تعزيز الثقة بالتجارة الإلكترونية: المسائل القانونية الخاصة باستخدام طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي

الأمم المتحدة

لجنـــة الأمـم المتحـدة للقـانون التجـاري الـدولي

تعزيز الثقة بالتجارة الإلكترونية : المسائل القانونية الخاصة باستخدام طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي

الأمم المتحدة
فيينا، ٢٠٠٩

منشـورات الأمم المتحـدة
Sales No. A.09.V.4
ISBN 978-92-1-633051-4

تصـــدير

في عام ٢٠٠٤، عندما استكمل الفريق العامل الرابع (المعني بالتجارة الإلكترونية)، التابع للجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال)، عمله بشأن الاتفاقية المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية، طلب إلى الأمانة أن تواصل رصد مختلف المسائل ذات الصلة بالتجارة الإلكترونية، بما فيها المسائل ذات الصلة بالاعتراف بالتوقيعات الإلكترونية عبر الحدود، وأن تنشر نتائج بحوثها بغية تقديم توصيات إلى اللجنة بشأن ما إذا كان من الممكن الاضطلاع بأعمال في هذه المجالات في المستقبل (انظر الوثيقة A/CN.9/571، الفقرة ١٢).

ثم في عام ٢٠٠٥، أحاطت اللجنة علما بالأعمال التي اضطلعت بها منظمات أخرى في مختلف المجالات ذات الصلة بالتجارة الإلكترونية، وطلبت إلى الأمانة إعداد دراسة أكثر تفصيلا وتتضمّن مقترحات بشأن شكل وطبيعة وثيقة مرجعية شاملة تُناقش فيها مختلف العناصر اللازمة لإنشاء إطار قانوني مؤاتٍ للتجارة الإلكترونية، وهي وثيقة قد تنظر اللجنة في إعدادها في المستقبل بغية تقديم المساعدة إلى المشرِّعين ومقرِّري السياسات العامة في جميع أنحاء العالم في هذا الصدد.[١]

وفي عام ٢٠٠٦، نظرت لجنة الأونسيترال في مذكّرة أعدّتها أمانتُها عملا بذلك الطلب (A/CN.9/604). وقد حدّدت المذكّرة المجالات التالية باعتبارها من جملة المكوّنات التي يمكن أن تشتمل عليها وثيقة مرجعية شاملة في هذا الخصوص، وهي: *(أ)* توثيق التوقيعات الإلكترونية والاعتراف بها عبر الحدود؛ *(ب)* مسؤولية مقدِّمي خدمات المعلومات ومعايير سلوكهم؛ *(ج)* الفوترة الإلكترونية والمسائل القانونية ذات الصلة بسلاسل التوريد في التجارة الإلكترونية؛ *(د)* إحالة الحقوق في السلع الملموسة وغيرها من الحقوق من خلال الخطابات الإلكترونية؛ *(هـ)* المنافسة غير الشريفة والممارسات التجارية الخداعية في التجارة الإلكترونية؛ *(و)* الخصوصية وحماية البيانات في التجارة الإلكترونية. وقد حدّدت تلك المذكّرة أيضا مسائل أخرى مما يمكن إدراجه في وثيقة من هذا القبيل، وإن كان ذلك على نحو أوجز، وهي: *(أ)* حماية حقوق الملكية الفكرية؛ *(ب)* الخطابات الإلكترونية التطفّلية (البريد الإلكتروني المزعج "Spam")؛ *(ج)* الجريمة السيبرانيّة. وفي تلك الدورة أُعرب عن تأييد للرأي الذي مفاده أن مهمّة المشرِّعين ومقرّري السياسات العامة، وخصوصا في البلدان النامية، قد تُسهَّل بقدر كبير إذا ما عمدت اللجنة إلى صوغ وثيقة مرجعية شاملة تعالج المواضيع الرئيسية التي حدّدتها الأمانة. وقيل أيضا إن تلك الوثيقة قد تساعد اللجنة أيضا على استبانة المجالات التي قد تضطلع فيها هي ذاتها بأعمال بخصوص المواءمة بين النظم في المستقبل. وقد طلبت اللجنة من أمانتها إعداد عيّنة جزئية من الوثيقة المرجعية الشاملة، تتناول فيها على وجه التحديد المسائل ذات الصلة بتوثيق التوقيعات الإلكترونية والاعتراف بها عبر الحدود، لغرض استعراضها في دورتها الأربعين في عام ٢٠٠٧.[٢]

---

[١] *الوثائق الرسمية للجمعية العامة، الدورة الستون، الملحق رقم ١٧* (A/60/17)، الفقرة ٢١٤.

[٢] المرجع نفسه، *الدورة الحادية والستون، الملحق رقم ١٧* (A/61/17)، الفقرة ٢١٦.

وقُدِّم الفصل الذي أعدّته الأمانة كعيِّنة وفقا لذلك الطلب (A/CN.9/630 وAdd.1 إلى Add.5) إلى اللجنة في دورتها الأربعين. وأشادت اللجنة بالأمانة لإعدادها ذلك الفصل وطلبت إلى الأمانة أن تنشره في شكل منشور مستقل.[٣]

وهذا المنشور يعرض دراسة تحليلية للمسائل القانونية الرئيسية الناشئة عن استخدام التوقيعات الإلكترونية وطرائق توثيقها في المعاملات الدولية. فالجزء الأول يقدّم لمحة عامة عن الطرائق المستخدمة لأغراض التوقيع والتوثيق الإلكترونيين ومعاملتهما القانونية في ولايات قضائية مختلفة. ويبحث الجزء الثاني في استخدام طرائق التوقيع والتوثيق الإلكترونية في المعاملات المالية والتجارية الدولية، ويحدّد المسائل القانونية الرئيسية ذات الصلة بالاعتراف بتلك الطرائق عبر الحدود. ولقد لوحظ، من منظور دولي، أن من المرجّح أن تنشأ صعوبات قانونية فيما يتعلق باستخدام طرائق التوقيع والتوثيق الإلكترونية عبر الحدود، والتي تتطلّب إشراك أطراف ثالثة في عملية التوقيع أو التوثيق. وهذه هي الحالة، مثلا، فيما يخص طرائق التوقيع والتوثيق الإلكترونية المدعومة بشهادات تصديق صادرة عن مقدِّم خدمات تصديق باعتباره طرفا ثالثا موثوقا به في توقيعات رقمية معيّنة في إطار مرفق مفاتيح عمومية (PKI). ولهذا السبب، فإن الجزء الثاني من هذه الوثيقة يخصّ بالاهتمام موضوع استخدام التوقيعات الرقمية على الصعيد الدولي في إطار مرفق مفاتيح عمومية. ولكن، لا ينبغي أن يُفهم هذا التركيز على أنه تفضيل أو تأييد لهذا النوع أو أي نوع آخر من طرائق أو تكنولوجيا التوثيق.

[٣] المرجع نفسه، *الدورة الثانية والستون، الملحق رقم ١٧* (A/62/17)، الفقرة ١٩٥.

المحتــويات

الصفحة

مقدّمة

١- استحدثت تكنولوجيا المعلومات والحاسوب عدّة وسائل مختلفة لربط المعلومات التي هي في صيغة إلكترونية بأشخاص معيّنين أو كيانات معيّنة، من أجل ضمان سلامة تلك المعلومات أو من أجل تمكين الأشخاص من إثبات الحق أو الإذن الممنوح لهم لإحراز سبل الوصول إلى خدمة معيّنة أو إلى مستودع معلومات. وهذه الوظائف يُشار إليها أحيانا بمصطلح عام هو طرائق "التوثيق" الإلكتروني أو طرائق "التوقيع" الإلكتروني. ولكن، هناك أحيانا تمييز بين "التوثيق" الإلكتروني و"التوقيع" الإلكتروني. ومن ثم فإن استخدام هذين المصطلحين على هذا النحو لا يتسبب في عدم الاتّساق فحسب، بل إنه مضلِّل إلى حد ما أيضا. ففي بيئة قائمة على الوسيلة الورقية، لا تحمل الكلمتان "التوثيق" و"التوقيع" ولا الفعلان المتصلان بهما، وهما "يوثّق" و"يوقّع"، الدلالة نفسها المسندة إليها في مختلف النظم القانونية، بل إن لها مدلولات وظيفية قد لا تتوافق بالضرورة مع غرض ووظيفة ما يسمى طرائق "التوثيق" و"التوقيع" الإلكترونية. علاوة على ذلك، فإن الكلمة "التوثيق" تُستخدم أحيانا بمعنى عام فيما يتعلّق بأي ضمان لمرجعية تحرير المعلومات وسلامتها، ولكنّ بعض النظم القانونية قد تميّز بين تلك العناصر. ولذا فإن من الضروري عرض لمحة عامة موجزة للاختلافات في المصطلحات والفهم القانوني، بغية تحديد نطاق هذه الوثيقة.

٢- فبمقتضى القانون العام بشأن أدلّة الإثبات المدنية، يُعتبر السجل أو المستند "موثَّقا" إذا كان ثمّة دليل يثبت أن ذلك المستند أو السجل "هو ما يدّعيه مؤيِّدُه".[١] ومفهوم "المستند" في حدّ ذاته واسع إلى حد ما ويشمل عموما "أي شيء تُسجَّل فيه معلومات أيّا كان وصفها".[٢] ومن شأن ذلك أن يشمل، مثلا، أشياء كالصور الضوئية لشواهد القبور والمساكن،[٣] ودفاتر الحسابات[٤] والرسوم والمخطّطات.[٥] أما جدارة اعتبار مستند ما دليل إثبات فتُقرّر بربط ذلك المستند بشخص أو مكان أو شيء بعينه، وهي عملية تُعرف في بعض الولايات القضائية التي تطبّق القانون العام باسم "التوثيق".[٦] والتوقيع على مستند هو وسيلة شائعة—وإن

---

[١] الولايات المتحدة الأمريكية، (Federal Rules of Evidence) القواعد الاتحادية الخاصة بأدلة الإثبات، القاعدة ٩٠١، البند الفرعي *(أ)*: ("اقتضاء التوثيق أو إثبات الهويّة كشرط سابق للقبول يُستوفى بدليل إثبات كاف لدعم استنتاج بأن المسألة المعنية هي ما يدّعيه مؤيِّدها.").

[٢] المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية، قانون أدلّة الإثبات المدنية (Civil Evidence Act) لعام ١٩٩٥، الفصل ٣٨، القسم ١٣.

[٣] *Lyell v. Kennedy* (No. 3) (1884) 27 Ch.D. 1 (United Kingdom, Chancery Division).

[٤] *Hayes v. Brown* [1920] 1 K.B. 250 (United Kingdom, Law Reports, King's Bench).

[٥] *J. H. Tucker & Co., Ltd. v. Board of Trade* [1955] 2 All ER 522 (United Kingdom, All England Law Reports).

[٦] *Farm Credit Bank of St. Paul v. William G. Huether,* 12 April 1990 (454 N.W.2d 710, 713) (United States, Supreme Court of North Dakota, North Western Reporter).

لم تكن حصرية—من وسائل "التوثيق". وتبعا للسياق، من الجائز أن يُستخدم التعبيران "يوقّع" و"يوثّق" باعتبارهما مترادفين.[٧]

٣- وأما "التوقيع" فهو "أي اسم أو رمز يستخدمه طرف ما بنيّة تكوين توقيعه منه".[٨] ومن المفهوم أن الغرض الذي تتوخّاه القوانين التشريعية، التي تقتضي أن يوقّع شخص معيّن على مستند معيّن، هو إثبات أصالة المستند.[٩] وتتمثّل الحالة النموذجية للتوقيع في وجود اسم الشخص الموقِّع، مكتوبا بخط يد الموقِّع نفسه، على مستند ورقيّ (أي توقيع "مكتوب بخط اليد" أو "مخطوط").[١٠] غير أن التوقيع المكتوب بخط اليد ليس هو النوع الوحيد المتصوَّر من أنواع التوقيع. فنظرا لكون المحاكم تعتبر التوقيعات "علامة فحسب"، ما لم يقتض القانون التشريعي المعني أن يكون التوقيع بخط يد الموقِّع ذاته، فإن "الاسم المطبوع الخاص بالطرف المطالَب بأن يوقّع على المستند يكفي"، أو إن التوقيع "يجوز دَمغه على المستند بختم محفورة عليه صورة طبق الأصل عن التوقيع الاعتيادي الخاص بالشخص الموقِّع"، شريطة أن يُقدَّم برهان يثبت في هذه الحالات "أن الاسم المطبوع على الختم قد مهره الشخص الموقِّع"، أو أن ذلك التوقيع "قد اعتُرف به وبُيِّن لـه بأنه تمّ بناء على سلطته وذلك لتخصيصه لغرض مَهْر الصك المعيّن".[١١]

٤- ومقتضيات التوقيع القانونية كشرط لصحّة تصرّفات معيّنة، في الولايات القضائية التي تُطبّق القانون العام، توجد نمطيا في القانون التشريعي البريطاني بشأن ممارسات الاحتيال،[١٢] وفي الصيغ المنسوخة عنه في بلدان أخرى.[١٣] وبمرور الزمن، أخذت المحاكم تميل إلى تفسير القانون التشريعي بشأن ممارسات الاحتيال بطريقة متحرّرة، إدراكا منها بأن مقتضياته الشكلية الصارمة كانت متوخّاة بناء على خلفية معيّنة،[١٤]

---

[٧] في سياق المادة ٩ المنقّحة من المدونة التجارية الموحّدة للولايات المتحدة الأمريكية، يُعرَّف التعبير "يوثّق"، على سبيل المثال، بأنه "(ألف) يوقّع"؛ أو "(باء) ينفّذ رمزا أو يعتمده بشكل آخر، أو يشفِّر أو يجهّز على نحو مماثل سجلا كليا أو جزئيا، بناء على النيّة الحالية لدى الشخص الموثِّق بأن يعيّن هويّة الشخص ويعتمد سجلا أو يقبل به".

[٨] *Alfred E. Weber v. Dante De Cecco,* 14 October 1948 (1 N.J. Super. 353, 358) (United States, New Jersey Superior Court Reports).

[٩] *Lobb v. Stanley* (1844), 5 QB 574, 114 E.R. 1366 (United Kingdom, Law Reports, Queen's Bench).

[١٠] *Lord Denning in Goodman v. Eban* [1954] QBD 550 at 56: "في الممارسة العادية الإنكليزية الحديثة، عندما يكون من اللازم أن يوقّع شخص ما على مستند يعني ذلك أنه يجب عليه أن يكتب اسمه عليه بيده هو نفسه." (United Kingdom, Queen's Bench Division).

[١١] *R. v. Moore: ex parte Myers* (1884) 10 V.L.R. 322 at 324 (United Kingdom, Victorian Law Reports).

[١٢] صدر القانون التشريعي بشأن ممارسات الاحتيال أصلا في بريطانيا العظمى في عام ١٦٧٧ "من أجل منع الكثير من الممارسات الاحتيالية التي يشيع اللجوء إليها في شهادة الزور والاستمالة إلى الإدلاء بشهادة الزور". وقد أُلغيت معظم أحكامه في المملكة المتحدة أثناء القرن العشرين.

[١٣] على سبيل المثال، البند الفرعي (١) من البند ٢-٢٠١ من مدونة القوانين التجارية الموحّدة في الولايات المتحدة (Uniform Commercial Code)، الذي عبّر صراحة عن القانون التشريعي بشأن الاحتيالات كما يلي: "باستثناء ما هو منصوص عليه خلافا لذلك في هذا البند، لا يجوز إنفاذ عقد بشأن بيع بضائع بثمن قدره ٥٠٠ دولار أو أكثر باللجوء إلى إجراء قانوني أو دفاع، ما لم يكن ثمة نص مكتوب كاف لكي يبيّن أن عقد بيع قد أُبرم بين الطرفين ووقّع عليه أحد الطرفين الذي يُلتمس الإنفاذ تجاهه، أو وكيله أو سمساره المأذون".

[١٤] "صدر القانون التشريعي بشأن ممارسات الاحتيال في فترة كان فيها المشرِّع يميل بقدر ما إلى النص على أنه ينبغي البت في القضايا وفقا لقواعد محدّدة، بدلا من ترك ذلك للمحلّفين لكي ينظروا في مفعول دليل الإثبات في كل قضية. ولا شكّ في أن ذلك نشأ إلى حدّ ما من أنّ المدّعي والمدّعى عليه لم يكونا آنذاك في عداد الشهود العدول." (J. Roxborough في القضية *Leeman v. Stocks* [1951] 1 Ch 941 at 947-8 (United Kingdom, Law Reports, Chancery Division)، عند الاستشهاد باستحسان اجتهادات J. Cave في القضية *Evans v. Hoare* [1982] 1 QB 593 at 597 (United Kingdom, Law Reports, Queen's Bench)).

وبأن التقيّد الصارم بقواعده قد يؤدي دونما ضرورة إلى تجريد العقود من مفعولها القانوني.[١٥] ومن ثم فإن الولايات القضائية التي تطبّق القانون العام أخذت تشهد، خلال المائة والخمسين سنة الماضية، تطوّرا في مفهوم "التوقيع" تدرّج من التركيز الأصلي على الشكل إلى التركيز على الوظيفة التي يؤديها.[١٦] وأخذت المحاكم الإنكليزية تنظر من حين لآخر في صيغ متنوعة من هذا المفهوم الأساسي، بدءا من التبديلات البسيطة، ومنها مثلا استخدام علامات الصليب[١٧] أو الأحرف الأولى من الاسم،[١٨] ومرورا بالأسماء المستعارة[١٩] وعبارات التعريف بالهويّة،[٢٠] وانتهاء بالأسماء المطبوعة،[٢١] والتوقيعات من قبل أطراف ثالثة،[٢٢] والأختام المطاطيّة.[٢٣] وفي جميع هذه الأحوال، استطاعت المحاكم أن تسوّي المسألة المتعلقة بما إذا كان من الجائز إمضاء توقيع صحيح برسم نظير لتوقيع مخطوط. ومن ثم، يمكن أن يُقال إنه بناء على خلفية من بعض المقتضيات العامة المتصلة بشأن الشكل، أخذت المحاكم تنزع في الولايات القضائية التي يسري فيها القانون العام إلى تطوير فهم رحب لما يعنيه المفهومان "التوثيق" و"التوقيع"، بالتركيز على النيّة التي تقصدها الأطراف المعنيّة، أكثر منه على شكل تصرّفاتها.

٥- أما النهج الذي يُتّبع بشأن "التوثيق" و"التوقيع" في الولايات القضائية التي تُطبّق القانون المدني، فهو ليس متطابقا من جميع النواحي مع النهج المتّبع في القانون العام. ذلك أن معظم الولايات القضائية التي يسري فيها القانون المدني تتبع قاعدة الحرّية في الشكل بخصوص التعهّدات التعاقدية في مسائل القانون الخاص، إما صراحة[٢٤] وإما ضمنا،[٢٥] ولكن رهنا بفهرس مستفيض من الاستثناءات تبعا للولاية القضائية

---

[١٥] مثلما أوضح اللورد بنغهام أوف كورنهيل (Lord Bingham of Cornhill)، "سرعان ما تبيّن أنه إذا عُني في حل هذه المشكلة المعتمد في القرن السابع عشر بمعالجة واحد من الشرور، فقد كان من شأن ذلك الحلّ أن يتيح ظهور شر آخر: ذلك أن الطرف الذي يعمل ويتصرّف بناء على ما كان يظن أنه اتفاق شفهي ملزم، سوف يجد أن توقعاته التجارية قد أُحبطت عندما يحين أوان الإنفاذ، وأن الطرف الآخر قد نجح في التعويل على عدم وجود مذكّرة أو ورقة مكتوبة عن الاتفاق". القضية (*Actionstrength Limited v. International Glass Engineering*)، ٣ نيسان/ أبريل ٢٠٠٣ (United Kingdom, House of Lords) [2003] UKHL 17.

[١٦] Chris Reed, "What is a signature?", *Journal of Information, Law and Technology*, vol. 3, 2000, والإحالة المرجعية الواردة في تلك الدراسة إلى مدوّنة السوابق القضائية، وهما متاحتان في الموقع الشبكي: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/ (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

[١٧] *Baker v. Dening* (1838) 8 A. & E. 94 (United Kingdom, Adolphus and Ellis' Queen's Bench Reports).

[١٨] *Hill v. Hill* [1947] Ch 231 (United Kingdom, Chancery Division).

[١٩] *Redding, in re* (1850) 14 Jur. 1052, 2 Rob.Ecc. 339 (United Kingdom, Jurist Reports and Robertson's Ecclesiastical Reports).

[٢٠] *Cook, In the Estate of (Deceased) Murison v. Cook and Another* [1960] 1 All ER 689 (United Kingdom, All England Law Reports).

[٢١] *Brydges v. Dicks* (1891) 7 T.L.R. 215 (cited in Brennan v. Kinjella Pty Ltd., Supreme Court of New South Wales, 24 June 1993, 1993 NSW LEXIS 7543, 10). Typewriting has also been considered in *Newborne v. Sensolid* (Great Britain), Ltd. [1954] 1 QB 45 (United Kingdom, Law Reports, Queen's Bench).

[٢٢] *France v. Dutton,* 24 April 1891 [1891] 2 QB 208 (United Kingdom, Law Reports, Queen's Bench).

[٢٣] *Goodman v. J. Eban Ltd.,* [1954] 1 QB 550, *cited in Lazarus Estates, Ltd. v. Beasley*, Court of Appeal, 24 January 1956 ([1956] 1 QB 702); London County Council v. Vitamins, Ltd., *London County Council v. Agricultural Food Products, Ltd.,* Court of Appeal, 31 March 1955 [1955] 2 QB 218 (United Kingdom, Law Reports, Queen's Bench).

[٢٤] هذا معترف به، على سبيل المثال، في الفقرة ١ من المادة ١١ من مدوّنة قوانين الالتزامات في سويسرا. وعلى نحو مماثل، ينص البند ٢١٥ من مدوّنة القوانين المدنية في ألمانيا على أن الاتفاقات لا تُعتبر غير صحيحة إلا في حال عدم مراعاتها لصيغة يحدّدها القانون أو تتفق عليها الأطراف. باستثناء تلك الحالات المحدّدة، من المفهوم عموما أن العقود بمقتضى القانون الخاص لا تخضع لمقتضيات شكلية محدّدة. وأما عندما يحدّد القانون صراحة شكلا معيّنا، فإن تلك المقتضيات يجب تفسيرها بدقة شديدة.

[٢٥] في فرنسا، على سبيل المثال، الحرّية في الشكل مضمّنة في القواعد الأساسية بشأن صوغ العقود بمقتضى مدوّنة القوانين المدنية (Civil Code). ووفقا للمادة ١١٠٨ من مدوّنة القوانين المدنية الفرنسية، تقتضي صحة عقد ما توافر رضا الواعد بالالتزام وأهليته القانونية وغرض معيّن وسبب مشروع: ولدى توافر هذه العناصر، يصبح العقد "قانونا بين الأطراف" المعنية، وفقا للمادة ١١٣٤. وهذه هي القاعدة أيضا في إسبانيا، بمقتضى المادتين ١٢٥٨ و١٢٧٨ من مدوّنة القوانين المدنية. وكذلك تتّبع إيطاليا القاعدة نفسها، وإن كان ذلك بقدر أقل من البيان الصريح (انظر مدوّنة القوانين المدنية في إيطاليا، المادتين ١٣٢٦ و١٣٥٠).

المعنية. وهذا يعني، على سبيل القاعدة العامة، أنه لا لزوم إلى أن تكون العقود مصوغة "كتابة" أو "موقَّعة" لكي تكون صحيحة وواجبة الإنفاذ. غير أن هناك ولايات قضائية تطبّق القانون المدني تقتضي عموما وجود كتابة ما لإثبات محتويات العقد، ما عدا في المسائل التجارية.[٢٦] وعلى النقيض من الولايات القضائية التي تطبّق القانون العام، تنحو بلدان القانون المدني إلى تفسير قواعد أدلّة الإثبات على نحو صارم على الأرجح. وعادة ما يُلاحظ أن القواعد بشأن أدلّة الإثبات المدنية تقرّر ترتيبا هرميا لأدلة الإثبات من أجل البرهان على مضمون العقود المدنية والتجارية. وتأتي في أعلى ذلك الترتيب المستندات الصادرة عن السلطات العمومية، تليها المستندات الخصوصية الموثّقة. وكثيرا ما يُوضع ذلك الترتيب الهرمي على نحو قد يصبح فيه المفهومان "المستند" و"التوقيع" متلازمين تقريبا، وإن كانا متمايزين شكلا.[٢٧] غير أن هناك ولايات قضائية أخرى خاضعة للقانون المدني تربط ما بين مفهوم "المستند" ووجود "توقيع" عليه.[٢٨] لكن هذا لا يعني أن المستند الذي لم يُوقّع عليه مجرّد بالضرورة من أي قيمة كدليل إثبات، بل يعني أن المستند من هذا النحو لن يتّسم بأي قرينة مخصوصة، وهو يُعتبر عموما "بداية دليل إثبات".[٢٩] ومن ثم فإن "التوثيق" هو في معظم الولايات القضائية الخاضعة للقانون المدني مبدأ يُفهم فهماً ضيقاً على الأرجح بأنه يعني أن موثوقية مستند ما قد تحقّقت منها وصدّقتها سلطةٌ عمومية مختصّة أو كاتب عدل. والشائع في الإجراءات المدنية الإشارة بدلا من ذلك إلى مفهوم "صحة" المستندات.

٦- وعلى غرار الحالة في إطار القانون العام، فإن أنموذج التوقيع في بلدان القانون المدني هو التوقيع المهور بخط اليد. وأما فيما يخص التوقيع نفسه، فإن بعض الولايات القضائية يميل إلى القبول بطرائق مكافئة مختلفة، بما فيها التوقيعات المستنسخة آلياً، على الرغم من وجود نهج ميّال إلى الشكلية عموما في أدلة الإثبات.[٣٠] غير أن ولايات قضائية أخرى تقبل بالتوقيعات الآلية في المعاملات التجارية،[٣١] ولكنها استمرّت في اقتضاء توقيع بخط اليد من أجل إثبات أنواع أخرى من العقود، وذلك حتى ظهور التكنولوجيات الحاسوبية.[٣٢] ولذلك يمكن أن يُقال إنه، بناء على خلفية عامة من الحرّية في الشكل بشأن

---

[٢٦] تنص المادة ١٣٤١ من مدوّنة القوانين المدنية في فرنسا على وجوب وجود نص مكتوب لإثبات العقود التي تتجاوز قيمتها مبلغا معيّنا، لكن المادة ١٠٩ من مدوّنة القوانين التجارية تقرّ بأنواع مختلفة من أدلة الإثبات، دونما ترتيب هرميّ معيّن. وقد أدى ذلك إلى اعتراف محكمة النقض في فرنسا في عام ١٨٩٢ بالمبدأ العام بشأن الحرّية في أدلة الإثبات في القضايا التجارية (Cass. civ. 17 May 1892, DP 1892.1.604؛ رأي مستشهد به في Luc Grynbaum, *Preuve, Répertoire de droit commercial Dalloz,* June 2002, sections 6 and 11).

