الأمم المتحدة

A/CN.9/WG.IV/WP.120

الجمعية العامة

Distr.: Limited
27 July 2012
Arabic
Original: English

لجنة الأمم المتحدة للقانون التجاري الدولي
الفريق العامل الرابع (المعني بالتجارة الإلكترونية)
الدورة السادسة والأربعون
فيينا، ٢٩ تشرين الأول/أكتوبر – ٢ تشرين الثاني/نوفمبر ٢٠١٢

لمحة عامة عن إدارة الهويات

ورقة معلومات أساسية مقدَّمة من فرقة العمل القانونية المعنية بإدارة الهويات التابعة لرابطة المحامين الأمريكية

مذكرة من الأمانة

قدَّمت فرقة العمل القانونية المعنية بإدارة الهويات، التابعة لرابطة المحامين الأمريكية، الوثيقة المرفَقة إلى الأمانة، وذلك في إطار التحضير للدورة السادسة والأربعين للفريق العامل الرابع (المعني بالتجارة الإلكترونية).

وقد استُنسخت الوثيقة الواردة في المرفق بالشكل الذي تلقّتها به الأمانة.

050912 V.12-55144 (A)

أولاً- مقدِّمة

١- لاحظ تقرير صادر عن منظمة التعاون والتنمية في الميدان الاقتصادي عام ٢٠١١ أنَّ "إدارة الهويات الرقمية أمر لا غنى عنه لزيادة تطوير الاقتصاد الإلكتروني".[(١)] فهي متطلب أساسي لكلّ الأشكال الموضوعية للتجارة الإلكترونية.

٢- تقدِّم هذه الورقة لمحة عامة عن إدارة الهويات ودورها في التجارة الإلكترونية والمسائل القانونية التي تنشأ عنها والعقبات القانونية التي تطرحها.[(٢)] وتستند هذه الورقة إلى العمل الجاري الذي تقوم به فرقة العمل القانونية المعنية بإدارة الهويات التابعة لرابطة المحامين الأمريكية،[(٣)] وهي مقدَّمة على أنها ورقة معلومات أساسية ترمي إلى إطلاع الفريق العامل على المسائل ذات الصلة.[(٤)]

٣- وقد اتفقت اللجنة في دورتها الرابعة والأربعين، عام ٢٠١١، على أن يعاود الفريق العامل الرابع (المعني بالتجارة الإلكترونية) انعقاده لكي يضطلع بعمل في ميدان السجلات الإلكترونية القابلة للإحالة.[(٥)] واتفقت اللجنة في الوقت ذاته على أن تتابع في دورة مقبلة النظر في مسألة تمديد ولاية الفريق العامل لتشمل مواضيع أخرى نوقشت في الوثيقة A/CN.9/728 وAdd.1 كمواضيع منفصلة (وليس بحكم ارتباطها العرَضي بموضوع

(1) OECD (2011) "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy — Guidance for Government Policy Makers," *OECD Digital Economy Papers*, No. 196, OECD Publishing، الصفحة ٣، في الرابط www.oecd-ilibrary.org/science-and-technology/digital-identity-management-for-natural-persons_5kg1zqsm3pns-en.

(2) تركّز هذه الوثيقة على نُظم إدارة الهويات التجارية المراد استخدامها في سياق الأعمال التجارية، ويشمل ذلك الاتصالات فيما بين المنشآت التجارية، وبين المنشآت التجارية والحكومة، وبين المنشآت التجارية والمستهلكين.

(3) Identity Management Legal Task Force, Cyberspace Law Committee, American Bar Association, Section of Business Law; http://apps.americanbar.org/dch/committee.cfm?com=CL320041. ولم تخضع الآراء الواردة في هذه الورقة لتصديق مجلس مندوبي رابطة المحامين الأمريكية أو مجلس إدارتها، ومن ثم ينبغي عدم تفسيرها على أنها تمثل سياسة الرابطة.

(4) يرد أيضاً مزيد من المواد المستخلَصة من أعمال ندوة لجنة الأمم المتحدة للقانون التجاري الدولي حول التجارة الإلكترونية، المعقودة من ١٤ إلى ١٦ شباط/فبراير ٢٠١١ في نيويورك، على الرابط: www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010.html.

(5) الوثائق الرسمية للجمعية العامة، الدورة السادسة والستون، الملحق رقم ١٧ (A/66/17)، الفقرة ٢٥٠.

السجلات الإلكترونية القابلة للإحالة).[٦] وتشمل تلك المواضيع إدارة الهويات والنافذة الوحيدة والسداد بالأجهزة النقالة.[٧]

٤- كما نوقش أدناه (في الفقرتين ٦ و٧)، فإنَّ إدارة الهويات متطلَّب لا محيد عنه لكل موضوع من المواضيع التي نظرت فيها اللجنة في دورتها الرابعة والأربعين (وهي السجلات الإلكترونية القابلة للإحالة، والنافذة الوحيدة والسداد بالأجهزة النقالة). ومن ثَمَّ ستكون لها أهميتها للأعمال الجارية التي يقوم بها الفريق العامل بشأن السجلات الإلكترونية القابلة للإحالة وأيضاً لأي عمل يُحتمَل القيام به مستقبلاً بشأن المواضيع الأخرى.

٥- ومن المسلَّم به على نطاق واسع أنَّ لإدارة الهويات أهمية حاسمة في تيسير التجارة الإلكترونية على نحو جدير بالثقة. وهكذا فإنَّ العديد من المجموعات الحكومية الدولية والدول والمجموعات الدولية الخاصة والكيانات التجارية تعمل بنشاط على استكشاف المسائل المتعلقة بإدارة الهويات والفرص التي تنطوي عليها، ووضع معايير تقنية وعمليات تجارية، وتقصّي سبل تنفيذ نُظم لإدارة الهويات قابلة للتطبيق. فعلى سبيل المثال:

(أ) تشمل المجموعات الحكومية الدولية المنكبّة بنشاط على تقصّي المسائل والمعايير المتعلقة بإدارة الهويات منظمةَ التعاون والتنمية في الميدان الاقتصادي[٨] والمنظمة الدولية للتوحيد القياسي[٩] والاتحاد الدولي للاتصالات؛[١٠]

(ب) حددت دراسة استقصائية أجرتها منظمة التنمية والتعاون في الميدان الاقتصادي[١١] ١٨ بلداً من بلدان المنظمة تتّبع بنشاط استراتيجيات وطنية لإدارة الهويات (إسبانيا، أستراليا، ألمانيا، إيطاليا، البرتغال، تركيا، الدانمرك، سلوفينيا، السويد، شيلي، كندا، جمهورية كوريا، لكسمبرغ، النمسا، نيوزيلندا، هولندا، الولايات المتحدة الأمريكية،

(6) المرجع نفسه، الفقرة ٢٥١.

(7) المرجع نفسه، الفقرات ٢٤١-٢٤٩.

(8) www.oecd.org/document/38/0,3746,en_2649_34255_49319782_1_1_1_1,00.html.

(9) www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306.

(10) www.itu.int/ITU-T/studygroups/com17/fgidm.

(11) Bernat, L. (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing. doi: 10.1787/5kgdzvn5rfs2-en; at www.oecd-ilibrary.org/content/workingpaper/5kgdzvn5rfs2-en.

اليابان).[١٢] كما تتّبع بلدان أخرى عديدة، مثل إستونيا والهند ونيجيريا مثل هذه الاستراتيجيات على نحو نشِط؛

(ج) تَجري حالياً في الاتحاد الأوروبي عدة مشاريع إقليمية خاصة بإدارة الهويات، منها مشروع PrimeLife (وهو مشروع يندرج ضمن البرنامج الإطاري السابع للمفوضية الأوروبية)،[١٣] ومشروع GINI-SA (Global Identity Networking of Individuals — Support Action)،[١٤] ومشروع STORK (لإنشاء منصة أوروبية للاستخدام التبادلي لنُظم إدارة الهويات الإلكترونية)،[١٥] ومشروع الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)؛[١٦]

(د) تشمل المنظمات الخاصة التي تنشط في مجال المعايير والسياسات الخاصة بالهويات على صعيد دولي منظمةَ الارتقاء بمعايير نظم المعلومات البنيوية (OASIS)[١٧] و(the Open Identity Exchange (OIX[١٨] ومبادرة Kantara[١٩] ومؤسسة Open ID Foundation[٢٠] وtScheme[٢١] وThe Internet Society؛[٢٢]

(هـ) أُنشئت بعض نُظم إدارة الهويات التجارية، وهي تشتغل على نطاق عالمي في مناطق محدودة. وتشمل نُظماً يشغّلها برنامج Transglobal Secure Collaboration Program[٢٣] ونظام CertiPath[٢٤] في مجال صناعات الفضاء الخارجي والدفاع، ونظام SAFE-BioPharma Association[٢٥] في مجال صناعة المستحضرات الصيدلانية البيولوجية، ونظام IdenTrust[٢٦]

(12) المرجع نفسه، الصفحات ٢٨-٣٥، للاطلاع على قائمة روابط تحيل إلى الوثائق الوطنية.

(13) www.primelife.eu.

(14) www.gini-sa.eu.

(15) https://www.eid-stork.eu.

(16) www.enisa.europa.eu.

(17) www.oasis-open.org/home/index.php.

