الأمم المتحدة
A/CN.9/WG.IV/WP.163
الجمعية العامة
Distr.: Limited
20 February 2020
Arabic
Original: English

لجنة الأمم المتحدة للقانون التجاري الدولي
الفريق العامل الرابع (المعني بالتجارة الإلكترونية)
الدورة الستون
نيويورك، ٦-٩ نيسان/أبريل ٢٠٢٠

مشاريع أحكام بشأن استخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود

مقترح مقدَّم من البنك الدولي

مذكِّرة من الأمانة

قدَّم البنك الدولي إلى الفريق العامل ورقة لينظر فيها أثناء دورته الستين. وهي ترد في مرفق هذه المذكِّرة بالصيغة التي تلقتها بها الأمانة.

130320 130320 V.20-01480 (A)

المرفق

تعليقات البنك الدولي بشأن الوثيقة WP.162

يسُـــر البنك الدولي أن يقدم التعليقات التالية على الوثيقة A/CN.9/AG.IV/WP.162، المعنونة "مشـاريع أحكام بشـأن اسـتخدام خدمات إدارة الهوية وتوفير الثقة والاعتراف بها عبر الحدود" ("مشاريع الأحكام")، بمناسبة اجتماع الفريق العامل في نيويورك في الفترة من ٦ إلى ٩ نيسان/أبريل ٢٠٢٠.

أولاً- تعليقات وملاحظات عامة أساسية

١- التركيز على إدارة الهوية: بصفة عامة، يدعم البنك الدولي أعمال الفريق العامل الرابع، وبخاصة تلك المتعلقة بإدارة الهوية. ونظرا إلى أن مجال الاهتمام الرئيسي للبنك الدولي هو إدارة الهوية، تركز التعليقات التالية على الأقسام المتعلقة بإدارة الهوية في مشاريع الأحكام.

٢- نظم إدارة الهوية مقابل معاملات الهوية: تركز مشـــاريع الأحكام في المقام الأول على نظم إدارة الهوية ومقدِّمي خدمات إدارة الهوية، وليس على معاملات الهوية. ونظرا لأهمية معاملات الهوية، ولا سـيما من منظور الامتثال القانوني والاعتراف القانوني، ولأن معاملات الهوية الإلكترونية يمكن أن تجرى دون اسـتخدام نظام لإدارة الهوية أو مقدِّم لخدمات إدارة الهوية، وهو ما يحدث عادة، ينبغي للفريق العامل النظر في مواصـلة تناول المسـائل المتعلقة بمعاملات الهوية.

٣- الأدوار: تركز مشـاريع الأحكام في المقام الأول على تنظيم نظم إدارة الهوية ومقدِّمي خدمات إدارة الهوية، ولا تتناول على نحو فعلي احتياجات الأطراف المعوِّلة أو الكيانات أو المشاركين المحتملين الآخرين في نظم إدارة الهوية أو معاملات الهوية (فيما عدا المادتين ٥ و٨). فعلى سـبيل المثال، لا تتناول مشـاريع الأحكام حق الطرف المعوِّل في اسـتخدام طرف ثالث للتحقُّق من الهوية حيثما يشترط القانون على الطرف المعوِّل التحقُّق من الهوية. وكما هو الحال بالنسبة لمعاملات الهوية، ينبغي للفريق العامل النظر في زيادة التركيز على المسائل التي تؤثر على أدوار بخلاف دور مقدِّمي الخدمة في سياق نظم إدارة الهوية.

٤- العلاقة بين نظم إدارة الهوية التابعة للقطاع العام وتلك التابعة للقطاع الخاص: تركز مشـاريع الأحكام على نظم إدارة الهوية ومقدِّمي خدمات إدارة الهوية التابعين للقطاع الخاص. ومن الناحية الشـكلية، لا تنطبق مشـاريع الأحكام على نظم إدارة الهوية أو مقدِّمي خدمات إدارة الهوية التابعين للقطاع العام، مثل النُّظُم الوطنية لإدارة الهوية. ولأن الحكومات تدير العديد من النُّظُم الوطنية لإدارة الهوية (على سـبيل المثال في الهند وإسـتونيا وغيرهما)، فإنها تقع بالتالي خارج نطاق نِتاج العمل المتوخى في مشاريع الأحكام.

ومع ذلك، من المهم التسـليم بأن من المرجح وجود تفاعل كبير بين نظم إدارة الهوية التابعة للقطاع العام وتلك التابعة للقطاع الخاص. فعلى سبيل المثال، يُفترض أن تنطبق مشاريع الأحكام إذا كانت هيئة حكومية هي الزبون (على سـبيل المثال كطرف معوِّل أو الكيان موضـوع البيانات) لمقدِّم

خدمات من القطاع الخاص، أو كانت تعوِّل على نظام موحد لإدارة الهوية تابع للقطاع الخاص بدلاً من نظام تديره الحكومة. وبالإضافة إلى ذلك، تعتمد عمليات تدقيق الهوية والتوثُّق منها التي يستخدمها مقدِّمو خدمات إدارة الهوية التابعون للقطاع الخاص في كثير من الأحيان على إثباتات الهوية التأسيسية الصادرة عن النُّظُم الحكومية، والتي غالباً ما تُعتبر مصدراً موثوقاً يمكن التعويل عليه بشدة.

وبالتالي، ينبغي للفريق العامل فحص طبيعة العلاقة بين نظم إدارة الهوية التابعة للقطاع العام وتلك التابعة للقطاع الخاص، وتوضيح تلك العلاقة، بما يشمل على سبيل المثال لا الحصر تناول متى يكون من الملائم لنظم إدارة الهوية التابعة للقطاع الخاص أن تستفيد من المعلومات الخاصة بالهوية التأسيسية وعمليات التوثُّق منها التي توفرها الحكومات، و/أو كيفية الاستفادة من تلك المعلومات والعمليات. وقد يشمل ذلك، على سبيل المثال، النظر في قواعد تتعلق بنظام إدارة الهوية التابع للقطاع الخاص، منها:

- استخدام أرقام الهوية أو غيرها من معلومات تعريف الهوية الصادرة عن الحكومة
- استخدام إثباتات الهوية الصادرة عن الحكومة
- الوصول إلى قواعد البيانات الحكومية الخاصة بعمليات تدقيق الهوية والتوثُّق منها
- الاعتماد عموما على المعلومات أو العمليات التي توفرها الحكومة

٥- أُطر توفير الثقة: لا تتناول مشاريع الأحكام دور القواعد التعاقدية لفرادى نظم إدارة الهوية، والتي غالباً ما يشار إليها بأُطر توفير الثقة، أو القواعد الخاصة بالنُّظم، أو القواعد الخاصة بالمخططات (ويشار إليها مجتمعة في هذه الوثيقة بعبارة "أُطر توفير الثقة")، وكيفية تفاعلها مع مشاريع الأحكام.[(١)] وينبغي للفريق العامل النظر في تنقيح مشاريع الأحكام لتوضيح العلاقة بين مشاريع الأحكام وأُطر توفير الثقة المعنية بإدارة الهوية، وتوضيح المسائل التي ينبغي لمشاريع الأحكام تناولها ومستوى تفصيلها، بدلاً من تناول فرادى أُطر توفير الثقة الخاصة بنظم إدارة الهوية. فعلى سبيل المثال، كثيراً ما يجري تناول مسائل مثل التزامات المشاركين والموثوقية ومستويات الضمان في إطار توفير الثقة الفريد لنظام واحد لإدارة الهوية.

وبالمثل، ينبغي للفريق العامل النظر في تناول مسألة إلى أي مدى يمكن للشروط الواردة في إطار توفير الثقة أن تعدِّل تلك الواردة في مشاريع الأحكام أو تَحُبَّها. فعلى سبيل المثال، وبصرف النظر عن مشاريع الأحكام المتعلقة بالمسؤولية، ليس من الواضح ما إذا كان يمكن للأطراف وضع قواعد مسؤولية خاصة بها في إطارها لتوفير الثقة الخاص بإدارة الهوية.

٦- الاعتماد على النماذج القانونية للتوقيع الإلكتروني: يعتمد هيكل مشاريع الأحكام والنهج المتبع فيها إلى حد كبير على قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، ومن ثم، فإنهما لا يراعيان حقيقة أن المسائل المتعلقة بالتوقيعات تختلف اختلافا كبيرا عن تلك

(١) يرد مصطلح "القواعد التي تحكم تشغيل نظام إدارة الهوية" في المواد ٦ (ج)، و٦ (و)، و١٠ (١) (ب)، و٢٣ (١) (أ) من مشاريع الأحكام، ومع ذلك فهو غير معرَّف ولا يجري تناوله بالتفصيل.

اللازمة لتناول مسألة الهوية (على الرغم من أن الهوية تكون في بعض الأحيان أحد مكونات التوقيع)، وبالتالي، إذا كانت مشاريع الأحكام تضع مقابلا قانونيا إلكترونيا واحدا لمتطلبات التوقيع، فإن الأمر نفسه لا يسهل تطبيقه فيما يتعلق بمتطلبات التحقُّق من الهوية.