[٢٧] التوقيع، بمقتضى القانون الألماني، مثلا، ليس عنصرا أساسيا في مفهوم "المستند" (Urkunde) (Gerhard Lüke and Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992) section 416, No. 5). ومع ذلك فإن الترتيب الهرمي لأدلة الإثبات المستندية، الذي أرسته البنود ٤١٥ و٤١٦ و٤١٩ من مدوّنة قوانين الإجراءات المدنية في ألمانيا، يربط بوضوح ما بين التوقيع والمستند. والواقع أن البند ٤١٦ بشأن القيمة الإثباتية في المستندات الخصوصية (*Privaturkunden*) ينص على أن المستندات الخصوصية تكوّن "إثباتا تاما" بشأن المعلومات التي تحتوي عليها ما دامت موقّعا عليها من قبل المحرّر أو موثّقة بتوقيع كاتب عدل. ونظرا لعدم وجود نص على شيء بخصوص المستندات بلا توقيع، يبدو أن هذه المستندات تلقى مصير المستندات الناقصة (أي المحرّفة أو المشوبة بخلل)، التي تمارس المحاكم "الحرّية" في تقرير قيمتها الإثباتية (مدوّنة قوانين الإجراءات المدنية في ألمانيا، البند ٤١٩).

[٢٨] في فرنسا، يعتبر التوقيع "عنصرا أساسيا" من عناصر المستندات الخصوصية (*actes sous seing privé*) (انظر *Recueil Dalloz, Preuve*, No. 638).

[٢٩] هذه هي الحال في فرنسا، انظر على سبيل المثال، *Recueil Dalloz, Preuve,* Nos. 657-658.

[٣٠] يبيّن المعلِّقون على مدوّنة قوانين الإجراءات المدنية الألمانية أن اشتراط توقيع بخط اليد من شأنه أن يعني استبعاد جميع أشكال العلامات المعمولة آليا، وهي نتيجة من شأنها أن تتعارض مع الممارسة الاعتيادية والتقدّم التكنولوجي (انظر Gerhard Lüke and Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992), section 416, No. 5).

[٣١] على سبيل المثال، فرنسا (انظر *Recueil Dalloz, Preuve,* No. 662).

[٣٢] في فرنسا، على سبيل المثال، لا يمكن الاستعاضة عن التوقيع بعلامة صليب أو غيرها من العلامات، أو بختم أو ببصمات الأصابع (انظر *Recueil Dalloz, Preuve,* No. 665).

إبرام عقود الأعمال التجارية، تميل البلدان التي تعمل بالقانون المدني إلى تطبيق معايير صارمة من أجل تقدير القيمة الإثباتية للمستندات الخصوصية، وقد تكون ميّالة إلى رفض المستندات التي لا يمكن الاعتراف فورا بصحّتها استنادا إلى توقيع.

٧- إن المناقشة الواردة أعلاه لا تقتصر على تبيان عدم وجود فهم واحد لمفهومي التوقيع والتوثيق، بل تبيّن أيضا أن الوظائف التي يؤدّيانها تختلف فيما بين النظم القانونية المختلفة. ولكن، على الرغم من هذه التباينات يمكن العثور على بضعة عناصر عامة مشتركة. ذلك أن المفهومين "التوثيق" و"الصحة" يُفهمان عموما في القانون بأنهما يشيران إلى أصالة مستند أو سجل ما، أي أن المستند هو الحجّة الداعمة "الأصلية" بخصوص المعلومات التي يحتوي عليها، في الشكل الذي سُجّلت فيه ودونما أي تحوير طرأ عليها. وكذلك فإن التوقيعات تؤدي ثلاث وظائف رئيسية في البيئة القائمة على الوسائل الورقية: ذلك أن التوقيعات تتيح التعرّف على هويّة الموقِّع (وظيفة تعريف الهويّة)؛ وهي توفّر اليقين بشأن ضلوع ذلك الشخص في فعل التوقيع (الوظيفة الإثباتية)؛ وهي تربط ما بين الموقِّع ومضمون المستند (الوظيفة الإسنادية). ويمكن أن يُقال إن التوقيعات تؤدي كذلك عدّة وظائف أخرى تبعا لطبيعة المستند الموقَّع عليه. فعلى سبيل المثال، من الجائز أن يشهد التوقيع على نيّة طرف ما الالتزام بمضمون عقد موقَّع عليه؛ ونيّة شخص ما الإقرار بمرجعية تأليف نص ما (مما يُظهر الوعي بالتبعات القانونية التي من الممكن أن تتأتّى عن فعل التوقيع)؛ ونيّة شخص ما الإقرار بارتباطه بمضمون مستند كتبه شخص آخر؛ وواقعة وزمن وجود شخص ما في مكان بعينه.[٣٣]، [٣٤]

٨- ولكن، ينبغي أن يُلاحظ أن التوقيع، حتى وإن أدّى وجوده في كثير من الأحيان إلى افتراض الصحة، فإنه وحده لا "يوثّق" مستندا؛ بل إن هذين العنصرين قد يكونان قابلين للفصل بينهما، تبعا للظروف. ذلك أن التوقيع قد يحتفظ "بصحته" حتى وإن حُوّر لاحقا المستندُ المعهور عليه التوقيع. كذلك فإن المستند قد يظل "صحيحا" حتى وإن كان التوقيع الذي يحتوي عليه مزوّرا. علاوة على ذلك، فإن سلطة التدخّل في معاملة ما من جهة وهويّة الشخص المعني الفعلية من جهة أخرى، مع أنهما عنصران مهمّان لضمان صحة مستند أو توقيع ما، لا يبرهن عليهما التوقيع وحده برهنة تامة ولا يكفيان لضمان صحة المستندات أو التوقيعات.

٩- وهذه الملاحظة تفضي إلى جانب آخر من المسألة قيد المناقشة حاليا. إذ بصرف النظر عن التقليد القانوني المعيّن، ليس التوقيع شيئا قائما بذاته، مع بعض الاستثناءات القليلة جدا. ذلك أنّ مفعولـه القانوني يعتمد على الرابط بين التوقيع والشخص الذي يمكن أن يُسنَدَ إليه ذلك التوقيع. وفي الممارسة العملية، من الجائز القيام بعدّة خطوات مختلفة بغية التحقّق من هويّة الموقِّع. فالأطراف، عندما تكون كلها حاضرة في المكان نفسه في الوقت نفسه، قد لا تتعرّف على بعضها البعض إلاّ بالوجه؛ أما إذا تفاوضت هاتفيا، فقد يتعرّف كل منها على صوت الآخر، وهكذا. وهذا كثيرا ما يحدث باعتباره مسألة عادية، وهو لا يخضع

---

[٣٣] *قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الاشتراع ٢٠٠١* (منشورات الأمم المتحدة، رقم المبيع A.02.V.8)، الجزء الثاني، الفقرة ٢٩ (متاح على الموقع الشبكي http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html، وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[٣٤] هذا التحليل قد استُخدم من قبل كأساس لمعايير التكافؤ الوظيفي في المادة ٧ من الصيغة السابقة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع ١٩٩٦ ومع المادة الإضافية ٥ مكرّرا بصيغتها المعدّلة في عام ١٩٩٨ (منشورات الأمم المتحدة، رقم المبيع A.99.V.4)، وهو متاح على الموقع الشبكي: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

لقواعد قانونية محدّدة. أمّا عندما تتفاوض الأطراف بالمراسلة، أو عندما تُحال مستندات عبر سلسلة تعاقدية، فقد لا تكون هناك سوى سبل قليلة للتثبّت من أن العلامات التي تظهر على مستند معيّن قد عملها بالفعل الشخص الذي يظهر أنها ترتبط باسمه، وكذلك للتثبت مما إذا كان الشخص المأذون لـه حسب الأصول هو الشخص الوحيد فعلا الذي أنشأ التوقيع المفترض فيه أن يلزم شخصا بعينه.

١٠- ومع أن التوقيع اليدوي هو شكل مألوف من أشكال "التوثيق" ويؤدي الغرض من مستندات المعاملات المتبادلة بين أطراف معروفة، فإنّ التوقيع يكون في كثير من الحالات التجارية والإدارية غير مأمون نسبيا. ذلك أن الشخص الذي يعوّل على المستند كثيرا ما لا تكون لديه أسماء الأشخاص المأذون لهم بالتوقيع ولا عيّنة من التوقيعات متاحة لأغراض المقارنة.[٣٥] وتصح هذه الملاحظة خصوصا بشأن كثير من الوثائق التي يُعوَّل عليها في البلدان الأجنبية في المعاملات التجارية الدولية. وحتى في الحالات التي تكون فيها عيّنة من التوقيع المأذون به متاحة لأغراض المقارنة، فقد يكون الخبير فقط هو القادر على كشف تزوير مُتقَن. وفي الحالات التي تُعالج فيها أعداد كبيرة من المستندات، لا يتسنّى أحيانا حتى مقارنة التوقيعات، ما عدا ما يخص أهم المعاملات. ومن ثم فإن الثقة هي واحد من الأركان الأساسية التي تقوم عليها علاقات الأعمال التجارية الدولية.

١١- غير أن لدى أكثر النظم القانونية إجراءات أو مقتضيات خاصة، القصد منها تعزيز قابلية التعويل على التوقيعات بخط اليد. وقد يكون بعض الإجراءات إلزاميا لكي ينتج عن مستندات معيّنة مفعولٌ قانوني. وهي قد تكون أيضا خيارية ومتاحة للأطراف التي ترغب في التصرّف على نحو يحول دون إمكانية صدور أي احتجاجات على صحة بعض المستندات. وتشمل الأمثلة النمطية ما يلي:

(أ) *التوثيق العدلي* - في ظروف معيّنة، ينطوي فعل التوقيع على دلالة شكلية معيّنة تُعزى إلى تعزيز الثقة فيما يقترن بمراسم تقليدية خاصة. وهذه هي الحالة، على سبيل المثال، بخصوص التوثيق العدلي، أي التصديق من قِبل كاتب عدل لإثبات صحة توقيع على مستند قانوني، وهو ما يستوجب في كثير من الأحيان حضور الشخص جسديا لدى الكاتب العدل؛

(ب) *الإشهاد* - الإشهاد هو فعل مشاهدة شخص ما يوقّع على مستند قانوني، ثم توقيع المُشاهد بكتابة اسمه على المستند بصفته شاهدا. والغرض من الإشهاد هو الحفاظ على دليل إثبات تصديقاً على التوقيع. ولدى المصادقة بالإشهاد، يصرّح الشاهد ويؤكّد أن الشخص الذي شاهده يوقّع على المستند فعل ذلك في الواقع. لكن هذا الإشهاد لا ينسحب على ضمان دقّة المستند أو مطابقته للحقيقة. ويمكن أن يُستدعى الشاهد لأجل الإدلاء بشهادته بخصوص الظروف المحيطة بالتوقيع ذاته؛[٣٦]

---

[٣٥] تعترف بعض مجالات القانون بسمة انعدام الأمان المتأصّلة في التوقيعات بخط اليد وعدم الإمكانية العملية في الإصرار على مقتضيات شكلية صارمة بشأن صحة السندات القانونية على حد سواء، وتقرّ بأنه حتى التوقيع المزوّر لا يؤدي في بعض الحالات إلى تجريد مستند من مفعوله القانوني. وهكذا فإن المادة ٧، على سبيل المثال، من قانون السفاتج (الكمبيالات) والسندات الإذنية الموحّد، المرفق بالاتفاقية المتضمّنة لقانون السفاتج (الكمبيالات)، والسندات الإذنية الموحّد، المحرّرة في جنيف ٧ حزيران/ يونيه ١٩٣٠، تنص على أنه "إذا كانت السفتجة (الكمبيالة) تحمل توقيعات أشخاص غير قادرين على الالتزام بسفتجة (كمبيالة)، أو توقيعات مزوّرة، أو توقيعات أشخاص وهميين، أو توقيعات لا يمكن لأي سبب آخر أن تلزم الأشخاص الذين وقّعوا على السفتجة (الكمبيالة) أو الذين وُقّع عليها بالنيابة عنهم، فإن التزامات الأشخاص الآخرين الذين وقّعوا عليها تصبح مع ذلك باطلة" (عصبة الأمم، *مجموعة المعاهدات*، المجلّد ١٤٣، الرقم ٣٣١٣).

[٣٦] Adrian McCullagh, Peter Little and William Caelli, "Electronic signatures: understand the past to develop the future", *University of New South Wales Law Journal,* vol. 21, No. 2 (1998)، انظر الفصل الثالث، القسم دال، بشأن مفهوم شهادة الشهود.

(ج) *الأختام* – ممارسة استخدام الأختام إضافة إلى التوقيعات، أو عوضا عنها، ليست غير مألوفة، وخاصة في مناطق معيّنة من العالم.[٣٧] فالتوقيع أو الختم قد يوفّر، على سبيل المثال، دليلا على هويّة الموقّع؛ أو على أن الموقّع قد اتفق على الالتزام بالاتفاق وفَعل ذلك طواعية؛ أو على أن المستند نهائي وتام؛ أو على أن المعلومات لم تُحوَّر بعد التوقيع.[٣٨] كما إن هذه الممارسة قد تنبّه الموقّع وتبيّن النيّة في التصرّف على نحو قانوني ملزم.

١٢- وما عدا هذه الحالات الخاصة، ما فتئت التوقيعات المهورة بخط اليد تُستخدم في المعاملات التجارية، الداخلية منها والدولية على حد سواء، طوال قرون من الزمن من غير وجود أي إطار تشريعي أو تنفيذي مصمّم خصوصا لهذا الغرض. ويلجأ الأشخاص المرسلةُ إليهم المستنداتُ الموقَّعة أو حائزوها إلى تقدير قابلية التعويل على التوقيعات على أساس كل حالة على حدة تبعا لمستوى الثقة التي يتمتّع بها الموقّع. والواقع أن الغالبية الكبرى من العقود المكتوبة الدولية—هذا إن وجدت أي "كتابة" على الإطلاق—ليست بالضرورة مشفوعة بأي إجراء شكلي أو توثيقي خاص.

١٣- لكن استخدام الوثائق الموقّعة عبر الحدود يزداد تعقّدا عندما تكون السلطات العمومية مشمولة في هذا الخصوص، إذ إن السلطات المستلمة في بلد أجنبي تعمد عادة إلى اشتراط تقديم دليل على هويّة الموقّع ومرجعيته. وهذه الاشتراطات تُستوفى تقليديا بما يُسمّى إجراءات "التصديق القانوني"، حيث تكون التوقيعات واردة ضمن مستندات داخلية موثّقة من جانب السلطات الدبلوماسية المعنية من أجل استخدامها في الخارج. وفي المقابل، فإن الممثلين القنصليين أو الدبلوماسيين للبلد الذي يُقصد من المستندات أن تُستخدم فيه قد يوثّقون أيضا توقيعات السلطات العمومية الأجنبية في بلد المنشأ، وفي كثير من الأحيان تقتصر السلطات القنصلية والدبلوماسية على توثيق توقيعات سلطات معيّنة رفيعة الرتبة في البلدان التي أصدرت المستندات، مما يقتضي وجود عدّة طبقات متدرّجة من توثيق التوقيعات عندما يكون المستند صادرا أصلا عن موظف أدنى رتبة، أو يقتضي توثيقا عدليا مسبقا للتوقيعات من جانب كاتب عدل في البلد المصدر. علما بأن التصديق القانوني هو في معظم الحالات إجراء مرهق ومستنزف للوقت وباهظ التكلفة. ولذلك فقد جرى التفاوض على الاتفاقية اللاغية لشرط التصديق القانوني على الوثائق العمومية الأجنبية،[٣٩] التي حُرّرت في لاهاي في ٥ تشرين الأول/أكتوبر ١٩٦١، من أجل الاستعاضة عن الاشتراطات الحالية بصيغة مبسّطة وموحّدة قياسيا (أي مذكّرة التصديق "apostille the") تُستخدم للتصديق على مستندات عمومية معيّنة في الدول الأطراف في الاتفاقية.[٤٠] ولا يجوز إصدار مذكّرة تصديق إلا من جانب سلطة مختصة تعيّنها الدولة التي صدر منها المستند العمومي. ومذكّرات التصديق تصدّق على موثوقيّة التوقيع والصفة الأهلية التي تصرّف بها الشخص الموقّع على المستند، وكذلك، كلّما كان مناسبا، هويّة الختم أو الدمغة على المستند؛ لكنها لا تتعلق بمضمون المستند الأساسي نفسه.

---

(٣٧) تُستخدم الأختام في عدّة بلدان في شرقي آسيا، ومنها الصين واليابان.

(٣٨) Mark Sneddon, "Legislating to facilitate electronic signatures and records: exceptions, standards and the impact of the statute book", *University of New South Wales Law Journal*, vol. 21, No. 2 (1998)، انظر بخاصة الجزء ٢، الفصل الثاني، بشأن "أهداف السياسة العامة في مقتضيات الكتابة والتوقيع".

(٣٩) الأمم المتحدة، *مجموعة المعاهدات*، المجلّد ٥٢٧، الرقم ٧٦٢٥.

(٤٠) تشمل تلك المستندات الوثائق الصادرة عن سلطة أو موظف ذي علاقة بمحكمة أو هيئة قضائية في الدولة (بما في ذلك المستندات التي تصدرها محكمة أو هيئة قضائية إدارية أو دستورية أو كنسيّة (شرعية)، أو نائب عام، أو موظف ديوان، أو مأمور محكمة)؛ والمستندات الإدارية؛ والسندات العدلية؛ وشهادات التصديق الرسمية التي تُوضع على المستندات الموقّع عليها من قبل أشخاص بصفتهم الخصوصية.

١٤- ومثلما ذُكر أعلاه، ليس من اللازم دائما، في كثير من النظم القانونية، أن تكون العقود التجارية مضمّنة في مستند أو مُثبتة كتابة لكي تكون صحيحة. فحتى في حال وجود نص مكتوب، ليس التوقيع إلزاميا بالضرورة لكي يكون العقد ملزما للأطراف. ولكن، عندما يشترط القانون أن تكون العقود مصوغة كتابة أو أن تكون موقّعا عليها، فإن عدم استيفاء هذين الاشتراطين من شأنه أن يجعل العقد باطلا. وربما تكون اشتراطات الشكل لأغراض الأدلة الإثباتية أكثر دلالة من مقتضيات الشكل لأغراض صحة العقود. أما الصعوبة في إثبات الاتفاقات الشفهية فهي واحد من الأسباب الرئيسية الداعية إلى تجسيد العقود التجارية في مستندات مكتوبة أو تحريرها في وثائق متبادلة بالمراسلة، حتى وإن كان من شأن أي اتفاق شفهي أن يكون صحيحا على أي نحو آخر. ذلك أن الأطراف التي تكون التزاماتها موثّقة في نصوص كتابية موقّعة لا يُحتمل أن تنجح فيما قد تشرع فيه من محاولات لإنكار مضمون التزاماتها. وأما القواعد الصارمة بشأن الأدلة الإثباتية المستندية فهي تهدف في العادة إلى توفير درجة عالية من قابلية التعويل على المستندات التي تفي بتلك القواعد، وهو ما يُعتقد عموما بأنه يرفع بالتالي درجة اليقين القانوني. ولكن، كلّما ازداد التوسّع في مقتضيات الأدلة الإثباتية، اتسعت الفرصة المتاحة لأي طرف من الأطراف للاحتجاج بالعيوب الشكلية بغية إبطال أو إنكار وجوب إنفاذ الالتزامات التي لم تعد تلك الأطراف تعتزم أداءها، وذلك على سبيل المثال لأن العقد قد أصبح خلوا من المزايا التجارية. ولذلك فإن المصلحة في تعزيز الأمان في تبادل الخطابات الإلكترونية لا بدّ من أن تكون على توازن مع المخاطرة المحتملة من توفير طريقة سهلة يستغلّها بعض التجّار الذين يتصرفون بسوء نيّة للتنكّر لالتزاماتهم القانونية التي يأخذونها على عاتقهم بحرّية. ومن ثم فإن تحقيق هذا التوازن، من خلال قواعد ومعايير معترف بها دوليا وقابلة للعمل بها عبر الحدود الوطنية، هو مهمّة كبيرة في تقرير السياسات العامة في مجال التجارة الإلكترونية. والغرض من هذه الوثيقة هو مساعدة المشرّعين ومقرّري السياسات العامة على استبانة المسائل القانونية الرئيسية التي ينطوي عليها استخدام طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي، والنظر في إيجاد حلول ممكنة لها.

الجزء الأول

طرائـــق التوقـيع والتـــوثيق الإلكـــترونيـــة

المحتــويات

الصفحة

أولا- تعريف التوقيع والتوثيق الإلكترونيين وطرائقهما

ألف- ملاحظات عامة عن المصطلحات

١٥- يُستخدم المصطلحان "التوثيق الإلكتروني" و"التوقيع الإلكتروني" للإشارة إلى مختلف التقنيات المتاحة حاليا في السوق أو التي لا تزال قيد التطوير لغرض استنساخ بعض أو كل الوظائف المحدّدة باعتبارها من خصائص التوقيعات المكتوبة بخط اليد أو غيرها من طرائق التوثيق التقليدية، ولكن في بيئة إلكترونية.

١٦- وقد جرى تطوير عدد من تقنيات التوقيع الإلكترونية المختلفة على مدى السنين. وتهدف كل تقنية منها إلى تلبية احتياجات مختلفة، وتوفير مستويات مختلفة من الأمن، كما إن لكل تقنية منها مقتضيات تقنية مختلفة. ومن الجائز تصنيف طرائق التوثيق والتوقيع الإلكترونية في ثلاث فئات: الطرائق التي تستند إلى معرفة المستعمل أو المستلم (مثلا، كلمات السر، أرقام تعريف الهوية الشخصية (PIN))، والطرائق التي تستند إلى السمات البدنية الخاصة بالمستعمل (مثلا، الخصائص البيومترية)، والطرائق التي تستند إلى حيازة المستعمل شيئا معيّنا (مثلا، الرموز، أو غيرها من المعلومات المخزّنة على بطاقة مغنطيسية).[٤١] وهناك فئة رابعة قد تشمل عدّة أنواع مختلفة من طرائق التوثيق والتوقيع التي لا تندرج في نطاق أي من الفئات المذكورة أعلاه، لكنها قد تُستعمل أيضا لتبيان منشئ خطاب إلكتروني (ومن ذلك مثلا نسخة مصوّرة طبق الأصل عن توقيع مكتوب بخط اليد، أو اسم مطبوع في الجزء الأدنى من رسالة إلكترونية). وأما التكنولوجيات المستخدمة حاليا فتشمل التوقيعات الرقمية ضمن نطاق مرفق مفاتيح عمومية، والأجهزة البيومترية، وأرقام تعريف الهوية الشخصية (PIN)، وكلمات السر المحدّدة من المستعمل أو كلمات السر المخصّصة، والتوقيعات المكتوبة بخط اليد ثم المصوّرة بالمسح الإلكتروني، والتوقيع بواسطة قلم رقمي، واستعمال خانات "OK" (حسنا، موافق) أو "I accept" (أقبلُ) القابلة للنقر عليها.[٤٢] وقد أخذ يزداد شيوع اتّباع حلول هجينة تستند إلى مجموعة مؤتلفة من التكنولوجيات المختلفة، ومنها على سبيل المثال الطريقة المتّبعة في حالة الجمع بين استعمال كلمات السر وتكنولوجيا التشفير (TLS/SSL) (القائمة على البروتوكولين الحاسوبيين التشفيريين: أمن طبقة النقل/ طبقة المقابس الآمنة) وهي تكنولوجيا يُستعمل فيها خليط من تشفيرات المفاتيح العمومية وتشفيرات المفاتيح المتماثلة. ويرد أدناه وصف للسمات البارزة في التقنيات الرئيسية المستعملة حاليا (انظر الفقرات ٢٥-٦٦ أدناه).

١٧- وكما هي الحال في كثير من الأحيان، فقد تطوّرت التكنولوجيا قبل اهتمام القانون بهذا المجال بزمن طويل. ومن ثم فإن الفجوة الناتجة عن ذلك بين القانون والتكنولوجيا لا تؤدي إلى تباين مستويات المعرفة القائمة على الخبرة فحسب، بل تؤدي أيضا إلى عدم الاتّساق في استخدام هذه المصطلحات. ذلك أن التعابير التي كانت تُستخدم تقليديا بدلالة ضمنية معيّنة في إطار القوانين الوطنية باتت تُستخدم لوصف

---

[٤١] انظر تقرير الفريق العامل المعني بالتجارة الإلكترونية عن أعمال دورته الثانية والثلاثين، التي عُقدت في فيينا من ١٩ إلى ٣٠ كانون الثاني/ يناير ١٩٩٨ (A/CN.9/446)، الفقرة ٩١ وما يليها).

[٤٢] *قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية* . . . ، الجزء الثاني، الفقرة ٣٣.

تقنيات إلكترونية لا تتوافق خاصيتُها الوظيفية بالضرورة مع وظائف أو خصائص المفهوم المقابل لها في الاستعمال القانوني العادي. ومثلما رُئي أعلاه (انظر الفقرات ٧-١٠)، فإن المفاهيم "التوثيق" و"الموثوقيّة" و"التوقيع" و"الهويّة"، وإن تكن وثيقة الصلة بعضها ببعض في سياقات معيّنة، ليست متطابقة في الدلالة أو تبادلية في الاستخدام. غير أن الاستعمال العادي في صناعة تكنولوجيا المعلومات، الذي تطوّر أساسا بناء على دواعي القلق بشأن الأمن عبر الشبكات، لا يطبّق بالضرورة هذه الفئات نفسها باعتبارها كتابات قانونية.