(18) www.openidentityexchange.com.

(19) http://kantarainitiative.org, formerly known as the Liberty Alliance, www.projectliberty.org.

(20) http://openid.net/foundation.

(21) www.tscheme.org.

(22) www.internetsociety.org.

(23) www.tscp.org.

(24) https://www.certipath.com.

(25) www.safe-biopharma.org.

بالنسبة للقطاع المالي، ونظام CA/Browser Forum[٢٧] بالنسبة لشهادات طبقة المقابس الآمنة للتحقق الموسَّع (EV SSL) للمواقع الشبكية، واتحاد نُظم إدارة الهويات وإصدار وسائل إثبات الهويات (FiXs).[٢٨] ويركز عمل هذه المجموعات بالدرجة الأولى على المعايير التقنية والمسائل الخاصة بالعمليات التجارية لا على المسائل القانونية.

ثانياً- ما هي أوجه صلة إدارة الهويات بالتجارة الإلكترونية؟

٦- تُعتبر إدارة الهويات مسألة أساسية لمعظم معاملات التجارة الإلكترونية وسائر الأنشطة التي تُنجَز بالاتصال الحاسوبي المباشر. فَمنْ الشواغل الأساسية التحقُّق من هويات أطراف بعيدين، مثل تحديد هوية مَن يسعى إلى الوصول إلى قاعدة بيانات على الإنترنت تحتوي على معلومات حساسة، ومَن يحاول تحويل أموال من حساب ما بالاتصال الحاسوبي المباشر، ومَن وقّع عقداً إلكترونياً، ومَن أذِن عن بعد بشحن منتَج معيَّن، ومَن أرسل بريداً إلكترونياً. فلئن كان المشاركون في العديد من المعاملات الإلكترونية القليلة المخاطر مستعدين لأن يثقوا في أنهم بصدد التعامل مع شخص أو كيان بعينه، إلا أنه مع ازدياد حساسية أو قيمة المعاملة تزداد أيضاً أهمية ضمان توافر وموثوقية معلومات دقيقة عن هوية الطرف البعيد بهدف اتخاذ قرار قائم على الثقة.

٧- وتشكِّل إدارة الهويات متطلَّباً أساسياً من متطلبات التوقيعات الإلكترونية، وكذا لموضوع السجلات الإلكترونية القابلة للإحالة، ولأي عمل يُحتمَل القيام به مستقبلاً بشأن المواضيع الأخرى (النافذة الوحيدة والسداد بالأجهزة النقالة).[٢٩]

(أ) يشكِّل إثبات هوية الموقّع أحد شروط صحة التوقيع الإلكتروني. فالمادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (١٩٩٦) والمادة ٩ من اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية (٢٠٠٥، اتفاقية الخطابات الإلكترونية) تشترطان لصحة التوقيع الإلكتروني، "استخدام طريقة لتعيين هوية" الموقّع جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أُنشئت أو أُبلغت من أجله رسالة

(26) www.identrust.com.

(27) www.cabforum.org.

(28) www.fixs.org.

(29) الوثائق الرسمية للجمعية العامة، الدورة السادسة والستون، الملحق رقم ١٧ (A/66/17)، الفقرات ٢٤١-٢٥٢.

البيانات. وفضلاً عن ذلك، تشترط المادة ٢ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية تضمين بيانات "يجوز أن تُستخدم لتعيين هوية الموقّع" كمكون من مكونات التوقيع الإلكتروني؛

(ب) ويُعتبر التحقُّق من الهوية أيضاً متطلباً أساسياً للسجلات الإلكترونية القابلة للإحالة والنافذة الوحيدة والسداد بالأجهزة النقالة. ويقضي القانون القائم بشأن السجلات الإلكترونية القابلة للإحالة بضرورة إثبات هوية كل من الموقّع على السجل والحائز الذي يحق له إنفاذه.[٣٠] كما أنَّ عمليات النافذة الوحيدة تقتضي تحديد هوية الموقّع على الوثائق الجمركية، وكذلك هوية الشخص أو الكيان الذي يودِعها والشخص أو الكيان الذي يحق له إنفاذها.[٣١] أما الأداءات بالأجهزة النقالة فتستلزم (لأغراض إصدار الإذن)، شأنها في ذلك شأن سائر نُظم الأداء، تحديد هوية الشخص الذي يدّعي تحويل الأموال.[٣٢]

ثالثاً- ما المقصود بإدارة الهويات؟

٨- يكمن الهدف من إدارة الهويات، في جوهرها، في الإجابة عن سؤالين بسيطين يطرحهما كل طرف من طرفي معاملة إلكترونية بشأن الطرف الآخر: "من أنت؟" و"كيف لك أن تُثبت ذلك؟". وسرعان ما أصبحت القدرة على توفير إجابة معوَّل عليها وجديرة بالثقة عن هذين السؤالين شرطاً بالغ الأهمية للأنشطة التجارية الإلكترونية، خصوصاً وأن طبيعة تلك المعاملات وقيمتَها وحساسيتها تتعاظم. ويمكن لطرف في معاملة إلكترونية أن يقرر، من خلال الإجابة عن ذينك السؤالين، ما إذا كان سيدخل في تلك المعاملة أم لا (مثل ما إذا كان سيبرم عقداً مع الطرف الآخر، أو ما إذا كان سيسمح للطرف الآخر بالاطلاع على قاعدة بيانات حساسة، أو ما إذا كان سيمنح الطرف الآخر امتيازاً آخر من نوع ما أو يتيح له الوصول إلى شيء ما).

٩- ويمكن لكل كيان يشترك في معاملات رقمية أن ينشئ نظاماً خاصاً به لتحديد وتوثيق هوية كل شريك من شركائه التجاريين (على نحو ما تفعله حالياً عدة مؤسسات تجارية عن طريق استخدام عمليات التسجيل الفردي مشفوعة بنظام لاسم المستخدم وكلمة السر)، بيد أنه قد ثبت على نحو متزايد أنَّ هذا المسعى مكلف وغير ملائم، إذ يستتبع

(30) الوثيقة A/CN.9/WG.IV/WP.115، الفقرات ٢٤-٢٦ و٤٥-٤٨.

(31) الوثيقة A/CN.9/728/Add.1، الفقرة ٤٢ و٤٥.

(32) انظر الوثيقة A/CN.9/728، الفقرة ٥٢.

تحديات أمام توسيع نطاق النظام ليشمل عدداً أكبر من المتعاملين. وعلاوة على ذلك، فإنَّ الحاجة المتزايدة إلى التعاون فيما بين المنظمات، والشواغلَ القائمة فيما يتعلق بمسألة الأمن، ومشكلة إدارة كلمة السر الخاصة بالمستخدم، كلها عوامل تبيّن أنَّ النهج التقليدي الخاص باسم المستخدم وكلمة السر الصادرين عن الشركة أو البائع لم يعد ملائماً.

١٠- ونتيجة لذلك، باتت نُظم إدارة الهويات التي يضطلع فيها طرف ثالث من موفّري عناصر الهوية (أو موفّري صفات الهوية) بدور أساسي نهجاً مفضَّلاً. ويتمثل الهدف المنشود من ذلك في تمكين المؤسسات التجارية والوكالات الحكومية من إجراء معاملات إلكترونية مع أطراف بعيدة بناءً على المعلومات الخاصة بالهوية وعمليات توثيقها التي يوفرها أيٌّ من عدة أطراف ثالثة تُوفِّر عناصر الهوية ولا تربط بينهما أي صلة. وكثيراً ما يشار إلى هذا الإجراء باسم النظام "الاتحادي" لإدارة الهويات. وبعبارة أخرى، فإنَّ المعلومات الخاصة بالهوية التي يتحقق منها أحد الكيانات تتاح، بطريقة متَّفق عليها وخاضعة للإدارة، لأطراف متعددة في نُظم شتى تحتاج إلى معلومات عن الهوية لأغراض متعددة. ومن شأن ذلك، على سبيل المثال، أن يتيح للأفراد والمؤسسات التجارية استعمال وسيلة لإثبات الهوية من اختيارهم لإجراء معاملات إلكترونية مع منشآت عديدة، تماماً كما قد يستعمل أحد الأفراد رخصة قيادة لإنجاز طائفة من مختلف المعاملات غير الحاسوبية مع كيانات شتى، من قبيل شراء الكحول أو الحصول على الإذن بدخول منطقة صعود الطائرة بالمطار أو فتح حساب مصرفي.

١١- ويقتضي وضع نظام اتحادي لإدارة الهويات جملة من النُّظم والمعايير التقنية[٣٣] والعمليات والإجراءات التجارية والقواعد القانونية التي تُنشئ مجتمعةً نظاماً جديراً بالثقة يكفل ما يلي: '١' التحقق من الهوية وربطها بإنسان أو كيان اعتباري أو جهاز أو شيء رقمي، '٢' وتوفير معلومات الهوية تلك إلى طرف يطلبها لإصدار الإذن بإجراء المعاملة، '٣' وحفظ تلك المعلومات وحمايتها على مدى دورة حياتها. ومن الجوهري لتشغيل ذلك النظام في سياق تجاري إرساء إطار قانوني ملائم يقوم عادةً على العقود، يحدد حقوق الأطراف ومسؤولياتها ويبيِّن المخاطر ويتيح أساساً للإنفاذ. وغالباً ما يشار إلى هذا الإطار القانوني باسم "القواعد التشغيلية" أو "إطار الثقة".