ويعود جانب من المشكلة إلى أن جميع القوانين التي تشترط توقيعاً تشترط الأمر نفسه (أي التوقيع)، في حين أن القوانين التي تشترط تحديد هوية شخص ما كثيرا ما تفرض مجموعة متنوعة من المتطلبات التي يتعين على عمليات التحقُّق من الهوية استيفاؤها (على سبيل المثال، تبعاً لما إذا كانت الهوية "تأسيسية" أم "وظيفية"،[٢] والغرض من تحديد الهوية، والمخاطر المترتبة على ذلك، وما إلى ذلك). وبالتالي، يسهل نسبيا وضع مقابل قانوني لمفهوم التوقيع بوصفه أمرا واحدا، في حين لا يكون النهج نفسه مناسبا بالضرورة فيما يتعلق بالنُّهج القانونية المختلفة لتحديد الهوية. ومن ثم، من المهم ألا يحصر الفريق العامل نفسه في هيكل محدد مسبقا يستند إلى قانون التوقيعات الإلكترونية، وأن ينظر بدلا من ذلك بصورة مستقلة في المسائل القانونية التي يلزم تناولها فيما يتعلق بالهوية.

٧- خيارات التحقُّق من الهوية: لدى أي طرف معوِّل خياران للتحقق من هوية الشخص الذي يتعامل معه – أي أنه يمكن للطرف المعوِّل القيام بأي مما يلي:

- التحقُّق من الهوية بنفسه؛
- استخدام مقدِّم لخدمات إدارة الهوية من الأطراف الثالثة

وفي حين تستخدم معظم الأطراف المعوِّلة الخيار الأول، فإن مشاريع الأحكام تركز على الخيار الثاني فقط. ولعلَّ الفريق العامل يودُّ النظر فيما إذا كان ينبغي لمشاريع الأحكام أن تعتمد نهجا أوسع نطاقا فيما يتعلق بموضوع الهوية، وأن تتناول المسائل المعنية في الحالتين.

٨- حقوق الطرف المعوِّل في التعويل: في الوضع المثالي، ينبغي لمشاريع الأحكام أن تتناول المسائل المتعلقة بحق الطرف المعوِّل في التعويل. وقد يشمل ذلك، على سبيل المثال، حق الطرف المعوِّل في '١' التعويل على إثباتات الهوية بصفة عامة؛ '٢' التعويل على إثباتات من طرف ثالث لاستيفاء متطلبات محددة في قانون معين يفرض واجب تحديد الهوية؛ '٣' استخدام مقدِّم لخدمات إدارة الهوية من الأطراف الثالثة للوفاء بالتزاماته القانونية بتحديد هوية شخص ما.

٩- حقوق الطرف المعوِّل في استخدام أطراف ثالثة: في سياق متصل، في حين أن بعض القوانين التي تفرض واجب تحديد الهوية تأذن على وجه الخصوص باستخدام مقدِّمي خدمات من الأطراف الثالثة (على سبيل المثال، اللائحة المنظمة لقانون خصوصية المستهلك في كاليفورنيا)،[٣] تُغفل العديد من القوانين هذا الأمر (أو تشترط أن يقوم الطرف المعوِّل بتحديد الهوية بنفسه). وينبغي للفريق العامل النظر أيضاً في تلك المسائل المتعلقة بتحديد الهوية.

(٢) انظر، على سبيل المثال، "Practitioners Guide" (World Bank, 2019)، الصفحتين ١٢ و١٣ (وغيرهما)، متاح في الرابط: https://id4d.worldbank.org/guide.

(٣) انظر California Consumer Privacy Act Regulations at Article 4, Section 999.323(b)؛ متاح في الرابط: www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?.

ثانياً- تعليقات على كل قسم

١- المادة ١- التعاريف

(أ) **مصطلحات ناقصة:** بعض المصطلحات المستخدمة في جميع أجزاء مشروع الأحكام غير معرَّفة، ومن تلك المصطلحات:

- "عوامل التحديد الإلكتروني للهوية؛" انظر المادة ٦ (د) '١'
- "آليات التحديد الإلكتروني للهوية؛" انظر المواد ٦ (د) '٢'، و٨ (أ)، و٨ (ب)
- "إدارة الهوية؛" وهو مستخدم كعنصر وصفي في جميع أجزاء مشروع الأحكام على الرغم من عدم تعريفه
- "محدد هوية؛" انظر المادة ١ (ب)
- "القواعد التي تحكم نظام إدارة الهوية؛" – انظر المواد ٦ (ج)، و٦ (و)، و١٠ (ب)، و٢٣ (أ)
  - قد يكون الغرض من هذا المصطلح الإشارة إلى فرادى أُطر توفير الثقة الخاصة بنظم إدارة الهوية، وإن كانت صيغته الحالية قد تنطبق على أي قانون أو لائحة تنظيمية تحكم نظام إدارة الهوية، ولذا ينبغي توضيح كيفية استخدامه.
- "التحقُّق؛" – انظر المادة ٦ (أ) '٢'
  - قد يكون من المهم أيضاً توضيح مفهوم "التحقُّق"، لأن هذا المصطلح كثيرا ما يؤدي إلى قدر كبير من الالتباس. فعلى سبيل المثال، يُستخدم مصطلح "التحقُّق من الهوية" في بعض الحالات بمعنى تحديد هوية الكيان موضوع البيانات، في حين يُستخدم في حالات أخرى بمعنى التوثُّق من الكيان موضوع البيانات. ونظرا لتواتر استخدام هذا المصطلح، ينبغي توضيحه بعناية واستخدامه بصورة سليمة في جميع أجزاء مشاريع الأحكام.

(ب) **التوثُّق:** يُستخدم مصطلحا "التوثُّق" و"التحديد الإلكتروني للهوية" ليعنيا نفس الشيء في الأساس، على الرغم من أن التوثُّق يستخدم في سياق خدمات توفير الثقة، والتحديد الإلكتروني للهوية في سياق خدمات إدارة الهوية. وبما أن المفهومين متماثلان، يمكن للفريق العامل النظر في استخدام نفس المصطلح في الحالتين.

(ج) **التحديد الإلكتروني للهوية:** تمثل الاستعاضة عن مصطلح "تحديد الهوية" بمصطلحي "تدقيق الهوية" و"التحديد الإلكتروني للهوية" خطوة هامة لتوضيح جانبين من جوانب العمليات المتعلقة بالهوية والتمييز بينهما. بيد أنه قد يثار شاغل مفاده أنَّ مصطلح "التحديد الإلكتروني للهوية" يصف كامل عملية تدقيق الهوية وإصدار إثباتات الهوية والتوثُّق من العلاقة بين بيانات

إثبات الهوية والفرد، أو أنه يسهل الخلط بينه وبينها. وبالتالي، يوصى بأن ينظر الفريق العامل فيما إذا كان يمكن استخدام مصطلح آخر بدلا من "التحديد الإلكتروني للهوية".

وبالإضافة إلى ذلك، قد يسبب استخدام كلمة "إلكتروني" في هذا المصطلح، ويُقصد به وصف "عملية توفير الضمان والربط بين الكيان والهوية"، التباساً بشأن طبيعة العمليات والنُّظُم والخدمات التي تتناولها مشاريع الأحكام. وتَبرز نفس المسألة في تعريفي "خدمات إدارة الهوية" و"نظم إدارة الهوية"، اللذين يتطلبان أن تكون الخدمات والنُّظُم "في شكل إلكتروني". ويتجاهل وصف عملية الربط بأنها "إلكترونية" وخدمات إدارة الهوية ونظم إدارة الهوية بأنهما "في شكل إلكتروني" أن العملية كلها، أو في جزء منها، قد لا تكون في بعض الحالات إلكترونية. فعلى سبيل المثال، يمكن أداء بعض الوظائف في شكل غير إلكتروني، أو الاعتماد فيها على مستندات ورقية، ومن ذلك مثلا تدقيق الهوية. وبناء على ذلك، يوصى بأن ينظر الفريق العامل في التسليم بأن العمليات والنُّظُم والخدمات التي تشملها مشاريع الأحكام قد تتضمن مجموعة متنوعة من العناصر غير الإلكترونية.

(د) **الهوية:** تعريف الهوية بأنها مجموعة من النعوت التي تتيح "تمييز" [كيان] [شخص] "بشكل متفرد" ضمن سياق معين هو تعريف مُقيِّد أكثر من اللازم. ففي كثير من الحالات، يُستخدم تحديد الهوية لأغراض التأهُّل وليس لأغراض التفرُّد. فيمكن مثلا استخدام تحديد الهوية ببساطة لتحديد ما إذا كان شخص معين عضوا في جماعة محددة – على سبيل المثال، هل يزيد عمرك عن ٢١ عاما؟ هل أنت عضو في النادي؟ هل أنت مواطن؟ وما إلى ذلك. ويُفترض أن تلك النعوت تخص العديد من الناس، وبالتالي لا داعي لأن تكون الهوية فريدة وإنما ينبغي أن تميز الكيان موضوع البيانات على نحو كافٍ في السياق الذي يتطلب هذا التعريف المحدود للهوية.

(هـ) **إثباتات الهوية:** ينبغي للفريق العامل النظر في التطورات الجديدة المتعلقة بوسائل الإبلاغ عن المعلومات الخاصة بالهوية. ففي حين أن إثباتات الهوية هي الوسيلة المعتادة التي يتم بها تأكيد الهوية والتحقُّق منها، تجدر الإشارة إلى أن العديد من النُّظُم الجديدة لإدارة الهوية لا تستخدم إثباتات الهوية بحد ذاتها. ومن ثم، فإنه على الرغم من أن التعريف قد يكون ملائما، ينبغي توخي الحذر لتجنب أن تتضمن مشاريع الأحكام افتراضاً بأن إثباتات الهوية ستُستخدم دائما. وبالإضافة إلى ذلك، يلاحَظ أن التعريف يقتصر على "الشكل الإلكتروني". ولعلَّ الفريق العامل يودُّ النظر فيما إذا كان ينبغي لمشاريع الأحكام أن تشمل أيضاً الأشكال التقليدية لتحديد الهوية سواء كانت ورقية أو بالحضور الشخصي.