١٨- وفي بعض الحالات، يُستخدَم التعبير "التوثيق الإلكتروني" للإشارة إلى تقنيات قد تشتمل، تبعا للسياق الذي تُستخدم فيه، على عناصر شتّى، مثل تعريف هويّة الأفراد، أو تأكيد سلطة شخص ما (أي في الأحوال النمطية، السلطة المخوّلة له للتصرّف بالنيابة عن شخص أو كيان آخر) أو امتيازات الصلاحية الممنوحة له (على سبيل المثال، العضوية في مؤسسة ما، أو اكتتاب خدمة ما)، أو ضمان بشأن سلامة المعلومات. وفي بعض الحالات أيضا، يكون التركيز على الهوية فقط،[٤٣] ولكنه يمتد أحيانا ليشمل السلطة،[٤٤] أو مجموعة مؤتلفة من أي من تلك العناصر أو منها كلها.[٤٥]

١٩- ولا يستخدم قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية،[٤٦] ولا قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية[٤٧] المصطلح "التوثيق الإلكتروني"، وذلك بالنظر إلى اختلاف معنى "التوثيق" في مختلف النظم القانونية، وإلى ما يمكن أن يُحدثه من إرباك بشأن إجراءات أو مقتضيات شكلية معيّنة. لكن قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية يستخدم بدلا عن ذلك مفهوم "الشكل الأصلي" لتوفير معايير التكافؤ الوظيفي بخصوص المعلومات الإلكترونية "الموثوقة". فوفقا للمادة ٨ من القانون النموذجي المذكور، عندما يشترط القانون تقديم معلومات أو الاحتفاظ بها في شكلها الأصلي، تستوفي رسالة البيانات هذا الاشتراط إذا:

(أ) وُجد "ما يُعوّل عليه لتأكيد سلامة المعلومات منذ الوقت الذي أُنشئت فيه للمرة الأولى في شكلها النهائي، بوصفها رسالة بيانات أو غير ذلك؛"

---

[٤٣] على سبيل المثال، تعرّف إدارة التكنولوجيا، في وزارة التجارة في الولايات المتحدة، التوثيق الإلكتروني بأنه "عملية إثبات الثقة بهويات المستعملين المقدّمة إلكترونيا إلى نظام معلومات" (الولايات المتحدة، وزارة التجارة، *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-63, version 1.0.2 (Gaithersburg, Maryland, April 2006) منشور متاح على الموقع الشبكي http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf، (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

[٤٤] على سبيل المثال، استحدثت حكومة أستراليا إطارا للتوثيق الإلكتروني، يُعرَّف فيه التوثيق الإلكتروني بأنه "عملية إقرار مستوى من الثقة فيما إذا كانت إفادة ما حقيقية أو صحيحة حين إجراء معاملة على الخط الحاسوبي المباشر أو بالهاتف. وهو يساعد على بناء الثقة في إبرام معاملة على الخط الحاسوبي المباشر بإتاحة ضمان ما للأطراف المعنية بأن معاملاتها شرعية. وقد تشمل تلك الإفادات: تفاصيل الهويّة؛ أو المؤهلات المهنية؛ أو السلطة المفوّضة لإجراء المعاملات" (أستراليا، وزارة المالية والشؤون الإدارية، *Australian Government e-Authentication Framework: An Overview* (كومنولث أستراليا، ٢٠٠٥)، منشور متاح على الموقع الشبكي http://www.agimo.gov.au/infrastructure/authentication/agaf_b/overview/introduction#e-authentication، (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

[٤٥] مبادئ التوثيق الإلكتروني التي أعدّتها حكومة كندا، على سبيل المثال، تعرّف "التوثيق" بأنه "عملية تشهد على السمات المسندة إلى المشاركين في اتصال إلكتروني، أو على سلامة الاتصال". وأما "السمات الإسنادية" فتُعرّف بأنها "معلومات بخصوص امتيازات أو حقوق هويّة مشارك ما أو أي هويّة موثّقة أخرى (كندا، الصناعة في كندا، *Principles for Electronic Authentication: a Canadian Framework* (Ottawa, May 2004)، منشور متاح على الموقع الشبكي http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html، (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

[٤٦] *قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية . . . .*

[٤٧] *قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية . . . .*

(ب) و"كانت تلك المعلومات مما يمكن عرضه على الشخص المقرّر أن تُقدّم إليه"، وذلك عندما يُشترط تقديم تلك المعلومات.

٢٠- وحفاظا على التمييز المعمول به في أكثر النظم القانونية بين التوقيع (أو الأختام، عندما تُستخدم بدلا عنه) باعتباره وسيلة "توثيق"، من ناحية، و"الموثوقية" باعتبارها نوعية مستند أو سجل ما، من ناحية أخرى، فإن القانونين النموذجيين كليهما يكملان مفهوم "الصحة" بمفهوم "التوقيع". إذ أن الفقرة الفرعية (أ) من المادة ٢ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية تعرّف التوقيع الإلكتروني بأنه بيانات في شكل إلكتروني، مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تُستخدم "لتعيين هويّة الموقِّع" فيما يتعلق برسالة البيانات، و"لبيان موافقة الموقِّع على المعلومات الواردة في رسالة البيانات".

٢١- ومن ثم فإن تعريف "التوقيع الإلكتروني" في نصوص الأونسيترال واسع النطاق عمدا، وذلك لكي يشمل جميع طرائق "التوقيع الإلكتروني" الموجودة حاليا والتي يمكن أن توجد في المستقبل. وما دامت الطرائق المستخدمة "جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أُنشئت أو أُبلغت من أجله رسالة البيانات، في ضوء كل الظروف، بما في ذلك أي اتفاق متصل بالأمر"،[٤٨] ينبغي لها أن تُعتبر مستوفية لمقتضيات التوقيع القانونية. كما إن نصوص الأونسيترال ذات الصلة بالتجارة الإلكترونية، إضافة إلى عدد كبير من النصوص التشريعية الأخرى، تستند إلى مبدأ الحياد التكنولوجي، ولذا فهي تهدف إلى استيعاب جميع أشكال التوقيع الإلكتروني. إذن فإن تعريف التوقيع الإلكتروني لدى الأونسيترال من شأنه أن يشمل كامل نطاق تقنيات "التوقيع الإلكتروني"، منذ المستوى الأعلى للأمان، ومن ذلك مثلا مخططات ضمان التوقيعات القائمة على أساس التشفير، والمرتبطة بمخطط يُعتمد فيه مرفق المفاتيح العمومية (وهو شكل شائع من أشكال "التوقيع الرقمي" (انظر الفقرات ٢٥-٥٣)، وحتى المستويات الأدنى من الأمان، ومنها مثلا الرموز الاصطلاحية غير المشفّرة أو كلمات السر. وبالتالي فإن الاقتصار على طباعة اسم المحرِّر في نهاية رسالة بريد إلكتروني، وهو أشيع أشكال "التوقيع" الإلكتروني، من شأنه على سبيل المثال أن يؤدي وظيفة تعريف هويّة محرِّر الرسالة على نحو صحيح، كلما كان معقولا استخدام طريقة ذات مستوى أمان منخفض من هذا القبيل.

٢٢- ولا يعالج قانونا الأونيسترال النموذجيان على أي نحو آخر المسائل ذات الصلة بمراقبة الوصول إلى البيانات أو التحقّق من الهوية. وهذا أيضا حفاظا على أن التوقيعات، في بيئة ورقيّة، قد تكون علامات على الهوية، ولكن يمكن بالضرورة أن تكون أيضا من السمات المسندة إلى الهوية. غير أن قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية يعالج الشروط التي بمقتضاها يحق لمن تُرسَل إليه رسالة بيانات أن يفترض أن تلك الرسالة صادرة بالفعل عن منشئها المزعوم. فالمادة ١٣ من القانون النموذجي تنص فعلا على أن رسالة البيانات تُعتَبر، في العلاقة بين المنشئ والمرسل إليه، صادرة عن المنشئ إذا أُرسلت من شخص "له صلاحية التصرّف نيابة عن المنشئ فيما يتعلق برسالة البيانات" أو "من نظام معلومات مبرمَج على يد المنشئ أو نيابة عنه للعمل تلقائيا". وكذلك في العلاقة بين المنشئ والمرسل إليه، يحق للمرسل إليه أن يعتبر رسالة البيانات صادرة عن المنشئ وأن يتصرّف على أساس هذا الافتراض، إذا (أ) "طبّق المرسل إليه تطبيقا سليما، من أجل التأكّد من أن رسالة البيانات قد صدرت عن المنشئ، إجراء سبق أن وافق عليه المنشئ لهذا الغرض؛" أو (ب) كانت رسالة البيانات كما تسلّمها المرسل إليه ناتجة عن تصرّفات شخص تمكّن بحكم

[٤٨] *قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية* . . . ، الفقرة ١ (ب) من المادة ٧.

علاقته بالمنشئ أو بأي وكيل للمنشئ من الوصول إلى طريقة يستخدمها المنشئ لإثبات أن رسائل البيانات صادرة عنه فعلا. وهذه القواعد بكليتها تتيح المجال لطرف ما لأن يستدل على هويّة شخص آخر، سواء تم "التوقيع" إلكترونيا على الرسالة أم لم يتم ذلك، وسواء أمكن استخدام الطريقة المستخدمة لإسناد الرسالة إلى المنشئ، لأغراض "التوقيع" على نحو صحيح أم لم يمكن. وهذا يتوافق مع الممارسة المتّبعة حاليا في البيئة الورقية. ذلك أن التأكّد من صوت شخص ما أو مظهره البدني أو أوراق هويته (جواز سفره الوطني)، مثلا، قد يكفي للاستنتاج بأن الشخص هو من يزعم أنه هو لغرض الاتصال بالشخص المعني، ولكن ذلك لن يكون كافيا قانونيا لاعتباره "توقيع" ذلك الشخص بمقتضى معظم النظم القانونية.

٢٣- وإلى جانب الإرباك الذي يسبّبه عدم التوافق في استعمال المصطلحات تقنيا وقانونيا في كل من البيئة الورقية والبيئة الإلكترونية، فإن مختلف التقنيات المذكورة آنفا (انظر الفقرة ١٦ أعلاه والمناقشة الأكثر تفصيلا في الفقرات ٢٤-٦٦ أدناه) يمكن أن تُستخدم لأغراض مختلفة وأن توفّر قابلية وظيفية مختلفة أيضا، تبعا للسياق. ذلك أن كلمات السر أو الرموز، على سبيل المثال، يجوز استخدامها من أجل "التوقيع" على مستند إلكتروني، ولكن من الجائز أيضا استخدامها من أجل إحراز سبل الوصول إلى شبكة ما أو قاعدة بيانات أو أي خدمة إلكترونية أخرى، تماما كما يمكن استخدام مفتاح لفتح خزانة أو باب. غير أن كلمة السر، في حين أنها في الحالة الأولى إثبات للهوية، فهي في الحالة الثانية إشارة اعتماد أو علامة على سلطة مفوَّضة، ومع أنها تكون في الأحوال الاعتيادية مرتبطة بشخص معيّن، فإن بالمستطاع أيضا إحالتها إلى شخص آخر. أما فيما يخص التوقيعات الرقمية، فإن عدم مناسبة المصطلحات الحالية يزداد جلاء. فالتوقيع الرقمي ينظر إليه على نطاق واسع باعتباره تكنولوجيا معيّنة من أجل "التوقيع" على الوثائق الإلكترونية. غير أن من الممكن التشكّك على الأقل، من وجهة نظر قانونية، فيما إذا كان تطبيق الترميز اللامتناظر لأغراض التوثيق ينبغي اعتباره "توقيعا" رقميا، لأن وظائفه تتجاوز في نطاقها الوظائف النمطية الخاصة بتوقيع مكتوب بخط اليد. فالتوقيع الرقمي يتيح وسائل من أجل "التحقق من صحّة الرسائل الإلكترونية" و"ضمان سلامة مضمونها". علاوة على ذلك فإن تكنولوجيا التوقيع الرقمي "لا تقتصر على إثبات المنشأ أو النزاهة فيما يتعلق بالأفراد حسبما تقتضيه القواعد بخصوص أغراض التوقيع، بل تستطيع أيضا أن توثّق، على سبيل المثال، الخوادم أو المواقع الشبكية أو البرامجيات الحاسوبية أو أي بيانات أخرى موزّعة أو مخزونة رقميا"، مما يوفّر للتوقيعات الرقمية نطاق استخدام أوسع بكثير من أي بديل إلكتروني عن التوقيعات بخط اليد.[٤٩]

باء- طرائق التوقيع والتوثيق الإلكترونية الرئيسية

٢٤- لأغراض هذه المناقشة، تُبحث أربع طرائق رئيسية للتوقيع والتوثيق وهي: التوقيع الرقمي؛ والطرائق البيومترية؛ وكلمات السر والطرائق الهجينة؛ والتوقيعات المستنسخة بالمسح التصويري أو المطبوعة بالآلة.

[٤٩] Babette Aalberts and Simone van der Hof, Digital Signature Blindness: *Analysis of Legislative Approaches toward Electronic Authentication*، (تشرين الثاني/ نوفمبر ٢١٩٩٩)، صفحة ٨، متاح على الموقع الشبكي http://rechten.uvt.nl/simone/Digsigbl.pdf (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

١- التوقيعات الرقمية التي تعتمد على الترميز بالمفتاح العمومي

٢٥- "التوقيع الرقمي" هو الاسم الذي يُطلق على التطبيقات التكنولوجية التي تستخدم نظم الترميز غير المتناظرة، ويشار إليها أيضا بنظم الترميز بالمفتاح العمومي، من أجل كفالة صحة الرسائل الإلكترونية وضمان سلامة محتويات هذه الرسائل. ويظهر التوقيع الرقمي بمظاهر مختلفة كثيرة، منها التوقيعات الرقمية بتقنية كشف التزوير والوقف الفوري، والتوقيع المعمَّى، والتوقيعات الرقمية التي لا يمكن إنكارها.

(أ) المفاهيم التقنية والمصطلحات

'١' الترميز

٢٦- تُنشأ التوقيعات الرقمية ويُتحقق من صحتها باستخدام الترميز، وهو فرع من الرياضيات التطبيقية يُعنى بتحويل الرسائل إلى صيغة تبدو غير مفهومة ثم إعادتها إلى صيغتها الأصلية. وتستخدم التوقيعات الرقمية ما يُعرف باسم الترميز بالمفتاح العمومي، الذي كثيرا ما يستند إلى استخدام دوالّ خوارزمية لإنتاج "مفتاحين" مختلفين ولكن مترابطين رياضيا (والمفاتيح هي أعداد ضخمة يُحصل عليها باستخدام سلسلة من الصيغ الرياضية المطبقة على أعداد أولية).[٥٠] ويُستخدم أحد هذين المفتاحين في إنشاء توقيع رقمي أو في تحويل بيانات إلى صيغة غير مفهومة في ظاهرها، ويستخدم المفتاح الثاني للتحقق من صحة توقيع رقمي أو إعادة رسالة البيانات إلى صيغتها الأصلية.[٥١] وكثيرا ما يشار إلى أجهزة وبرامجيات الحاسوب التي تستخدم مثل هذين المفتاحين بعبارة جامعة هي "نظم الترميز" (cryptosystems) أو بعبارة أكثر تحديدا هي "نظم الترميز غير المتناظرة" "asymmetric cryptosystems" عندما تعتمد على خوارزميات غير متناظرة.

'٢' مفاتيح الترميز العمومية والخصوصية

٢٧- هناك مفتاح مكمل يُستَخدم للتوقيعات الرقمية ويسمى "المفتاح الخصوصي"، وهو المفتاح الذي لا يستخدمه إلا الموقّع في إنشاء توقيع رقمي، وينبغي أن يُحافَظ على سرِّيته، في حين يكون "المفتاح العمومي" عادة معروفا على نطاق أوسع ويستخدمه طرف معوِّل في التحقق من صحة التوقيع الرقمي. ويمكن أن يُحفظ المفتاح الخصوصي على "بطاقة ذكية" أو أن يتاح الوصول إليه عن طريق رقم لتحديد الهوية

---

[٥٠] جدير بالذكر مع ذلك أن مفهوم الترميز بالمفتاح العمومي، على النحو المبين هنا، لا يقتضي ضمنا بالضرورة استخدام الخوارزميات المبنية على الأعداد الأولية. ذلك أنه توجد في الوقت الراهن تقنيات رياضية مستخدمة أو قيد التطوير، يُذكر منها نظم الترميز التي تعتمد على المنحنيات الاهليلجية، والتي كثيرا ما يقال عنها إنها تتيح درجة عالية من الأمان من خلال استخدام مفاتيح مخفضة الطول بدرجة كبيرة.

[٥١] مع أن استخدام الترميز هو أحد السمات الرئيسية للتوقيعات الرقمية، فإن كون التوقيع الرقمي لا يستخدم سوى لتوثيق رسالة تحتوي على معلومات مقدّمة في صيغة رقمية ينبغي ألا يُخلط بينه وبين الاستخدام الأعم للترميز لأغراض الحفاظ على السرية، الذي هو طريقة تستخدم لترميز الرسالة الإلكترونية بحيث لا يتمكن من قراءتها أحد غير منشئ الرسالة والمرسل إليه. وفي عدد من البلدان يقيد القانون استخدام الترميز لأغراض الحفاظ على السرية، وذلك لأسباب ذات صلة بالسياسة العامة المنطوية على اعتبارات تتعلق بالدفاع القومي. ومن جهة أخرى فإن استخدام الترميز لأغراض التوثيق بإنتاج توقيع رقمي لا يعني بالضرورة استخدام الترميز لإضفاء السرية على أي معلومات أثناء عملية الاتصال، وذلك نظرا لأن التوقيع الرقمي المرمَّز قد لا يكون سوى إضافة إلى رسالة غير مرمّزة.

الشخصية (PIN)، أو عن طريق أداة بيومترية لتحديد الهوية، وذلك مثلا عن طريق التعرّف على بصمة الإبهام. وإذا احتاج عدد كبير من الناس إلى التحقق من صحة التوقيع الرقمي للموقّع، وجب أن يُتاح المفتاح العمومي لهم جميعا أو أن يوزع عليهم جميعا، وذلك مثلا بإلحاق شهادات التصديق بالتوقيع أو بواسطة طرائق أخرى تضمن ألا يحصل على الشهادات ذات الصلة إلا الأطراف المعوّلة والأطراف التي عليها أن تتحقق من التوقيعات. وعلى الرغم من أن زوج المفاتيح مترابط رياضيا، فإنه إذا ما صُمّم ونُفّذ نظام ترميز لامتناظر بطريقة مأمونة أصبح في حكم المستحيل فعلا اشتقاق المفتاح الخصوصي انطلاقا من معرفة المفتاح العمومي. وأشيع الخوارزميات في الترميز باستخدام المفتاح العمومي والمفتاح الخصوصي تستند إلى سمة مهمة من سمات الأعداد الأولية الكبيرة: وهي أن ضرب تلك الأعداد معا لإنتاج عدد جديد يجعل معرفة أي عددين أوليين أدّيا إلى إنتاج ذلك العدد الجديد الأكبر عملية شاقة جدا ومستغرقة وقتا طويلا.[٥٢] وهكذا، فعلى الرغم من أن كثيرا من الناس قد يعرفون المفتاح العمومي لموقّع معين ويستخدمونه في التحقق من صحة توقيعه، فإنهم لا يستطيعون أن يكتشفوا المفتاح الخصوصي للموقّع وأن يستخدموه في تزوير توقيعات رقمية.

'٣' *دالة البعثرة*

٢٨- إلى جانب عملية إنتاج أزواج المفاتيح توجد عملية أساسية أخرى يشار إليها عموما بعبارة "دالة البعثرة" (hash function) وتستخدم في إنشاء التوقيعات الرقمية وفي التحقق من صحتها. ودالة البعثرة عملية رياضية مبنية على خوارزمية تنشئ تمثيلا رقميا للرسالة أو شكلا مضغوطا من الرسالة، (كثيرا ما يشار إليهما بعبارة "خلاصة الرسالة" (message digest) أو "بصمة" الرسالة (message fingerprint)) تتخذ شكل "قيمة بعثرة" (hash value) أو "نتيجة بعثرة" (hash result) ذات طول موحد قياسيا يكون عادة أصغر كثيرا من الرسالة ولكن تنفرد به الرسالة جوهريا. وأي تغيير يطرأ على الرسالة تترتب عليه دائما نتيجة بعثرة مختلفة عندما تستخدم دالة البعثرة نفسها. وفي حالة دالة بعثرة مأمونة، تعرف أحيانا باسم "دالة بعثرة ذات اتجاه واحد"، يستحيل عمليا اشتقاق الرسالة الأصلية عند معرفة قيمة البعثرة الخاصة بها. ومن المزايا الأساسية الأخرى لدالة البعثرة أنه يستحيل عمليا أيضا إيجاد شيء رقمي ثنائي (مختلف عن الشيء الذي اشتُقت منه الخلاصة أصلا) ينتج الخلاصة نفسها. ومن ثم، فإن دوالّ البعثرة تمكّن من تشغيل البرنامج الحاسوبي المعد لإنشاء التوقيعات الرقمية بمقادير من البيانات أصغر ويمكن التنبؤ بها بسهولة أكبر، كما تمكّن في الوقت نفسه من تحقيق ارتباط إثباتي قوي بمحتوى الرسالة الأصلية، والتوصل بذلك بفعالية إلى توفير ضمان على أن الرسالة لم يطرأ عليها أي تعديل منذ أن وُقّع عليها رقميا.

---

[٥٢] تشير بعض المعايير الموجودة إلى مفهوم "الاستحالة الحسابية (computational unfeasibility)" لوصف توقُّع عدم قابلية العملية للعكس، أي الأمل في استحالة اشتقاق المفتاح الخصوصي السري للمستعمل من المفتاح العمومي لذلك المستعمل. و"الاستحالة الحسابية" مفهوم نسبي يستند إلى قيمة البيانات المحمية، وتكلفة العمليات الحوسبيّة اللازمة لحمايتها، وطول الفترة التي تلزم حمايتها أثناءها، والتكلفة والوقت اللازمين للاعتداء على البيانات، مع تقدير كل هذه العوامل على ما هي عليه في الوقت الراهن وعلى ضوء التقدم التكنولوجي في المستقبل." (المبادئ التوجيهية للتوقيعات الرقمية، رابطة المحامين الأمريكيين: *Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (شيكاغو، رابطة المحامين الأمريكيين، ١ آب/ أغسطس ١٩٩٦)، صفحة ٩، الحاشية ٢٣، متاح في الموقع الشبكي http://www.abanet.org/ scitech/ec/isc/dsgfree.html، (اطلع عليه في ٤ حزيران/ يونيه ٢٠٠٨).

'٤' إنشاء التوقيع الرقمي

٢٩- قبل التوقيع على مستند أو على أي معلومات أخرى، يتعين على الموقّع أن يبين بدقة حدود ما يريد التوقيع عليه. ثم تحوسِب دالةُ بعثرة في البرنامج الحاسوبي لدى الموقّع نتيجةَ بعثرة تنفرد بها (بخصوص كل الأغراض العملية المقصودة) المعلوماتُ التي يراد التوقيع عليها. وعندئذ يحوِّل البرنامجُ الحاسوبي لدى الموقّع نتيجةَ البعثرة إلى توقيع رقمي باستخدام المفتاح الخصوصي للموقّع. وبذلك يكون التوقيع الرقمي الناتج توقيعا فريدا خاصا بالمعلومات التي يجري التوقيع عليها وبالمفتاح الخصوصي المستخدم في إنشاء التوقيع الرقمي معا. وفي العادة، يُلحق التوقيع الرقمي (أي ترميز نتيجة البعثرة المستخلصة من الرسالة بواسطة المفتاح الخصوصي لدى الموقّع) بالرسالة، ويُخزن أو يُنقل مع تلك الرسالة. غير أن من الممكن أيضا إرساله أو خزنه على أنه عنصر بيانات منفصل، ما دام مرتبطا بالرسالة المناظرة ارتباطا يمكن التعويل عليه. ولأن التوقيع الرقمي هو توقيع فريد يخص رسالته دون سواها، فإنه غير قابل للعمل به إذا كان مفصولا دوما عن الرسالة.

'٥' التحقق من صحة التوقيع الرقمي

٣٠- التحقق من صحة التوقيع الرقمي هو عملية تدقيق للتوقيع الرقمي بالرجوع إلى الرسالة الأصلية والى مفتاح عمومي معين، من أجل البتّ فيما إذا كان ذلك التوقيع الرقمي قد أنشئ لتلك الرسالة ذاتها باستخدام المفتاح الخصوصي المناظر للمفتاح العمومي المذكور في المرجع. ويتم التحقق من صحة التوقيع الرقمي بحوسبة نتيجة بعثرة جديدة للرسالة الأصلية بواسطة دالة البعثرة نفسها التي استُخدمت لإنشاء التوقيع الرقمي. ثم يدقق الشخص المتحقق، باستخدام المفتاح العمومي ونتيجة البعثرة الجديدة، فيما إذا كان التوقيع الرقمي قد أنشئ باستخدام المفتاح الخصوصي المناظر، وفيما إذا كانت نتيجة البعثرة المحوسبة مجددا تطابق نتيجة البعثرة الأصلية التي حُولت إلى التوقيع الرقمي أثناء عملية التوقيع.

٣١- ومن شأن برامجية التحقق أن تؤكد أن التوقيع الرقمي قد تم "التحقق" من صحته فيما يخص الترميز *(أ)* إذا كان المفتاح الخصوصي للموقّع قد استخدم للتوقيع على الرسالة رقميا، ومعروف أن ذلك هو الذي يحدث إذا استُخدم المفتاح العمومي للموقّع في التحقق من صحة التوقيع لأن المفتاح العمومي للموقّع يقتصر على التحقق من صحة توقيع رقمي منشأ بواسطة المفتاح الخصوصي للموقّع؛ و*(ب)* إذا كانت الرسالة لم يطرأ عليها أي تحوير، ومعروف أن ذلك هو الذي يحدث إذا كانت نتيجة البعثرة التي حسبها المتحقق مطابقة لنتيجة البعثرة المستخرجة من التوقيع الرقمي أثناء عملية التحقق من صحته.