(33) مرافق المفاتيح العمومية نهجٌ يمكن استخدامه في إنشاء نظام لإدارة الهويات. إلا أنه يجري أيضاً استحداث وتنفيذ كثير من التكنولوجيات والنُّهُج الأخرى.

رابعاً- أسس إدارة الهويات

١٢- صحيح أنَّ مصطلح "إدارة الهويات" حديث العهد نسبياً، إلا أنَّ المفهوم ليس كذلك. فالعمليات المؤسسة له تُستخدم منذ وقت طويل في بيئة غير حاسوبية. فجوازات السفر ورخص القيادة وبطاقات هوية الموظفين كلُّها مكونات لنُظم إدارة الهويات (أي أنها مستندات لإثبات الهوية يُصدرها كيان إلى أفراد متحقَّق من هوياتهم لكي يُثبتوا هوياتهم فيما بعد). ويمكن إجراء عملية تحديد هوية شخص معيَّن وإصدار وسيلة إثبات الهوية من جانب الطرف الذي يقبل أيضاً تلك الوسيلة (كما هو الحال في بطاقة هوية الموظفين التي تُصدرها الشركات) أو من جانب طرف ثالث (مثل رخصة القيادة أو جواز السفر). ومن العناصر الرئيسية في النُّظم الاتحادية التي يكون فيها طرف ثالث هو المُصدر أنَّ استخدام وسائل إثبات الهوية هذه لا يقتصر على المعاملات مع الكيانات التي أصدرتها، بل إنها تصمَّم وتُنشر مع توقع قبول أطراف ثالثة وسائلَ إثبات الهوية (مثل أمن المطار أو المصرف أو نادل الحانة إذا تعلّق الأمر برخصة قيادة) عندما يُشترط إثبات بعض صفات هوية الشخص (مثل الاسم أو السن).

١٣- على أنَّ التحدِّي المطروح في هذا الصدد يكمن في تنفيذ مثل هذه الإمكانية في بيئة إلكترونية، أي إنشاء نظام خاص بوسائل لإثبات الهوية الرقمية تكون آمنة وجديرة بالثقة والتعويل عليها ويمكن استعمالها عن بعد بين مختلف النُّظم والكيانات (أي إنشاء نظام اتحادي لإدارة الهويات). وهذا الأمر يتيح لأصحاب البيانات استعمال نفس وسيلة إثبات الهوية في تحديد هوياتهم بهدف الوصول إلى الموارد أو إجراء معاملات مع منظمات متعددة.

١٤- ولئن كانت هناك نُهُج مختلفة لإدارة الهويات، إلا أنها تنطوي أساساً على عمليتين أساسيتين: '١' جمع بعض صفات الهوية عن شخص ما (أو كيان أو جهاز أو شيء رقمي)[٣٤] والتحقق منها، ثم إصدار وسيلة لإثبات الهوية تعكس تلك الصفات ("تحديد الهوية")، و'٢' عملية التحقق بعد ذلك من أنَّ الشخص الذي يُبرز تلك الوسيلة ويدّعي أنه الشخص الذي جرى تحديد هويته سابقاً هو فعلاً ذلك الشخص ("التوثيق"). ويمكن أن تشتمل كل عملية من هاتين العمليتين الأساسيتين على عدة عمليات فرعية، تبعاً لطبيعة البيانات المتوافرة والسياق الذي تُجرى فيه العمليتان. وعند نجاح توثيق صفات هوية الفرد، يُجري الكيان الذي يعتزم التعويل على الهوية الموثَّقة مجموعةً ثالثة من العمليات، تسمى "الإذن"، لتحديد الحقوق والامتيازات التي تُمنح لذلك الشخص (على سبيل المثال ما إن

(34) يمكن جمع المعلومات عن الهوية والتحقق منها وإصدار وسائل إثبات الهوية بالنسبة للأفراد والكيانات الاعتبارية والأجهزة والأشياء الرقمية. ولا تتناول هذه الورقة إلا نُظم إدارة الهويات الخاصة بالأفراد.

كان ينبغي إبرام عقد مع ذلك الشخص أو ينبغي أن يتاح له الوصول إلى قاعدة بيانات، أو إلى حساب مصرفي على الإنترنت).

ألف- تحديد الهوية

١٥- ترمي عملية تحديد الهوية إلى الإجابة عن السؤال "من أنت؟". وتتعلق هذه العملية التي يقوم بها شخص يضطلع بدور موفّر الهوية[٣٥] بربط صفات الهوية (مثل الاسم أو رقم العضوية أو العنوان أو تاريخ الميلاد) بالشخص المعني بهدف تحديد هوية ذلك الفرد والتعريف به بقدر كاف لتحقيق الغرض المتوخى. وغالباً ما تُجرى هذه العملية، التي تسمى أحياناً "إثبات الهوية" أو "التسجيل"، مرة واحدة. وتتعلق عادةً بجمع موفّر الهوية معلومات عن الشخص المطلوب تحديد هويته (يشار إليه بـ"الشخص")، وكثيراً ما تستند إلى خليط من المستندات التي تُصدرها الحكومة (مثل شهادة الميلاد وبطاقة الضمان الاجتماعي ورخصة القيادة وجواز السفر)، فضلاً عن وسائل لإثبات الهوية تُصدرها كيانات القطاع الخاص (مثل شارة الموظفين وشريحة الاشتراك اللاسلكية للهواتف النقالة وبطاقات الائتمان). ورغم أنَّ مستندات الهوية ووسائل إثبات الهوية هذه قد أُصدرت لأغراض أخرى، فإنَّ من الممكن في حالات كثيرة إعادةَ استعمالها لاحقاً في تيسير عمليات تحديد الهوية في سياقات جديدة. ويحدث ذلك، على سبيل المثال، عندما يُبرز شخص رخصة القيادة لإثبات هويته عند استلام شارة تعريف الموظف.

١٦- وفي نهاية عملية تحديد الهوية، تصاغ صفات هوية الشخص ذات الصلة عادةً في شكل بيانات يتضمنها مستند إلكتروني يُصدره موفّر الهويات ويُشار إليه باعتباره وسيلة إثبات الهوية. وتقدِّم وسيلة إثبات الهوية بيانات (أو تحيل إلى بيانات) تُستخدم في توثيق الهوية الرقمية أو الصفات المدّعاة للشخص أو الكيان أو الجهاز.[٣٦] ويمكن تجسيد وسيلة إثبات الهوية في عدد من الوسائط. ففي العالم المادي، تشمل أمثلة وسيلة إثبات الهوية ختماً ملكياً أو رخصة القيادة أو جواز السفر أو بطاقة المكتبة أو شارة تعريف الموظف. أما في الساحة الإلكترونية، فإنَّ وسيلة إثبات الهوية قد تكون بسيطة مثل تعريف المستخدم، أو معقدة مثل

(35) في بعض الحالات التي لا تستلزم فيها عملية تحديد الهوية سوى صفات منتقاة، يضطلع بهذا الدور كيان يسمى موفّر الصفات.

(36) OECD Guidance for Electronic Authentication (2007)، في الصفحة ١٢، يمكن الاطلاع عليه في الرابط: http://www.oecd.org/dataoecd/32/45/38921342.pdf.

شهادة رقمية قائمة على الشفرات يمكن تخزينها على حاسوب أو هاتف خلوي أو على بطاقة ذكية أو بطاقة صراف آلي أو محرك أقراص أو جهاز مماثل.

باء- توثيق الهوية

١٧- عندما يُبرز شخص وسيلة لإثبات هويته (مثل رخصة قيادة في المطار أو إدخال تعريف المستخدم في شبكة إحدى الشركات)، ويدعي أنه الشخص الذي تُثبت تلك الوسيلة هويته ويسعى إلى ممارسة حق أو امتياز ممنوحيْن لذلك الفرد (مثل الصعود إلى الطائرة أو الاطلاع على شبكة الشركة أو على قاعدة بيانات حساسة)، ينجز "طرف معوِّل" عملية توثيق لتَبيّن ما إذا كان ذلك الشخص هو فعلاً الشخص الذي يدعي تلك الهوية. وبعبارة أخرى، فإنه عند تصريح شخص ما بهويته (بادعاء أنه الشخص الذي يُثبت المستند هويته)، يُقصد من التوثيق الإجابة عن سؤال "حسناً، كيف لك أن تُثبت ذلك؟" إنه حدث خاص بمعاملة يتعلق بربط شخص ما بإحدى وسائل إثبات الهوية للتحقق من أنَّ الشخص الذي يحاول الاشتراك في المعاملة هو حقاً الشخص الذي حدد المستند هويته سابقاً.

١٨- ويقتضي توثيق الهوية عادةً شيئاً ما يربط الشخص بوسيلة إثبات الهوية، يشار إليه عموماً بأداة التوثيق. فإذا كانت وسيلة إثبات الهوية هي رخصة القيادة أو جواز السفر، فأداة التوثيق هي الصورة، وتجري عملية الربط في هذه الحالة عادةً بمقارنة الصورة التي تحملها رخصة القيادة أو جواز السفر بالشخص الذي يُبرز تلك الوسيلة. أما فيما يتعلق بالوسائل الإلكترونية المخصصة لإثبات الهوية، فإنَّ أداة التوثيق تكون عادةً شيئاً "يعرفه" الفرد (من قبيل كلمة سر أو رقم تحديد الهوية الشخصية)، أو شيئاً "يملكه" الفرد (مثل مفتاح تشفير خاص أو جهاز مادي مثل بطاقة ذكية أو ناقل تسلسلي عام (USB) أو غيرها من أنواع العلامات الرمزية)، أو شيئاً "يجسّده" الفرد، مثل خاصية مادية (من قبيل صورة أو بصمة أو غيرها من البيانات البيومترية).

