبات تاريخ إبرام عقد ما حتى تتمكن أطراف ثالثة من الطعن فيه.

196- 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.

197- 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

198- 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 تتوفر 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).

199- والمادة 19 مستلهمة من مواد 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 المقدّمة بذلك الشرط (أي الأرشفة الإلكترونية).

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

201- 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. وتستوعب الفقرة (ج) 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.

202- ولا تتناول المادة 19 مسألة ما إذا كان ينبغي أن تكون السجلات الإلكترونية المحفوظة قابلة للنقل بحيث يمكن الوصول إليها على الرغم من التقدم 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 المسجّل الإلكتروني

203- توفر المادة 20 ضماناً لإرسال خطاب إلكتروني بواسطة المرسل ولتلقّي المرسل إليه له، ولوقت حدوث الإرسال والاستلام، وسلامة البيانات المتبادلة، وهوية المرسل والمتلقّي.

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

205- ولا تشير المادة 20 إلى مفاهيم مستخدمة في نصوص الأونسيترال السابقة مثل "الإرسال" و"التلقّي" (انظر المادة 10 من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية) لأنها صيغت بالتركيز على التكافؤ الوظيفي بين خدمات البريد المسجّل وخدمات التوصيل المسجّل 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- التوثيق من المواقع الشبكية

206- تتناول المادة 21 التوثيق 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 التوثيق من المواقع الشبكية من عنصرين هما: تحديد هوية حائز اسم النطاق الخاص بالموقع الشبكي، وربط ذلك الشخص بالموقع الشبكي. ولا يهدف التوثيق من المواقع الشبكية إلى تحديد هوية الموقع الشبكي.

- 207- والمادة 21 ليست قاعدة للتكافؤ الوظيفي بالنظر إلى أن أي موقع شبكي لا وجود له إلا في شكل إلكتروني، ومن ثم فإن التوثيق من المواقع الشبكية ليس له مكافئ بدون اتصال عبر الإنترنت.
- 208- ويشير مصطلح "حائز اسم النطاق" إلى الأشخاص الذين خصّصت 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.
- 209- 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 التوثيق 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

- 210- تتضمن المادة 22 قائمة غير حصرية بالظروف التي قد تكون ذات وجهة 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.
- 211- وعلى غرار مفهوم الطريقة الموثوقة المستخدمة لخدمات إدارة الهوية (انظر الفقرة 141 أعلاه)، يعد مفهوم الطريقة الموثوقة المستخدمة في خدمات توفير الثقة مفهوماً نسبياً ويختلف باختلاف الغرض المطلوب أداءه. ويجسّد الطابع النسبي للموثوقية في الفقرة الفرعية 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

- 212- يميز قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية وعدد من القوانين الإقليمية والوطنية 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 تعيّن توقيعات إلكترونية إلا التي توفر مستوى أعلى من الموثوقية. ولم يُتبع هذا النهج في القانون النموذجي ويمكن تعيين خدمات توفير الثقة بغض النظر عن مستوى الموثوقية التي تقدمها.
- 213- 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؛ A/CN.9/1087، الفقرات 87 و105 و106.

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

214- تكمل المادة 23 المادة 22 بإتاحة تعيين خدمات توفير الثقة وفقاً لنهج التقرير المسبق للموثوقية. وبعبارة أدق، فهي تورد الشروط التي يجب أن تستوفيها خدمة توفير الثقة حتى تُدرج في قائمة خدمات توفير الثقة المعيّنة التي يُفترض أنها موثوقة لأغراض المواد من 16 إلى 21.

215- 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 يُفترض 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 مقدّم خدمات محدد.

216- 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 التقرير اللاحق لموثوقية الطريقة.

217- وتلزم المادة 23 السلطة القائمة بالتعيين بأن تنشر قائمة بخدمات توفير الثقة المعيّنة، 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 مقدّم خدمات توفير الثقة

218- كمبدأ عام، ينبغي تحميل مقدّم 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 المقدمة، لتقرير مدى تلك المسؤولية.