'٦' استخدام تكنولوجيا التوقيع الرقمي لأغراض أخرى

٣٢- كما ذكر أعلاه، فإن لتكنولوجيا التوقيع الرقمي استخداما أوسع نطاقا بكثير من "التوقيع" فحسب على الخطابات الإلكترونية بالطريقة نفسها التي تستخدم بها التوقيعات الخطية للتوقيع على المستندات. فشهادات التصديق الموقّعة رقميا كثيرا ما تُستخدم فعلا "لتوثيق" الخوادم أو المواقع الشبكية، على سبيل المثال، من أجل طمأنة مستعملي الخادم أو الموقع الشبكي أن ذلك الخادم أو الموقع الشبكي هو ذاته

المدعى أنه المقصود، أو أنه تابع حقا إلى الشركة التي تدعي بأنها تدير الخادم أو الموقع الشبكي. كما يمكن استخدام تكنولوجيا التوقيع الرقمي لغرض "توثيق" برامجيات الحاسوب، على سبيل المثال، من أجل ضمان صحّة برامجية منـزَّلة من موقع شبكي؛ أو لضمان استخدام خادم تطبيقات معين لتكنولوجيا معتَرف على نطاقٍ واسع بأنها توفر مستوى معينا من الأمان في الاتصال الشبكي، أو لغرض "توثيق" أي بيانات أخرى موزعة أو مخزَّنة رقميا.

(ب) مرافق المفاتيح العمومية ومقدّمو خدمات التصديق

٣٣- للتحقق من صحة توقيع رقمي، يجب أن تتوافر للمتحقق سبل الوصول إلى المفتاح العمومي الخاص بالموقّع وأن يكون لديه ما يضمن له تناظره مع المفتاح الخصوصي للموقّع. غير أنه ليس لزوج من المفاتيح، عمومي وخصوصي، أي ارتباط جوهري بأي شخص معين؛ إذ إنه مجرد زوج من الأرقام. لذلك، فإن من الضروري أن توافر آلية إضافية للربط على نحو جدير بالتعويل عليه بين شخص معين أو هيئة معينة وزوج المفاتيح. وهذا مهم جدا، لأنه قد لا تكون هناك علاقة ثقة مسبقة بين الموقِّع ومتلقي الخطابات الموقّعة رقميا. ولهذا الغرض، يجب أن تتوافر لدى الأطراف المشمولة درجة من الثقة فيما يصدر من مفاتيح عمومية وخصوصية.

٣٤- وقد يتوافر مستوى الثقة المطلوب بين الأطراف التي يثق بعضها ببعض، أو التي تكون قد تعاملت فيما بينها طوال فترة من الزمن، أو التي تقيم اتصالات فيما بينها ضمن نظم مغلقة، أو التي تعمل ضمن مجموعة مغلقة، أو التي لديها القدرة على إحكام معاملاتها تعاقديا، كأن يكون بينها مثلا اتفاق شراكة تجارية. أما في معاملة لا تشمل سوى طرفين، فإنه يمكن لكل منهما الاقتصار على إبلاغ الآخر (عبر قناة مأمونة نسبيا، مثل ساع خاص أو هاتف) بالمفتاح العمومي من زوج المفاتيح الذي سوف يستخدمه كل منهما. غير أنه قد لا يكون المستوى نفسه من الثقة متوافرا إذا كانت الأطراف لا تتعامل فيما بينها إلا نادرا، أو إذا كانت تجري اتصالاتها بواسطة نظم مفتوحة (مثل الشبكة العالمية عبر الإنترنت)، أو لا تعمل ضمن مجموعة مغلقة، أو لم تكن لديها اتفاقات شراكة تجارية أو قوانين أخرى تحكم ما بينها من علاقات. علاوة على ذلك، ينبغي أن يوضع في الحسبان أنه إذا كانت هناك حاجة إلى تسوية المنازعات في المحكمة أو باللجوء إلى التحكيم، فإنه قد يكون من الصعب إثبات أن المالك المشروع لمفتاح عمومي معين هو الذي أعطاه أو لم يعطه فعلا إلى المستلِم.

٣٥- وقد يصدر موقّع مرتقب بيانا عاما يذكر فيه أن التوقيعات التي يمكن التحقق من صحتها بمفتاح عمومي معين ينبغي أن تعامل على أنها ناشئة من الموقّع. ويخضع شكل ذلك البيان وفعاليته القانونية لقانون الدولة المشترعة. فقرينة إسناد توقيعات إلكترونية إلى موقّع معيّن يمكن إثباتها مثلا من خلال نشر ذلك البيان في مجلة رسمية أو في وثيقة تعترف السلطات العمومية بأنها "صحيحة". غير أن أطرافا أخرى قد لا تكون على استعداد لقبول البيان، وبخاصة في حال عدم وجود عقد سابق يُرسي عن يقين المفعول القانوني لذلك البيان المنشور. فالطرف الذي يعوّل على مثل ذلك البيان المنشور في نظام مفتوح ودون سند يدعمه سيكون عرضة لمخاطرة كبيرة من جرّاء وضعه ثقته بعدم احتراز في شخص محتال أو نتيجة لاضطراره إلى دحض إنكار زائف لتوقيع رقمي (وهي مسألة كثيرا ما يشار إليها في سياق "عدم التنصل" من التوقيعات الرقمية) إذا تبين أن معاملة ما ليست في صالح الموقّع المزعوم.

٣٦- ويتمثل أحد الحلول لبعض هذه المشاكل في استخدام واحد أو أكثر من الأطراف الثالثة في الربط بين موقّع محدد الهوية أو اسم الموقّع من جهة ومفتاح عمومي معيّن من جهة أخرى. ويشار إلى هذا الطرف الثالث عموما بعبارة "سلطة التصديق" أو "مقدّم خدمات التصديق" أو "مورِّد خدمات التصديق" في معظم المعايير التقنية والمبادئ التوجيهية (في قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، اختيرت عبارة "مقدّم خدمات التصديق"). وفي عدد من البلدان، تُنظَّم سلطات التصديق هذه هرميا لتصبح كيانا يشار إليه في أحيان كثيرة بعبارة "مرفق مفاتيح عمومية". إذ إن سلطات التصديق ضمن مرفق للمفاتيح العمومية يمكن إنشاؤها في بنية هرمية، حيث تقتصر وظيفة بعض سلطات التصديق على تصديق سلطات تصديق أخرى تقدِّم الخدمات مباشرة إلى المستعملين. وفي بنية كهذه، تكون بعض سلطات التصديق تابعة لسلطات تصديق أخرى. وفي بنى أخرى يمكن تصورها، قد تعمل جميع سلطات التصديق على قدم المساواة بعضها مع البعض الآخر. وفي أي مرفق كبير للمفاتيح العمومية، يُرجّح أن توجد سلطات تصديق تابعة وسلطات تصديق أعلى مستوى. وقد تشمل الحلول الأخرى المتبعة في هذا الخصوص، مثلا، اللجوء إلى شهادات التصديق التي تصدرها أطراف معوِّلة.

'١' *مرفق المفاتيح العمومية*

٣٧- إن إنشاء مرفق مفاتيح عمومية هو وسيلة لتوفير الثقة: *(أ)* بأن المفتاح العمومي لمستعمِل ما لم يُعبث به وبأنه يناظر بالفعل المفتاح الخصوصي لذلك المستعمل؛ و*(ب)* بأن تقنيات الترميز المستخدمَة هي تقنيات سليمة. وبغية توفير الثقة المبينة أعلاه، يمكن أن يقدّم مرفق المفاتيح العمومية عددا من الخدمات تشمل ما يلي: *(أ)* إدارة مفاتيح الترميز المستعملة لأغراض التوقيع الرقمي؛ و*(ب)* التصديق على أن مفتاحا عموميا معيّنا يناظر مفتاحا خصوصيا؛ و*(ج)* توفير مفاتيح للمستعملين النهائيين؛ و*(د)* نشر معلومات عن إلغاء المفاتيح العمومية أو شهادات التصديق؛ و*(هـ)* إدارة الوسائل الرمزية الشخصية (كالبطاقات الذكية مثلا) التي يمكنها تحديد هوية المستعمل بمعلومات هوية شخصية فريدة، أو يمكنها أن تنتج وتخزن المفاتيح الخصوصية الخاصة بالأفراد؛ و*(و)* التدقيق في هوية المستعملين النهائيين وتزويدهم بالخدمات؛ و*(ز)* تقديم خدمات ختم الوقت؛ و*(ح)* إدارة مفاتيح الترميز المستخدمة لأغراض السرّية حيثما يكون استخدام هذه التقنية مأذونا به.

٣٨- وقد يكون مرفق المفاتيح العمومية مستندا إلى مستويات هرمية مختلفة من السلطة. من أمثلة ذلك أن النماذج التي يجري النظر فيها في بلدان معيّنة لإنشاء مرافق مفاتيح عمومية ممكنة تشتمل على إحالات مرجعية إلى المستويات التالية: *(أ)* "سلطة رئيسية" (root authority) فريدة تصدّق على تكنولوجيا وممارسات جميع الأطراف المأذون لها بإصدار أزواج مفاتيح ترميز أو شهادات تصديق تتعلق باستخدام تلك الأزواج من المفاتيح؛ كما تسجل سلطات التصديق التابعة لها؛[٥٣] و*(ب)* سلطات تصديق مختلفة، في مرتبة أدنى من السلطة الرئيسية، تصدّق على أن المفتاح العمومي لأحد المستعملين يناظر بالفعل المفتاح الخصوصي لذلك المستعمل (أي أنه لم يُعبث به)؛ و*(ج)* سلطات تسجيل محلية مختلفة، على مستوى أدنى من مستوى سلطات التصديق، تتلقى الطلبات من المستعملين للحصول على أزواج مفاتيح الترميز أو على شهادات التصديق المتعلقة باستخدام تلك الأزواج من المفاتيح، وتشترط إثبات هوية المستعملين المحتملين وتدقق في تلك الهوية. وفي بلدان معيّنة، يُتوخى أن يقوم الكُتّاب العدول بدور سلطات التسجيل المحلية أو بمساندة تلك السلطات في مهمتها.

[٥٣] مسألة ما إذا كان ينبغي أن تكون لدى الحكومة القدرة التقنية على الاحتفاظ بالمفاتيح الخصوصية المستخدمة لأغراض السرية أو على إعادة إنشاء تلك المفاتيح هي مسألة يمكن تناولها على مستوى السلطة الرئيسية.

٣٩- ويمكن توسيع نطاق مرافق المفاتيح العمومية المنظَّمة في بنية هرمية وذلك بإدماج "مجموعات" جديدة من هذه المرافق من خلال قيام السلطة الرئيسية بإنشاء علاقة ثقة بالسلطة الرئيسية للمجموعة الجديدة.[٥٤] ويجوز إدماج السلطة الرئيسية للمجموعة الجديدة مباشرة في "الكيان الرئيسي" لمرفق المفاتيح العمومية المستقبل، لتصبح بالتالي مقدّما لخدمات تصديق تابعا ضمن ذلك المرفق. كما يمكن للسلطة الرئيسية للمجموعة الجديدة أن تصبح مقدّما لخدمات تصديق تابعا لأحد مقدّمي خدمات التصديق التابعين ضمن المرفق القائم. ومن السمات الجذابة الأخرى للمرافق الهرمية للمفاتيح العمومية أنها تسهِّل تطوير مسارات التصديق لأنها تسير في اتجاه واحد فقط، أي من الشهادة الموجودة بحيازة المستعمل رجوعا إلى جهة الثقة. إضافة إلى ذلك، فإن مسارات التصديق ضمن أي مرفق هرمي للمفاتيح العمومية قصيرة نسبيا، ويعلم مستعملو البنية الهرمية ضمنيا التطبيقات التي يجوز أن تُستعمل لها كل شهادة، بحسب مكانة مقدّم خدمات التصديق داخل البنية الهرمية. غير أن لهذه المرافق الهرمية الخاصة بالمفاتيح العمومية سلبياتها أيضا، ولا سيما السلبيات الناجمة عن التعويل على جهة ثقة وحيدة. فإذا ضعفت السلطة الرئيسية ضعف مرفق المفاتيح العمومية بكامله. إضافة إلى ذلك، وجدت بعض البلدان أن من الصعب اختيار كيان واحد ليكون سلطة رئيسية وفرض تلك البنية الهرمية على جميع مقدّمي خدمات التصديق الآخرين.[٥٥]

٤٠- أما ما يسمى بمرفق المفاتيح العمومية "المتشابك" فيعتبر بنية بديلة عن المرفق الهرمي. ففي إطار هذا النموذج، يرتبط مقدّمو خدمات التصديق بعلاقة بين الأقران. ويمكن لجميع مقدّمي خدمات التصديق في هذا النموذج أن يكونوا جهات ثقة. وعموما، سوف يثق المستعملون بمقدّمي خدمات التصديق الذين أصدروا شهادة التصديق. وسوف يصدر مقدّمو خدمات التصديق الشهادات بعضهم إلى بعض؛ ويبين زوج الشهادات علاقة الثقة المتبادلة بينهم. ويعني غياب الترتيب الهرمي في هذا النظام أن مقدّمي خدمات التصديق لا يستطيعون فرض شروط تحكم أنواع الشهادات التي يصدرها مقدّمون آخرون لخدمات التصديق. وإذا رغب مقدّم خدمات تصديق تقييد حدود الثقة المتاحة إلى مقدّمي خدمات تصديق آخرين، وجب عليه تحديد هذه القيود في الشهادات التي يصدرها لأقرانه.[٥٦] غير أن المواءمة بين شروط وقيود الاعتراف المتبادل قد تكون هدفا معقدا للغاية.

٤١- وهناك بنية بديلة ثالثة تستند إلى مقدّم خدمات تصديق يسمى مجازا "الجسر". وقد تكون هذه البنية مفيدة جدا، إذ يمكن لمجموعات مرافق المفاتيح العمومية من خلالها أن تثق بشهادات كل منها. وعلى خلاف مقدّم خدمات التصديق في مرفق المفاتيح العمومية "المتشابك"، فإن مقدّم خدمات التصديق "الجسر" لا يصدر شهادات التصديق مباشرة إلى المستعملين. وليس المقصود أن يقوم مستعملو مرفق المفاتيح العمومية باستخدام مقدّم خدمات التصديق "الجسر" كجهة ثقة، كما هو الحال فيما يتعلق بمقدّم خدمات التصديق "الرئيسي". وعوضا عن ذلك، ينشئ مقدّم خدمات التصديق "الجسر" علاقة ثقة بمختلف مجموعات المستعملين بوصفها أقرانا، وبالتالي يمكّن المستعملين من الإبقاء على جهات الثقة الطبيعية الخاصة بهم ضمن كل مرفق من مرافق المفاتيح العمومية لديهم. وإذا ما نفّذت مجموعة من المستعملين تكوين مجال ثقة على

---

[٥٤] William T. Polk and Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, National Institute of Standards and Technology (أيلول/ سبتمبر ٢٠٠٠)، منشور متاح على الموقع الشبكي http://csrc.nist.gov/pki/documents/B2B-article.pdf (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

[٥٥] يذكر بولك وهاستينغس (*Bridge Certification Authorities* ...) أن في الولايات المتحدة الأمريكية، كان من الصعب جدا اختيار وكالة واحدة من وكالات الحكومة الفدرالية للاضطلاع بكامل السلطة على مرفق المفاتيح العمومية الفدرالية.

[٥٦] *Polk and Hastings, Bridge Certification Authorities...*.

شكل مرفق مفاتيح عمومية هرمي، فإن مقدّم خدمات التصديق "الجسر" سوف يقيم علاقة بالسلطة الرئيسية لذلك المرفق. ولكن، إذا نفّذت مجموعة المستعملين تكوين مجال ثقة من خلال إنشاء مرفق مفاتيح عمومية متشابك، فلن يحتاج مقدّم خدمات التصديق "الجسر" إلا إلى إرساء علاقة بأحد مقدّمي خدمات التصديق التابعين لمرفق المفتاح العمومي، الذي يصبح عندئذ مقدّم خدمات التصديق "الرئيسي" داخل ذلك المرفق لغرض إرساء "جسر الثقة" لمرفق المفتاح العمومي الآخر. وبفضل "جسر الثقة" الذي يصل مرفقين أو أكثر من مرافق المفاتيح العمومية من خلال علاقتهما المشتركة بمقدّم خدمات التصديق "الجسر" يتمكّن المستعملون من مجموعات المستعملين المختلفة من التفاعل فيما بينهم من خلال مقدّم خدمات التصديق "الجسر" بمستوى ثقة محدد.[٥٧]

'٢' *مقدِّم خدمات التصديق*

٤٢- للربط بين زوج من المفاتيح وموقِّع مرتقب، يصدر مقدّم خدمات التصديق (أو سلطة التصديق) شهادة هي عبارة عن سجل إلكتروني يتضمن في قوائمه المفتاح العمومي إلى جانب اسم المكتتب في الشهادة، باعتباره "موضوع" الشهادة، وقد يؤكد أن الموقّع المرتقب المحددة هويته في الشهادة حائز على المفتاح الخصوصي المناظر. والوظيفة الرئيسية للشهادة هي ربط مفتاح عمومي بموقِّع معين. وبوسع "متلقي" الشهادة الراغب في التعويل على توقيع رقمي أنشأه الموقِّع المسمى في الشهادة أن يستعمل المفتاح العمومي المذكور في الشهادة للتحقق من أن التوقيع الرقمي أنشئ باستخدام المفتاح الخصوصي المناظر. فإذا صح هذا التحقق، توفّر مستوى من الضمان تقنيا بأن الموقِّع هو الذي أنشأ التوقيع الرقمي، وأن الجزء من الرسالة المستخدم في دالة البعثرة (وبالتالي رسالة البيانات المناظرة) لم يعدَّل منذ أن وقِّع عليها رقميا.

٤٣- ولتأكيد صحة الشهادة فيما يتعلق بمضمونها ومنشئها، يوقّع عليها رقميا مقدّم خدمات التصديق. ويمكن التحقق من صحة التوقيع الرقمي لمقدّم خدمات التصديق على الشهادة باستخدام المفتاح العمومي الخاص بمقدّم خدمات التصديق المذكور في شهادة أخرى صادرة عن مقدّم خدمات تصديق آخر (قد يكون هذا الأخير، ولكن ليس ذلك لازما، أعلى منه مستوى في الترتيب الهرمي)، ويمكن أن تُوثّق تلك الشهادة الأخرى بدورها باستخدام المفتاح العمومي المذكور في شهادة أخرى، وهكذا دواليك إلى أن يطمئن الشخص المعوّل على التوقيع الرقمي اطمئنانا كافيا إلى أصالة التوقيع. وكذلك يُعدّ تسجيل التوقيع الرقمي في شهادة تصديق صادرة عن مقدّم خدمات التصديق (يشار إليها أحيانا بعبارة "الشهادة الرئيسية") وسيلة أخرى للتحقق من التوقيع الرقمي.[٥٨]

٤٤- وفي كل من هذه الحالات، يجوز لمقدّم خدمات التصديق المصدر للشهادة أن يوقّع رقميا على شهادته هو أثناء فترة سريان الشهادة الأخرى المستخدمة في التحقق من صحة التوقيع الرقمي لمقدّم خدمات التصديق. وبموجب قوانين بعض الدول، قد يكون نشر المفتاح العمومي لمقدّم خدمات التصديق، أو بعض البيانات الخاصة بالشهادة الرئيسية (مثل "البصمة الرقمية")، في نشرة رسمية، طريقة من طرائق بناء الثقة في التوقيع الرقمي لمقدّم خدمات التصديق.

---

[٥٧] اختير في نهاية المطاف مقدّم خدمات التصديق "الجسر" كبنية لإقامة نظام مرفق المفاتيح العمومية للحكومة الفيدرالية للولايات المتحدة. (Polk and Hastings, *Bridge Certification Authorities*...) وكان ذلك أيضا هو النموذج المتبع لاستحداث نظام مرفق المفاتيح العمومية لحكومة اليابان.

[٥٨] *قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية* . . . ، الجزء الثاني، الفقرة ٥٤.

٤٥- والتوقيع الرقمي المناظر لرسالة ما، سواء أنشأه الموقِّع لتوثيق رسالة أو أنشأه مقدّم خدمات تصديق لتوثيق شهادته، ينبغي عموما أن يُختم زمنيا على نحو يعوَّل عليه، وذلك لكي يتاح للشخص المتحقق أن يعرف قطعا ما إذا كان التوقيع الرقمي قد أنشئ أثناء "فترة السريان" المذكورة في الشهادة، وما إذا كانت الشهادة صالحة (أي مثلا أنها غير مذكورة في قائمة من قوائم إلغاء الشهادات) في الوقت المعين، وهو شرط من شروط قابلية التحقق من صحة التوقيع الرقمي.

٤٦- ولتيسير التحقق من المفتاح العمومي ومن مناظرته لموقِّع معين، من الجائز نشر الشهادة في مستودع، أو إتاحة الاطلاع عليها بوسائل أخرى. وفي العادة، تكون المستودعات قواعد بيانات على خط الحاسوب تحوي معلومات عن الشهادات ومعلومات أخرى متاحة للاسترجاع والاستخدام في التحقق من صحة التوقيعات الرقمية.

٤٧- وربما يتبين، بعد صدور الشهادة، أنها لا يُعوّل عليها، وهذا يحدث، مثلا، عندما يدعي موقِّع الشهادة أمام مقدّم خدمات التصديق هوية غير هويته. وفي ظروف أخرى، ربما يمكن التعويل على الشهادة حين صدورها، ولكنها قد تفقد صلاحيتها للتعويل عليها بعد ذلك. فإذا لحق بالمفتاح الخصوصي، "ما يثير الشبهة"، كأن يفقد الموقِّع سيطرته على المفتاح الخصوصي، فقد تفقد الشهادة جدارتها بالثقة أو تصبح غير جديرة بالتعويل عليها، وقد يعمد مقدّم خدمات التصديق (بناء على طلب الموقِّع أو حتى من دون موافقته، رهنا بالظروف) إلى تعليق الشهادة (بوقف فترة سريانها مؤقتا) أو إلى إلغائها (إبطالها بصفة دائمة). ويتوقع من مقدّم خدمات التصديق أن ينشر في الوقت المناسب بعد تعليق الشهادة أو إلغائها إشعارا بذلك الإلغاء أو التعليق أو يبلّغ ذلك إلى الأشخاص المستفسرين أو إلى الأشخاص الذين يُعرَف أنهم تلقوا توقيعا رقميا يمكن التحقق من صحته بالرجوع إلى الشهادة التي فقدت صلاحية التعويل عليها. كذلك، ينبغي أيضا، كلما اقتضى الأمر ذلك، مراجعة شهادة مقدّم خدمات التصديق نفسه للتأكد من عدم إلغائها، وكذلك مراجعة الشهادة الصادرة للتحقق من توقيع سلطة ختم الوقت على أدوات ختم الوقت وعلى شهادات مقدّم خدمات التصديق الذي يصدر هذه الشهادات الخاصة بسلطات ختم الوقت.

٤٨- ويمكن أن يدير سلطات التصديق مقدّمو خدمات من القطاع الخاص أو جهات حكومية. ومن المتوخّى في بعض البلدان، لأسباب تتعلق بالسياسة العامة، أن تكون الهيئات الحكومية هي وحدها التي لها صلاحية القيام بدور سلطات التصديق. غير أن تقديم خدمات التصديق في معظم البلدان يكون إما مجالا متروكا بالكامل للقطاع الخاص، وإما يتعايش فيه مقدّمو خدمات التصديق الحكومية مع مقدّمي خدمات التصديق من القطاع الخاص. وتوجد أيضا نظم تصديق مقفلة، حيث تقوم مجموعات صغيرة بإيجاد مقدّم خدمات التصديق الخاص بها. وفي بعض البلدان يصدِر مقدّمو خدمات التصديق الحكومية الشهادات فقط لدعم التوقيعات الإلكترونية التي تستخدمها الإدارات العمومية. وبصرف النظر عما إذا كانت سلطات التصديق تشغّلها هيئات حكومية أو يشغّلها مقدّمو خدمات من القطاع الخاص، وعما إذا كانت سلطات التصديق ستحتاج أو لن تحتاج إلى الحصول على رخصة للعمل، يوجد نموذجيا أكثر من مقدّم خدمات تصديق عامل في مرفق المفاتيح العمومية. ومن دواعي الاهتمام الخاص ما يقام من علاقات بين سلطات التصديق المختلفة (انظر الفقرات ٣٨-٤١ أعلاه).

٤٩- وقد يتعين على مقدّم خدمات التصديق، أو على السلطة الرئيسية، ضمان استيفاء المقتضيات المفروضة بموجب سياستهما العامة باستمرار. فقد يستند اختيار سلطات التصديق إلى عدد من العوامل، يُذكر منها قوة المفتاح العمومي المستخدم وهوية مستعمله، إلا أن الجدارة بالثقة التي يتمتع بها أي مقدّم خدمات تصديق قد تتوقف أيضا على إنفاذه معايير بشأن إصدار الشهادات ومدى إمكانية التعويل على تقييمه

للبيانات التي يتلقاها من المستعملين الراغبين في الحصول على شهادات. ومما يتسم بأهمية بالغة نظام المسؤولية الذي ينطبق على أي مقدّم خدمات تصديق فيما يتعلق بامتثاله لمقتضيات السياسة العامة والأمان الصادرة عن السلطة الرئيسية أو عن مقدّم خدمات التصديق من مرتبة عليا، أو بامتثاله لأي مقتضيات أخرى منطبقة، وذلك على أساس مستمر. ومما يتسم بالقدر ذاته من الأهمية الالتزام بأن يتصرف مقدّم خدمات التصديق وفقا للتأكيدات التي يقدمها بخصوص سياساته العامة وممارساته، كما هو متوخى في الفقرة ١ *(أ)* من المادة ٩ من القانون النموذجي بشأن التوقيعات الإلكترونية.

(ج) مشاكل عملية في استخدام مرفق المفتاح العمومي

٥٠- على الرغم من المعرفة الواسعة في مجال تكنولوجيات التوقيع الرقمي والطريقة التي تعمل بها، فإن تنفيذ تدابير إنشاء مرافق المفاتيح العمومية ومخططات التوقيعات الرقمية واجه عمليا بعض المشكلات التي أبقت مستوى استخدام التوقيعات الرقمية أدنى من التوقعات.