جيم- إصدار الإذن

١٩- عند نجاح توثيق هوية الشخص، يجوز للطرف المعوِّل أن يستخدم عمليةَ إذْنٍ خاصةً به لتحديد الحقوق والامتيازات التي تُمنح لهذا الشخص (مثلاً ما إذا كان ينبغي أن يتاح لهذا الشخص الوصول إلى موقع شبكي أو قاعدة بيانات أو دخول حانة أو منطقة صعود إلى الطائرة في المطار). وتتناول هذه العملية السؤال "ما الذي تستطيع فعله؟" ومن ثم فإنَّ توثيق الهوية ليس غاية في ذاته. ذلك أنه كثيراً ما يُستخدم في تيسير قرارات الطرف المعوِّل بإصدار

الإذن من قبيل منح حقوق أو امتيازات (مثل الوصول إلى موارد النُّظم على الإنترنت)، أو الدخول في معاملة. فعلى سبيل المثال، عند توثيق هوية شخص يسعى إلى الوصول إلى شبكة حاسوب، يجوز لمالك النظام (أي الطرف المعوِّل) أن يستخدم عمليةَ إذنٍ لتحديد ما ينبغي منحه لهذا الشخص من حقوق الاطلاع. كما أنه عند توثيق هوية شخص يسعى إلى الدخول في معاملة إلكترونية (مثل عقد إلكتروني)، يجوز للطرف المعوِّل استخدام عملية إذن لتحديد ما إذا كان يتعين الاستمرار في المعاملة مع الشخص المعني أو الاكتفاء بدل ذلك بالإبلاغ عن هويته.

دال- الهوية الاتحادية

٢٠- جرت العادة فيما يتعلق بالمعاملات على الإنترنت أن يقوم نفس الطرف الذي يعتزم أيضاً التعويل على وسيلة إثبات الهوية بتحديد الهوية وإصدار وسيلة إثباتها. فعلى سبيل المثال، قد تحدد مؤسسة تجارية هوية موظف وتُصدر له اسم مستخدم وكلمة سر بحيث يتاح له الوصول إلى شبكة الشركة. في هذه الحالة تتصرف الشركة بصفة موفّر الهوية (بما أنها حددت هوية الشخص على أنه من موظفيها وأصدرت وسيلة لإثبات الهوية) وأيضاً بصفة الطرف المعوِّل (بما أنها تقبل أيضاً وسائل إثبات الهوية تلك وتعوّل عليها في منح الوصول إلى شبكتها).

٢١- ولا يضطلع نفس الكيان بالضرورة، فيما يتعلق بالنظام "الاتحادي" لإدارة الهويات، بوظائف موفّر الهوية والطرف المعوِّل، بل يمكن أن يعوّل عدد من الأطراف المعوِّلة التي لا صلة بينها على وسائل إثبات الهوية التي يوفرها أيٌّ من عدة موفّري هويات مستقلين. ويمكن، في إطار هذا النموذج، أن تعوّل منظمات متعددة لم تشارك مباشرة في الإصدار الأصلي لوسيلة إثبات الهوية على وسيلة وحيدة.

٢٢- ومن الأمثلة المألوفة لعمليات إدارة الهويات الاتحادية غير الحاسوبية كيفية إصدار واستخدام رخص القيادة حالياً. فهذه الرخص، التي تُصدرها وكالة حكومية، تستخدمها عدة أطرف معوِّلة لا صلة بينها للتحقق من صفات هوية حامل الرخصة. فعلى سبيل المثال، يمكن أن يستخدمها موظف أمن للتحقق من اسم شخص يريد دخول منطقة الصعود إلى الطائرة بالمطار، أو يستخدمها نادل حانة للتحقق من سن الشخص الذي يطلب شراباً.

٢٣- ومن أمثلة النظام الاتحادي لإدارة الهوياتب على الإنترنت نظام جهاز الصرف الآلي. ففي معاملة نموذجية من معاملات هذا الجهاز، يمكن لفرد لديه حساب بالمصرف أَلِف أن يستخدم وسيلة إثبات الهوية الصادرة عن مصرفه (بطاقة جهاز الصرف الآلي) للحصول على

النقود من جهاز صرف آلي يتولى تشغيله المصرف باء (الذي لا تربطه به أي علاقة). ولإجراء المعاملة، بالرغم من غياب تلك العلاقة، يقوم المصرف باء بالاتصال بالمصرف ألف عن طريق شبكة أجهزة الصرف الآلي لاستبانة ما إذا كان ذلك الفرد زبوناً فعلاً للمصرف ألف وليوثّق المصرف ألف هوية الفرد (هل أدخل ذلك الشخص كلمة السر الصحيحة)، وللحصول من المصرف ألف على بعض المعلومات عن هوية ذلك الفرد (مثلاً هل لدى حساب الشخص ما يكفي من المال لتغطية مبلغ السحب المطلوب، وأيضاً الرصيد المتوفر في حساب ذلك الشخص بحيث يمكن للمصرف باء طبعه على إيصال المعاملة).

رابعاً- المخاطر المتعلقة بنُظم إدارة الهويات

٢٤- هناك العديد من المخاطر المحتملة للمشاركة في نظام لإدارة الهويات والتعويل على بيانات الهوية. وتشمل تلك المخاطر ما يلي:

(أ) المخاطر المتعلقة بتحديد الهوية: تُعتبر موثوقية المعلومات التي يجري جمعها والتثبت منها عن هويات الأشخاص أساسية لاستخدام أي نظام لإدارة الهويات. وتتمثل المخاطر المتعلقة بتحديد الهوية في عدم دقة بيانات صفات الهوية التي يجري جمعها وربطها بشخص معيَّن. وكثيراً ما تكون تلك المخاطر مرتبطة بجودة وسائل إثبات الهوية غير الحاسوبية التي يُبرزها الشخص من أجل إثبات هويته؛

(ب) المخاطر المتعلقة بتوثيق الهوية: يظل تحديد الهوية خلواً من أي قيمة ما لم يكن في مقدور طرف معوِّل توثيق الهوية (أي نسبة صفات الهوية المدّعاة إلى الشخص الصحيح). وتشمل المخاطر المتعلقة بتوثيق الهوية كلاً من مخاطر عدم إمكانية توثيق هوية شخص مشروع توثيقاً سليماً، ومخاطر أن تسفر عملية توثيق الهوية خطأً عن بيان أنَّ شخصاً محتالاً هو الشخص المشروع؛

(ج) المخاطر المتعلقة بالخصوصية: عندما يتعلق الأمر بأفراد، تتعلق إدارة الهويات بجمع موفّر الهويات معلوماتٍ شخصية عن الشخص والتحقق منها وتقاسمها مع عدد من الأطراف المعوِّلة. وعلاوة على ذلك، فإنَّ المعاملات القائمة على الهوية يمكن أن تسهّل تعقّب الأنشطة التي يقوم بها فرد ما، مما يفرز معلومات شخصية إضافية. وتركز المخاطر المتعلقة بالخصوصية على الاستعمال غير المأذون به للمعلومات الشخصية عن الشخص أو إساءة استعمالها من قِبَل طرف يصل إليها، وأيضاً على التزامات الأطراف بالامتثال فيما يتعلق بمعالجة تلك البيانات وحمايتها؛

(د) المخاطر المتعلقة بأمن البيانات: تُعتبر حماية المعلومات الشخصية الخاصة بالأشخاص، وحفظ أمن العمليات اللازمة لإنشاء وسائل آمنة لإثبات الهوية، وإعطاء معلومات دقيقة عن الهوية، والتحقق من وضعية وسائل إثبات الهوية، وتوثيق هوية الأشخاص، أمراً أساسياً لأي نظام لإدارة الهويات. وتشمل تلك المخاطر إمكانية وصول طرف غير مأذون له إلى البيانات الشخصية، والإضرار بأي من العمليات الأساسية للتشغيل العام لنظام إدارة الهويات أو أي معاملات هوية فردية؛

(هـ) المخاطر المتعلقة بالمسؤولية: حتماً تقع في كل نظام لإدارة الهويات أعطال تنجم عنها أضرار. وهكذا يتوجَّب على المشاركين في نظام من نُظم إدارة الهويات معالجة المخاطر المتعلقة بتحميلهم مسؤولية الأضرار التي يتكبدها شخص آخر نتيجةً لمشكلة تسبّبوا فيها أو يُعتبرون مسؤولين عنها قانوناً. ويمثل عدم اليقين القانوني بشأن المسؤولية المرتبطة بأي تصرف أو عطل بعينه أو عدم تصرف أحد المشاركين في نظام لإدارة الهويات، لا سيما النظام الذي يشمل عدداً من القطاعات الصناعية والولايات القضائية، جانباً رئيسياً من جوانب المخاطر المتعلقة بالمسؤولية؛