(و) **تدقيق الهوية:** لا يلزم أن تقوم عملية تدقيق الهوية بـ"تحديد وتأكيد" الهوية بشكل كامل. أي أن من الممكن افتراض أن تدقيق الهوية يتضمن جمع نعت أو أكثر و/أو التحقُّق من صحتها و/أو اعتمادها، وهذه النعوت وحدها لا تكفي لتحديد الهوية وتأكيدها، وإن كان يمكن لآخرين استخدامها لتأكيد هوية ما. ومن ثمَّ، لعلَّ الفريق العامل يودُّ النظر في تعريف أوسع نطاقاً لتدقيق الهوية.

(ز) **الطرف المعوِّل:** قد لا يكون من الملائم حذف هذا التعريف والاستعاضة عنه بمصطلح "المشترك"، إذ يوحي مفهوم المشترك بالمشاركة النشطة في النظام والإلزام بالقواعد. وعلى الرغم من أن ذلك قد يشمل الطرف المعوِّل، فإنه يمكن لأشخاص آخرين/جهات أخرى، منها الكيانات على سبيل المثال، الدخول في ترتيب لتقديم خدمات إدارة الهوية. ونتيجة لذلك، قد يؤدي عدم التمييز بين الأطراف المعوِّلة والكيانات (أو المستخدمين الآخرين لنظام إدارة الهوية) إلى التباس في تطبيق القواعد الواردة في مشاريع الأحكام. ويُقترح أن ينظر الفريق العامل في الاحتفاظ بتعريف مصطلح "الطرف المعوِّل" بحيث تنطبق المسائل التي تتناولها الأقسام اللاحقة على نحو ملائم إما على الأطراف المعوِّلة أو الكيانات.

(ح) **الكيان:** في سياق خدمات إدارة الهوية، الكيان هو الشخص أو الشيء الذي تتحدد هويته، أو يدخل على الأقل في عملية تدقيق الهوية. وبحذف الإشارة إلى تحديد الهوية يصبح المصطلح عاما، وغير مفيد على الأرجح.

(ط) **المشترك:** كما ذُكر أعلاه، يبدو مفهوم المشترك كشخص "يدخل في ترتيب لتقديم خدمات إدارة الهوية أو خدمات توفير الثقة مع مقدِّم خدمة إدارة الهوية أو مقدِّم خدمة توفير الثقة" شاملاً أكثر مما ينبغي، حيث يمكن أن يتضمن أدواراً متعددة في نظام إدارة الهوية، فضلا عن الكيانات. فعلى سبيل المثال، صيغت الفقرة ٣ من الخيار جيم للمادة ١٢ بافتراض أن المشتركين أطراف معوِّلة، في حين يمكن أن يكون المشتركون أيضاً كيانات أو أيا من الأدوار العديدة الأخرى في نظام إدارة الهوية، وفي هذه الحالة لا تكون أحكام هذا القسم ملائمة.

٢- المادة ٢- نطاق الانطباق

ينبغي للفريق العامل النظر في إعادة تقييم نطاق مشاريع الأحكام من حيث صلتها بإدارة الهوية. ويقتصر نطاق المادة ٢ بصيغتها الحالية على موضوعين: (١) **استخدام نظم إدارة الهوية**، (٢) **الاعتراف عبر الحدود بنظم إدارة الهوية**.

ولعلَّ الفريق العامل يودُّ النظر فيما إذا كان ينبغي للنطاق أن يتناول أيضاً **معاملات إدارة الهوية**، وربما أن يشير كذلك إلى **سير العمل** في نظام إدارة الهوية و/أو **تقديم** خدمات إدارة الهوية.

وعلاوة على ذلك، ينبغي للفريق العامل النظر في تنقيح القسم الثاني بحيث يوضح أنه "ينطبق على ... نُظم إدارة الهوية التابعة **للقطاع الخاص**"، بما أنه سلَّم بأنه ليست لديه صلاحية صياغة قواعد تخص نظم إدارة الهوية التي تديرها الحكومات.

٣- المادة ٣- الاستخدام الطوعي لخدمات إدارة الهوية وتوفير الثقة

بموجب المادة ٣ (٢)، يمكن الاستدلال على موافقة الشخص على استخدام نظام إدارة الهوية من خلال مسلكه. ومع ذلك، ينبغي للفريق العامل أن يحيط علماً بأن هذا الاستدلال لا يكون ملائماً إذا كانت هوية الشخص قد جرى انتحالها، على سبيل المثال، إذا استخدم منتحل هوية

إثباتات هوية مزيفة، أو استخدم إثباتات هوية حقيقية صادرة لشخص آخر. وفي هذه الحالات، فإن الشخص الذي استُدل على موافقته ليس هو الشخص الذي يقوم بالسلوك المشار إليه.

٤- المادة ٤- التفسير

لعلَّ الفريق العامل يودُّ النظر في ضمان ألا تميز مشاريع الأحكام بين نماذج نظم إدارة الهوية بإدراج مفهوم **حياد نظام إدارة الهوية** (أو حياد معاملات الهوية). ونظراً لوجود العديد من أساليب تسيير معاملات الهوية بالاتصال الحاسوبي المباشر (مثل نظم مقدِّمي خدمات الهوية الواحدة، والنُّظم الموحدة (مقدِّمون متعددون لخدمات الهوية)، والنظم التي يتحكم بها سيطرة المستعمل/التي تركز على المستعمل، ونظم توزيع البيانات، ونظم دفتر الأستاذ الموزَّع، والنُّظم غير المستندة إلى إثباتات الهوية، ونظم إدارة الهوية ذات السيادة الذاتية، وغير ذلك)، من المهم ألا تشترط مشاريع الأحكام أو تفترض اتباع نهج معين فيما يتعلق بعمليات تحديد الهوية و/أو عمليات التوثُّق، أو النُّظُم المستخدمة في تلك العمليات. ومن ثم، ينبغي للفريق العامل النظر في سُبل لضمان ألا توحي مشاريع الأحكام بوجود نموذج معين للنظام أو تشترط ذلك النموذج.

٥- المادة ٥- الاعتراف القانوني بإدارة الهوية

قد يلزم إجراء المزيد من المراجعة والتحليل فيما يتعلق بالمادة ٥ (أ). وينص هذا القسم على أنه لا يجوز إنكار الأثر القانوني للتحديد الإلكتروني للهوية استنادا إلى مجرد كونه في شكل إلكتروني. ونفترض (وإن كنا لم نتحقق من ذلك) أن بعض القوانين المتعلقة باستخدام إثباتات الهوية تشترط تقديم مستند ورقي أو في شكل مادي آخر، وليس في شكل إلكتروني. ونوصي من ثم، قبل استبعاد تطبيق هذه القوانين، بإجراء المزيد من المراجعة والتحليل لتحديد أثر هذا الحكم.

٦- المادة ٦- التزامات مقدِّمي خدمات إدارة الهوية

مدى ملاءمة نهج الحل الواحد الذي يلائم الجميع: تفرض المادة ٦ مجموعة التزامات على مقدِّمي خدمات إدارة الهوية. وتناسب تلك الالتزامات النموذج التقليدي لنظام إدارة الهوية، وتفترض أن مقدِّم خدمات إدارة الهوية يؤدي جميع وظائف النظام التقليدي، أو يكون مسؤولا عنها. غير أن نماذج نظم إدارة الهوية تخضع لطائفة من التغيرات والتجارب، مما يثير شواغل من أن استخدام قائمة الالتزامات هذه يستند إلى نموذج قديم قد لا يناسب النُّظُم الأحدث لإدارة الهوية و/أو يعوق دون مبرر إجراء المزيد من التجارب. ففي العديد من النُّظُم الأحدث لإدارة الهوية، قد تكون بعض وظائف مقدِّم خدمات إدارة الهوية الواردة في المادة ٦، على سبيل المثال، مسؤولية عدة جهات مختلفة (مثل مقدِّمي خدمات توفير الثقة، وأمناء السجلات، ووكلاء القيد، ومقدِّمي خدمات إثبات الهوية، والوكلاء المسؤولين، ومقدِّمي خدمات التوثُّق، ومراكز توزيع البيانات، وغير ذلك). وبالنظر للتنوع المتزايد لنماذج نظم إدارة الهوية، ينبغي للفريق العامل النظر فيما إذا كان لا يزال من الملائم أن تفرض مشاريع الأحكام على مقدِّمي خدمات إدارة الهوية مجموعة من الالتزامات التي تتبع نهج الحل الواحد الذي يلائم الجميع.