٥١- والتوقيعات الرقمية تؤدي عملها جيدا كوسيلة للتحقق من التوقيعات التي تُنشأ خلال فترة صلاحية شهادة ما. غير أنه حالما تنتهي صلاحية الشهادة أو تُلغى، يفقد المفتاح العمومي المناظر صلاحيته، حتى وإن لم يكن هناك ما يثير الشبهة في زوج المفاتيح. وعليه، فإن مخطط مرفق المفتاح العمومي يتطلب نظاما لإدارة شؤون التوقيعات الرقمية بغية ضمان إتاحة التوقيع طوال الوقت اللازم. وتنجم الصعوبة الرئيسية عن احتمال أن تصبح السجلات الإلكترونية "الأصلية" (أي الأرقام الثنائية، أو "البتّات" (bits) التي يتكوّن منها الملف الحاسوبي الذي سُجِّلت فيه المعلومات)، بما في ذلك التوقيع الرقمي، غير مقروءة أو غير جديرة بالتعويل عليها مع مرور الوقت، وذلك أساسا بسبب تقادم البرامجية أو المعدات أو كلتيهما. إضافة إلى ذلك، قد يصبح التوقيع الرقمي غير مأمون، نتيجة التطورات العلمية في تحليل الترميز (الجفرة)، أو قد لا تتوافر برامجية التحقق من التوقيع طوال فترات طويلة من الزمن أو قد لا يبقى المستند سليما.[٥٩] وهذا يجعل الاحتفاظ بالتوقيعات الإلكترونية لفترة طويلة مسألة إشكالية عموما. ومع أن الاعتقاد ساد لفترة من الزمن بأن التوقيعات الرقمية أساسية لأغراض المحفوظات، فقد بينت التجربة أنها ليست محصنة من المخاطر على المدى الطويل. وبما أن أي تغيير في السجل بعد وقت إنشاء التوقيع سوف يتسبب في إخفاق التحقق من التوقيع، فإن عمليات إعادة التشكيل بما يحفظ السجل مقروءا في المستقبل (من قبيل نقل البيانات أو تحويلها) قد يؤثر على ديمومة التوقيع.[٦٠] والحقيقة أن فكرة استخدام التوقيعات الرقمية نشأت من أجل توفير الأمان

---

[٥٩] Jean-François Blanchette, "Defining electronic authenticity: an interdisciplinary journey"، منشور متاح على الموقع الشبكي: http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨) (ورقة منشورة في مجلد إضافي بشأن International Conference on Dependable Systems and Networks (DSN 2004) ٢٠٠٤، فلورنسا، إيطاليا، ٢٨ حزيران/ يونيه - ١ تموز/ يوليه ٢٠٠٤)، الصفحات ٢٢٨-٢٣٢.

[٦٠] "في النهاية، كل ما يمكن الاحتفاظ به في السياق الإلكتروني هو البتّات (bits). غير أنه كان واضحا لوقت طويل أن من الصعب جدا الاحتفاظ بمجموعة من البتّات (bits) إلى ما لا نهاية. فمع مرور الزمن، تصبح مجموعة البتّات غير مقروءة (للحاسوب وبالتالي للبشر) بسبب التقادم التكنولوجي لبرنامج التطبيق و/ أو للأجهزة الحاسوبية (ومنها القارئ). ولم تُدرَس حتى الآن مشكلة ديمومة التوقيعات الرقمية المستندة إلى مرافق المفاتيح العمومية على نحو جيد بسبب تعقدها. ومع أن أدوات التوثيق التي كانت مستخدمة في الماضي، كالتوقيعات الخطية، والأختام، والطوابع، وبصمات الأصابع، الخ معرضة أيضا إلى إعادة تشكيل (مثل استخدام الميكروفيلم) بسبب تقادم الحامل الورقي، فإنها لا تصبح أبدا عديمة الفائدة بعد إعادة التشكيل. فهناك دوما نسخة واحدة على الأقل متاحة لمقارنتها بأدوات توثيق أصلية أخرى." (Jos Dumortier and Sofie Van den Eynde, *Electronic Signatures and Trusted Archival Services*، الصفحة ٥، والمنشور متاح على الموقع الشبكي http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where، وقد اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

في تبليغ المعلومات أكثر من كونها نشأت لحفظ المعلومات على مدى الزمن.[٦١] ولم تؤد المبادرات الرامية إلى تجاوز هذه المشكلة إلى حل دائم بعد.[٦٢]

٥٢- وثمة مجال آخر قد تؤدي فيه التوقيعات الرقمية ومخططات مرافق المفاتيح العمومية إلى مشكلات عملية، وهو يتعلق بأمن البيانات وحماية الخصوصية (الحرمة) الشخصية. فعلى مقدّمي خدمات التصديق تأمين حفظ المفاتيح التي تُستخدم لتوقيع الشهادات التي يصدرونها لزبائنهم، وقد تتعرض لمحاولات خارجية للوصول إليها دون إذن (انظر أيضا الجزء الثاني، الفقرات ٢٢٣-٢٢٦ أدناه). وبالإضافة إلى ذلك، يتعين على مقدّمي خدمات التصديق الحصول على سلسلة من البيانات الشخصية والمعلومات التجارية من الأشخاص الذين يتقدمون بطلب للحصول على شهادات التصديق. كما يتعين على مقدّم

[٦١] في عام ١٩٩٩، أطلق أمناء محفوظات من بلدان مختلفة مشروع الأبحاث الدولية الخاصة بالسجلات ذات الحجية الدائمة في النظم الإلكترونية (InterPARES) الذي يهدف إلى "تطوير المعارف النظرية والمنهجية اللازمة لحفظ السجلات ذات الحجية المنشأة و/ أو المحتفظ بها بالشكل الرقمي" (انظر الموقع الشبكي http://www.interpares.org/، وقد اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨). وأشار مشروع تقرير فرقة العمل المعنية بالتحقق من الحجية (متاح على الموقع الشبكي http://www.interpares.org/documents/ atf_draft_final_report.pdf ، وقد اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨) الذي كان جزءا من المرحلة الأولى من مشروع (InterPARES 1) التي انتهت في عام ٢٠٠١، إلى أن "التوقيعات الرقمية ومرافق المفاتيح العمومية هي أمثلة على التكنولوجيات التي تم تطويرها وتنفيذها كوسائل توثيق للسجلات الإلكترونية التي تُنقل عبر الفضاء. ومع أن حافظي السجلات والعاملين في مجال تكنولوجيا المعلومات يثقون في تكنولوجيات التوثيق لضمان حجية السجلات، لم يكن القصد من هذه التكنولوجيات هو ضمان حجية السجلات الإلكترونية عبر الزمن، وهي لا تمثل وسيلة قابلة للاستمرار في هذا المجال." التقرير النهائي عن (InterPARES 1) متاح على الموقع الشبكي. http://www.interpares.org/book/index.htm وتهدف مواصلة المرحلة الثانية من المشروع (InterPARES 2) إلى وضع وتحديد المفاهيم والمبادئ والمعايير والطرائق التي يمكن بها ضمان إنشاء سجلات دقيقة وموثوقة وصيانتها والحفاظ على السجلات الأصلية على المدى الطويل في سياق الأنشطة الفنية والعلمية والحكومية المنفذة بين عامي ١٩٩٩ و٢٠٠١.

[٦٢] على سبيل المثال، أُطلقت عام ١٩٩٩ المبادرة الأوروبية بشأن التوحيد القياسي للتوقيعات الإلكترونية (EESSI) من جانب مجلس معايير تكنولوجيا المعلومات والاتصالات، وهو فريق تعاون بين المنظمات المعنية بالتوحيد القياسي والأنشطة ذات الصلة في مجال تكنولوجيات المعلومات والاتصالات، أنشئ من أجل تنسيق أنشطة التوحيد القياسي بهدف دعم تنفيذ التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية (انظر *Official Journal of the European Communities,* L 13/12، ١٩ كانون الثاني/ يناير ٢٠٠٠) وسعى اتحاد مؤسسات المبادرة الأوروبية بشأن التوحيد القياسي للتوقيعات الإلكترونية (وهو جهد للتوحيد القياسي يهدف إلى تحويل المقتضيات الواردة في التوجيه الإداري الأوروبي بشأن التوقيعات الإلكترونية إلى معايير قياسية أوروبية) إلى تلبية الحاجة إلى ضمان الاحتفاظ بالوثائق الموقعة من خلال تقنيات الترميز على المدى الطويل من خلال معياره الخاص "بنماذج تشكيل التوقيع الإلكتروني" (Electronic Signature Formats ES 201 733, ETSI, 2000). ويميز النموذج التشكيلي بين لحظتي التحقق من صحة التوقيع، وهما تحقق أولي وتحقق لاحق. ويحوي نموذج التحقق اللاحق جميع المعلومات التي يمكن استعمالها في عملية التحقق النهائي مثل معلومات الإلغاء، وأختام الوقت، والسياسات العامة بشأن التوقيع، إلخ. وتُجمع هذه المعلومات في مرحلة التحقق الأولي. وكان التهديد الأمني لصحة التوقيع الذي ينتج عن تفسُّخ قوة الترميز من بين شواغل مصممي نماذج التوقيع الإلكتروني. ولتجنب التهديد الذي يمثله هذا التفسخ، يجدد ختم الوقت بانتظام على التوقيعات بحسب مقتضيات المبادرة، مع توفير خوارزميات توقيع وأحجام مفاتيح مناسبة لأحدث طرائق الترميز. وجرى تناول مشكلة عمر البرامجية في تقرير المبادرة لعام ٢٠٠٠، الذي عرَّف "خدمات المحفوظات الموثوقة"، وهو نوع جديد من الخدمات التجارية التي ستقدمها أجهزة مختصة ومهنيون في هذا المجال، بهدف ضمان حفظ الوثائق الموقعة بتقنية الترميز، على المدى الطويل. ويورد التقرير عددا من المقتضيات التقنية التي ينبغي أن توفرها خدمات المحفوظات الموثوقة ومنها "التوافق الارتجاعي" مع الأجهزة والبرامجيات الحاسوبية إما من خلال المحافظة على المعدات و/ أو من خلال المضاهاة. (انظر Blanchette,) "... Defining electronic authenticity". ويمكن الاطلاع على دراسة متابعة بشأن توصية المبادرة (EESSI) المتعلقة بخدمات المحفوظات الموثوقة، التي أجراها المركز المتعدد التخصصات للقانون وتكنولوجيا المعلومات والاتصالات في جامعة لوفن الكاثوليكية للتكنولوجيا، بلجيكا، (Interdisciplinary Centre for Law and ICT of the Catholic University of Leuven Technology)، والمعنونة *European Electronic Signature Standardization Initiative: Trusted Archival Services* (المرحلة ٣، التقرير النهائي، ٢٨ آب/ أغسطس ٢٠٠٠) على الموقع الشبكي http://www.law.kuleuven.ac.be/ icri/publications/91TAS-Report.pdf?where=، (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨). وقد فُرغ من تنفيذ المبادرة في تشرين الأول/ أكتوبر ٢٠٠٤. ولا يبدو أن نظم تنفيذ هذه التوصيات تعمل حاليا (انظر Dumortier and Van den Eynde, Electronic Signatures and Trusted Archival Services...).

خدمات التصديق تخزين هذه المعلومات للرجوع إليها مستقبلا. كذلك يجب على مقدّمي خدمات التصديق اتخاذ التدابير اللازمة لضمان أن يكون الوصول إلى هذه المعلومات وفقا لقوانين حماية البيانات المعمول بها.[٦٣] غير أن الوصول إلى المعلومات من دون إذن لا يزال يمثل تهديدا حقيقيا.

٢- القياسات البيومترية

٥٣- يُستخدم القياس البيومتري لتحديد هوية فرد ما من خلال مميزاته البدنية أو السلوكية الجوهرية الخاصة به. وتشمل المميزات التي يمكن استعمالها في القياسات البيومترية للتعرّف على الشخصية ما يلي: الحمض الخلوي الصبغي (حمض د. ن. أ.)، وبصمات الأصابع، وقزحية العين، وشبكية العين، وشكل وخطوط اليد أو الوجه، والمخطط الحراري للوجه، وشكل الأذن، والصوت، ورائحة الجسم، ونمط الأوعية الدموية، وخط الكتابة باليد، وطريقة المشي، وأنماط الطباعة.

٥٤- ويشمل استخدام أدوات القياس البيومترية عادة أخذ عيّنة بيومترية لإحدى المميزات الحيوية (البيولوجية) الفردية للشخص. وتكون هذه العينة بالشكل الرقمي. ثُم تُستخرج البيانات البيومترية من تلك العينة لإنشاء قالب حاسوبي مرجعي. ثم تؤكّد هوية الشخص الذي تخصه العينة البيومترية ويتم التحقق من صحة الرسائل التي يزعم أنها صادرة عن ذلك الشخص، وذلك بمقارنة البيانات البيومترية التي تخصّه بالبيانات المخزّنة في القالب الحاسوبي المرجعي.[٦٤]

٥٥- وهناك عدد من المخاطر تتعلق بتخزين البيانات البيومترية، لأن الأنماط البيومترية غير قابلة للإلغاء عادة. وعندما يقع المساس بالنظم البيومترية بما يثير الشبهة، لا سبيل أمام المستعمل المشروع سوى إلغاء بيانات تحديد الهوية والانتقال إلى مجموعة أخرى من بيانات تحديد الهوية لم تُمس بما يثير الشبهة. ولذلك، ثمة حاجة إلى قواعد خاصة لمنع إساءة استعمال قواعد البيانات البيومترية.

٥٦- ولا يمكن أن تكون دقّة التقنيات البيومترية مطلقة، لأن السمات البيولوجية البارزة تميل في جوهرها إلى التغير، وقد ينطوي أي قياس على انحراف ما. وفي هذا الخصوص، لا تعتبر القياسات البيومترية محدِّدات فريدة بل شبه فريدة للهوية. ولاستيعاب تلك التغيرات، يمكن التأثير في دقة القياسات البيومترية من خلال وضع حد أدنى لتطابق القالب الحاسوبي المرجعي مع العينة المستخرَجة. غير أن وضع حد أدنى منخفض قد يميل باتجاه قبول زائف، بينما يميل تحديد حد أدنى مرتفع إلى حالات رفض زائف. ومع ذلك، قد تكون دقة التوثّق التي توفرها القياسات البيومترية كافية في أغلب التطبيقات التجارية.

---

[٦٣] انظر المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي (OECD) بشأن حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود (باريس، ١٩٨٠)، متاحة على الموقع الشبكي http://www.oecd.org/document./18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html، (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨)؛ واتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم ١٠٨)، متاحة على الموقع الشبكي http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (اطلع عليه في حزيران/ يونيه ٢٠٠٨)؛ ومبادئ الأمم المتحدة التوجيهية لتنظيم ملفات البيانات الشخصية المحوسبة (قرار الجمعية العامة ٤٥/ ٩٥)؛ والتوجيه الإداري الصادر عن البرلمان الأوروبي ومجلس أوروبا 95/46/EC المؤرخ ٢٤ تشرين الأول/ أكتوبر ١٩٩٥ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وبشأن حرّية حركة هذه البيانات (*Official Journal of the European Communities,* L 281, 23 November 1995)، وهو متاح على الموقع الشبكي http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett)، (اطلع عليه في حزيران/ يونيه ٢٠٠٨)).

[٦٤] الرابطة الدولية للقياسات البيومترية والرابطة الدولية لأمن الحواسيب، *قائمة مصطلحات القياسات البيومترية لعام ١٩٩٩*. (نسخة من هذه القائمة متاحة لدى الأمانة).

٥٧- إضافة إلى ذلك، فإن مسألتي حماية البيانات وحقوق الإنسان تبرزان فيما يتعلق بتخزين البيانات البيومترية والكشف عنها. وقد لا تشير قوانين حماية البيانات[٦٥] صراحة إلى القياسات البيومترية، ومع ذلك فهي تهدف إلى حماية البيانات الشخصية المتعلقة بالأشخاص الطبيعيين، والتي تُعتبر معالجتها في شكلها الخام وكقوالب حاسوبية مرجعية عمليةً في صميم تكنولوجيا القياسات البيومترية.[٦٦] علاوة على ذلك، قد تكون هناك حاجة إلى تدابير لحماية المستهلكين من المخاطر المتأتية عن الاستخدام الخصوصي لبيانات القياسات البيومترية، وكذلك في حالة سرقة الهوية. وقد يشمل ذلك مجالات قانونية أخرى، منها قانون العمل والصحة.[٦٧]

٥٨- وقد تساعد الحلول التقنية على العناية ببعض الشواغل. فتخزين البيانات البيومترية مثلا على بطاقات ذكية أو أمارات رمزية قد يمنع الوصول إلى هذه البيانات من دون إذن، وهي حالة قد تحدث إذا كانت البيانات مخزنة في نظام حاسوبي مركزي. وبالإضافة إلى ذلك، استحدثت مجموعة من أفضل الممارسات لتقليص المخاطر في مجالات مختلفة مثل: النطاق والقدرات؛ وحماية البيانات؛ وتحكُّم المستعمِل بالبيانات الشخصية، وإفشاء البيانات، وتدقيقها، والمساءلة بشأنها والإشراف عليها.[٦٨]

٥٩- وعموما، يُنظر إلى الأدوات البيومترية على أنها وسيلة توفر مستوى عاليا من الأمان. ومع أنها ملائمة لطائفة من الاستعمالات، فإن نطاقها الرئيسي الحالي يتعلق بالتطبيقات الحكومية، وخصوصا تطبيقات إنفاذ القانون، ومنها مثلا التطبيقات الخاصة بإجراءات الموافقة في دائرة الهجرة وتدابير مراقبة الدخول.

٦٠- كما استُحدثت تطبيقات تجارية حيثما كانت القياسات البيومترية تُستخدم كثيرا في سياق عملية توثيق تقوم على عاملين، فتستلزم توفير عنصر يكون ملازما للشخص الفرد (القياسات البيومترية) وعنصر يكون بعلم الشخص (عادة، كلمة سر أو رقم لتحديد الهوية الشخصية (PIN)). إضافة إلى ذلك، استُحدثت تطبيقات لتخزين ومقارنة خصائص التوقيع الخطي لشخص ما. إذ تسجّل لوحة بيانية إلكترونية رقمية ضغط القلم ومدة عملية التوقيع. ثم تُخزَّن البيانات على شكل خوارزمية تُستخدم لمقارنتها بالتوقيعات في المستقبل. ولكن، على ضوء السمات الفطرية التي تميز القياسات البيومترية، لا بد أيضا من التزام الحيطة إزاء أخطار الزيادة التدريجية وغير المراقبة فيما يتعلق باستخدامها في المعاملات التجارية المعتادة.

٦١- وقد تبرز مشكلة في الإثبات إذا استُخدمت توقيعات بيومترية كبديل عن التوقيعات الخطية. فكما ذُكر آنفا، تتغير قابلية التعويل على الأدلة الإثباتية المستمدة من القياسات البيومترية بحسب اختلاف التكنولوجيات المستخدمة ونسبة القبول الزائف المختارة. وبالإضافة إلى ذلك، من المحتمل أن يحصل تلاعب بالبيانات البيومترية المخزنة بالشكل الرقمي أو لتزييفها.

---

[٦٥] انظر الحاشية ٦٣.

[٦٦] Paul de Hert, *Biometrics: Legal Issues and Implications,* background paper for the Institute for Prospective Technological Studies of the European Commission (European Communities, Directorate General Joint Research Centre, (2005، ص١٣، الدراسة متاحة على الموقع الشبكي http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March 2005/LegalImplications_Paul_de_Hert.pdf (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

[٦٧] في كندا، على سبيل المثال، نوقش استعمال القياسات البيومترية فيما يتعلق بتطبيق قانون حماية المعلومات الشخصية والوثائق الإلكترونية (٢٠٠٠، c. 5) في أماكن العمل (Personal Information Protection and Electronic Documents Act in the workplace (Federal Court of Canada) (انظر Turner v. TELUS Communications Inc., 2005 FC 1601, 29 November 2005).

[٦٨] للحصول على مثال على أفضل الممارسات، انظر International Biometric Group BioPrivacy Initiative, "Best practices for privacy-sympathetic biometric deployment"، النص متاح على الموقع الشبكي: http://www.bioprivacy.org (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

٦٢- ويمكن تطبيق اختبارات قابلية التعويل العامة بمقتضى قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، والقانون النموذجي بشأن التجارة الإلكترونية، وكذلك بمقتضى اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية،[٦٩] وهي أحدث عهدا، بشأن استخدام التوقيعات البيومترية. وبغية ضمان التوحيد، قد يكون من المفيد أيضا وضع مبادئ توجيهية دولية بشأن استخدام طرائق القياس البيومتري وإدارتها.[٧٠] ويتعين النظر بعناية فيما إذا كان وضع معايير قياسية من هذا القبيل سابقا لأوانه، نظرا إلى الحالة الراهنة لتطور تكنولوجيات القياس البيومتري، وفيما إذا كان من المحتمل أن تؤدي إلى إعاقة التطور المتواصل في هذه التكنولوجيات.

٣- كلمات السر والطرائق الهجينة

٦٣- تُستخدم كلمات السر والرموز من أجل ضبط سبل الوصول إلى المعلومات أو الخدمات و"توقيع" الخطابات الإلكترونية. وفي الممارسة العملية يُلاحظ أن الاستخدام الثاني أقل شيوعا من الأول، بسبب احتمال المساس بالرمز عندما يرسل في رسائل غير مرمّزة. ومع ذلك، فإن كلمات السر والرموز هي طريقة "التوثيق" الأوسع استعمالا بغرض ضبط سبل الوصول إلى المعلومات والتحقق من الهوية في طائفة واسعة من المعاملات، بما في ذلك غالبية العمليات المصرفية عبر الإنترنت، والسحوبات النقدية من أجهزة الصرف الآلي والمعاملات الاستهلاكية التي تُجرى بواسطة بطاقات الائتمان.

٦٤- وينبغي التسليم بإمكانية استخدام تكنولوجيات متعددة "لتوثيق" معاملة إلكترونية. ويمكن الاستعانة بعدة تكنولوجيات أو بعدة استخدامات لتكنولوجيا واحدة لإجراء معاملة واحدة. فعلى سبيل المثال، يمكن الجمع بين ديناميات التوقيع بغرض التوثيق وتقنيات الترميز لضمان سلامة الرسالة. وبدلا من ذلك، يمكن إرسال كلمات السر عبر الإنترنت باستخدام تقنيات الترميز (أي طبقة المقابس الآمنة في المتصفِّح SSL) لحمايتها، وذلك اقترانا باستخدام القياسات البيومترية لإطلاق توقيع رقمي (يعتمد على نظم الترميز غير المتناظرة) ينتج عند استلامه ما يسمى ببطاقة كيربيروس في نافذة خاصة على الشاشة (نظم الترميز المتناظرة). ولدى وضع الأطر القانونية وأطر السياسة العامة للتعامل مع هذه التكنولوجيات، ينبغي إيلاء الاعتبار لدور التكنولوجيات المتعددة. ويتعين أن تكون الأطر القانونية وأطر السياسة العامة للتوثيق الإلكتروني مرنة بما يكفي لتغطية نهوج التكنولوجيا الهجينة، لأن الأطر التي تركز على تكنولوجيات محددة يمكن أن تعيق استخدام التكنولوجيات المتعددة.[٧١] ومن شأن الأحكام المحايدة إلكترونيا أن تسهل قبول النهوج الهجينة في التكنولوجيا.

---

[٦٩] اعتمدت الأونسيترال مشروع اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية في دورتها الثامنة والثلاثين (فيينا، ٤-١٥ تموز/ يوليه ٢٠٠٥) وأقرّتها الجمعية العامة رسميا بمقتضى قرارها ٦٠/ ٢١ المؤرّخ ٢٣ تشرين الثاني/ نوفمبر ٢٠٠٥.

[٧٠] يمكن مقارنتها بمعايير قابلية التعويل الواردة في دليل اشتراع قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية (قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية...، الجزء الثاني، الفقرة ٧٥).

[٧١] انظر مؤسسة أبحاث السياسات العامة بشأن المعلومات، تجميع الاستشارات بشأن تعليمات التوقيع، ٢٨ تشرين الأول/ أكتوبر ١٩٩٨، Foundation for Information Policy Research, *Signature Directive Consultation Compilation*، والتي توفر تجميعا للردود أثناء المشاورات حول مشروع التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية، الذي أُعدَّ بطلب من المفوضية الأوروبية، وهو متاح على الموقع الشبكي www.fipr.org/publications/sigdirecon.html (اطلع عليه في ٥ حَزيران/ يونيه ٢٠٠٨).

٤- التوقيعات المستنسخة بالمسح التصويري والأسماء المطبوعة

٦٥- يعود السبب الرئيسي لاهتمام المشرِّعين بالتجارة الإلكترونية في مجال القانون الخاص إلى القلق من أن التكنولوجيات الجديدة قد تؤثر في تطبيق قواعد القانون التي وُضِعت لوسائط أخرى. وغالبا ما أدى هذا الاهتمام بالتكنولوجيا، عمدا أو عن غير قصد، إلى التركيز على التكنولوجيات المتطورة التي تقدم مستوى أعلى من الأمان لطرائق التوثيق والتوقيع الإلكترونية. وغالبا ما يُهمَل، في هذا السياق، أن عددا كبيرا جدا من الخطابات التجارية، إن لم يكن أكثرها، التي يجري تبادلها عبر العالم لا تُستخدم فيها تكنولوجيا محددة للتوثيق أو التوقيع.

٦٦- وفي الممارسات اليومية، كثيرا ما تكون الشركات في أنحاء مختلفة من العالم مقتنعة بتبادل الرسائل بواسطة البريد الإلكتروني من دون استخدام أي شكل من أشكال التوثيق أو التوقيع غير الاسم المطبوع، مع اسم وعنوان الأطراف في أسفل الخطابات. وفي بعض الأحيان، يكون للخطاب طابع رسمي أكثر من خلال استخدام صور مأخوذة بطريقة التصوير البرقي أو مستنسخة بالمسح التصويري للتوقيعات الخطية، والتي لا تمثل بالطبع إلا نسخة بالشكل الرقمي للأصل الخطي. ولا تقدم الأسماء المطبوعة ولا التوقيعات المستنسخة بالمسح التصويري على رسائل البريد الإلكتروني غير المرمَّزَة مستوى عاليا من الأمان، ولا يمكنها على نحو مؤكد إثبات هوية منشئ الخطابات الإلكترونية التي تظهر فيها. ومع ذلك فإن الكيانات التجارية تختار بحرية استخدام هذه الأشكال من "التوثيق" بسبب سهولتها وملاءمتها في الخطابات وفعاليتها من حيث التكلفة. ومن المهم أن يضع المشرِّعون ومقرّرو السياسات العامة في اعتبارهم هذه الممارسات الواسعة الانتشار في الميدان التجاري لدى النظر في التنظيم الرقابي للتوثيق والتوقيع الإلكترونيين. ذلك أن فرض اشتراطات صارمة على التوثيق والتوقيع الإلكترونيين، وخصوصا فرض طريقة أو تكنولوجيا معينة، قد يلقي، دون قصد، بظلال من الشكوك على صحة وقابلية إنفاذ عدد كبير من المعاملات التي تُبرم يوميا من دون استخدام أي نوع معين من التوثيق أو التوقيع الإلكترونيين. وقد يشجع ذلك بدوره الأطراف التي تتصرف بسوء نية على التهرّب من تبعات الالتزامات التي قبلتها عن طيب خاطر، وذلك من خلال التشكيك في قابلية التعويل على خطاباتها الإلكترونية. وليس من الواقعي أن يتوقع المرء أن يؤدي فرض مقتضيات ذات مستوى عال بدرجة ما على التوقيع والتصديق الإلكترونيين إلى قيام جميع الأطراف في نهاية المطاف باستخدامها يوميا وبصورة فعلية. وقد بينت التجربة الحديثة فيما يتعلق بالطرائق المتطورة، كالتوقيعات الرقمية، أن الشواغل بشأن التكلفة ومدى التعقّد كثيرا ما تحدُّ من الاستخدام العملي لتقنيات التوثيق والتوقيع.