(و) المخاطر المتعلقة بإمكانية الإنفاذ: المخاطر المتعلقة بإمكانية الإنفاذ تكمِّل المخاطر المتعلقة بالمسؤولية. وتتمثل هذه المخاطر في عدم قدرة أحد المشاركين على إنفاذ '١' حقه في امتثال مشارك آخر للقواعد المقرَّرة، أو '٢' حقه في الحصول على تعويض إذا لحقت به فعلاً أضرار كان مشارك آخر "مسؤولاً" عنها بحكم القانون. وتسري هذه المخاطر إذا حصل خطأ في أمر من الأمور وكان هناك شخص يريد الحصول على تعويض عن ذلك. كما تسري في الحالات التي لم تنشأ فيها مشكلة بعدُ، لكن خللاً في الأداء من جانب مشارك واحد أو أكثر من شأنه أن يعرّض نظام إدارة الهويات برمّته للخطر. وهذا الأمر على درجة كبيرة من الأهمية على الخصوص في النظام الذي يشمل عدة ولايات قضائية. ففي هذه الحالة تشير المخاطر المتعلقة بإمكانية الإنفاذ إلى كل من القدرة على كشف هذه المشكلة والقدرة على مطالبة المشارك بتصحيح أدائه أو بالانسحاب من النظام؛

(ز) المخاطر المتعلقة بالامتثال التنظيمي: تثير المشاركة في نظام لإدارة الهويات في العديد من الحالات مسائل الامتثال القانوني بالنسبة لمشارك واحد أو أكثر (أي ما إذا كان سلوك المشارك يمتثل لأحكام القانون المحلي الساري). أما في حالات أخرى فتكون المشاركة في نظام إدارة الهويات، في حدِّ ذاتها، جزءاً من مجهود يرمي إلى الامتثال للمقتضيات القانونية المفروضة على المشارك في النظام. فعلى سبيل المثال، يجوز لمؤسسة مالية أن تشارك وتعوّل على وسائل إثبات الهوية بهدف الوفاء بالتزاماتها القانونية بتوثيق هوية الأفراد الذين يُمنحون

الوصول إلكترونياً إلى الحسابات المصرفية وتسهيلات الأداء توثيقاً سليماً. في هذه الحالات تركِّز المخاطر المتعلقة بالامتثال على ما إذا كانت هذه المشاركة تفي بالتزاماتها القانونية.

٢٥- وكما هو الشأن في كل نظام، فإنَّ المخاطر التي تقدّم ذكرها تتوقَّف على التكنولوجيا المستخدمة وشتى العمليات المنفَّذة وكيفية تأدية المشاركين أنفسهم لواجباتهم أو تخلفهم عن ذلك (والتأثير المحتمل من أطراف خارجية). وتستلزم إقامة نظام موثوق به لإدارة الهويات تدابير لمعالجة هذه المخاطر، أيْ تدابير ترمي إلى ضمان إمكانية ثقة أولئك المشاركين بالتكنولوجيا المستخدَمة (أي أنها تعمل على نحو سليم)، وبالعمليات المعتمَدة (أي أنها أتَت بالنتيجة الصحيحة)، وبالمشاركين الآخرين (أي أنهم سيؤدون واجباتهم كما ينبغي).

خامساً- معالجة فعالية التشغيل والمخاطر: القواعد التشغيلية

٢٦- لا يقتضي تشغيل نظام اتحادي لإدارة الهويات في وسط إلكتروني، ومعالجةُ المخاطر من قبيل ما تقدّم ذكره، فقط تنفيذ التكنولوجيا المناسبة، بل أيضاً تقيّد جميع المشاركين (مثل الأشخاص وموفّري الهويات والأطراف المعوِّلة) بمجموعة موحَّدة من المعايير التقنية والمقتضيات التشغيلية والقواعد القانونية. وعادةً ما تسعى نُظم إدارة الهويات التجارية إلى تحقيق ذلك الهدف من خلال وضع "قواعد تشغيلية" مناسبة (تسمى أحياناً إطار ثقة) يلتزم بها المشاركون في إطار تعاقدي.

٢٧- وتتألف القواعد التشغيلية الخاصة بنظام إدارة الهويات من فئتين عامتين من المكونات: '١' القواعد التشغيلية والمواصفات التجارية والتقنية اللازمة لضمان فعالية تشغيل النظام وموثوقيته، و'٢' القواعد القانونية القائمة على العقود التي تحدد، إلى جانب القوانين واللوائح التنظيمية المنطبقة، حقوقَ والتزامات الأطراف القانونيةَ الخاصة بنظام إدارة الهويات وتيسّر الإنفاذ عند الضرورة.

(أ) تحدد القواعد التشغيلية التجارية والتقنية متطلبات تشغيل نظام إدارة الهويات على نحو سليم، وتحدد أدوار المشاركين ومسؤولياتهم التشغيلية، وتوفر ضمانة كافية فيما يتعلق بدقة وسلامة وخصوصية وأمن عمليات النظام وبياناته (أي بحيث تكون مختلف الأطراف راغبة في المشاركة؛ ومن ثم يكون النظام جديراً بالثقة). وتستند تلك القواعد في العديد من الحالات إلى المعايير القائمة؛

(ب) تتألف القواعد القانونية القائمة على العقود من اتفاقات تعاقدية بين المشاركين تحدد وتنظّم حقوق المشاركين ومسؤولياتهم القانونية وأيضاً التبعات القانونية التي

يواجهونها فيما يتعلق بنظام إدارة الهويات بعينه، وتوضّح المخاطر القانونية التي تواجهها الأطراف عند المشاركة في نظام إدارة الهويات (من قبيل الضمانات، والمسؤولية عن الخسائر المتكبدة، والمخاطر المحدقة ببياناتهم الشخصية)؛ وتوفر سبل انتصاف في حال تنازع الأطراف، بما فيها أساليب تسوية المنازعات، وآليات الإنفاذ وحقوق الإنهاء والتدابير الخاصة بالتعويضات والغرامات وغيرها من أشكال التبعات. كما أنها تجعل القواعد التشغيلية التجارية والتقنية ملزمة قانوناً للمشاركين وواجبة الإنفاذ إزاءهم.

٢٨- ويخضع كل من القواعد التشغيلية التجارية والتقنية والقواعد القانونية القائمة على التعاقد، بالطبع، إلى الواجبات والالتزامات الأخرى القائمة الناشئة بمقتضى القانون التشريعي والتنظيمي المنطبق على الأطراف، وعادةً ما توضع تلك القواعد بالقياس إلى تلك الواجبات والالتزامات. ويخضع كِلا مكوني القواعد التشغيلية لنظام إدارة الهويات (أي القواعد التشغيلية التجارية والتقنية والقواعد القانونية) إلى التشريعات واللوائح التنظيمية المنطبقة في الولاية (الولايات) القضائية التي سيعمل أو يُستخدم فيها نظام إدارة الهويات.

٢٩- وتشبه القواعد التشغيلية لنظام إدارة الهويات إلى حد بعيد القواعد التشغيلية المستخدَمة في نُظم بطاقات الائتمان أو نُظم السداد الإلكتروني، التي يجب أن تكون قادرة على استيعاب كثير من المشاركين في ولايات قضائية متعددة بموجب مجموعة موحَّدة من القواعد. فعلى سبيل المثال، تنظم القواعد التشغيلية الخاصة ببطاقات الائتمان شؤون الأطراف المصْدرة للبطاقات والمعالِجة لها والأطراف المعوِّلة من التجار، وحاملي البطاقات من الأفراد، وتحدد المواصفاتِ والقواعدَ المنطبقة على المشاركين في المعاملات الائتمانية الإلكترونية والمعالجَة اللاحقة.[٣٧] كما أنَّ القواعد التشغيلية الخاصة بنظام التحويل الإلكتروني للأموال تنظّم مسؤوليات جميع المصارف في عملية السداد، وإلى حد ما مسؤوليات المستهلكين أو الدافعين الآخرين المعنيين، وتحدد

(37) تشمل القواعد التشغيلية لبطاقات الائتمان المواصفات والقواعد الخاصة بالأطراف المصْدرة لتلك البطاقات (مثل the Visa International Operating Regulations في: http://usa.visa.com/merchants/operations/ op_regulations.html وthe Payment Card Industry Data Security Standards— PCIDSS في: https://www.pcisecuritystandards.org/security_standards/index.php) التي أصبحت ملزمة للمصارف المعالِجة للبطاقات والتجار، فضلاً عن العقود المبرمة بين الأطراف المصْدرة لبطاقات الائتمان والمصارف المعالِجة لها، والعقود المبرمة بين المصارف المعالِجة للبطاقات وحاملي البطاقات. وتكمّل هذه القواعدَ القوانينُ واللوائح التنظيمية التي تحكم معالجة بطاقات الائتمان في كل ولاية قضائية معنية.

المواصفاتِ والقواعدَ المنطبقة كلما استُخدمت التحويلات الإلكترونية للأموال (مثل التحويلات بواسطة نظام "سويفت") في تيسير السداد في معاملة إلكترونية.[٣٨]

٣٠- ورغم التسليم، على العموم، بالحاجة إلى قواعد تشغيلية لنُظم إدارة الهويات تحتوي على قواعد قانونية ملائمة، فإنَّ وضع تلك القواعد يبقى مسعى محفوفاً بالمجاهيل إلى حد كبير. ذلك أنَّ من الواجب استبانة ومعالجة كثير من القضايا والعقبات القانونية.