219- وتصاغ المادة 24 على غرار المادة 12، بشأن مسؤولية مقدمي خدمات إدارة الهوية، ومن ثم قد تنطبق أيضاً الاعتبارات المرعية في إطار المادة 12 على المادة 24. وعلى وجه الخصوص، ترسي المادة 24، مثل المادة 12، أساساً قانونياً للمسؤولية يعمل جنباً إلى جنب مع المسؤولية التعاقدية وغير التعاقدية، ولا يتأثر تطبيق أحكام القانون الداخلي المتعلقة بالمسؤولية التعاقدية وغير التعاقدية ذات الصلة بمقدمي خدمات توفير الثقة بالمادة 24، على النحو المبين في الفقرة 2 (أ).

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

221- ومن بين نصوص الأونسيترال السابقة، يتضمن قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية أحكاماً تتناول العواقب القانونية الناشئة عن سلوك الموقع (المادة 8) ومقدم خدمة التصديق (المادة 9) والطرف المعول (المادة 11). وتحدد هذه الأحكام التزامات كل كيان يشارك في دورة حياة التوقيع الإلكتروني. وعلاوة على ذلك، يسلم قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية بإمكانية أن يحد مقدمو خدمات التصديق من نطاق أو مدى مسؤوليتهم<sup>(30)</sup>.

### المراجع

A/CN.9/1005، الفقرات 74-76؛ A/CN.9/1045، الفقرات 62-66؛ A/CN.9/1087، الفقرة 89.

## دال - الفصل الرابع - الجوانب الدولية (المواد من 25 إلى 27)

### 1- المادة 25- الاعتراف عبر الحدود بتحديد الهوية إلكترونياً

222- تنص المادة 25 على آلية للاعتراف القانوني عبر الحدود بتحديد الهوية إلكترونياً، تهدف إلى منح المعاملة القانونية المتماثلة لنظم إدارة الهوية وخدمات إدارة الهوية وإثباتات الهوية، المحلية والأجنبية. وهي تستند إلى مبدأ عدم التمييز ضد المنشأ الجغرافي وتركز على تحديد الهوية إلكترونياً نتيجة لاستخدام نظم إدارة الهوية وخدمات إدارة الهوية وإثباتات الهوية.

223- ويتمثل أحد أهداف المادة 25 في الحد من حاجة مقدمي الخدمات إلى تقديم طلب لاقتناء صفة الخدمات المعينة بموجب المادة 23 في ولايات قضائية متعددة. 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.

224- وقد لا يوجد اتساق تام بين الولايات القضائية المختلفة بشأن تعريف مستوى الموثوقية. وعدم الاتساق هذا وضعٌ محتمل نظراً لعدم وجود تعاريف متفق عليها عالمياً لمستويات محددة من الموثوقية. وللتغلب على التحديات التي تواجه الاعتراف عبر الحدود الناشئة عن عدم الاتساق، تشير المادة 25 إلى مفهوم "مستوى مكافئ على الأقل من الموثوقية"، الذي يشمل مستويات من الموثوقية ماثلة أو أعلى من المستوى المطلوب. وينبغي ألا يفسر هذا المفهوم على أنه إلزام بالامتثال لاشتراطات تقنية صارمة، مما قد يؤدي إلى إيجاد عقبات في سبيل الاعتراف المتبادل، وفي نهاية المطاف، في سبيل التجارة.

225- 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 بتحديد الهوية إلكترونياً. ومن الناحية العملية، قد يكون من الأفضل التركيز على خدمة محددة 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 واحدة منها أو أكثر تقدم مستوى أقل من الموثوقية. وعلاوة على ذلك، ينبغي للاعتراف بإثباتات الهوية أن يتجنب تلك الإثباتات التي بقيت دون تغيير على الرغم من وقوع تلاعب في خدمة إدارة الهوية المستخدمة لإصدارها.

(30) للاطلاع على مناقشة حالات محددة للمسؤولية في إطار مرافق المفاتيح العمومية، انظر تعزيز الثقة بالتجارة الإلكترونية، الفقرات 211-232.

226- وقد يقتضي الاعتراف بنظم وخدمات إدارة الهوية وإثباتات الهوية الأجنبية من مقدم الخدمة أن يعدّل شروط خدماته. فعلى سبيل المثال، قد يؤثر القانون الإلزامي للولاية القضائية المعترفة على قدرة مقدم الخدمة على الحد من المسؤولية.