جيم- إدارة شؤون الهوية الإلكترونية

٦٧- في العالم الإلكتروني، يستطيع الأشخاص الطبيعيون والاعتباريون الوصول إلى خدمات عدد من مقدّمي الخدمات. وكلما سَجَّل شخص ما نفسه لدى مقدّم خدمات للحصول على هذه الخدمات أُنشئت "هوية" إلكترونية له. إضافة إلى ذلك، يمكن ربط هوية واحدة بعدد من الحسابات الخاصة بالخدمات الإلكترونية لكل تطبيق أو منصّة حاسوبية. ومن شأن تعدد الهويات والحسابات الخاصة بها أن يعيق إدارتها على كل من المستعمِل ومقدّم الخدمات على حد سواء. ويمكن اجتناب هذه الصعوبات من خلال هوية إلكترونية واحدة لكل شخص.

٦٨- ويقتضي التسجيل لدى مقدّم الخدمات وإنشاء هوية إلكترونية إقامة علاقة ثقة متبادلة بين الشخص ومقدّم الخدمات. ويتطلب إنشاء هوية إلكترونية واحدة تجميع تلك العلاقات الثنائية في إطار أوسع يمكن من خلاله إدارتها على نحو مشترك، وهو ما يشار إليه بإدارة شؤون الهوية. وقد تشمل المنافع التي يجنيها مقدّم الخدمات من هذه الإدارة تحسين تدابير الأمان، وتسهيل الامتثال للوائح التنظيم الرقابي وزيادة سرعة التنفيذ؛ أما المنافع التي يجنيها المستعمل فقد تشمل تيسير سبل الوصول إلى المعلومات.

٦٩- ويمكن وصف إدارة شؤون الهوية في سياق نهجين اثنين هما:

(أ) *النهج التقليدي القائم على دخول المستعمل*. وهذا النهج يعتمد على أنموذج تسجيل الدخول، وهو يقوم عادة على استعمال المعلومات التي تتضمنها أداة تسمى بطاقة ذكية أو أداة أخرى يملكها الزبون ويستخدمها لتسجيل وصوله إلى خدمة ما. ويركز نهج دخول المستعمل المتَّبع في إدارة شؤون الهوية على إدارة التوثّق من المستعمل، وحقوق الدخول، وقيود الدخول، ومواصفات الحساب، وكلمات السر وغير ذلك من الخصائص، في واحد أو أكثر من التطبيقات أو النظم. وهو يهدف إلى تسهيل ومراقبة الوصول إلى التطبيقات والموارد، كما يهدف في الوقت نفسه إلى حماية المعلومات الشخصية والتجارية السرية من المستعملين غير المأذون لهم؛

(ب) *النهج القائم على الخدمات*. ويمثل هذا النهج أنموذجا أكثر ابتكارية، وهو يقوم على نظام يقدم خدمات شخصية إلى المستعملين وأدواتهم. وفي إطار هذا النهج، يصبح نطاق إدارة شؤون الهوية أوسع ليشمل جميع موارد الشركة المستخدَمة لتقديم خدمات على خط الحاسوب، منها معدات الشبكات والخوادم والبوّابات والمحتويات والتطبيقات والمنتجات، علاوة على وثائق الاعتماد الخاصة بالمستعمل، ودفاتر العناوين، والأفضليات والاستحقاقات. ومن الناحية العملية، يمكن أن يشمل هذا النطاق مثلا المعلومات المتعلقة بوسائل رقابة الآباء على المواقع، والمشاركة في برامج الزبائن الأوفياء.

٧٠- وثمة جهود مبذولة على المستويين التجاري والحكومي لتوسيع إدارة شؤون الهوية. غير أنه تجدر الإشارة إلى أن الخيارات في السياسة العامة قد تختلف اختلافا كبيرا بين مشهدي هذين المستويين. فالنهج الحكومي قد يكون موجها بقدر أكبر نحو تلبية احتياجات المواطنين على نحو أفضل، وبالتالي فقد يتم تصميمه بحيث يضمن التفاعل مع الأشخاص الطبيعيين. ومن ناحية أخرى، لا بد من أن تأخذ التطبيقات التجارية في الاعتبار تزايد استخدام الآلات المؤتمتة في المعاملات التجارية، وبالتالي فقد تعتمد خصائص ترمي إلى تلبية الاحتياجات المحددة لتلك الآلات.

٧١- وأما الصعوبات التي تتعلق بنظم إدارة شؤون الهوية فتشمل شواغل الخصوصية (الحرمة) الشخصية بسبب المخاطر المرتبطة بسوء استخدام العلامات الفريدة للتعرف على الهوية. إضافة إلى ذلك، قد تنشأ أيضا مسائل تتعلق بالفوارق بين الأنظمة القانونية السارية، وبخاصة ما يتعلق بإمكانية الحصول على تفويض سلطة للتصرّف بالنيابة عن شخص آخر. وقد اقتُرحت حلول تستند إلى تعاون تجاري طوعي يقوم على ما يسمى بدائرة الثقة، حيث يُطلب إلى المشاركين التعويل على صحة ودقة المعلومات التي يقدمها إليهم أعضاء آخرون من الدائرة. غير أن هذا النهج قد لا يكون كافيا تماما لتنظيم جميع المسائل ذات الصلة، وقد

يبقى بحاجة إلى اعتماد إطار قانوني لـه. كما وُضِعَت مبادئ توجيهية لتوفير إطار قانوني لحلقات البنى التحتية الموثوقة.[٧٢]

٧٢- أما فيما يتعلق بقابلية التشغيل البيني من الناحية التقنية، فقد أنشأ الاتحاد الدولي للاتصالات فريقا مختصا معنيا بإدارة شؤون الهوية لتسهيل ومواصلة تطوير إطار عام لإدارة شؤون الهوية ووسائل اكتشاف الهويات المستقلة الموزعة ومجموعات الهويات وسبل التنفيذ.[٧٣]

٧٣- ويجري أيضا استحداث حلول لإدارة شؤون الهوية في سياق بيئة الحكومة الإلكترونية. فعلى سبيل المثال، بدأ في سياق مبادرة "الاتحاد الأوروبي لعام ٢٠١٠ لمجتمع معلومات أوروبي من أجل النمو والعمالة"،[٧٤] الاضطلاع بدراسة بشأن إدارة شؤون الهوية في بيئة الحكومة الإلكترونية لتسهيل التقدم نحو نهج متسق في إدارة شؤون الهوية الإلكترونية في بيئة الحكومة الإلكترونية في الاتحاد الأوروبي، بالاستناد إلى الخبرات والمبادرات المتوافرة في دول الاتحاد الأوروبي.[٧٥]

٧٤- وقد أخذ يتسع توزيع أدوات التوقيعات الإلكترونية، وغالبا على شكل بطاقات ذكية، في سياق المبادرات المعنية ببيئة الحكومة الإلكترونية. وبدأت عملية توزيع البطاقات الذكية على النطاق الوطني. ففي بلجيكا، مثلا، بدأ العمل بهذه البطاقات في عدد من المقاطعات في عام ٢٠٠٣،[٧٦] ثم أصبح يُعمل بها في البلد بكامله في نهاية المطاف، بعد نجـاح الفترة التجريبية.[٧٧] ويتمثل النظام البلجيكي أساسا في إصدار بطاقات هوية ملموسة مجهزة برقاقة إلكترونية تتضـمن البيانات التي يحتاج إليها المواطن من أجل إنشاء توقيع رقمي.[٧٨]

---

[٧٢] مشروع تحالف الحرية (The Liberty Alliance Project) (انظر www.projectliberty.org) هو تحالف يضم أكثر من ١٥٠ من الشركات والمنظمات غير الربحية والمنظمات الحكومية من مختلف أنحاء العالم. ويلتزم الاتحاد بوضع معيار مفتوح لهوية شبكية في إطار نظام حكومي موحد يكون مناسبا لجميع الأدوات الشبكية الموجودة حاليا والتي ستظهر قريبا. وتقدم هذه الهوية للشركات والحكومات والمستخدمين والزبائن وسيلة أكثر ملاءمة وأكثر أمانا لضبط المعلومات الخاصة بالهوية في الاقتصاد الرقمي القائم حاليا، وهي مكوِّن رئيسي في تطوير استخدام التجارة الإلكترونية وخدمات البيانات الشخصية الطابع، وكذلك الخدمات الشبكية. والعضوية في التحالف مفتوحة لجميع المؤسسات التجارية وغير التجارية.

[٧٣] انظر http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html (اطلع عليه في ٢٠ آذار/ مارس ٢٠٠٨).

[٧٤] رسالة من مفوضية الجماعات الأوروبية إلى مجلس أوروبا والبرلمان الأوروبي واللجنة الاقتصادية والاجتماعية الأوروبية ولجنة المناطق: "٢٠١٠- مجتمع معلومات أوروبي من أجل النمو والعمالة" COM (2005) 229 final (Brussels, 1 June 2005) متاح على الموقع الشبكي http://eur-lex.europa.eu (accessed on 20 March 2008) (اطلع عليه في ٢٠ آذار/ مارس ٢٠٠٨).

[٧٥] انظـر European) *Modinis Study on Identity Management in eGovernment: Identity Management Issue Report* Commission, Directorate General Information Society and Media, 18 September 2006), pp. 9-12، التقرير متاح على الموقع الشبكي https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[٧٦] اعتمدت بلجـيكا بطاقة الهوية الإلكترونية في عام ٢٠٠٣ بمقتـضى القانون المؤرّخ ٢٥ آذار/ مارس ٢٠٠٣ المعدل لقانون ٨ آب/ أغسطس ١٩٨٣ الذي ينظم السجل الوطني للأشخاص الطبيعيين ولقـانون ١٩ تمـوز/ يوليه ١٩٩١ المتعـلق بسجلات السكان وبطاقات الهوية، والمعـدل لقانون آب/ أغسطس ١٩٨٣ الذي ينظم السجل الوطني للأشخاص الطبيعيين (Moniteur belge, Ed. 4, 28 March 2003, p. 15921).

[٧٧] انظر المرسوم الملكي المؤرّخ ١ أيلول/ سبتـمبر ٢٠٠٤ الذي ينص على قرار تعميم العمل ببطاقة الهوية الإلكترونية (Moniteur belge, Ed. 2, 15 September 2004, p. 56527). وللاطلاع على معلومات عامة، انظر http://eid.belgium.be (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[٧٨] للاطلاع على معلومات عامة، انظر http://eid.belgium.be (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

٧٥- واستحدثت النمسا نظاما لإدارة شؤون الهوية، وهو نظام يدوّن أوصاف الهوية بشأن كل مواطن نمساوي، لكنه لا يُدرج تلك الأوصاف في وثائق هوية المواطنين الرسمية. وبدلا من ذلك، اختارت النمسا معايير محايدة تكنولوجيا، ونتيجة لذلك وُضعت مجموعة من الحلول التكنولوجية واعتمدها المستهلكون. ويقوم النظام النمساوي على "رابط هوية الشخص"، وهو عبارة عن بنية موقَّع عليها من قِبل سلطة عمومية تُسند سمة فريدة لتحديد هوية الشخص (رقم تسجيل مثلا) إلى شهادة أو أكثر من شهادات ذلك الشخص. وهكذا، يمكن استخدام رابط هوية الشخص من أجل تحديد هوية الشخص الفريدة بشكل مؤتمت عندما يتصل ذلك الشخص بالسلطة العمومية أثناء سير إجراء ما.[٧٩] ويمكن خزن "سمة الهوية الفريدة" هذه في أي بطاقة ذكية من اختيار الشخص (كأن تكون مثلا بطاقة لسحب الأموال من موزع آلي أو بطاقة ضمان اجتماعي أو بطاقة هوية الطالب أو بطاقة عضوية في نقابة عمال أو رابطة مهنية أو حاسوبا شخصيا). ويمكن أيضا إرسال أدوات التوقيع عبر الهاتف الجوال، في شكل رموز تستعمل مرة واحدة وينشئها مقدم خدمات الهاتف الجوال، حيث يقوم مقدم هذه الخدمات بدور حارس سمة الهوية الخاصة بالشخص.

٧٦- وهذا النظام يسمح بإصدار محددات للهوية خاصة بقطاع معين ويُحتفظ بها منفصلة عن بعضها البعض ولكن مرتبطة كلها بمخزن مركزي للهويات. فهذه البنية الهندسية تحول دون التشارك في البيانات وتحمي خصوصية البيانات. ويُقصد من البطاقة التي تُعرف باسم "بطاقة المواطن" أن تصبح وثيقة الهوية الرسمية للإجراءات الإدارية الإلكترونية، ومن هذه الإجراءات إيداع تطبيقات عبر الإنترنت. فبطاقة المواطن تنشئ بنية تحتية أمنية متاحة للجميع، بمن فيهم الزبائن التجاريون. ويمكن للشركات أن تستحدث لزبائنها خدمات آمنة على خط الحاسوب بالاعتماد على البنية التحتية التي توفرها بطاقة المواطن.

٧٧- ونتيجة لمبادرات من قبيل المبادرات الموصوفة أعلاه، يمكن أن يتلقى عدد كبير جدا من المواطنين أدوات قليلة التكلفة تتضمن فيما تتضمن قدرات على التوقيع الإلكتروني الآمن. ومع أن الهدف الرئيسي لهذا النوع من المبادرات قد لا يكون تجاريا، فإن هذه الأدوات يمكن استخدامها في الميدان التجاري أيضا. فقد أصبح هناك اعتراف متزايد بتلاقي كلا مجالي التطبيقات.[٨٠]

---

[٧٩] Zentrum für sichere Informationstechnologie Austria (A-Sit), *XML Definition of the Person Identity Link* (متاح على الموقع الشبكي http://www.buergerkarte.at/konzept/personenbindung/spezifikation/aktuell/ (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨)).

[٨٠] انظر، على سبيل المثال Korea Internet White Paper (Seoul, National Internet Development Agency of Korea, 2006)، صفحة ٨١، فيما يتعلق بالاستعمال المزدوج لقانون التوقيع الإلكتروني في جمهورية كوريا في تطبيقات الحكومة الإلكترونية والتجارة الإلكترونية (متاح على الموقع الشبكي http://www.ecommerce.or.kr/activities/documents_view.asp?bNo=642&Page=1 ، وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

ثانيا- المعاملة القانونية للتوثيق الإلكتروني والتوقيعات الإلكترونية

٧٨- إن لبناء الثقة بالتجارة الإلكترونية أهمية كبيرة في تطوير هذه التجارة. وقد تكون هناك حاجة أيضا إلى قواعد خاصة لتعزيز اليقين والأمان في استخدامها. وقد تُقدَّم هذه القواعد في طائفة من النصوص التشريعية: الصكوك القانونية الدولية (المعاهدات والاتفاقيات)؛ أو القوانين النموذجية عبر الوطنية؛ أو التشريعات الوطنية (التي كثيرا ما تستند إلى القوانين النموذجية)؛ أو الصكوك المحمية بالتنظيم الرقابي الذاتي؛[٨١] أو الاتفاقات التعاقدية.[٨٢]

٧٩- ويجري إنجاز عدد كبير من معاملات التجارة الإلكترونية داخل شبكات مغلقة، أي داخل مجموعات تتكون من عدد محدود من المشاركين، وهي مجموعات لا يُسمح بالدخول إليها إلا للأشخاص أو الشركات من المأذون لهم مسبقا بذلك. وتدعم الشبكات المغلقة عمل كيان منفرد أو عمل مجموعة موجودة ومغلقة من المستعملين، كالمؤسسات المالية المشاركة في نظام المدفوعات المشترك بين المصارف، أو بورصات السندات المالية والسلع الأساسية، أو رابطة شركات الطيران ووكلاء السفر. وفي هذه الحالات، عادة ما تكون المشاركة في الشبكة محصورة في المؤسسات والشركات التي سبق أن قُبلت في المجموعة. وقد أنشئت غالبية هذه الشبكات قبل عدة عقود زمنية، وهي تستخدم تكنولوجيا متطورةَ واكتسبت مستوى عاليا من الخبرة في عمل هذا النظام. وقد أدّت سرعة نمو التجارة الإلكترونية في العقد الماضي إلى تطوير نماذج شبكية أخرى، مثل سلاسل العرض أو المنصّات الحاسوبية التجارية.

٨٠- ومع أن هذه المجموعات الجديدة قد نُظّمت أصلا في بنية تتمحور حول التوصيلات المباشرة من حاسوب إلى آخر، كما كان الحال فيما يتعلق بمعظم الشبكات المغلقة التي كانت موجودة في ذلك الوقت، ثمة اتجاه متزايد نحو استخدام الوسائل التي يمكن للعموم الوصول إليها، كالإنترنت، بوصفها وسيلة توصيل مشتركة. وحتى ضمن هذه النماذج الحديثة، لا تزال الشبكة المغلقة تحتفظ بسمات تقتصر عليها دون غيرها. وفي الأحوال النمطية، تعمل الشبكات المغلقة بموجب معايير تعاقدية متفق عليها مسبقا، وبموجب اتفاقات وإجراءات وقواعد تُعرَف بتسميات مختلفة، ومنها "قواعد النظام" أو "قواعد التشغيل" أو "اتفاقات الشركاء

---

[٨١] انظر، على سبيل المثال، اللجنة الاقتصادية لأوروبا، مركز الأمم المتحدة لتيسير التجارة وللمعاملات التجارية الإلكترونية، التوصية رقم ٣٢ المعنونة "صكوك التنظيم الرقابي الذاتي في مجال التجارة الإلكترونية (مدونات قواعد السلوك)" (ECE/TRADE/277)، وهي متاحة في الموقع الشبكي http://www.unece.org/cefact/recommendations/rec_index.htm (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

[٨٢] تهدف مبادرات كثيرة على المستويين الوطني والدولي إلى وضع عقود نموذجية. انظر، مثلا، اللجنة الاقتصادية لأوروبا، الفرقة العاملة المعنية بتيسير إجراءات التجارة الدولية، التوصية ٢٦، المعنونة "الاستخدام التجاري لاتفاقات التبادل في التبادل الإلكتروني للبيانات" (TRADE/WP.4/R.1133/Rev.1)؛ والتوصية الصادرة عن مركز الأمم المتحدة لتيسير التجارة والمعاملات التجارية الإلكترونية، المعنونة "اتفاق التجارة الإلكترونية" (ECE/TRADE/257)، وكلتاهما متاحتان في الموقع الشبكي http://www.unece.org/cefact/recommendations/rec_index.htm (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

التجاريين"، وهي مصمَّمة لتوفير وضمان ما يلزم من خاصية وظيفية تشغيلية، وقابلية تعويل وأمن لأعضاء المجموعة. وكثيرا ما تتناول هذه القواعد والاتفاقات مسائل من قبيل الاعتراف بالقيمة القانونية للخطابات الإلكترونية، ووقت ومكان إرسال رسائل البيانات وتلقيها، وإجراءات الأمن للوصول إلى الشبكة، وطرائق التوثيق أو التوقيع التي ينبغي للأطراف استخدامها.[٨٣] وفي حدود الحرية التعاقدية بمقتضى القانون الواجب تطبيقه، عادة ما تكون هذه القواعد والاتفاقات ذاتية الإنفاذ.

٨١- ولكن، في غياب القواعد التعاقدية، وفي إطار القيود التي قد يحدّ بها القانون الواجب تطبيقه من قابلية إنفاذها، فإن القيمة القانونية لطرائق التوثيق والتوقيع الإلكترونية التي تستخدمها الأطراف تحددها القواعد القانونية الواجب تطبيقها على شكل قواعد احتياطية أو إلزامية. ويناقش هذا الفصل مختلف الخيارات المستخدمة في مختلف الولايات القضائية لوضع إطار قانوني للتوقيعات الإلكترونية والتوثيق الإلكتروني.

ألف- النهج الخاص بالتكنولوجيا في النصوص التشريعية

٨٢- اتخذت التشريعات واللوائح التنظيمية الخاصة بالتوثيق الإلكتروني أشكالا عديدة مختلفة على المستويين الدولي والداخلي. ويمكن تحديد ثلاثة نهوج رئيسية للتعامل مع تكنولوجيات التوقيع والتوثيق: *(أ)* نهج الحد الأدنى؛ و*(ب)* نهج التكنولوجيا المحدّدة؛ و*(ج)* نهج المستويين أو الشقين.[٨٤]

١- نهج الحد الأدنى

٨٣- تعترف بعض الولايات القضائية بجميع التكنولوجيات التي تستخدم في التوقيع الإلكتروني، تبعا لسياسة عامة بشأن الحياد التكنولوجي.[٨٥] ويسمّى هذا النهج أيضا بنهج الحد الأدنى لأنه يعطي وضعا قانونيا بالحد الأدنى لجميع أشكال التوقيع الإلكتروني. وبمقتضى نهج الحد الأدنى تُعتبر التوقيعات الإلكترونية النظير الوظيفي للتوقيعات الخطية، شريطة أن تهدف التكنولوجيا المستخدمة إلى خدمة وظائف محددة، وأن تلبي كذلك بعض متطلبات قابلية التعويل ذات الحياد إزاء التكنولوجيا.

٨٤- ويقدّم قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مجموعة المعايير التشريعية الأوسع انتشارا لإرساء نظير وظيفي عام بين التوقيعات الإلكترونية والخطية. فالفقرة ١ من المادة ٧ من القانون النموذجي تنص على ما يلي:

---

[٨٣] للاطلاع على مناقشة المسائل التي تشتمل عليها عادة اتفاقات الشركاء التجاريين، انظر Amelia H. Boss, "Electronic data interchange agreements: private contracting toward a global environment" *Northwestern Journal of International Law and Business*، المجلد ١٣، العدد ١ (١٩٩٢)، الصفحة ٤٥.

[٨٤] Susanna F. Fischer "Saving Rosencrantz and Guildenstern in a virtual world? A comparative look at recent global electronic signature legislation," *Journal of Science and Technology Law*, vol. 7, No. 2 (2001), pp. 234 ff.

[٨٥] على سبيل المثال، أستراليا ونيوزيلندا.

"(١) عندما يشترط القانون وجود توقيع من شخص، يُستوفى ذلك الشرط بالنسبة إلى رسالة البيانات إذا:

"*(أ)* استُخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات؛ و

"*(ب)* كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أُنشئت أو أُبلغت من أجله رسالة البيانات، في ضوء كل الظروف، بما في ذلك أي اتفاق متصل بالأمر."

٨٥- ويتوخّى هذا الحكم الوظيفتين الرئيسيتين للتوقيعات الخطية وهما: تعيين هوية الموقِّع، وتبيان نيّته فيما يخص المعلومات الموقَّع عليها. ووفقا للقانون النموذجي بشأن التجارة الإلكترونية، ينبغي النظر إلى أي تكنولوجيا يمكنها توفير هاتين الوظيفتين بالشكل الإلكتروني على أنها تلبي شرطا من الشروط القانونية للتوقيع الإلكتروني. ولذلك، فإن القانون النموذجي محايد تكنولوجيا؛ أي إنه لا يتوقف على استخدام نوع معيّن من التكنولوجيا أو لا يفترض مسبقا استخدام هذا النوع، ويمكن تطبيقه على إرسال وتخزين جميع أنواع المعلومات. ويتسم الحياد التكنولوجي بأهمية خاصة نظرا إلى سرعة الابتكار التكنولوجي، وهو يساعد على ضمان بقاء التشريع قادرا على استيعاب التطورات المستقبلية وألا يتقادم عهده بسرعة كبيرة. وبالتالي، فإن القانون النموذجي يتجنّب أي إشارة إلى طرائق تقنية معينة لإرسال المعلومات أو تخزينها.

٨٦- وقد أُدرج هذا المبدأ العام في قوانين الكثير من البلدان. ذلك أن مبدأ الحياد التكنولوجي يتيح المجال أيضا لاستيعَاب التطورات التكنولوجية المستقبلية. إضافة إلى ذلك، يبرز هذا النهج حرية الأطراف في اختيار التكنولوجيا المناسبة لاحتياجاتها. وبالتالي، فإن الأمر يتوقف على قدرة الأطراف على تحديد مستوى الأمن الكافي لاتصالاتها. وقد يؤدي ذلك إلى تجنب التعقد المفرط من الناحية التكنولوجية وما يرتبط به من تكاليف.[٨٦]

٨٧- وباستثناء أوروبا حيث تأثرت التشريعات أساسا بالتوجيهات الإدارية الصادرة عن الاتحاد الأوروبي،[٨٧] فإن معظم البلدان التي وضعت تشريعات في مجال التجارة الإلكترونية استخدمت القانون

[٨٦] S. Mason,"Electronic signatures in practice" Journal of High Technology Law, vol. VI, No. 2 (2006), p. 153.

[٨٧] خاصة التوجيه الإداري الصادر عن البرلمان الأوروبي ومجلس أوروبا 1999/93/EC بشأن إطار مجتمعي للتوقيعات الإلكترونية (*الجريدة الرسمية للجماعات الأوروبية*، العدد L.13، ١٩ كانون الثاني/ يناير ٢٠٠٠). ويلي التوجيه بشأن التوقيعات الإلكترونية توجيه آخر أعمّ، وهو التوجيه الإداري 2000/31/EC الصادر عن البرلمان الأوروبي ومجلس أوروبا في ٨ حزيران/ يونيه ٢٠٠٠ بشأن بعض الجوانب القانونية لخدمات مجتمع المعلومات، وخصوصا التجارة الإلكترونية، في السوق الداخلية (*الجريدة الرسمية للجماعات الأوروبية*، العدد L.178، ١٧ تموز/ يوليه ٢٠٠٠)، المتعلق بمختلف جوانب توفير خدمات تكنولوجيا المعلومات وبعض مسائل التعاقد الإلكتروني.