سادساً- القانون المنظِّم لنُظم إدارة الهويات

٣١- توجد في معظم الولايات القضائية قوانين ولوائح تنظيمية عديدة سيكون لها أثر تنظيمي لا يستهان به (ومن شأنها أن تفرض عقبات و/أو متطلبات تتعلق بالامتثال و/أو مخاطر تتعلق بالمسؤولية) على المشاركة في نظام إدارة الهويات. وعلاوة على ذلك، فإنَّ الاختلافات القائمة بين قوانين مختلف الولايات القضائية تشكل، عند النظر إليها في ضوء الطابع العالمي للإنترنت، فسيفساء مشهد تنظيمي من شأنه هو ذاته أن يستعصي على الهيكلة القانونية. فبعض تلك القوانين واللوائح التنظيمية يركز تحديداً على الأنشطة المتصلة بالهوية. فلئن كان معظمها قد وُضع في سياق لا صلة له إطلاقاً بإدارة الهويات (مثل قانون المسؤولية التقصيرية وقانون العقود وقانون الضمانات)، إلا أنَّ من الممكن أن يكون لها أثر لا يستهان به، ومن وجوه في الغالب لم تكن في الحسبان وقت اعتمادها الأصلي.

٣٢- وتشمل بعض فئات القانون الساري على نُظم إدارة الهويات (أو على المشاركين فيها) ما يلي:

(أ) القانون الذي ينظّم دقة المعلومات عن الهوية: تركّز أنشطة نُظم إدارة الهويات على جمع موفّري الهويات أو موفّري صفات الهوية معلومات عن الأشخاص والتحقق من تلك المعلومات، وتزويد الأطراف المعوِّلة ببعض من تلك المعلومات. وكثيراً ما يحدث ذلك في الحالات التي تكون فيها دقة تلك المعلومات و/أو موثوقيتها ذات أهمية. ومن ثم فإنَّ القوانين المتعلقة بتقديم معلومات كاذبة أو غير صحيحة، سواء أكان ذلك عمداً أم

(38) تشمل القواعد التشغيلية الخاصة بالتحويل الإلكتروني للأموال المواصفات والقواعد الخاصة بمعاملات التحويل الإلكتروني للأموال (من قبيل القواعد التشغيلية والمبادئ التوجيهية الخاصة بمؤسسة NACHA — The Electronic Payments Association التي تتخذ من الولايات المتحدة مقراً لها، http://www.nacha.org)، التي أصبحت ملزمة للمصارف المعالِجة والتجار، فضلاً عن العقود المبرمة بين التجار والدافعين من الأفراد. وتكمّل هذه القواعدَ القوانينُ واللوائح التنظيمية التي تحكم التحويلات الإلكترونية للأموال مثل the Electronic Funds Transfer Act وRegulation E (في الولايات المتحدة).

سهواً، ستكون ذات صلة في تقييم حقوق المشاركين في نُظم إدارة الهويات وواجباتهم ومسؤولياتهم. ومن أهم تلك القوانين قانون المسؤولية التقصيرية الذي ينظم تزييف الحقائق الناجمَ عن الإهمال والمصادقة الناجمة عن الإهمال وتشويه السمعة، إلى جانب قوانين الضمانات، والقوانين الخاصة بانتحال الشخصية، والقوانين التي تنظّم الممارسات التجارية الخداعية وغير المشروعة؛

(ب) القانون الذي يحكم خصوصية المعلومات عن الهوية: تقتضي إدارة الهويات، بطبيعتها، في العادة جمع (موفّر هويات أو وكلائه) معلوماتٍ شخصيةً عن الشخص وتبليغها (إلى طرف معوِّل).[٣٩] ومن ثم فإنَّ للقوانين الخاصة بحماية البيانات والقوانين المتعلقة بالخصوصية وغيرها من القوانين واللوائح التنظيمية التي تنظّم جمع واستخدام ومعالجة وتحويل وتخزين البيانات الشخصية أثراً كبيراً في أنشطة إدارة الهويات. ولئن كان العديد من هذه القوانين قد وُضع قبل ظهور نُظم إدارة الهويات الرقمية، وبالتالي لم يكن لها أن تتحسب للعمليات الخاصة أو للأضرار المحتملة التي تنطوي عليها مثل هذه النُّظم، إلا أنَّ من شأنها مع ذلك أن يكون لها وقع مباشر على مثل هذه الأنشطة؛

(ج) القانون الذي ينظم جمع المعلومات الخاصة بالهوية: إلى جانب القوانين المتعلقة بالخصوصية والقوانين المتعلقة بحماية البيانات، تسري القوانين المنظِّمة لإعادة استخدام معلومات القطاع العام على المؤسسات التجارية التي تُنتج نواتج معلومات وخدمات استناداً إلى بيانات متأتية من القطاع العام. ومن شأن تلك القوانين أن تضع عقبات قانونية في طريق الاستخدام الواسع للبيانات التي تحتفظ بها هيئات القطاع العام في سياق خدمات إدارة الهويات؛[٤٠]

(د) القانون المنظِّم لأمن المعلومات والعمليات الخاصة بالهوية: يفرض العديد من القوانين التزامات على الشركات فيما يتعلق بأمن المعلومات الشخصية (على اختلاف تعريفها في شتى الولايات القضائية، وبموجب القوانين الخاصة بكل قطاع) وسائر البيانات التي تحوزها. ففضلاً عن القوانين واللوائح التنظيمية التي تستوجب تنفيذ تدابير أمنية من أجل حماية البيانات، سنّت ولايات قضائية كثيرة أيضاً قوانين ووضعت لوائح تنظيمية تُوجب إطلاع الأشخاص المعنيين على المخالفات الأمنية التي تمس المعلومات الشخصية؛

(39) إلا إذا لم يكن الشخص إنساناً –كأن يكون مؤسسة أو جهازاً أو تطبيقاً من تطبيقات البرامجيات، وغير ذلك.

(40) انظر، على وجه العموم، Global Networking of Individuals (GINI), Legal provisions for Deploying INDI Services (٥ تشرين الأول/أكتوبر ٢٠١١)، الباب الخامس، متاح في الرابط: www.gini-sa.eu/images/stories/2011.11.06_GINI_D3.1_Legal%20Provisions%20for%20Deploying%20INDI%20Services_FINAL.pdf.

(هـ) القوانين التي تركز على واجب تحديد الهوية: تشترط قوانين ولوائح تنظيمية عديدة الإفصاح عن الهوية باعتباره عنصراً من العناصر المكوّنة، لا سيما في البيئة الإلكترونية. فعلى سبيل المثال، تشترط اتفاقية الخطابات الإلكترونية صراحةً تعيين الهوية باعتباره مكوناً من مكونات التوقيع الإلكتروني الملزم قانوناً. وهكذا تنص الاتفاقية تحديداً على أنه حيثما يشترط القانون أن يكون الخطاب أو العقد ممهوراً بتوقيع طرف ما، يُستوفى شرط التوقيع إذا استُخدمت طريقة ما لتعيين هوية الطرف المعني وتبيين نية ذلك الطرف فيما يخص المعلومات الواردة في الخطاب الإلكتروني؛[٤١]

(و) القوانين التي تركز على واجب توثيق الهوية: "تنظّم عدة قوانين عنصراً أو أكثر من عناصر توثيق الهوية. فبعض تلك القوانين يفرض على المؤسسات التجارية واجب توثيق هوية الأشخاص الذين تتعامل معهم عن بعد، بينما تنظّم أخرى جوانب من عملية توثيق الهوية. ومن أبرز الأمثلة على ذلك الاشتراطاتُ التي تضعها الهيئات التنظيمية المصرفية الأمريكية لتوثيق الأنشطة المصرفية الإلكترونية. وهكذا يجب على المؤسسات المالية التي تعرض على زبائنها منتجات وخدمات على الإنترنت، على وجه التحديد، أن "تستخدم طرائق فعالة في توثيق هويات الزبائن الذين يستخدمون تلك المنتجات والخدمات".[٤٢] واعتمدت بلدان أخرى مثل سنغافورة اشتراطات مماثلة؛[٤٣]

(ز) القوانين التي تنظم تحديداً الأنشطة الخاصة بنُظم إدارة الهويات: تمتلك بعض الولايات القضائية قوانين تنظم صراحةً بعض جوانب الأنشطة الخاصة بإدارة الهويات. ومن أمثلة تلك القوانين التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية[٤٤] الذي ينص على أنْ تنظّم الدول الأعضاء جمع بيانات شخصية عن الأشخاص من جانب بعض موفري الهويات (ممن يسمّون مقدمي خدمات التصديق)، والذي ينظّم إصدار وسائل إثبات الهوية.[٤٥] كما أنَّ قانون الأونسيترال النموذجي بشأن التوقيعات

(41) الفقرة ٣ من المادة ٩ من اتفاقية الخطابات الإلكترونية.

(42) Federal Financial Institutions Examination Council ("FFIEC"), "Authentication in an Internet Banking Environment,"، ١٢ تشرين الأول/أكتوبر ٢٠٠٥، الصفحة الأولى، متاح في الرابط: www.ffiec.gov/pdf/authentication_guidance.pdf.