227- وتوضح الفقرة 3 كذلك كيف يمكن لسلطات التعيين أن تعيّن خدمات إدارة الهوية وتوفير الثقة الأجنبية. وهي تتوسع في تبيان الآلية المنصوص عليها في المادة 11 (4)، التي تنص 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، ويتضمن نظم إدارة الهوية وإثباتات الهوية كمجالات محتملة للتعين. ولذلك فإن الفقرة 3 تنفذ نهج التقرير المسبق للموثوقية.

228- وينبغي للسلطة المختصة، لدى تقرير التكافؤ، أن تأخذ في الاعتبار قائمة الظروف ذات الصلة بتقرير موثوقية الطرائق المستخدمة في خدمات إدارة الهوية الواردة في المادة 10 (2) لضمان الاتساق في تقرير الموثوقية.

229- وعملية تقرير موثوقية خدمة إدارة الهوية أو نظام إدارة الهوية أو إثباتات الهوية عملية تستغرق وقتاً طويلاً وتستهلك موارد كثيفة، وقد لا تتوافر لدى جميع الولايات القضائية موارد كافية. وقد تستفيد تلك الولايات القضائية ذات الموارد المنخفضة بشكل خاص من إمكانية الاعتراف بخدمات ونظم إدارة الهوية وإثباتات الهوية الأجنبية بالاعتماد على عمليات تقرير الموثوقية والتعيينات الأجنبية. ويمكن أيضاً للآليات التي تستند إلى الفقرة 3 أن تحل محل الترتيبات القائمة على إبرام اتفاقات مخصصة للاعتراف المتبادل بين الهيئات الإشرافية.

230- 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 التي تعينها السلطة الأجنبية بمركز قانوني بوصفها خدمات معيّنة في الولاية المشترعة)، أو في شكل افتراض (على سبيل المثال، أن تُفترض في الولاية القضائية المشترعة موثوقية خدمات إدارة الهوية التي تعينها السلطة الأجنبية، ولكن لا يكون لها مركز قانوني بوصفها خدمات معيّنة في تلك الولاية القضائية دون أن تتخذ سلطة التعيين إجراءات أخرى في هذا الصدد).

#### 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؛ A/CN.9/1087، الفقرات 90-101.

#### 2- المادة 26- الاعتراف عبر الحدود بنتيجة استخدام خدمات توفير الثقة

231- تنص المادة 26 على آلية للاعتراف عبر الحدود بنتيجة استخدام خدمات توفير الثقة تماثل تلك المنصوص عليها في المادة 25 لتحديد الهوية إلكترونياً. وبناء عليه، يجوز أن تنطبق الاعتبارات المرعية في إطار المادة 25 على المادة 26.

232- وتتوافق المادة 26 عموماً مع استخدام الآليات القائمة للاعتراف عبر الحدود بنتيجة استخدام خدمات توفير الثقة، مثل الاعتراف المتبادل والتصديق المتبادل بين مرافق المفاتيح العمومية<sup>(31)</sup>.

#### المراجع

A/CN.9/1087، الفقرات 90-101.

(31) لمزيد من المعلومات بشأن الاعتراف المتبادل والتصديق المتبادل، انظر تعزيز الثقة بالتجارة الإلكترونية، الفقرات 163-172.



## 3- المادة 27- التعاون

233- قد تسهم آليات التعاون المؤسسي إسهاماً كبيراً 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.

234- وعلاوة على ذلك، قد تيسر المادة 27 الاتفاق على وضع تعاريف مشتركة للمعايير التقنية، بما في ذلك مستويات الضمان ومستويات الموثوقية، لدعم تقرير التكافؤ. وفي الممارسة التجارية، يُستخدم مفهوم مستوى الضمان ومستوى الموثوقية كمصطلحين فنيين، على التوالي، لتقييم خدمات إدارة الهوية وتوفير الثقة. ولا يضع القانون النموذجي 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.

235- وينبغي أن يكون التعاون على أساس طوعي وبما يتماشى مع القوانين واللوائح الوطنية المنطبقة. وتهدف الإشارة إلى "الكيانات الأجنبية" إلى استيعاب جميع الكيانات، بصرف النظر عن طبيعتها القانونية، التي قد تسهم في تحقيق الأهداف المتوخاة.

## 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؛ A/CN.9/1087، الفقرتان 108 و109.