النموذجي بشأن التجارة الإلكترونية كنموذج لها.[٨٨] كما اتُخِذ القانون النموذجي أساسا لمواءمة التشريعات الداخلية الخاصة بالتجارة الإلكترونية في البلدان المنظَّمة على أساس اتحادي (فيدرالي)، مثل كندا[٨٩] والولايات المتحدة الأمريكية.[٩٠] وقد حافظت البلدان التي اشترعت القانون النموذجي، باستثناء عدد قليل جدا منها،[٩١] على نهج الحياد التكنولوجي، ولم تنص في قانونها على استخدام تكنولوجيا معينة ولم تبد أي تفضيل لتكنولوجيا معيّنة. ويتبع قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، (الذي اعتمد

[٨٨] حتى كانون الثاني/ يناير ٢٠٠٧، كانت البلدان التالية على الأقل قد اعتمدت تشريعات تنفذ أحكام قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية: الأردن، قانون المعاملات الإلكترونية، ٢٠٠١؛ أستراليا، قانون المعاملات الإلكترونية، ١٩٩٩؛ إكوادور، قانون التجارة الإلكترونية والتوقيعات الإلكترونية ورسائل البيانات (٢٠٠٢)؛ إيرلندا، قانون التجارة الإلكترونية، ٢٠٠٠؛ باكستان، قانون المعاملات الإلكترونية، ٢٠٠٢؛ بنما، قانون التوقيعات الرقمية (٢٠٠١)؛ تايلند، قانون المعاملات الإلكترونية (٢٠٠١)؛ الجمهورية الدومينيكية، القانون المتعلق بالتجارة الإلكترونية والمستندات والتوقيعات الرقمية (٢٠٠٢)؛ جنوب أفريقيا، قانون الاتصالات والمعاملات الإلكترونية (٢٠٠٢)؛ سري لانكا، قانون المعاملات الإلكترونية (٢٠٠٦)؛ سلوفينيا، قانون التجارة الإلكترونية والتوقيع الإلكتروني (٢٠٠٠)؛ سنغافورة، قانون المعاملات الإلكترونية (١٩٩٨)؛ جمهورية كوريا، القانون الإطاري للتجارة الإلكترونية (٢٠٠١)؛ الصين، قانون التوقيعات الإلكترونية الذي صدر عام ٢٠٠٤؛ فرنسا، القانون ٢٠٠٠-٢٣٠ بشأن تكييف قانون الإثبات مع تكنولوجيات المعلومات والمتعلق بالتوقيع الإلكتروني (٢٠٠٠)؛ الفلبين، قانون التجارة الإلكترونية (٢٠٠٠)؛ فنزويلا (جمهورية - البوليفارية)، القانون المتعلق برسائل البيانات والتوقيعات الإلكترونية (٢٠٠١)؛ فييت نام، قانون المعاملات الإلكترونية (٢٠٠٦)؛ كولومبيا، قانون التجارة الإلكترونية؛ المكسيك، مرسوم إصلاح وتجميع مختلف أحكام القانون المدني فيما يتعلق بالشؤون الفيدرالية للعاصمة الفيدرالية، وأحكام القانون الفيدرالي للإجراءات المدنية، وقانون التجارة والقانون الفيدرالي لحماية المستهلك (٢٠٠٠)؛ موريشيوس، قانون المعاملات الإلكترونية لعام ٢٠٠٠؛ نيوزيلندا، قانون المعاملات الإلكترونية لعام ٢٠٠٢؛ الهند، قانون تكنولوجيا المعلومات، ٢٠٠٠. كما اعتُمد القانون النموذجي في أقاليم تابعة لتاج المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية، هي بايليويك أوف غيرنسي (قانون (غيرنسي) للمعاملات الإلكترونية لعام ٢٠٠٠)، وبايليويك أوف جيرسي (قانون (جيرسي) للخطابات الإلكترونية لعام ٢٠٠٠) وجزيرة مان (قانون المعاملات الإلكترونية لعام ٢٠٠٠)؛ وفي ثلاثة من أقاليم ما وراء البحار التابعة للمملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية، هي برمودا (قانون المعاملات الإلكترونية لعام ١٩٩٩)، وجزر كايمان (قانون المعاملات الإلكترونية لعام ٢٠٠٠) وجزر تركس وكايكوس (قانون المعاملات الإلكترونية لعام ٢٠٠٠)؛ وفي منطقة هونغ كونغ الإدارية الخاصة التابعة للصين (قانون المعاملات الإلكترونية (٢٠٠٠)). وتحيل المراجع المذكورة أدناه بخصوص الأحكام التشريعية لأي من هذه البلدان إلى الأحكام الواردة في القوانين المذكورة أعلاه، ما لم يُذكر خلاف ذلك.

[٨٩] تجسّد اشتراع القانون النموذجي داخليا في كندا في قانون التجارة الإلكترونية الموحّد، الذي اعتمده في عام ١٩٩٩ مؤتمر القانون الموحد لكندا (متاح مع تعليق رسمي في الموقع الشبكي http://www.chlc.ca/en/poam2/index.cfm?sec=1999&sub=1999ia، وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨). ومنذ ذلك الحين، اشتُرع القانون في عدد من المقاطعات والأقاليم الكندية منها ألبرتا، وأونتاريو، وجزيرة الأمير إدوارد، وساسكاتشوان، وكولومبيا البريطانية ولابرادور، ومانيتوبا، ونوفا سكوشيا، ونيو برانزويك، ونيوفاوندلاند، ويوكون. واشترعت مقاطعة كيبيك تشريعا خاصا (قانون إنشاء إطار قانوني لتكنولوجيا المعلومات (٢٠٠١))، ومع أنه أوسع نطاقا ومختلف جدا من حيث الصياغة، فهو يحقق الكثير من أهداف القانون الموحد للتجارة الإلكترونية ومتسق عموما مع قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية. ويمكن الحصول على معلومات حديثة العهد عن اشتراع القانون الموحّد للتجارة الإلكترونية من الموقع الشبكي http://www.ulcc.ca (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

[٩٠] في الولايات المتحدة الأمريكية، استخدم المؤتمر الوطني للمفوضين المعنيين بتوحيد قوانين الولايات قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية كأساس لإعداد قانون الولايات المتحدة الأمريكية الموحّد بشأن المعاملات الإلكترونية، الذي اعتمده المؤتمر عام ١٩٩٩ (ويمكن الاطلاع على نص القانون والتعليق الرسمي على الموقع الشبكي http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm، وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨). ومنذ ذلك الحين، تم اشتراع القانون الموحد بشأن المعاملات الإلكترونية في مقاطعة كولومبيا وفي الولايات الست والأربعين التالية: أركانساس، أريزونا، ألاباما، ألاسكا، إنديانا، يوتا، أوريغون، أوكلاهوما، أوهايو، أيداهو، بنسيلفانيا، تكساس، تينيسي، رود آيلاند، داكوتا الشمالية، داكوتا الجنوبية، ديلاوير، فرمونت، فيرجينيا الغربية، فلوريدا، كارولاينا الجنوبية، كارولاينا الشمالية، كاليفورنيا، كانساس، كوناتيكات، كنتاكي، كولورادو، آيووا، لويزيانا، ماريلاند، مَين، ماساشوستس، مشيغان، ميسيسبي، مينيسوتا، نبراسكا، نيفادا، نيوجيرزي، نيومكسيكو، نيوهامبشاير، هاواي، وايومنغ، ويسكنسن. ومن المرجح أن تعتمد ولايات أخرى تشريعات تنفيذ في المستقبل القريب، منها ولاية إلينوي التي اشترعت قانون الأونسيترال النموذجي من خلال قانون أمن التجارة الإلكترونية. ويمكن الحصول على معلومات حديثة العهد عن اشتراع قانون الولايات المتحدة الأمريكية الموحد بشأن المعاملات الإلكترونية من الموقع الشبكي http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp، (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[٩١] إكوادور، بنما، الجمهورية الدومينيكية، جنوب أفريقيا، كولومبيا، موريشيوس، الهند.

في عام ٢٠٠١)، واتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية وهي أحدث عهدا منه (التي اعتمدتها الجمعية العامة بمقتضى قرارها ٦٠/ ٢١ المؤرّخ ٢٣ تشرين الثاني/ نوفمبر ٢٠٠٥، وفُتح باب التوقيع عليها في ١٦ كانون الثاني/ يناير ٢٠٠٦) النهج نفسه، مع أن قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية يحتوي على بعض النصوص الإضافية (انظر الفقرة ٩٥ أدناه).

٨٨- وعندما تعتمد التشريعات نهج الحد الأدنى، فإن مسألة إثبات التكافؤ بين التوقيعات الإلكترونية تقع عادة على عاتق قاض أو محكَّم أو سلطة عمومية، للبتّ فيها عموما، من خلال ما يسمى "الاختبار المناسب لقابلية التعويل". وبموجب هذا الاختبار، تعتبر جميع أنواع التوقيع الإلكتروني التي تستوفي معايير الاختبار صحيحة؛ ومن ثم يجسّد الاختبار مبدأ الحياد التكنولوجي.

٨٩- ويجوز وضع طائفة واسعة من العوامل القانونية والتقنية والتجارية في الاعتبار لدى البتّ فيما إذا كانت هناك طريقة معيّنة للتوثيق تتيح مستوى مناسبا من قابلية التعويل عليها، تبعا للظروف، تتضمن ما يلي: *(أ)* مستوى التطور التقني للمعدات التي يستخدمها كل طرف من الأطراف؛ و*(ب)* طبيعة النشاط التجاري لتلك الأطراف؛ و*(ج)* التواتر الذي تحدث به المعاملات التجارية بين الأطراف؛ و*(د)* طبيعة المعاملة وحجمها؛ و*(هـ)* وظيفة المقتضيات الخاصة بالتوقيع في أية بيئة قانونية وتنظيمية معيّنة؛ و*(و)* قدرات نظم الاتصال؛ و*(ز)* الامتثال لإجراءات التوثيق التي يحدّدها الوسطاء؛ و*(ح)* النطاق المتنوع من إجراءات التوثيق الذي يتيحه أي وسيط؛ و*(ط)* الامتثال للأعراف والممارسات التجارية؛ و*(ي)* وجود آليات للتغطية التأمينية إزاء الرسائل غير المأذون بها؛ و*(ك)* أهمية وقيمة المعلومات الواردة في رسالة البيانات؛ و*(ل)* توافر طرائق بديلة لتحديد الهوية، وتكاليف التنفيذ؛ و*(م)* مدى قبول طريقة تحديد الهوية أو عدم قبولها في الصناعة المعنية أو الميدان المعني، في وقت الاتفاق على الطريقة وفي الوقت الذي يتم فيه إرسال رسالة البيانات.

٢- نهج التكنولوجيا المحدّدة

٩٠- يثير الاهتمام بتعزيز حياد الوسائط مسائل مهمّة أخرى. فاستحالة ضمان الأمن المطلق من الاحتيال وأخطاء الإرسال لا تنحصر في عالم التجارة الإلكترونية، بل تنطبق كذلك على عالم الوثائق الورقية. ولدى صوغ قواعد للتجارة الإلكترونية، يميل المشرعون غالبا إلى العمل على تحقيق أعلى مستويات الأمن التي توفرها التكنولوجيا الموجودة حاليا.[٩٢] ولا شك في أن هناك حاجة عملية إلى تطبيق معايير أمنية مشدّدة بغية اجتناب حالات الوصول إلى البيانات دون إذن، وضمان سلامة الخطابات، وحماية النظم

---

[٩٢] قانون يوتا للتوقيع الرقمي، الذي اعتُمد عام ١٩٩٥، هو أحد الأمثلة الأولى على ذلك، لكنه أُلغِي اعتبارا من ١ أيار/ مايو ٢٠٠٦ بموجب قانون الولاية رقم ٢٠، المتاح في الموقع الشبكي http://www.le.state.ut.us/~2006/htmdoc/sbillhtm/sb0020.htm (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨). كما يمكن ملاحظة الانحياز التكنولوجي في قانون يوتا في عدد من البلدان حيث لا يعترف القانون إلا بالتوقيعات الرقمية التي تُنشأ في إطار مرفق مفتاح عمومي كوسيلة صحيحة للتوثيق الإلكتروني. وهذا هو الحال، مثلا، في الأرجنتين، في قانون التوقيع الرقمي (٢٠٠١) والمرسوم رقم ٢٦٢٨/ ٢٠٠٢ *(اللائحة التنظيمية لقانون التوقيع الرقمي)*. كما إن هذا ملاحظ في إستونيا (قانون التوقيعات الرقمية) (٢٠٠٠)؛ وألمانيا، قانون التوقيع الرقمي، الذي اشترع بوصفه المادة ٣ من قانون خدمات المعلومات والاتصالات المؤرخ ١٣ حزيران/ يونيه ١٩٩٧؛ والهند، قانون تكنولوجيا المعلومات لعام ٢٠٠٠؛ وإسرائيل، قانون التوقيعات الإلكترونية (٢٠٠١)؛ واليابان، قانون التوقيعات الإلكترونية وخدمات التوثيق (٢٠٠١)؛ وليتوانيا، قانون التوقيعات الإلكترونية (٢٠٠٠)؛ وماليزيا، قانون التوقيعات الرقمية لسنة ١٩٩٧؛ وبولندا، قانون التوقيعات الإلكترونية (٢٠٠١)؛ والاتحاد الروسي، قانون التوقيع الرقمي الإلكتروني (٢٠٠٢).

الحاسوبية ونظم المعلومات. بيد أنه قد يكون من الأنسب، من منظور قانون الأعمال التجارية الخاص، اتّباع التدرج في مقتضيات الأمن بخطوات مماثلة لدرجات الأمان القانوني التي تُقابَل في المعاملات الورقية. ففي عالم المعاملات الورقية، يكون رجال الأعمال، في أغلب الحالات، أحرارا في الاختيار من بين طائفة واسعة من الطرائق لتحقيق سلامة الخطابات ووثاقتها (على سبيل المثال، مختلف مستويات التوقيع الخطي التي تُشاهَد في مستندات العقود البسيطة والصكوك الموثقة عدليا). وفي نهج محدِّد للتكنولوجيا، تشترط اللوائح التنظيمية استخدام تكنولوجيا محدّدة لاستيفاء المقتضيات القانونية لصحة التوقيع الإلكتروني. وهذه هي الحالة، على سبيل المثال، عندما يقتضي القانون الرامي إلى تحقيق مستوى أعلى من الأمن، تطبيقات تستند إلى مرفق المفتاح العمومي. وبما أن هذا النهج ينص على استخدام تكنولوجيا معينة، فهو يسمى أيضا النهج "الإيعازي".

٩١- أما عيوب نهج التكنولوجيا المحدّدة فهي أنه ينطوي، بسبب تفضيله لأنواع محددة من التوقيع الإلكتروني، على "مخاطر استبعاد تكنولوجيات أخرى، قد تكون أكثر تطورا، من دخول السوق والمنافسة فيه."[٩٣] وبدلا من تسهيل نمو التجارة الإلكترونية واستخدام تقنيات التوثيق الإلكتروني، قد يكون لهذا النهج أثر عكسي. ومن مخاطر وضع تشريعات خاصة بالتكنولوجيا المحدّدة أنه يؤدي إلى تثبيت المقتضيات قبل أن تنضج التكنولوجيا المختارة.[٩٤] وبالتالي، فإن تلك التشريعات قد تمنع أي تطورات إيجابية لاحقة في التكنولوجيا المعنية أو قد يعتريها التقادم سريعا نتيجة التطورات اللاحقة. وبالإضافة إلى ذلك، قد لا تحتاج جميع التطبيقات إلى مستوى من الأمن يوازي المستوى الذي توفره تقنيات محددة، مثل التوقيعات الرقمية. وقد تكون سرعة الاتصال وسهولته أو اعتبارات أخرى أكثر أهمية للأطراف من ضمان سلامة المعلومات الإلكترونية عبر عملية معينة. كما إن اشتراط استخدام وسيلة توثيق مفرطة الأمان قد يؤدي إلى تكاليف إضافية وضياع الجهد، مما قد يعيق انتشار التجارة الإلكترونية.

٩٢- وتحبّذ التشريعات الخاصة بالتكنولوجيا المحدّدة استخدام التوقيعات الإلكترونية ضمن إطار مرفق للمفاتيح العمومية. أما الطريقة التي يتم فيها تنظيم بنية مرافق المفاتيح العمومية فتختلف من بلد إلى آخر بحسب مستوى التدخل الحكومي. وهنا أيضا يمكن تحديد ثلاثة نماذج هي:

(أ) *التنظيم الرقابي الذاتي.* يترك هذا النموذج ميدان التوثيق واسعا للغاية. فمع أن الحكومة قد تعمد إلى إرساء مخطّط أو أكثر من مخططات التوثيق داخل إداراتها وداخل المؤسسات ذات الصلة، يظل القطاع الخاص حرا في وضع مخططات توثيق، تجارية أو غير تجارية، حسبما يراه مناسبا. ولا توجد في هذا النموذج سلطة توثيق إلزامية ذات مستوى عال، بل يكون فيه مقدّمو خدمات التوثيق مسؤولين

---

(٩٣) Stewart Baker and Matthew Yeo, in collaboration with the secretariat of the International Telecommunication Union ITU "Background and issues concerning authentication and the ITU"، وهي ورقة إحاطة قدّمها المؤلفان ستيوارت بيكر وماثيو يوو (Stewart Baker and Matthew Yeo)، بالتعاون مع أمانة الاتحاد الدولي للاتصالات، إلى اجتماع الخبراء حول السلطات المعنية بالتوقيعات الإلكترونية والتوثيق الإلكتروني: مسائل متعلقة بالاتصالات، جنيف، ٩ و١٠ كانون الأول/ ديسمبر ١٩٩٩، الوثيقة رقم ٢، متاحة في الموقع الشبكي www.itu.int/osg/spu/ni/esca/meetingdec9-101999/briefingpaper.html (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

(٩٤) ولكن، نظرا إلى كون تكنولوجيا مرفق المفاتيح العمومية أصبحت الآن ناضجة وراسخة بما فيه الكفاية، فإن بعض هذه الشواغل قد لا توجد الآن بالحدة التي كانت عليها من قبل.

عن ضمان صلاحية المخططات للعمل تبادليا مع مقدّمي خدمات آخرين محليا ودوليا، بحسب أهداف إنشاء مخطط التوثيق. ولا يتطلب هذا النموذج إصدار رخص أو الحصول على الموافقة على التكنولوجيات المستخدمة من مقدّمي خدمات التوثيق (ربما باستثناء اللوائح التنظيمية لحماية المستهلك)؛[٩٥]

(ب) *تدخّل حكومي محدود*. قد تقرر الحكومة إنشاء سلطة توثيق رفيعة المستوى تكون اختيارية أو إلزامية. وفي هذه الحالة، قد يرى مقدّمو خدمات التوثيق ضرورة العمل تبادليا مع سلطة التوثيق الرفيعة المستوى كي تكون أمارات الترميز التي يستخدمونها في التوثيق (أو غيرها من أدوات التوثيق) مقبولة خارج النظم الخاصة بهم. وفي هذه الحالة، يجب أن تُنشَر المواصفات التقنية والإدارية لمقدّمي خدمات التوثيق بأسرع وقت ممكن حتى تتمكن الإدارات الحكومية والقطاع الخاص أيضا من وضع الخطط على أساس هذه المواصفات. ويمكن اشتراط الحصول على رخص وموافقات تكنولوجية لكل مقدّم خدمات توثيق؛[٩٦]

(ج) *عملية تقودها الحكومة*. قد تقرّر الحكومة إنشاء مؤسسة مركزية حصرية لتقديم خدمات التوثيق. كما يمكن إنشاء مؤسسات لتقديم خدمات التوثيق ذات أغراض خاصة، وذلك بموافقة الحكومة.[٩٧] وتمثّل نظم إدارة شؤون الهوية (انظر الفقرات ٦٧-٧٧ أعلاه) طريقة أخرى قد تتولى الحكومات من خلالها توجيه عملية التوقيع الرقمي على نحو غير مباشر. وقد قامت بعض الحكومات من قبلُ بمباشرة برامج خاصة بإصدار وثائق هوية مقروءة آليا لمواطنيها ("وثائق هوية إلكترونية") مزوّدة بخصائص وظيفية للتوقيع الرقمي.

٣- نهج المستويين أو الشقّين

٩٣- في هذا النهج، تضع التشريعات عتبة منخفضة من المقتضيات لكي تحظى طرائق التوثيق الإلكترونية بحد أدنى معيّن من الوضع القانوني، وتمنح بعض طرائق التوثيق الإلكترونية مفعولا قانونيا أكبر (يشار إليها على نحو متفاوت بأنها توقيعات إلكترونية مأمونة أو متقدّمة أو معزّزة أو شهادات تصديق مستوفية الشروط).[٩٨] وعلى المستوى الأساسي، فإن التشريعات التي تعتمد نظاما من مستويين عموما تمنح التوقيعات الإلكترونية وضعية التكافؤ الوظيفي مع التوقيعات الخطية، بالاستناد إلى معايير محايدة تكنولوجيا. أما التوقيعات ذات المستوى الأعلى، والتي تنطبق عليها بعض الافتراضات القابلة للدحض، فمن اللازم أن تمتثل لمقتضيات محدّدة قد ترتبط بتكنولوجيا معيّنة. وحاليا، يعرّف هذا النوع من التشريعات عادة هذه التوقيعات المأمونة من حيث هي تكنولوجيا بشأن مرافق المفاتيح العمومية.

---

[٩٥] رابطة التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC)، *Assessment Report on Paperless Trading of APEC Economies* (تقرير تقييمي عن التجارة اللاورقية لاقتصادات بلدان الرابطة) (بيجين، أمانة آبيك، ٢٠٠٥)، الصفحتان ٦٣ و٦٤، حيث تُذكر الولايات المتحدة كمثال على تطبيق هذا النموذج.

[٩٦] المرجع نفسه، حيث تُذكر سنغافورة كمثال.

[٩٧] المرجع نفسه، حيث تُذكر كل من الصين وماليزيا كمثالين.

[٩٨] Aalberts and van der Hof, *Digital Signature Blindness* ...، الفقرة ٣-٢-٢.

٩٤- ويقع الاختيار على هذا النهج عادة في الولايات القضائية التي ترتئي أن من المهم تناول بعض المقتضيات التكنولوجية في تشريعاتها، لكنها ترغب في الوقت نفسه في إتاحة المجال للتطورات التكنولوجية. ويمكن لهذا النهج أن يوفر توازنا بين المرونة واليقين فيما يتعلق بالتوقيعات الإلكترونية، فهو يتيح للأطراف أن تحكم من وجهة نظر تجارية وتقرر ما إذا كانت التكاليف المتكبَّدة والصعوبات المواجَهة في استخدام طريقة أكثر أمنا تسوِّغ اختيار هذا النهج لتلبية احتياجاتها. كما توفر هذه النصوص دليلا توجيهيا بشأن معايير الاعتراف بالتوقيعات الإلكترونية في سياق نموذج وجود سلطة تصديق. ويمكن عموما الجمع بين النهج المؤلف من مستويين وأي نوع من نماذج التصديق (سواء أكانت نماذج ذاتية التنظيم الرقابي، أم نماذج اعتماد طوعي أم مخططا تديره الحكومة)، بالطريقة نفسها تقريبا المتبعة في النهج الخاص بتكنولوجيا محدّدة (انظر الفقرات ٩٠-٩٢ أعلاه). وبالتالي، مع أن بعض القواعد قد تكون مرنة بما يكفي لاستيعاب مختلف نماذج تصديق التوقيعات الإلكترونية، فإن بعض النظم لن تعترف إلا بمقدّمي خدمات التصديق المرخَّص لهم ليكونوا من مصدِري الشهادات "المأمونة" أو "المستوفية الشروط".

٩٥- وكانت سنغافورة[٩٩] والاتحاد الأوروبي[١٠٠] أولى الولايات القضائية التي سنّت تشريعات لاعتماد نهج المستويين. ثم تبعهما عدد من الولايات القضائية الأخرى.[١٠١] ويتيح قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية للدولة المشترعة إقامة نظام من مرحلتين من خلال عدد من اللوائح التنظيمية وإن كان لا يروّج لذلك فعلا.[١٠٢]

---

[٩٩] يعترف قانون المعاملات الإلكترونية في سنغافورة في الباب ٨ بأي شكل من أشكال التوقيع الإلكتروني، لكن التوقيعات الإلكترونية التي تلبي شروط الباب ١٧ من القانون (أي "*(أ)* التوقيع الفريد للشخص الذي يستخدمه؛ و*(ب)* التوقيع الذي يمكن من خلاله التعرف على هوية ذلك الشخص؛ و*(ج)* التوقيع الذي أُنشئ بطريقة يتحكم بها الشخص الذي يستخدمه فقط أو باستخدام وسيلة تخضع لمراقبته دون غيره؛ و*(د)* التوقيع المقترن بسجل إلكتروني يرتبط به بطريقة من شأنها أن تبطل التوقيع الإلكتروني عند حصول أي تغيير في السجل")، هي فقط التوقيعات التي تتمتع بالقرائن المذكورة في الباب ١٨ (ومن بينها أن التوقيع "يعود للشخص الذي يقترن به" وأن "ذلك الشخص مهر التوقيع بنية توقيع السجل الإلكتروني أو الموافقة عليه"). ولأغراض ذلك القانون، فإن التوقيعات الإلكترونية المدعومة بشهادة جديرة بالثقة تمتثل لأحكام الباب ٢٠ من القانون، هي التوقيعات التي تعتبر تلقائيا "توقيعات إلكترونية مأمونة".