(43) Monetary Authority of Singapore, Circular No. SRD TR 02/2005، ٢٥ تشرين الثاني/نوفمبر ٢٠٠٥.

(44) Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures ("EU Electronic Signatures Directive")، المواد ٦-٨ والمرفقان ١ و٢، متاح في الرابط: http://europa.eu/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.

(45) EU Electronic Signatures Directive، المادة ٨.

الإلكترونية يضع (في مواده من ٨ إلى ١٢) قواعد لإصدار واستخدام وسائل إثبات الهوية المطلوبة لإنشاء بعض التوقيعات الإلكترونية.

حاء- التحديات والعقبات القانونية المطروحة

٣٣- تطرح القوانين واللوائح التنظيمية القائمة، من الأنواع المشار إليها آنفاً، ومن أنواع أخرى، عدة مشكلات أساسية تعترض وضع وتشغيل نُظم لإدارة الهويات في القطاع الخاص. وتشمل تلك التحديات ما يلي:

(أ) لم يوضَع قانون يتناول خصيصاً مسألة إدارة الهويات: لا يتطرق القانون القائم إلى عدد من المسائل المستجدة التي تُفرزها عمليات إدارة الهويات. فجلّ القوانين القائمة المنطبقة في هذه السياقات لم تُصَغ من منظور نُظم إدارة الهويات الرقمية، وبالتالي فهي لا تتناول ولا تنظّم الأنشطة الخاصة بإدارة الهويات على نحو كاف أو ملائم. فعلى سبيل المثال، لا يتطرق القانون الموجود إلى واجب توخي العناية الذي يجب أن يستوفيه مثْبت الهوية عند تقييم أصالة وثائق إثبات الهوية، ولا إلى نطاق أي واجب إفصاح يقع على عاتق موفّر الهويات إزاء الشخص صاحب البيانات؛

(ب) عدم اليقين/الالتباس القانوني: ثمة بعض المسائل الخاصة بإدارة الهويات يمكن أن تتناولها القوانين واللوائح التنظيمية القائمة، لكن انطباق تلك القوانين كثيراً ما يتسم بالالتباس وعدم الوضوح، بحيث يضع المشاركين في نُظم إدارة الهويات أمام قدر كبير من عدم اليقين القانوني من شأنه أن يبطئ عجلة النمو والابتكار والاستثمار. وعليه، فإنه حتى في الحالات التي ينطبق فيها القانون القائم على إدارة الهويات، قد لا تكون الكيفية التي سينطبق بها على مسألة محدَّدة أو نهج مقترح في نظام لإدارة الهويات واضحةً. وينسحب ذلك بالخصوص على القوانين التي تركز على تكنولوجيا بعينها. ومن شأن ذلك أن يحد من قدرة الأطراف في معاملات خاصة بالهوية على تقييم وتدبير المخاطر التي تتكبدها تلك الأطراف نتيجة دخولها في تلك المعاملات؛

(ج) المسائل المتعلقة بالخصوصية: عادة ما تنطوي إدارة الهويات، بطبيعتها، على جمع موفّر الهويات بعض المعلومات الشخصية عن الشخص وتبليغها إلى طرف معوِّل. ذلك أنه يجب على هؤلاء الأشخاص، لكي تتسنى لهم المشاركة في نظام لإدارة الهويات، الإفصاح عن معلومات شخصية مما يُعرِّضهم لخطر استخدام تلك المعلومات من دون إذن أو على نحو غير مناسب. وعلاوة على ذلك، فإنه لمّا كان هؤلاء الأشخاص يتفاعلون مع عدة أطراف

معوِّلة، فإنَّ الإفصاح المطلوب من موفّر الهويات عن المعلومات الخاصة بهم أو التحققَ منها يتيح له تعقّب أنشطة كل شخص من هؤلاء الأشخاص مما يثير شواغل بشأن جمع واستخدام تلك المعلومات الخاصة بالمعاملة. ومن ثم فإنَّ الخصوصية مسألة أساسية لأي نظام لإدارة الهويات. وقد يقتضي الأمر في هذه الحالة تناول أسئلة معيَّنة من قبيل: '١' ما المعلومات التي يمكن أن يجمعها موفّر الهويات؟ '٢' ما حجم المعلومات التي يمكن كشفها للأطراف المعوِّلة؟ '٣' ما نوع السيطرة التي يملكها الشخص فيما يتعلق بالكشف عن المعلومات؟ '٤' على أي نحو يجب على الأطراف أن تعالج البيانات بأمان؟ '٥' ما القيود المفروضة على استخدام موفّر الهويات أو الأطراف المعوِّلة للمعلومات المتوافرة؟ وهذه الأسئلة كثيراً ما تتناولها القوانين القائمة، التي يمكن أن تكمّلها أيضاً القواعد التشغيلية القائمة على التعاقد؛

(د) المسائل المتعلقة بالمسؤولية: يمثّل تحديد الطرف الذي سيتحمل المسؤولية المرتبطة بأي من المخاطر الناشئة (انظر الفقرة ٢٤ أعلاه) شاغلاً قانونياً بالغ الأهمية يساور المشاركين في أي نظام لإدارة الهويات. وقد قُدّم العديد من النظريات القانونية ونظريات في مجال القانون العام والعقود بهدف استبانة وتعريف وتوضيح منشأ ونطاق تلك التبعات المحتملة.[٤٦] إلا أنَّ هذه المخاطر القانونية كثيراً ما تتسم بسوء التعريف وبعدم اليقين. وتمثل الشواغل بشأن المسؤولية عقبة أساسية في طريق اعتماد القطاع الخاص حلولاً قابلة للتنفيذ المتبادل. وغالباً ما تكون معالجة المسائل المتعلقة بالمسؤولية من خلال القواعد التشغيلية أو غيرها من أشكال الاتفاق التعاقدي بين المشاركين أفضلَ النُّهُج، لأنَّ ذلك يسمح على الخصوص "بالتكييف" المطلوب للعقد مع أهداف خاصة من أجل معالجة التوزيع المناسب للمخاطر، والذي سيختلف من حالة إلى أخرى؛

(هـ) الاختلافات والتنازع بين الولايات القضائية: هناك قضايا أساسية يختلف بشأنها تطبيق القوانين واللوائح التنظيمية القائمة لتحديد الأنشطة المنجزة اختلافاً شديداً بين الولايات القضائية. وينسحب ذلك في الغالب على القوانين التي تنظم مسؤولية المشاركين والقوانين المتعلقة بحماية البيانات والتي تنظم خصوصية المعلومات الشخصية. وفضلاً عن ذلك، يمكن أن يطرح تنظيم أنشطة نُظم إدارة الهويات أو الترخيص لها، في بعض الحالات، عقبات إضافية أمام تشغيل نُظم إدارة الهويات عبر الحدود. وهكذا فإنَّ التحديات التي تواجه وضع قواعد تشغيلية مناسبة، عندما تعمل نُظم إدارة الهويات عبر حدود الولايات القضائية،

(46) انظر *Certification Authority Liability Analysis*، (دراسة موجَّهة لرابطة المصرفيين الأمريكيين تناقش مخاطر التبعات المحتمل أن يواجهها موفّر هويات يتصرف بصفة سلطة تصديق)، يمكن الاطلاع عليها في الرابط: http://64.78.35.30/article/ca-liability-analysis.pdf.

تتعاظم بسبب اختلاف القوانين واللوائح التنظيمية القائمة (اختلافاً شديداً في كثير من الحالات) بين الولايات القضائية؛

(و) الحاجة إلى العمل القانوني المشترك: تواجه نُظم إدارة الهويات تحدي إمكانية تفاوت القوانين المنطبقة فيما بين الولايات القضائية. ففي غياب قوانين موحَّدة تنظم أنشطة نُظم إدارة الهويات، كثيراً ما تسعى هذه النُّظم إلى معالجة هذه المشكلة عبر وضع قواعد تشغيلية تتيح للنظام برمّته العمل القانوني المشترك. ويطرح تفاوت القوانين واللوائح التنظيمية فيما بين الولايات القضائية تحدياً أمام وضع تلك القواعد التشغيلية وغيرها من العقود اللازمة لضمان قدر أكبر من الاتساق في أداء المشاركين في النظام عبر النُّظم الإلكترونية؛

(ز) القيود المفروضة على القدرة على تعديل أحد القوانين بواسطة عقد: يمكن تعديل بعض القوانين واللوائح التنظيمية بواسطة عقد. فعلى سبيل المثال، تتضمن عدة تشريعات مبادئ العقود أو القانون التجاري التي تكتفي بوضع "قواعد القصور" التي تنطبق في غياب اختيار صريح من جانب الأطراف، لكنها تسمح بتعديل تلك القواعد باتفاق بين أطراف المعاملة. في مثل هذه الحالات تُترك للأطراف في نظام إدارة الهويات حرية تعديل قواعد القصور وملء الفراغات باستخدام قواعد تشغيلية مناسبة قائمة على التعاقد. وبالمقابل، لا يمكن في حالات أخرى تجاهل القواعد القانونية الإلزامية بناء على مجرد اتفاق بين الأطراف، لكونها تخدم أغراض السياسات العامة من قبيل حماية المستهلكين أو أطراف ثالثة.