مصدر الالتزامات: لعلَّ الفريق العامل يودُّ أيضاً النظر في مسألة الحد الأدنى الأساسي، أي ما إذا كان ينبغي تحديد التزامات مقدِّمي خدمات إدارة الهوية من القطاع الخاص (أو أي أدوار أخرى في نظام إدارة الهوية) في مشـــاريع الأحكام وجعلها تنطبق على جميع نظم إدارة الهوية، أم أنه ينبغي لكل نظام من نظم إدارة الهوية التابعة للقطاع الخاص أن يحدد هذه الالتزامات في إطاره التعاقدي الخاص بتوفير الثقة. ويتيح إدراج التزامات كل دور في إطار توفير الثقة الخاص بنظام إدارة الهوية المنطبق لمشغل النظام والمشاركين فيه تكييف تلك الالتزامات لتتناسب مع غرض نظام إدارة الهوية المحدد واستخداماته، وكذلك الامتثال للقانون المنطبق.

القواعد التي تحكم نظام إدارة الهوية: أخيراً، تجدر الإشارة إلى أن هذا القسم يتناول "القواعد التي تحكم نظام إدارة الهوية"، وهي غير معرَّفة. فليس من الواضح، على سبيل المثال، ما إذا كان القصد أن تكون هذه القواعد إطارا تعاقديا لتوفير الثقة ينطبق على نظام معين لإدارة الهوية، أم شيئا آخر.

٧- المادة ٧- التزامات مقدِّمي خدمات إدارة الهوية في حال انتهاك سرية البيانات

المسؤولية عن التصدي للخرق الأمني: يبدو أن المادة ٧ في صيغتها الحالية تخلط بين نظم إدارة الهوية ومقدِّمي خدمات إدارة الهوية، وتفترض أن نظام إدارة الهوية سيتحكم به مقدِّم واحد لخدمات إدارة الهوية يؤدي جميع وظائف النظام. وعلاوة على ذلك، تفرض المادة ٧ التزامات على مقدِّم خدمات إدارة الهوية المعني في حال "وقوع" خرق أمني أو مساس بسلامة النظام، بصرف النظر عن معرفة مقدِّم الخدمات بهذا الخرق أو مسؤوليته عنه أو سيطرته عليه. أما في الواقع، فقد تشارك أطراف متعددة في نظام إدارة الهوية، وقد لا يتحمل الكثير منها أي مسؤولية عن الخادوم/الشبكة/النظام، أو الموظفين، أو أي شخص أو جهاز تعرض للخرق، ولا تكون لها سيطرة على أي من ذلك.

وفي العديد من النُّهج الحديثة المتبعة إزاء نظم إدارة الهوية، يمكن أن تؤدي جهات مختلفة بعض تلك الوظائف (على سبيل المثال، مقدِّمو خدمات توفير الثقة، وأمناء السجلات، ووكلاء القيد، ومقدِّمو خدمات إثبات الهوية، ومقدِّمو خدمات التوثُّق، ومراكز توزيع البيانات، وغير ذلك). وقد يكون أحد هذه الأدوار وحده هو مصدر الخرق الأمني، وقد لا يكون مقدِّم خدمات إدارة الهوية على علم حتى بوقوع الخرق.

ومن ثم، ينبغي للفريق العامل، عند تناول مسألة انتهاك سرية البيانات، النظر في التمييز بين نظم إدارة الهوية ومقدِّمي خدمات إدارة الهوية، وإمكانية مشاركة عدة مقدِّمين لخدمات إدارة الهوية (فضـــلاً عن عدة أدوار أخرى) في نظام واحد لإدارة الهوية. وبناء على ذلك، يرجح أن تكون أول مسألة هي تحديد المسؤولية عن موضوع الخرق، والمسؤولية عن التزامات التبليغ أولاً.

وفي الوضع المثالي، يحسن أن يقتصر فرض الواجبات المتعلقة بالتصدي للخرق الواردة في المادة ٧ (مثل معالجة الخرق، وإلغاء الإثباتات، وإبلاغ السلطات، وإبلاغ المتأثرين من الكيانات موضوع البيانات والأطراف المعوِّلة) على الطرف الذي تضرر فعليا من الخرق الأمني للخادوم/الشبكة/النظام المعني أو التلاعب بأي منها، أو الذي يكون بخلاف ذلك مسؤولا عن أي منها. فعلى سبيل المثال، في حالة نظام إدارة الهوية الذي يتضمن عدة مقدِّمين لخدمات إدارة الهوية أو عدة أدوار، قد يكون من الملائم '١' فرض واجب معالجة الخرق على الجهة التي تضررت فعليا منه والتي تكون في وضع

يتيح لها احتواء الخرق ومعالجته، '٢' فرض واجب إبلاغ الكيانات على الجهة التي لها علاقة بالكيانات.

الخرق الأمني على مستوى النظام: في سياق متصل، ينبغي للفريق العامل النظر أيضاً في تنقيح المادة ٧ لتتناول إمكانية حدوث خرق أمني جسيم على مستوى النظام في إطار نظام لإدارة الهوية يتضمن عدة مقدِّمين لخدمات إدارة الهوية (مثل التلاعب بالمفتاح الخصوصي الرئيسي) يؤدي إلى تعريض نظام إدارة الهوية بأكمله وجميع مقدِّمي الخدمات التابعين له للخطر، حسب نوع النظام وهيكله. وفي هذه الحالة، يمكن أن يؤثر الخرق على جميع مقدِّمي خدمات إدارة الهوية، بغض النظر عن مسؤوليتهم عن الخرق الفعلي. ومن ثم، من المرجح أن تكون هناك حاجة إلى تدابير تصدٍّ من نوع مختلف، ويُفترض أن يكون على جميع مقدِّمي خدمات إدارة الهوية التعهد بالتزامات محددة للتصدي حتى وإن كانوا لا يتحملون مسؤولية الخرق.

المسؤولية عن المساس بسلامة النظام: أخيراً، تشترط المادة ٧ (١) (ب) أن يقوم مقدِّم خدمات إدارة الهوية بـ"معالجة الخرق الأمني أو **المساس بسلامة النظام**". وقد يكون من الملائم مطالبة مقدِّمي خدمات إدارة الهوية بمعالجة الخرق (على الأقل الخرق الذي يمكنهم التحكم به)، وإن كان ينبغي للفريق العامل النظر فيما إذا كان من الملائم مطالبتهم أيضا بمعالجة "المساس بسلامة النظام". ويمكن أن يكون المساس بالسلامة جسيما، وينبغي عندها أن يحدَّد ما إذا كان مقدِّم خدمات إدارة الهوية مسؤولا عن ذلك، ومدى تلك المسؤولية، وفقا لقواعد المسؤولية المعمول بها، أيا كانت طريقة تحديدها.

٨- المادة ٨- التزامات المشتركين

التزامات الدور التي يتعين تناولها: على سبيل التعليق العام، إذا كانت مشاريع الأحكام ستتناول التزامات المشتركين في نظام إدارة الهوية (مثل المواد ٦ و٧ و٨)، فلعلَّ الفريق العامل يودُّ أن ينظر في تناول التزامات **جميع** المشتركين في النظام - مثل التزامات وكلاء القيد، ومقدِّمي نعوت الهوية، ومقدِّمي خدمات إدارة الهوية، ومقدِّمي خدمات التحقُّق من الهوية، والمستعملين، ومراكز توزيع البيانات، والأطراف المعوِّلة، ومقدِّمي خدمات توفير الثقة، والمشتركين، وما إلى ذلك. وسيكون ذلك هاما أيضا فيما يبدو لأغراض توزيع المسؤولية، وفقا للمادة ١٢ أدناه.

أين يمكن تناول الالتزامات: بالإضافة إلى ما تقدَّم، لعلَّ الفريق العامل يودُّ أن ينظر في تحديد أفضل موضع لتناول التزامات مقدِّمي خدمات إدارة الهوية والمشتركين وغيرهم من المشاركين في نظم إدارة الهوية. وتوفر المواد ٦ و٧ و٨ من مشاريع الأحكام نهج الحل الواحد الذي يناسب الجميع لتناول التزامات مقدِّمي خدمات إدارة الهوية والمشتركين. ولكن بالنظر إلى تنوع نظم إدارة الهوية، قد يكون من الأنسب أن يُسمح لكل نظام، أو أن يُشترط عليه، تناول الالتزامات المرتبطة بجميع أدواره المختلفة في إطار لتوفير الثقة صُمِّم خصيصا ليلائم هذا النظام من حيث التكنولوجيا الخاصة به ومنهجيته وغرضه، بدلا من استخدام أحكام المشاريع لفرض نهج الحل الواحد الذي يناسب الجميع على جميع نظم إدارة الهوية. ويُعزى ذلك جزئيا إلى أنَّ فئات الأدوار التي ينطوي عليها النظام وتعاريفها، وكذلك التزامات المشتركين الذين يؤدون تلك الأدوار، ستختلف اختلافا كبيرا

على الأرجح من نظام إدارة هوية إلى آخر. ويتمثل أحد العوامل التي تؤدي إلى هذه الاختلافات في الغرض الذي أُنشئ من أجله نظام معيَّن لإدارة الهوية (من تلك الأغراض مثلا تيسير الاتصال الحاسوبي المباشر داخل صناعة المستحضرات الصيدلانية، مثل نظام SAFE BioPharma IdM، وتيسير تبادل المعلومات الأكاديمية، مثل نظام InCommon IdM الذي تستخدمه الجامعات، أو تيسير الاتصالات مع الوكالات الحكومية، مثل نظام eIDAS).

وبالإضافة إلى ذلك، وكما ذُكر أعلاه فيما يتعلق بالمادة ٦، تخضع نماذج نظم إدارة الهوية لطائفة متنوعة من التغييرات والتجارب، وهو ما يثير شواغل بأنَّه قد لا يكون من المناسب إدراج قائمة موحدة بالالتزامات، نظرا لاحتمال أن يؤدي ذلك إلى فرض نموذج قديم لا يتناسب بصورة جيدة مع العديد من نظم إدارة الهوية الحالية، ويحول دون إجراء المزيد من التجارب.

واجبات المشتركين الخاضعين للنظام: تتعلق المادة ٨ بالمشتركين (أي الأشخاص الذين يدخلون في ترتيب متصل بخدمات إدارة الهوية). ومن المفترض أن يشمل ذلك العديد من المشاركين في نظام ما لإدارة الهوية، مثل الأطراف المعوِّلة، وفرادى الكيانات موضوع البيانات، وقد يشمل أيضا أدوارا أخرى مختلفة في نظام إدارة الهوية. وتفرض هذه المادة على المشتركين التزامات بإبلاغ مقدِّم خدمات إدارة الهوية إذا علم بوقوع تلاعب بإثباتات الهوية أو آليات التحديد الإلكتروني للهوية التابعة لنظام إدارة الهوية، أو كانت الملابسات المعلومة له توحي بشدة بوقوع تلاعب.

وفي حالة المشتركين من الأفراد (مثل الكيانات موضوع البيانات)، قد يشكل ذلك مطلبا مرهقا وغير معقول. فعلى سبيل المثال، هناك من المفترض العديد من الحالات التي قد يكون فيها أحد فرادى المشتركين في نظام إدارة الهوية على علم بملابسات تشير إلى احتمال وقوع تلاعب، ولكنَّه ببساطة لا يفهم أهميتها. وبالإضافة إلى ذلك، ونظرا لأنَّ هذا الالتزام ينطبق فيما يبدو على نظام إدارة الهوية بأكمله (بدلا من أن ينطبق مثلا على إثبات هوية واحد صادر إلى فرد معين)، يبدو أنَّ هذا الحكم يفرض عبئا كبيرا على الأفراد (وكذلك على مشتركين آخرين في النظام) الذين قد يكونون على علم بأن لمعلومات معينَّة أهمية على نطاق المنظومة بأكملها، ولكنَّهم ببساطة لا يفهمون تلك الأهمية.

وحتى فيما يتعلق بفقدان إثبات الهوية الشخصي الخاص بأي فرد أو التلاعب به، قد لا يكون من المناسب دائما أن يُفرض على هذا الفرد واجب الإبلاغ عن هذا الفقدان. وكما هو متَّبع في حالة أرقام بطاقات الائتمان المسروقة، قد يكون إلزام كيان ما بالإبلاغ عن هذه الأحداث ببساطة غير واقعي أو حتى غير مناسب (وخصوصا في حالة المستعملين البسطاء أو الخروق التي تحدث على شبكة الإنترنت أو تحدث بطرائق أخرى قد لا يملك المستعملون القدرة على تمييزها). وفي حالة نظم إدارة الهوية التي لا تعتمد على استخدام إثباتات مادية، قد لا تكون لدى الكيان ببساطة أي فكرة عن تعرُّض بيانات إثبات الهوية الخاص به (رقم الهوية على سبيل المثال) للتلاعب.

٩- المادة ٩- تحديد هوية [الكيانات] [الأشخاص] باستخدام خدمات إدارة الهوية

مدى ملاءمة أسبقية هذه المادة على القانون القائم: استُمدت المادة ٩ إلى حد كبير من القانون النموذجي بشأن التوقيعات الإلكترونية واتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات

الإلكترونية في العقود الدولية، ويبدو أنَّ من شأن تلك المادة أن تكون لها الأسبقية على القوانين القائمة التي تنص على متطلبات فريدة لتحديد الهوية في حالات معينة. وفيما يتصل بقوانين التوقيعات الإلكترونية، أدى هذا النهج العام المتمثل في أن تكون لهذه القوانين أسبقية على جميع قوانين التوقيعات الأخرى عمله بشكل جيد. ومع ذلك، لعلَّ الفريق العامل يودُّ أن يقيِّم ما إذا كان ذلك ينطبق بالضرورة في حالة تحديد هوية كيان ما. وعلى وجه التحديد، ونظرا لأنَّ بعض القوانين لا يتطلب سوى تحديد الهوية على نحو بسيط، في حين تنص قوانين أخرى على متطلبات محدَّدة للغاية فيما يتعلق بأسلوب تحديد الهوية وطريقته (بما في ذلك قوانين حماية الخصوصية، والقوانين المتعلقة بمبدأ "اعرف زبونك"، وقوانين التوثيق، وما إلى ذلك)، قد لا يكون وضع قاعدة عامة تشير إلى تحقيق الامتثال بمجرد الوفاء بأحد معايير الموثوقية أمرا مناسبا.

ومن المفترض أن من غير المرجح أن تفي عملية عامة لتحديد الهوية – حتى وإن كانت عملية "موثوقة" – بمختلف متطلبات تحديد الهوية المنصوص عليها في جميع القوانين القائمة. وبالإضافة إلى ذلك، وبقدر ما يكون لدى الأطراف في معاملة تجارية ما متطلباتها الخاصة لتحديد الهوية، قد لا يكون بديل إلكتروني يفي بالمعيار العام "للموثوقية" كافيا كذلك للوفاء بالمتطلبات الخاصة أو الفريدة للأطراف.

التضارب المحتمل بين المواد: ينبغي للفريق العامل أيضا أن ينظر فيما يبدو أنَّه تعارض محتمل بين المادة ٢ (٣) والمادة ٩. إذ تسلِّم المادة ٢ (٣) بأنَّ العديد من القوانين القائمة تفرض على الأطراف من القطاع الخاص مجموعة متنوعة من متطلبات تحديد الهوية، ولهذه الغاية، تنص على أنَّه "ليس في هذا الصك ما يمسُّ بأي شرط قانوني يقضي بأن تُحدَّد هوية [الكيانات] [الأشخاص] وفقا لإجراء معيَّن أو منصوص عليه في القانون." ومع ذلك، يبدو أنَّ نهج الحل الواحد الذي يناسب الجميع الذي تتبعه المادة ٩ يتعارض مع هذا الحكم.

فالخيار ألف من المادة ٩ ينص على ما يلي:

"حيثما يشترط حكم قانوني أو أحد الأطراف تحديد هوية [شخص] [كيان] ما، يُستوفى ذلك الحكم فيما يتعلق بخدمات إدارة الهوية عندما تستخدم [طريقة موثوقة] [نظام إدارة هوية موثوق] للتحديد الإلكتروني لهوية [الكيان] [الشخص]."

والخيار باء من المادة ٩ مشابه لذلك، إذ ينص على ما يلي:

"يجوز تحديد هوية كيان ما باستخدام خدمات إدارة الهوية إذا استخدمت طريقة موثوقة للتحديد الإلكتروني لهوية [الكيان] [الشخص]."

ونظرا للتنوُّع الكبير في المتطلبات الواردة في قوانين مختلفة بشأن عمليات تحديد الهوية، يبدو أنَّ نهج الحل الواحد الذي يناسب الجميع، الوارد في المادة ٩، غير عملي. ويبدو أنَّ جزءا من المشكلة يتمثل في أنَّ تحديد الهوية يُعامَل بنفس الطريقة التي تُعامَل بها التوقيعات الإلكترونية. ففي حالة التوقيع الإلكتروني، يفي إنشاء توقيع الكتروني وفقا للطريقة المحدَّدة في القانون النموذجي بمتطلبات أي قانون يشترط التوقيع. ولكنَّ الأمر نفسه لا ينطبق على متطلبات تحديد الهوية.

فالمتطلبات القانونية لتحديد هوية شـــخص ما تختلف اختلافا كبيرا تبعا للقانون المعني والغرض الذي يُطلب من أجله تحديد الهوية (الهوية التأسيسية مقابل الهوية الوظيفية)، وأهمية المسألة ذات الصلة. فعلى سبيل المثال، تفرض اللوائح الصادرة مؤخرا التي تنظم قانون خصوصية المستهلك في كاليفورنيا متطلبات كثيرة بشأن تحديد الهوية يجب الوفاء بها قبل إتاحة البيانات الشخصية أو حذفها بناء على طلب من شخص يدَّعي أنه هو الكيان المعني.(٤) وبالمثل، تفرض قواعد "اعرف زبونك" المعمول بها في القطاع المالي طائفة متنوعة من المتطلبات المحدَّدة بشـــأن تحديد الهوية. ومن ثمَّ، لعلَّ الفريق العامل يودُّ أن ينظر أيضا فيما إذا كان من المناسب، وتحت أية ظروف، أن تُستخدم عبارة شاملة تقوم على نهج الحل الواحد الذي يناسب الجميع مفادها أنَّ استخدام أحد النُّظُم الموثوقة يفي بشرط قانوني بشأن تحديد الهوية.

ويبيِّن تضـــارب هذين الحكمين المشـــكلة الناجمة عن محاولة وضـــع مجموعة من قواعد الهوية باستخدام نفس النهج المستخدم سابقا في التوقيعات الإلكترونية.