٣٤- ونتيجة لذلك، فإنَّ القوانين القائمة تضع عقبات أمام اعتماد نُظم لإدارة الهويات تتسم بالكفاءة ويمكن أن تعمل عبر الحدود وقابلة للتشغيل المتبادل وجديرة بالثقة. ذلك أنَّ وضع قواعد تشغيلية قائمة على العقود لنظام من نُظم إدارة الهويات هو الطريقة الرئيسية لمعالجة هذه التحديات القانونية والحد من عدم اليقين بالنسبة للمشاركين. كما أنه يسهّل تجريب النظام قياساً إلى مختلف النُّظم والنُّهُج المعتمدة في إطار سعي السوق لحل مسألة إدارة الهويات.

٣٥- ولجميع المشاركين في نظام اتحادي لإدارة الهويات مصلحة في التوزيع العادل، مقدّماً، لمخاطر المسؤولية المترتبة على المشاركة في العملية، وتخفيف تلك المخاطر إلى أدنى حد ممكن. فضروب عدم اليقين القانوني القائمة تشكِّل، عند عدم معالجة الكيفية التي ينبغي بها توزيع تلك المسؤولية، أو تحديد الطرف الأقدر على تحمُّل المخاطر، عقبة رئيسية في طريق تنفيذ نظام لإدارة الهويات جدير بالثقة. ولمّا كانت عمليات إدارة الهويات تُستخدم في معاملات شديدة الأهمية، وكانت المخاطر التي تواجه الأطراف تزداد تبعاً لذلك، فإنَّ جميع الأطراف تستفيد استفادة جمة من تنفيذ قواعد تشغيلية مناسبة لمعالجة تلك المخاطر مسبقاً

وتخفيف حدة تلك المخاطر (إلى أدنى حد ممكن) من خلال اشتراط تأدية كل من المشاركين التزامات محدَّدة.

٣٦- ويكمن التحدِّي المستقبلي بهذا الخصوص في وضع نُظم لإدارة الهويات للمعاملات التجارية في القطاع الخاص تكون قابلة للتشغيل المتبادل عبر الحدود. ويرجَّح أن تكون القواعد التشغيلية الخاصة بنُظم إدارة الهويات قائمة على العقود، على غرار نُظم بطاقات الائتمان والسداد الإلكتروني، لا سيما وأنه يراد لها أن تنتشر على نطاق الإنترنت عبر حدود الولايات القضائية. ولعلَّ التشريعات الرامية إلى إزالة العقبات التي تعترض سبيل هذه النُّظم (بدل تنظيمها) مناسبة للنظر فيها.

* * *

تعاريف

[ملاحظة: هذه التعاريف ذات طبيعة عامة، والغرض الوحيد من إيرادها هو المساعدة على فهم النص أعلاه]

الصفة: سمة معيَّنة أو خاصية متأصلة في شخص ما أو منسوبة إليه، مثل الاسم والعنوان والسن ونوع الجنس واللقب والراتب والثروة ورقم رخصة القيادة ورقم الاشتراك في الضمان الاجتماعي، وغير ذلك (فيما يتعلق بكائن بشري)، والنوع والطراز، والرقم التسلسلي والموقع والقدرة وغيرها من السمات (فيما يتعلق بجهاز)، إلى آخره.

مرادف: صفة الهوية.

موفّر صفات الهوية: كيان يتصرف بصفة مصدر موثوق لصفة واحدة أو أكثر من الصفات المميزة لهوية شخص ما، وهو مسؤول عن العمليات المتعلقة بجمع هذه الصفات والاحتفاظ بها. ويتثبت موفّر الصفات من ادعاءات الصفات الموثوقة والمتحقَّق منها استجابة للطلبات الصادرة عن موفّري الهويات والأطراف المعوِّلة بشأن توفير صفات الهوية. ومن أمثلة الجهات الموفّرة للصفات سجل حكومي لسندات الملكية، أو مكتب ائتمان وطني أو قاعدة بيانات خاصة بالتسويق التجاري.

توثيق الهوية: عملية التحقق من هوية الشخص المدّعاة عبر تأكيد تطابقها مع إحدى وسائل إثبات الهوية. مثلاً، يُفترض في عملية إدخال كلمة مرور مرتبطة باسم المستخدم التحققُ من أنَّ المستخدم هو الشخص الذي أُصدرت له كلمة المرور. وعلى نحو مماثل، فإنَّ مقارنة

شخص يُبرز جواز سفره بالصورة التي يحملها الجواز تمكّن من التحقق من أنه الشخص الذي يصفه الجواز أو تأكيد ذلك.

أداة توثيق الهوية: شيء يُستخدم في التحقق من الصلة القائمة بين الشخص ومستند إثبات الهوية، وعادة ما تكون أداة توثيق الهوية شيئاً أو بنداً معرفياً أو خاصية ما تميّز صاحبها وتُستخدم في إقامة صلة بين الشخص ووسيلة إثبات الهوية. فعلى سبيل المثال، تؤدي كلمة المرور دور أداة توثيق هوية المستخدم، بينما تؤدي الصورة دور أداة توثيق الهوية عندما يتعلق الأمر بجواز السفر أو رخصة القيادة.

الإذن: عملية منح حقوق وامتيازات إلى أشخاص وُثّقت هوياتهم استناداً إلى معايير يحددها الطرف المعوِّل. ويتوخى الإذن مراقبة الوصول إلى المعلومات أو الموارد بحيث لا يُتاح الوصول إلى تلك الموارد إلا لمن يُسمح له باستعمالها تحديداً.

وسيلة إثبات الهوية: البيانات المدلى بها لإثبات هوية الشخص المدّعاة. وتشمل الوسائل الورقية لإثبات الهوية جوازات السفر وشهادات الميلاد ورخص القيادة وبطاقات هوية الموظفين. أما الوسائل الرقمية لإثبات الهوية فتشمل أسماء المستخدمين والبطاقات الذكية والشهادات الرقمية.

نظام اتحادي لإدارة الهويات: نظام لإدارة الهويات يمكن أن يَستخدم فيه الشخص وسيلة لإثبات الهوية صادرة عن أيٍّ من عدة موفّري هويات لتوثيق هويته فيما يخص عدة أطراف معوِّلة لا صلة بينها عبر نُظم مختلفة.

تحديد الهويات: عملية جمع ما يكفي من المعلومات عن صفات شخص معيَّن للتعريف بهويته وتأكيدها في سياق معيَّن، والتحقق من تلك المعلومات واعتمادها (مترادفان: التسجيل، إثبات الهوية).

الهويات: معلومات عن شخص معيَّن في شكل صفة واحدة أو أكثر تتيح تمييز الشخص على نحو كاف في سياق محدَّد. إنها مجموعة من صفات الشخص التي تتيح تمييزه عن الأشخاص الآخرين في سياق معيَّن.

إدارة الهويات: العمليات والوظائف والقدرات المتوافرة الخاصة بجمع معلومات عن هوية شخص ما والتحقق منها وتوثيقها وتبليغها إلى الطرف المعوِّل بحيث يتسنى لهذا الأخير التحقق من تطابق تلك المعلومات مع شخص معيَّن.

موفّر الهويات: هو كيان مسؤول عن تحديد هويات أشخاص و/أو كيانات اعتبارية و/أو أجهزة و/أو أشياء رقمية، ثم إصدار وسائل مناظرة لإثبات تلك الهويات والاحتفاظ بتلك المعلومات عن هويات الأشخاص وإدارتها (مترادفات: مقدّم خدمات وسائل إثبات الهوية؛ السلطة المعنية بالتصديق؛ موفّر صفات الهوية (في الحالات التي يدلَى فيها ببيانات محدودة عن الصفات)).

نظام إدارة الهويات: هو بيئة إلكترونية لإدارة الهويات تنظّمها مجموعة من القواعد التشغيلية يمكن فيها ضمان الثقة المتبادلة فيما بين الأفراد والمنظمات والخدمات والأجهزة لأنَّ مصادر ذات حجية تحدد هويات تلك الكيانات وتوثّقها.

القواعد التشغيلية: العمليات التجارية والمواصفات التقنية والقواعد القانونية التعاقدية، التي تنظم تشغيل نظام معيَّن لإدارة الهويات. وعادةً ما توضع القواعد التشغيلية على نحو خاص (إذ يضعها مثلاً مشغّل نظام إدارة الهويات)، وتصبح ملزمة للمشاركين في النظام وواجبة الإنفاذ إزاءهم عبر عقد. (مترادفات: إطار الثقة؛ قواعد النظام؛ القواعد التشغيلية الموحَّدة؛ اللوائح التشغيلية).

الطرف المعوِّل: الشخص أو الكيان الاعتباري الذي يُعوِّل على وسيلة من وسائل إثبات الهوية أو تأكيد الهوية من أجل تقرير ما يتعين اتخاذه من إجراءات في سياق تطبيق معيَّن، مثل معالجة معاملة أو إتاحة الوصول إلى معلومات أو إلى نظام (مرادف: مقدّم الخدمات).

الشخص: الفرد أو الكيان الاعتباري أو الجهاز أو الشيء الرقمي الذي تحدد هويتَه وسيلة من وسائل إثبات الهوية ويمكن توثيق هويته أو ضمانها من طرف موفّر الهويات (مترادفان: الشخص موضوع البيانات؛ المستخدم).