الموثوقية كمفهوم نسبي: بالإضافة إلى ذلك، من المهم النظر فيما إذا كانت المادة ٩ تعترف على نحو كاف بأنَّ الموثوقية (مثل الأمن) مفهوم نســـبي. فطريقة موثوقة في ســـياق ما قد لا تكون موثوقة في سياق آخر. على سبيل المثال، غالبا ما يكون استخدام فيسبوك أو غوغل لتحديد هوية شخص ما إلكترونيا عملية موثوقة بما فيه الكفاية للسماح بالوصول البسيط إلى حساب على موقع إلكتروني، ولكن من المرجح ألا يكون كافيا للسماح بالوصول إلى حساب مصرفي وإعطاء الإذن بتحويل الأموال عبر الإنترنت من ذلك الحســـاب. ومن ثمَّ، بغية الإبقاء على نهج الموثوقية المتَّبع بشأن الحصول على الأثر القانوني، يُشجَّع الفريق العامل على النظر في تغيير نص المادة ٩ بحيث يسـلِّم بأنَّ "الطريقة الموثوقة" مفهوم نسبي. وأحد النُّهج الممكنة بهذا الشـأن هو إدراج ما يشبه مفهوم "موثوقة بالقدر المناسب" المستخدم في اتفاقية الأمم المتحدة – أي عندما تكون الطريقة المستخدمة إما: '١' موثوقة بالقدر المناسب للغرض الذي يُطلب من أجله تحديد الهوية، في ضـــوء كل الظروف المحيطة، بما فيها أيُّ اتفاق ذي صـــلة؛ أو '٢' ثبت فعليا أنَّها موثوقة بالقدر الكافي.

العمليات المتعددة المتصلة بالموثوقية: يبدو أيضا أنَّ المادة ٩، من خلال تطبيقها لشرط الموثوقية فقط على الطريقة المســـتخدمة في التحديد الإلكتروني للهوية،(٥) تتجاهل جميع ما تنطوي عليه عملية تحديد الهوية من متطلبات أخرى يمكن أن تؤثر أيضـــا على موثوقية النتيجة، وكذلك الطرائق المحتمل اســـتخدامها في تلك العمليات. وتشـــتمل هذه العمليات على عمليات تدقيق الهوية، وعمليات القيد، وأمن إثباتات الهوية، وعمليات التوثق، وعمليات التحديد الإلكتروني للهوية، والبرامجيات، وأمن البيانات، والموظفين، وما إلى ذلك. فعلى ســـبيل المثال، حتى إذا

(٤) انظر California Consumer Privacy Act Regulations at Article 4, متاح في الرابط: www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?.

(٥) انظر المادة ١ (د) من مشاريع الأحكام، التي تعرِّف التحديد الإلكتروني للهوية بأنَّه "عملية تُستخدم لتوفير قدر كاف من الضمان في الربط بين [الكيان] [الشخص] والهوية."

استُخدمت طريقة موثوقة موضوعيا في التحديد الإلكتروني لهوية شخص ما، فلن يكون لذلك قيمة إذا لم تكن عملية تدقيق الهوية موثوقة كذلك بما فيه الكفاية.

١٠- المادة ١٠- العوامل المتصلة بتحديد الموثوقية

تحدد المادة ١٠ فقط العوامل المتصلة بتحديد مدى موثوقية "طريقة ... التحديد الإلكتروني للهوية"[٦] المشار إليها في المادة ٩. غير أنَّها لا تحدد العوامل التي ينبغي تقييمها بهدف تحديد مدى موثوقية أي عمليات رئيسية أخرى يؤديها نظام لإدارة الهوية، مثل تدقيق الهوية.

وتركز المادة ١٠ على أربع فئات من العوامل، على النحو التالي:

- الامتثال للالتزامات الواردة في المادة ٦
- امتثال "القواعد التي تحكم تشغيل نظام إدارة الهوية" لأي معايير وإجراءات دولية معترف بها، بما في ذلك إطار مستوى الضمان
- أي إجراءات للإشراف على نظم إدارة الهوية أو لاعتمادها
- أي "اتفاق بين الأطراف."

ومع ذلك، في حين أنَّ العوامل الأربعة الواردة تركز على الامتثال للقواعد أو المعايير، والاعتماد، والاتفاق بين الأطراف، فإنها لا تنشئ بالضرورة الموثوقية. فوجود قواعد ومعايير أو اعتماد أو اتفاقات والامتثال لها لا يعني بالضرورة أنَّ نظام إدارة الهوية الممتثِل لها موثوق لأي استخدام معين. ومن ثمَّ، إذا قرَّر الفريق العامل معالجة العوامل التي تحدد مدى موثوقية "طريقة ... التحديد الإلكتروني للهوية"، فلعلَّه قد يودُّ أن ينظر في العمليات ليحدد أيها يتصل بالموثوقية (مثلا عمليات تدقيق الهوية، وعمليات القيد، وأمن إثباتات الهوية، وعمليات التوثُّق، وعمليات التحديد الإلكتروني للهوية، والبرامجيات، وأمن البيانات، والموظفون، وما إلى ذلك)، ثم ينظر في القواعد أو المعايير ليحدد أيها ينشئ الموثوقية في حالة كل من هذه العمليات.

وبالإضافة إلى ذلك، وكما تشير القائمة السابقة، تستخدم نظم إدارة الهوية العديد من العمليات المختلفة التي يمكن أن يُنفَّذ كل منها باستخدام طريقة واحدة أو أكثر من مجموعة متنوعة من "الطرائق" التي قد تكون، أو لا تكون، موثوقة. وبالإضافة إلى ذلك، فإنَّ التأكُّد من أنَّ "طريقة ... التحديد الإلكتروني للهوية" تُنفَّذ من خلال طريقة موثوقة، على سبيل المثال، لا يعني بالضرورة أنَّ عملية تدقيق الهوية التي تستند إليها عملية التحديد الإلكتروني للهوية قد نُفذت باستخدام طريقة موثوقة.

(٦) يقتصر تعريف التحديد الإلكتروني للهوية، على النحو المبيَّن في المادة ١ (د) من مشاريع الأحكام، على العملية المستخدمة لتوفير قدر كاف من الضمان في الربط بين [الكيان] [الشخص] والهوية". ولا يشمل التعريف العديد من العمليات الأخرى المطلوبة لنظم إدارة الهوية.

١١- المادة ١١- تحديد النُّظُم الموثوقة لإدارة الهوية

المعايير والاختصاص: تمنح المادة ١١ للجهات من الأفراد أو السلطات، التي تعينها الدولة، سواء أكانت جهات عامة أم خاصة ("**سلطة الموثوقية**")، الحق في تحديد نظم إدارة الهوية التي تعتبر موثوقة. غير أنَّ المادة ١١ لا تحدد أي معايير تتعلق باختصاص سلطة الموثوقية في القيام بهذا التحديد. وبالإضافة إلى ذلك، لا تحدد هذه المادة العملية التي ينبغي استخدامها في تحديد النُّظُم الموثوقة، بخلاف متطلب يقتضي مراعاة جميع الظروف ذات الصلة، بما في ذلك العوامل الواردة في المادة ١٠، ومتطلب عام بأن تكون تلك العملية متَّسقة مع "المعايير والإجراءات الدولية المعترف بها ذات الصلة بتحديد موثوقية نظم إدارة الهوية"، دون ذكرها على وجه التحديد. ونتيجة لذلك، يثير هذا الأمر شاغلا مفاده أنَّ سلطات الموثوقية غير المؤهلة قد تقيِّم الموثوقية باستخدام معايير غير مناسبة، ومن ثمَّ، هناك احتمال بأن تُحدَّد نظم إدارة هوية غير موثوقة باعتبارها موثوقة. وبالإضافة إلى ذلك، من المرجح أن يختلف تحديد مدى موثوقية نظم إدارة الهوية اختلافا كبيرا من دولة لأخرى، حتى بالنسبة لنفس نظام إدارة الهوية. وبالنظر إلى أهمية هذا التحديد ضمن إطار المادة ٩ (أي أنَّ المادة ٩ تفترض أنَّ نظم إدارة الهوية المحددة هذه تستخدم "طرائق موثوقة" يترتب عليها أثر قانوني)، فإنَّ ذلك يمكن أن يؤدي إلى مشاكل كبيرة.

ولعلَّ الفريق العامل يودُّ أيضا أن ينظر في كيفية تعيين دولة ما سلطةَ الموثوقية باعتبارها سلطة مختصَّة، وكذلك في كيفية ضمان هذه الدولة تزويد سلطة الموثوقية المشار إليها بالخبرات والعمليات والموارد اللازمة لتحديد نظم إدارة الهوية "الموثوقة". فعلى سبيل المثال، هل ينبغي أن تخضع سلطة الموثوقية التي تحددها الدولة لشكل من أشكال الاعتماد قبل أن تُمنح هذه الصلاحية؟

موثوقية النُّظُم مقابل موثوقية المعاملات: نظرا لأنَّ الموثوقية مفهوم نسبي، من المفترض أن تحتاج تقييمات الموثوقية إلى طرح السؤال "موثوقة لأي غرض؟". ويثير ذلك مسألة حاسمة بشأن ما إذا كان ينبغي للفريق العامل أن يركز على موثوقية نظم إدارة الهوية بوجه عام (بصرف النظر عن نوع معاملة الهوية التي تُستخدم هذه النُّظُم من أجلها) أم على موثوقية معاملات إدارة الهوية (التي توفر سياقا محددا للحكم على الموثوقية).

موثوقية نظم إدارة الهوية مقابل موثوقية "طريقة ... التحديد الإلكتروني للهوية": تركز المادة ١١ على موثوقية "نظم إدارة الهوية"، في حين تحدد المادة ٩ الأثر القانوني المترتب على تحديد الهوية بناء على موثوقية "طريقة ... التحديد الإلكتروني للهوية". ويبدو أنَّ هذين النهجين غير متَّسقين، وخصوصا لأنَّ موثوقية طريقة ما للتحديد الإلكتروني للهوية ليست سوى جزء من الموثوقية الإجمالية للوظائف التي ينفذها نظام ما لإدارة الهوية.

مسائل عملية: يشير التركيز على دور سلطة الموثوقية في المادة ١١ (وأهميته في الحصول على الأثر القانوني المنصوص عليه في المادة ٩) إلى الحاجة إلى آلية مؤسسية مركزية لتقييم نظم إدارة الهوية في كل دولة، وإلى مشاركة السلطات العامة، على الأقل لتعيين سلطة الموثوقية. ونشجِّع الفريق العامل على النظر فيما إذا كان ذلك عمليا.

وبالإضافة إلى ذلك، لعلَّ الفريق العامل يودُّ أن ينظر فيما إذا كان من شأن الحاجة إلى الحصول على الفوائد المستمدة من كون نظام إدارة الهوية محددا باعتباره نظاما موثوقا أن تميِّز ضد نظم

إدارة الهوية العاجزة عن تحمل نفقات عملية تحديد الموثوقية. وتشمل المسائل الأخرى التي قد يودُّ الفريق العامل أن ينظر فيها ما يلي:

- ما هي الجهة المناسبة لتعيينها كسلطة موثوقية؟
- كيف يمكن تحديد ما إذا كانت سلطة الموثوقية مؤهلة ومختصة؟
- إلى أي حد يمكن الركون إلى تحديد الموثوقية من قِبل سلطة الموثوقية (بالنظر إلى أنَّ تحديد الموثوقية هو عملية تقييم في نقطة زمنية ما)؟ وكم مرة يجب أن تُكرَّر هذه العملية؟
- هل ينبغي أن تتدخل الدولة في تعيين سلطات الموثوقية المعنية بنظم إدارة الهوية في القطاع الخاص، أو أن تجعل الحصول على تحديد الموثوقية المشار إليه شرطا لتحقُّق آثار قانونية معينة؟
- هل يترتب على ذلك الأثرُ العملي المتمثل في اشتراط استيفاء جميع نظم إدارة الهوية للمعايير التي اختارتها الدولة و/أو سلطة الموثوقية (بالنظر إلى أنَّ القائمين على جميع النُّظُم سيرغبون في أن تُحدَّد باعتبارها نظما موثوقة)، وهو ما قد يؤدي إلى عرقلة تطويرها في المستقبل؟
- ما المعيار المؤهل لأن يوصف بأنَّه "معيار دولي معترف به"؟ وما الجهة المعنية بالاعتراف؟ وماذا لو تغيَّر المعيار؟
- هل من المرجح أن يتطلب فرضُ معيار مختار والامتثالُ له إجراءاتِ اعتماد قد تكون مكلفة ومعقَّدة؟
- كيف ترتبط العوامل المتعلقة بتحديد الطرائق الموثوقة (في المادة ١٠) بمتطلبات تحديد نظم إدارة الهوية الموثوقة (في المادة ١١)؟

وأخيرا، نظرا لأنَّ المادة ١١ تتوخى تحديد موثوقية نظم إدارة الهوية بصرف النظر عن الموقع الجغرافي، ينبغي للفريق العامل أن ينظر فيما إذا كان ذلك سينشئ حاجة عملية إلى أن تسعى نظم إدارة الهوية إلى الحصول على تحديد الموثوقية في كل دولة يمارس فيها المشتركون في تلك النُّظُم أعمالهم، وما إذا كان ذلك سوف يمنع المعاملات عبر الحدود.

١٢- المادة ١٢- مسؤولية مقدِّم خدمات إدارة الهوية

هناك عدد من الشواغل المتعلقة بأحكام المسؤولية الواردة في هذا المشروع، ولعلَّ الفريق العامل يودُّ أن ينظر فيها.

الافتراض الأساسي: يبدو أنَّ المادة ١٢ (على الأقل الخياران باء وجيم منها)، على غرار المادة ٦، تستند إلى افتراض مفاده أنَّ القواعد نفسها يمكن أن تُطبَّق على جميع نظم الهوية. ولكن بالنظر إلى التباين المتزايد على الدوام بين أنواع نظم إدارة الهوية وأغراضها ونطاقها ووظائفها وتشغيلها وأدوار المشتركين فيها ومسؤولياتهم، يبدو من المستبعد للغاية أن تكون القواعد المحددة في المادة ٦، أو قواعد المسؤولية المحددة في الخيارين باء أو جيم من المادة ١٢، مناسبة في جميع الحالات.

ولا نحتاج إلا إلى مقارنة الاختلافات بين نظم إدارة الهوية التقليدية القائمة على مرافق المفاتيح العمومية، ونظم إدارة الهوية القائمة على سلاسل السجلات، ونظم إدارة الهوية التي تركز على المستعملين، ونظم إدارة الهوية القائمة على التحكم الذاتي، لكي نرى أنَّ هذه القواعد لن تكون ملائمة في جميع الحالات. ونظرا لأنَّ نظم إدارة الهوية قد تختلف بصورة كبيرة، قد لا يكون أي تحديد قياسي للمسؤولية مناسبا لنظم إدارة الهوية كافة. ومن ثمَّ، لعلَّ الفريق العامل يودُّ النظر فيما إذا كان اتِّباع نهج الحل الواحد الذي يناسب الجميع إزاء المسؤولية مناسبا.

الأدوار المشمولة: تتناول المادة ١٢ مسؤولية مقدِّم خدمات إدارة الهوية فحسب. وإذا خلص الفريق العامل إلى أنَّه ينبغي تناول مسألة المسؤولية في مشاريع الأحكام هذه، فقد يكون من المناسب النظر في توزيع المسؤولية على جميع المشاركين. وقد يشمل ذلك مثلا مسؤولية مقدِّمي خدمات إدارة الهوية، ووكلاء القيد، ومقدِّمي نعوت الهوية، ومقدِّمي الهويات، والكيانات، والمستعملين، ومراكز توزيع البيانات، ومقدِّمي خدمات التحقُّق من الهوية، ومقدِّمي خدمات توفير الثقة، والأطراف المعوِّلة، وما إلى ذلك. وهذا أمر مهم لأنَّ تناول مسؤولية أحد الأدوار التي ينطوي عليها نظام ما لا يخفف من الأضرار التي قد تنشأ عن مشكلة أو يزيلها، وإنما يكتفي بنقل تلك الخسارة من شخص إلى آخر. وينبغي أن ينظر التحديد المناسب للمسؤولية في الجهة التي ينبغي أن تتحمَّل هذه الخسارة على النحو الواجب.

الحق في إبراء الذمة أو تقييد المسؤولية: لعلَّ الفريق العامل يودُّ النظر فيما إذا كان ينبغي أن يكون لمقدِّم خدمات إدارة الهوية (أو غيره من المشاركين في النظام) الحق في إبراء ذمته أو تقييد مسؤوليته، بموجب عقد أو بوسائل أخرى. ويمكن أن يسمح الخيار ألف باستخدام إعلانات تقييد المسؤولية أو إبراء الذمة، على الأقل إلى المدى المسموح به بموجب القانون المنطبق. ومن المفترض أنَّ السماح بذلك يقرُّ بأنَّ هناك العديد من سيناريوهات وأنواع المسؤولية الأخرى التي قد يسعى بشأنها مقدِّمو خدمات إدارة الهوية أو آخرون بصورة مشروعة إلى أن يبرئوا ذمتهم أو أن يقيِّدوا مسؤوليتهم، ويحيلوا على الأقل إلى مرونة خيارات تقييد المسؤولية أو إبراء الذمة المتاحة بموجب القانون المنطبق.

وفي حين ينص الخيار جيم على حق محدود في إبراء الذمة من المسؤولية، فإنه محدود النطاق للغاية ولا يتيح المرونة. وبالإضافة إلى ذلك، ثمة مسألة تتعلق بما إذا كانت الأحكام الواردة في الخيارين باء أو جيم تمنع مقدِّم خدمات إدارة الهوية عموما من أن يبرئ ذمته من المسؤولية بالكامل (كما تفعل عادة الكيانات الحكومية).

وبقدر ما يفرض الخياران باء وجيم قيودا على مسؤولية مقدِّم خدمات إدارة الهوية عن الإخلال بالتزاماته المنصوص عليها في المادة ٦، هناك أيضا مسألة تتعلق بكيفية عمل هذه القيود في حالة منتحلي الهوية. أي أنَّه إذا أصدر أحد مقدِّمي خدمات إدارة الهوية إثبات هوية لأحد منتحلي الهوية، أو حدَّد هويته إلكترونيا، دون الإخلال بالأحكام الواردة في المادة ٦، فمن يتحمل الخسارة؟ هل ينبغي أن يتحمل هذه الخسارة ضحية انتحال الهوية، الذي قد لا يكون لديه أي تفاعل مع مقدِّم خدمات إدارة الهوية ولا يربطهما عقد؟

حدود المسؤولية في الخيار جيم: تستند الفقرة الفرعية ١٢ (٣) من الخيار جيم إلى افتراضين، هما: (١) من الممكن فرض قيود تتعلق بالغرض أو القيمة على معاملات هوية محددة (على الرغم من أنَّ الفقرة الفرعية المشار إليها لا تحدد موضع فرض تلك القيود أو كيفيته)، (٢) يمكن للطرف المعوِّل أن يعرف هذه القيود بسهولة قبل أن يعوِّل. ويبدو أنَّ ذلك من بقايا النهج الأصلي المستخدم في بعض النُّظُم القديمة القائمة على مرافق المفاتيح العمومية، حيث تحتوي الشهادة الصادرة عن سلطة الاعتماد على غرض أو حد أقصى مقوَّم بالدولار من المتوقع أن يستعرضه ذلك الطرف المعوِّل قبل أي تعويل. وبالنظر إلى التنوُّع الواسع النطاق لنظم إدارة الهوية الموجودة اليوم، لعلَّ الفريق العامل يودُّ أن ينظر فيما إذا كان فرض قيود على المسؤولية على أساس المعاملات قابلا للتطبيق. فعلى سبيل المثال، يمكن إدخال تغييرات على هذه المادة بحيث تسلم بأنَّ هذه القيود يمكن أن تُبيَّن ضمن إطار الثقة الخاص بمقدِّم خدمات تحديد الهوية أو في العقد المبرم مع الأطراف المعوِّلة، وليس في المعاملات الفردية.

التعامل مع الحكومة: أخيرا، لعلَّ الفريق العامل يودُّ أن ينظر في التفاعل المحتمل مع النُّظُم الحكومية لإدارة الهوية. ففي كثير من الحالات، يعتمد مقدِّمو خدمات إدارة الهوية على تأكيدات لنعوت الهوية صادرة من أطراف ثالثة، مثل النُّظُم الوطنية لإدارة الهوية أو قواعد البيانات الحكومية الأخرى (مثل إدارة المركبات). وبما أنَّ النُّظُم الحكومية لإدارة الهوية كثيرا ما تُعتبر ذات حجية، على الرغم من أنها لا تقبل عادة أي مسؤولية عن الأخطاء، ينبغي أيضا النظر في تحديد الجهة التي تتحمل الخسارة في حالة وجود أخطاء في المعلومات المقدَّمة من الحكومة. ومن ثمَّ، قد يلزم اتِّباع نهج مختلف بقدر ما يتعلق الأمر بكيانات عامة.

ونحثُّ الفريق العامل على النظر في تجنُّب محاولات تحديد المسؤولية، وخصوصا في ضوء التنوُّع الواسع النطاق لنظم إدارة الهوية وعملياتها والمشاركين فيها. وإذا قرَّر الفريق العامل معالجة المسؤولية، فإننا نشجِّع على الإشارة إلى الطرائق التي يمكن بها تحديد المسؤولية، ولكن ليس إلى المعايير أو المواصفات أو القواعد الفعلية المتعلقة بالمسؤولية بحد ذاتها. ويمكن أن تشمل هذه الطرائق مثلا الإشارة إلى القانون القائم (كما هو الحال في الخيار ألف)، أو الإشارة إلى أُطر الثقة القائمة على العقود، وهي الأُطر التي يعتمدها نظام ما لإدارة الهوية ويتَّفق عليها الأطراف بموجب عقد.

١٣- المادة ٢٦- الاعتراف عبر الحدود بنظم إدارة الهوية وخدمات توفير الثقة

- فيما يتعلق بمسألة "الاعتراف" عبر الحدود، لعلَّ الفريق العامل يودُّ توضيح الإجابات على ثلاثة أسئلة أساسية هي: ما الشيء الذي يُعترف به؟ ومن الجهة المعنية بالاعتراف؟ وما الغرض من الاعتراف؟

- ما الشيء الذي يُعترف به؟ تجيب المادة ٢٦ (١) على هذا السؤال فيما يبدو من خلال التركيز على "نظم إدارة الهوية" و"الأثر القانوني" المترتب على "نظم إدارة الهوية". غير أنَّه ليس من الواضح كيف يمكن أن يترتب على نظام ما لإدارة الهوية أثر قانوني، أو ماذا يمكن أن يكون أثره القانوني. ومن المفترض أنَّ التعويل على ما يقوم به نظام إدارة الهوية من

عمليات تدقيق للهوية و/أو تحديد للهوية إلكترونيا يمكن أن يكون له أثر قانوني، ولكن ليس من الواضح كيف يمكن أن يترتّب على نظام إدارة الهوية نفسه أثر قانوني.

وقياسا على ذلك، تعترف الدول بجوازات السفر الصادرة عن دول أخرى استنادا إلى المعايير التي وضعتها منظمة الطيران المدني الدولي (الإيكاو). ومن المفترض أنَّ كل الدول توافق على صحة معايير الإيكاو، ويمكن أن تقيِّم ما إذا كان نظام إصدار جوازات السفر المعمول به في كل دولة أخرى يمتثل لتلك المعايير أو أن لا تقيّمه، ولكنَّ إثبات الهوية – أي جواز السفر الصادر عن نظام كل دولة – هو ما يُعطى "الأثر القانوني" على الحدود.

- من الجهة المعنية بالاعتراف؟ من المفترض أن تكون الهيئة التي تعترف بنظام إدارة هوية أجنبي إما: (١) كيانا عاما، مثل الحكومة أو محكمة تطبِّق القانون/النظام القانوني المرتبط بذلك النظام (فيما يتصل مثلا باستيفائه شرط قانوني للتحقُّق من الهوية، أو كونه يمثِّل أدلة مقبولة في المحكمة)، أو (٢) طرفا معوِّلا (من القطاع العام أو الخاص). ويُفترض أنَّ مشروع المادة ٢٦ يركز على الخيار الأول، نظرا لأنَّه يشير إلى "الأثر القانوني" المترتب على الشيء الذي يُعترف به. وبالإضافة إلى ذلك، لا يتطلب الخيار الثاني قانونا أو استنتاجا قانونيا، نظرا لأنَّ الأطراف المعوِّلة تتمتَّع بالحرية في اتِّخاذ قراراتها الخاصة بشأن ما إذا كانت ستعترف بنظم إدارة الهوية أو الهوية و/أو تعوِّل عليها لأغراض أي معاملة تقوم بها.

- ما الغرض من الاعتراف؟ إذا كان قانون دولة أجنبية يعترف بـ"نظام ما لإدارة الهوية"، فماذا يعني ذلك؟ يبدو أنَّ مفهوم نظام إدارة الهوية الذي يترتَّب عليه أثر قانوني مربك إلى حد ما. فعلى سبيل المثال، هل يعني ذلك أنَّ الدولة الأجنبية ستقبل تلقائيا نتائج عملية التحديد الإلكتروني للهوية التي يقوم بها نظام إدارة الهوية المعترف به، أم يعني ببساطة أنَّه سيُسمح لنظام إدارة الهوية المعترف به بممارسة عمله في الولاية القضائية الأجنبية، ولكن قد يتعين تعديل عملياته بغية تلبية المتطلبات القانونية التي تفرضها الولاية القضائية الأجنبية على نظم إدارة الهوية الخاصة بها؟

وينبغي للفريق العامل أن ينظر في توضيح ما يعنيه القول بأنَّ لنظام إدارة الهوية الذي يُشغَّل خارج [الدولة المشترعة] نفس الأثر القانوني في [الدولة المشترعة] لنظام إدارة الهوية الذي يُشغَّل في [الدولة المشترعة].

١٤- المادة ٢٧- التعاون

القصد من المادة ٢٧ ليس واضحا. إذ يبدو أنَّ التركيز ينصب على تبادل المعلومات والخبرات والممارسات الجيدة – وهو أمر لا يثير بالتأكيد أي اعتراض، ومن الناحية المثالية، ينبغي تشجيعه، خصوصا إذا كان التبادل طوعيا ولا ينطوي على تفاوض بشأن اتفاقات ملزمة لكيانات ليست أطرافا في هذا التعاون. غير أنَّه في هذه الحالة، لا يبدو من الضروري اشتراط أن تحدِّد الدولة المشترعة الكيان الذي يتبادل المعلومات باعتباره جهة مختصة بذلك. وبالإضافة إلى ذلك، لا يبدو من الضروري تركيز التعاون على الفئات الثلاث المدرجة في المادة ٢٧.

وإذا كان التعاون والتبادل إلزاميين، أو يُشكلان أساسا للاعتراف القانوني من جانب دولة ما أو للتفاوض بشأن اتفاقات ملزمة لكيانات ليست أطرافا في المفاوضات، فيبدو أنَّ ذلك يثير مجموعة متنوعة من الشواغل التي تتطلب فيما يبدو مزيدا من المناقشة والتوضيح من جانب الفريق العامل.

ويلاحَظ أيضا أنَّ المادة ٢٧ تجيز (أو تشترط) تعاون الكيان أو الوكالة التي تحددها الدولة المشترعة كجهة مختصة "مع كيانات أجنبية". وليس من الواضح ما تشير إليه عبارة "كيانات أجنبية" – فهل هي مثلا الحكومة الأجنبية أو أي مقدِّم لخدمات إدارة الهوية يتصادف أنَّه يعمل في الدولة الأجنبية، وما إلى ذلك؟ ومن المفترض أن يقتصر هذا التعاون مع "الكيانات الأجنبية" على الكيانات الأجنبية التي تحددها الدولة الأجنبية كجهة مختصة.