[١٠٠] على غرار قانون المعاملات الإلكترونية في سنغافورة، يميز التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية (*Official Journal of the European Communities*, L 13/12, 19 January 2000) بين "التوقيع الإلكتروني" (المعرَّف في الفقرة ١ من المادة ٢ بوصفه "بيانات في شكل إلكتروني متصلة ببيانات إلكترونية أخرى أو مرتبطة بها منطقيا، وتستخدم كطريقة للتوثيق") و"التوقيع الإلكتروني المتقدّم" (بحسب التعريف الوارد في الفقرة ٢ من المادة ٢، بوصفه توقيعا إلكترونيا يلبي الشروط التالية: "*(أ)* يرتبط بالموقِّع وحده؛ و*(ب)* يمكّن من التعرّف على هوية الموقِّع؛ *(ج)* أُنشئ باستخدام وسائل يستطيع الموقِّع الحفاظ عليها تحت مراقبته وحده؛ و*(د)* يرتبط بالبيانات التي يقترن بها بطريقة تجعل من الممكن اكتشاف أي تغيير لاحق فيها"). وتلزم الفقرة ٢ من المادة ٥ من التوجيه الإداري الدول الأعضاء في الاتحاد الأوروبي بضمان "ألا يحرم التوقيع الإلكتروني من استخدام الفعالية والمقبولية القانونيتين كدليل إثبات في الإجراءات القانونية وذلك على أساس أنه "في شكل إلكتروني، أو أنه غير مستند إلى شهادة مستوفية للشروط، أو أنه غير مستند إلى شهادة مستوفية للشروط أصدرها مقدّم خدمات تصديق معتَمد، أو لم يُنشأ من خلال أداة مأمونة لإنشاء التوقيعات." لكن التوقيعات الإلكترونية المتقدمة "التي تستند إلى شهادة تصديق مستوفية للشروط والتي أُنشئت بواسطة أداة مأمونة لإنشاء التوقيعات هي وحدها التي يُعلَن أنها": "*(أ)* تستوفي شروط التوقيع القانونية فيما يخص البيانات بالشكل الإلكتروني بنفس الطريقة التي يستوفي بها التوقيع الخطي تلك الشروط فيما يتعلق بالبيانات الورقية؛ و*(ب)* تُقبل كدليل إثبات في الإجراءات القانونية." (انظر الفقرة ١ من المادة ٥ من التوجيه الإداري).

[١٠١] باكستان وموريشيوس على سبيل المثال. انظر الحاشية ٨٨ أعلاه للحصول على تفاصيل القوانين النظامية ذات الصلة.

[١٠٢] تنص الفقرة ٣ من المادة ٦ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، على أن التوقيع الإلكتروني يعتبر "قابلا للتعويل عليه . . . إذا: *(أ)* كانت بيانات إنشاء التوقيع مرتبطة، في السياق الذي تُستخدم فيه، بالموقّع دون أي شخص آخر؛ و*(ب)* كانت بيانات إنشاء التوقيع خاضعة، وقت التوقيع، لسيطرة الموقّع دون أي شخص آخر؛ و*(ج)* كان أي تغيير في التوقيع الإلكتروني، يُجرى بعد حدوث التوقيع، قابلا للاكتشاف؛ و*(د)* كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجرى في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف.

٩٦- أما فيما يتعلق بالمستوى الثاني، فقد اقتُرح أن تطلب البلدان استخدام توقيعات المستوى الثاني بخصوص المقتضيات الشكلية فيما يتعلق بالمعاملات التجارية الدولية وأن تُحصَر التوقيعات الإلكترونية المأمونة في مجالات القانون التي لا تؤثر كثيرا على التجارة الدولية (مثل الاتحادات، وقانون الأسرة، ومعاملات الأملاك العقارية، الخ).[١٠٣] علاوة على ذلك، اقتُرح أن تنص القوانين الخاصة بالمستويين، على نحو صريح، على إنفاذ مفعول الاتفاقات التعاقدية الخاصة باستخدام التوقيعات الإلكترونية والاعتراف بها، وذلك لضمان عدم تضارب نماذج التوثيق العالمية المستندة إلى العقود مع المقتضيات القانونية الوطنية.

باء- القيمة الإثباتية لطرائق التوقيع والتوثيق الإلكترونية

٩٧- أحد الأهداف الرئيسية لقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية وقانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية هو استباق عدم التناغم والإفراط المحتمل في التنظيم الرقابي، وذلك بتقديم معايير عامة لإرساء التكافؤ الوظيفي بين طرائق التوقيع والتوثيق الإلكترونية والورقية. ومع أن قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لاقى قبولا واسعا، وأن عددا متزايدا من الدول أخذت تستخدمه كأساس لتشريعاتها الخاصة بالتجارة الإلكترونية، فإنه لا يمكن بعدُ افتراض أن مبادئ هذا القانون النموذجي قد بلغت درجة التطبيق على نطاق عالمي. فالموقف الذي اتخذته مختلف الولايات القضائية فيما يتعلق بالتوقيعات الإلكترونية والتوثيق الإلكتروني يعكس نمطيا النهج العام للولاية القضائية إزاء اشتراطات الكتابة والقيمة الإثباتية للسجلات الإلكترونية.

١- *"التوثيق" والإسناد العام للسجلات الإلكترونية*

٩٨- ينطوي استخدام طرائق التوثيق الإلكترونية على جانبين لهما صلة بهذه المناقشة. أما الجانب الأول فيتعلق بالمسألة العامة المتمثلة في إسناد رسالة إلى منشئها المفترَض. وأما الجانب الثاني فيتعلق بمدى مناسبة طريقة تعيين الهوية التي تستخدمها الأطراف لغرض تلبية مقتضيات محددة بشأن الشكل، خصوصا مقتضيات التوقيع القانونية. ومما له صلة أيضا بالموضوع المفاهيم القانونية التي تدلّ ضمنا على وجود توقيع خطي، مثلما هو الحال فيما يتعلق بمفهوم "المستند" في بعض النظم القانونية. وحتى إذا جاز الجمع بين هذين الجانبين في كثير من الأحيان أو إذا تعذر التمييز بينهما تماما، حسب الظروف، فقد تجدي محاولة تحليلهما منفصلين، إذ يبدو أن المحاكم تتجه إلى استنتاجات مختلفة حسب الوظيفة المرتبطة بطريقة التوثيق.

(١٠٣) Baker and Yeo, "Background and issues concerning authentication ...".

٩٩- ويتناول القانون النموذجي بشأن التجارة الإلكترونية موضوع إسناد رسائل البيانات في المادة ١٣ . ويرجع أصل هذا النص إلى المادة ٥ من قانون الأونسيترال النموذجي للتحويلات الدائنة الدولية،[١٠٤] التي تحدّد التزامات مرسل أمر الدفع. والمقصود من المادة ١٣ من القانون النموذجي بشأن التجارة الإلكترونية هو أن تُطبَّق عندما يكون هناك تساؤل عما إذا كانت الرسالة الإلكترونية مرسَلة فعلا من الشخص المشار إليه بأنه هو المنشئ. وتظهر هذه المشكلة في حالة الرسائل الورقية نتيجة لادعاء بتزوير توقيع المنشئ المفترض. وأما في بيئة إلكترونية، فيمكن أن يكون شخص غير مأذون له هو الذي أرسل الرسالة، ولكن التوثيق بشيفرة أو ترميز أو بوسائل مشابهة لذلك من شأنه أن يكون دقيقا. والغرض من المادة ١٣ ليس إسناد مرجعية تحرير رسالة بيانات إلى طرف ما أو تحديد هوية الأطراف، بل معالجة إسناد رسائل البيانات بتقرير الشروط التي يمكن بمقتضاها لطرف ما أن يعوّل على الافتراض بأن رسالة البيانات صادرة فعلا عن المنشئ المفترض.

١٠٠- والفقرة ١ من المادة ١٣ من القانون النموذجي بشأن التجارة الإلكترونية تذكِّر بالمبدأ الذي مفاده أن المنشئ ملزم برسالة البيانات إذا كان هو الذي أرسلها فعلا. أما الفقرة ٢ فهي تخص الحالة التي يرسل فيها الرسالة شخص غير المنشئ كانت لديه صلاحية التصرّف نيابة عن المنشئ. وأما الفقرة ٣ فتعالج نوعين من الحالات يستطيع فيهما المرسل إليه أن يعوّل على اعتبار رسالة البيانات صادرة عن المنشئ، وهما: أولا الحالات التي طبَّق فيها المرسل إليه على نحو سليم إجراء توثيق سبق أن وافق عليه المنشئ؛ وثانيا، الحالات التي تكون فيها رسالة البيانات ناتجة عن تصرفات شخص كانت متاحة له، بحكم علاقته بالمنشئ، سبل الوصول إلى الإجراءات التي يتبعها المنشئ للتوثيق.

١٠١- وقد اعتمد عدد من البلدان القاعدةَ الواردةَ في المادة ١٣ من القانون النموذجي بشأن التجارة الإلكترونية، بما فيها افتراض الإسناد المنصوص عليه في الفقرة ٣ من تلك المادة.[١٠٥] وتشير بعض البلدان صراحة إلى استخدام الشيفرات أو كلمات السر أو غيرها من وسائل تعيين الهوية كعوامل توجد قرينة تدل على هوية المؤلِّف (المحرّر).[١٠٦] وهناك أيضا صيغ أكثر تعميما للمادة ١٣، حيث ترد القرينة الناشئة عن توثيق سليم بواسطة إجراء سبق الاتفاق عليه ولكن بصيغ أخرى على أنها دلالة على عناصر يمكن استخدامها لأغراض الإسناد.[١٠٧]

---

[١٠٤] منشورات الأمم المتحدة، رقم المبيع A.99.V.11، نص القانون النموذجي متاح في الموقع الشبكي http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٠٥] كولومبيا (المادة ١٧)؛ إكوادور (المادة ١٠)؛ الأردن (المادة ١٥)؛ موريشيوس (الباب ١٢، الفرع ٢)؛ الفلبين (الباب ١٨، الفقرة (٣))؛ جمهورية كوريا (المادة ٧، الفقرة ٢)؛ سنغافورة (الباب ١٣، الفقرة (٣))؛ تايلند (الباب ١٦)؛ فنزويلا (جمهورية-البوليفارية) (المادة ٩). وترد أيضا القواعد نفسها في قوانين جيرسي التابعة للتاج البريطاني (المادة ٨)، وأراضي برمودا البريطانية الواقعة ما وراء البحار (الباب ١٦، الفقرة ٢)، وجزر تركس وكايوكس (الباب ١٤). وللاطلاع على تفاصيل عن القوانين التشريعية ذات الصلة، انظر الحاشية ٨٨ أعلاه.

[١٠٦] المكسيك (انظر الحاشية ٨٨ أعلاه)، المادة ٩٠، الفقرة الأولى.

[١٠٧] مثلا، ينص قانون الولايات المتحدة الموحّد بشأن المعاملات الإلكترونية (انظر الحاشية ٩٠) في الباب ٩ *(أ)* على أن السجل الإلكتروني أو التوقيع الإلكتروني "ينسب إلى الشخص إذا كان من فعل ذلك الشخص. ويجوز أن يبيَّن فعل الشخص بأي طريقة، بما في ذلك بيان كفاءة أي إجراء أمني يستخدم لتعيين الشخص الذي يمكن أن ينسب إليه السجل الإلكتروني أو التوقيع الإلكتروني". كما ينص الباب ٩ *(ب)* على أن مفعول السجل الإلكتروني أو التوقيع الإلكتروني المنسوب إلى شخص بمقتضى الباب الفرعي *(أ)* "يحدد من السياق والظروف المحيطة وقت صوغه أو تنفيذه أو اعتماده، بما في ذلك موافقة الأطراف، إن وجدت، وخلافا لذلك حسبما ينص القانون".

١٠٢- غير أن بلدانا أخرى لم تعتمد إلا القواعد العامة الواردة في المادة ١٣، أي أن رسالة البيانات تعتبر صادرة عن المنشئ إذا كان المنشئ هو الذي أرسلها بنفسه، أو أرسلها شخص له صلاحية التصرّف نيابة عن المنشئ، أو أرسلها نظام مبرمج على يد المنشئ أو نيابة عنه للعمل تلقائيا.[١٠٨] وإضافة إلى ذلك، لم يدرج عدد من البلدان التي نفّذت القانون النموذجي بشأن التجارة الإلكترونية أي حكم محدد يستند إلى المادة ١٣.[١٠٩] وكان الافتراض في تلك البلدان أنه ليست هناك حاجة إلى قواعد محددة، وأن من الأفضل أن تُترك مسألة الإسناد لمعالجتها بطرائق الإثبات العادية، تماما مثلما يعالَج إسناد المستندات الورقية: أي "الشخص الذي يريد أن يعوّل على أي توقيع يعرِّض نفسه لمخاطرة عدم صحة التوقيع، ولا تتغير هذه القاعدة فيما يتعلق بالتوقيع الإلكتروني."[١١٠]

١٠٣- لكن بلدانا أخرى فضّلت أن تدرج أحكام القانون النموذجي بشأن التجارة الإلكترونية الخاصة بالإسناد منفصلة عن الأحكام الخاصة بالتوقيعات الإلكترونية. ويستند هذا النهج إلى الفهم الذي مفاده أن الإسناد في سياق مستندي يخدم غرضا رئيسيا هو توفير أساس لقدر معقول من التعويل، وقد يتضمّن أساليب أكثر اتساعا من تلك التي تستخدم في نطاق أضيق لتحديد هوية الأفراد. وتشدد بعض القوانين، مثل قانون الولايات المتحدة الموحّد بشأن المعاملات الإلكترونية، على هذا المبدأ إذ تبيّن، مثلا، أن "السجل الإلكتروني أو التوقيع الإلكتروني يُسند إلى الشخص إذا كان من فعل هذا الشخص"، ويجوز أن يبيَّن ذلك "بأي طريقة بما في ذلك بيان كفاءة أي إجراء أمني يُطبّق لتعيين الشخص الذي يمكن أن يُسند إليه السجل الإلكتروني أو التوقيع الإلكتروني".[١١١] وهذه القاعدة العامة بشأن الإسناد لا تؤثر في استخدام التوقيع كوسيلة لإسناد السجل لشخص، وإنما تستند إلى التسليم بأن "التوقيع ليس طريقة الإسناد الوحيدة".[١١٢] ولذلك، وفقا للتعليق على قانون الولايات المتحدة:

---

[١٠٨] أستراليا (الباب ١٥، الفقرة ١)؛ والهند بالأسلوب نفسه أساسا (الباب ١١)؛ وباكستان (الباب ١٣، الباب الفرعي ٢)؛ وسلوفينيا (المادة ٥)؛ انظر أيضا منطقة هونغ كونغ الإدارية الخاصة التابعة للصين (الباب ١٨) وإقليم جزيرة مان التابع للتاج البريطاني (الباب ٢). وللاطلاع على تفاصيل مختلف القوانين التشريعية انظر الحاشية ٨٨ أعلاه.

[١٠٩] مثلا، إيرلندا وجنوب أفريقيا وفرنسا وكندا ونيوزيلندا.

[١١٠] كندا، القانون الموحّد للتجارة الإلكترونية (Uniform Electronic Commerce Act) (مع تعليق رسمي) (انظر الحاشية ٨٩)، التعليق على الباب ١٠.

[١١١] الولايات المتحدة، القانون الموحد بشأن المعاملات الإلكترونية (١٩٩٩) (انظر الحاشية ٩٠)، الباب ٩. تقدم الفقرة ١ من التعليقات الرسمية على الباب ٩ الأمثلة التالية التي يمكن أن يسند فيها كل من السجل الإلكتروني والتوقيع الإلكتروني إلى شخص: "يطبع الشخص اسمه كجزء من طلب شراء بالبريد الإلكتروني"؛ أو "يطبع مستخدم الشخص، بموجب تفويض، اسم الشخص كجزء من طلب شراء بالبريد الإلكتروني"؛ أو "يُصدر الحاسوبُ الخاص بالشخص، المبرمَجُ لطلب سلع عند تلقي معلومات خاصة بقائمة جرد وفق معايير معينة، طلبَ شراء يتضمن اسم الشخص وغير ذلك من معلومات تعيين الهوية كجزء من الطلب".

[١١٢] تبيّن الفقرة ٣ من التعليقات الرسمية على الباب ٩ أن "استخدام الإرسال بالفاكس يقدّم عددا من الأمثلة على الإسناد باستخدام معلومات أخرى غير التوقيع. ويجوز أن يسند الفاكس إلى شخص بسبب المعلومات المطبوعة في أعلى الصفحة التي تشير إلى الآلة التي أُرسلت منها. ومثل ذلك قد تتضمن الرسالة ترويسة تعيِّن هوية المرسل. ورئي في بعض القضايا أن الترويسة تشكل في الواقع توقيعا لأنها رمز اختاره المرسل بقصد توثيق الرسالة المرسلة بالفاكس. غير أن حكم التوقيع جاء من ضرورة تقرير القصد في هذه القضية. وفي قضايا أخرى رئي أن ترويسات رسائل الفاكس ليست توقيعات نظرا لعدم توافر القصد الضروري. والنقطة الحرجة هي أن المعلومات الموجودة داخل السجل الإلكتروني قد تكفي فعلا لتوفير الوقائع المؤدية إلى إسناد سجل إلكتروني إلى طرف معين، سواء كان ذلك بتوقيع أو دونه."

"٤- قد توجد معلومات معينة في بيئة إلكترونية لا يبدو أنها تُستخدم للإسناد، بل تربط بوضوح بين شخص ما وسجل محدد. فالشيفرات العددية وأرقام تحديد الهوية الشخصية وأشكال الجمع بين المفاتيح العمومية والمفاتيح الخصوصية، كلها تُستخدم من أجل تعيين الطرف الذي يجب أن يسند إليه سجل إلكتروني. وطبعا تكون إجراءات الأمن بيِّنة إثباتية أخرى متاحة لتقرير الإسناد.

"يعد إدراج إشارة خاصة إلى إجراءات الأمن كوسيلة لإثبات الإسناد مفيدا نظرا للأهمية الفريدة التي تتسم بها إجراءات الأمن في البيئة الإلكترونية. وفي إجراءات قانونية معينة قد يكون إجراء الأمن التقني والتكنولوجي أفضل طريقة لإقناع فاحص الوقائع بأن سجلا إلكترونيا أو توقيعا إلكترونيا معيناً يخصّ شخصا معيناً. وفي ظروف معينة، قد يكون من الضروري استخدام إجراء أمني لإثبات أن السجل والتوقيع المتصل به جاءا من منشأة أعمال الشخص المعني، وذلك لدحض ادّعاء بأن أحد مخترقي البرامجيات قد تدخّل. وليس المقصود من الإشارة إلى إجراءات الأمن الإلماح إلى وجوب منح أشكال أخرى من إثبات الإسناد مفعولا إقناعيا أدنى. ويهم أيضا التذكر بأن القوة المعيّنة لإجراء ما لا تؤثّر في وضع هذا الإجراء بصفته إجراء أمنيا، بل إنها لا تؤثّر إلا في الرجحان الممنوح لبيِّنة إثبات إجراء الأمن على أنها تميل إلى إنشاء الإسناد."[١١٣]

١٠٤- ومن المهم أيضا ألاَّ يغيب عن البال أن قرينة الإسناد لا تحل وحدها محل تطبيق القواعد القانونية التي تحكم التوقيعات حيثما كان التوقيع لازما لصحة فعل أو لإثباته. وعندما يتقرر أنه يمكن إسناد سجل أو توقيع إلى طرف معيّن، "يجب تقرير مفعول السجل أو التوقيع في ضوء السياق والظروف المحيطة، بما في ذلك اتفاق الأطراف، إن وجد"، وكذلك "المقتضيات القانونية الأخرى المأخوذة بعين الاعتبار على ضوء السياق".[١١٤]

١٠٥- وبناء على هذه الخلفية من المرونة في فهم الإسناد، يبدو أن المحاكم في الولايات المتحدة سلكت نهجا متحرّرا إزاء جواز قبول السجلات الإلكترونية، بما في ذلك البريد الإلكتروني، كدليل إثبات في الإجراءات المدنية.[١١٥] فقد رفضت محاكم في الولايات المتحدة دعاوى تحتج بأن رسائل البريد الإلكتروني غير مقبولة كدليل إثبات لأنها أدلة إثبات غير موثقة وشفوية.[١١٦] ورأت المحاكم بدلا من ذلك أن رسائل البريد الإلكتروني التي يُحصل عليها من المدّعي أثناء عملية الكشف تعتبر ذاتية التوثيق، حيث إن "تقديم مستندات أثناء الكشف من ملفات الأطراف الخاصة يكفي لتسويغ استخلاص قرار بشأن التوثيق

[١١٣] التعليقات الرسمية على الباب ٩.

[١١٤] الفقرة ٦ من التعليقات الرسمية على الباب ٩.

[١١٥] *Commonwealth Aluminum Corporation v. Stanley Metal Associates,* United States District Court for the Western District of Kentucky, 9 August 2001, Federal Supplement, 2nd series, vol. 186, p. 770; and *Central Illinois Light Company (CILCO) v. Consolidation Coal Company (Consol)*, United States District Court for the Central District of Illinois, 30 December 2002, Federal Supplement, 2nd series, vol. 235, p. 916.

[١١٦] *Sea-Land Service, Inc. v. Lozen International, LLC,* United States Court of Appeals for the Ninth Circuit, 3 April 2002, Federal Reporter, 3rd series, vol. 285, p. 808.

الذاتي".[١١٧] وتميل المحاكم إلى أن تأخذ في الاعتبار كل أدلة الإثبات المتاحة، ولا ترفض السجلات الإلكترونية على أنها أدلة ظاهرية غير كافية.

١٠٦- أما في البلدان التي لم تعتمد القانون النموذجي بشأن التجارة الإلكترونية، فيبدو أنه لا توجد أحكام تشريعية محددة تعالج مسألة الإسناد بأسلوب مماثل. وفي تلك البلدان عادة ما يتوقف الإسناد على الاعتراف القانوني بالتوقيعات الإلكترونية والافتراضات المتصلة بالسجلات الموثّقة بأنواع معينة من التوقيعات الإلكترونية. وقد دعت شواغل تتعلق بمخاطر التلاعب بالسجلات الإلكترونية، مثلا، إلى عدم التفات المحاكم في بعض تلك البلدان إلى قيمة رسائل البريد الإلكتروني كدليل إثبات في الإجراءات القضائية، بسبب أن رسائل البريد الإلكتروني لا توفر ضمانات كافية على سلامتها.[١١٨] وتوجد أمثلة أخرى على نهوج أكثر تقييدا بشأن القيمة الإثباتية للسجلات الإلكترونية والإسناد في قضايا حديثة العهد كانت تتعلق بالمزادات عبر الإنترنت، طبّقت فيها المحاكم معيارا عالي المستوى بخصوص إسناد رسائل البيانات. وكانت هذه القضايا متعلقة غالبا بدعاوى إخلال بعقد بسبب عدم تسديد ثمن سلع زُعم أنها مشتراة في مزادات على الإنترنت. وتمسّك المدّعون بأن المدّعى عليهم كانوا هم الطرف المشتري، حيث إن أعلى عرض لشراء السلع كان موثقا بكلمة سر المدّعى عليه وأُرسل من عنوان البريد الإلكتروني الخاص بالمدّعى عليه. ورأت المحاكم أن هذه العناصر لا تكفي للوصول إلى استنتاج راسخ بأن المدّعى عليه هو الذي شارك فعلا في المزاد وقدم العرض الفائز لشراء السلع. واستخدمت المحاكم حججا مختلفة لتسويغ هذا الموقف. فمثلا، قيل إن كلمات السر لا يُعوّل عليها لأنه يمكن لأي شخص يعلم كلمة سر المدّعى عليه أن يستخدم عنوان المدّعى عليه في البريد الإلكتروني من أي مكان وأن يشارك في المزاد مستخدما اسم المدّعى عليه،[١١٩] وهي مخاطرة رأت بعض المحاكم أنها شديدة الاحتمال، وذلك على أساس مشورة الخبراء بشأن الأخطار التي يتعرّض لها أمن شبكات الاتصال بواسطة الإنترنت، وخصوصا باستخدام ما يُطلق عليه "حصان طروادة" القادر على "سرقة" كلمة سر خاصة بشخص ما.[١٢٠] وقيل إن تبعة مخاطرة استخدام وسيلة تعيين هوية الشخص (أي كلمة السر) دون إذن يجب أن يتحمّلها الطرف الذي عرض سلعا أو خدمات من خلال واسطة

---

(١١٧) *Superhighway Consulting, Inc. v. Techwave, Inc.*, United States District Court for the Northern District of Illinois, Eastern Division, 16 November 1999, U.S. Dist. LEXIS 17910.

(١١٨) Germany, Amtsgericht (District Court) Bonn, Case No. 3 C 193/01, 25 October 2001 *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 332/2002، متاح في الموقع الشبكي http://www.jurpc.de/rechtspr/20020332.htm (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

(١١٩) Germany, Amtsgericht (District Court) Erfurt, Case No. 28 C 2354/01, 14 September 2001, JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht, JurPC Web-Dok. No. 71/2002، متاح في الموقع الشبكي http://www.jurpc.de/rechtspr/20020071.htm (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨). انظر أيضا Landesgericht (Land Court) Bonn, Case No. 2 O 472/03, 19 December 2003, JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht, JurPC Web-Dok. No. 74/2004، متاح في الموقع الشبكي http://www.jurpc.de/rechtspr/20040074.htm (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

(١٢٠) Germany, Landesgericht (Land Court) Konstanz, Case No. 2 O 141/01 A, 19 April 2002, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht,* JurPC Web-Dok. No. 291/2002، متاح في الموقع الشبكي http://www.jurpc.de/rechtspr/20020291.htm (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

معيَّنة، حيث إنه لا توجد قرينة قانونية على أن الرسائل المرسلة عبر موقع على شبكة الإنترنت باللجوء إلى كلمة سر أحد الأشخاص لدخول ذلك الموقع، يمكن إسنادها إلى ذلك الشخص.[١٢١] ويمكن تصوّر إلحاق مثل هذه القرينة بـ"توقيع إلكتروني متقدم" كما يرد تعريفه في القانون، إلا أنه يجب ألا يتحمل صاحب "كلمة سر" بسيطة مخاطر إساءة استخدامها من جانب أشخاص غير مأذون لهم بذلك.[١٢٢]

٢- القدرة على الوفاء بمقتضيات التوقيع القانونية

١٠٧- اتجهت المحاكم في بعض البلدان إلى تفسير مقتضيات التوقيع بأسلوب متحرّر. وكانت هذه هي الحال عادة في بعض الولايات القضائية التي تعمل بمقتضى القانون العام، كما سبق بيانه (انظر المقدمة، الفقرات ٢-٤) فيما يتعلق بمقتضيات قانون الاحتيالات الذي يقضي بأن معاملات معيَّنة يجب أن تكون كتابة وأن تحمل توقيعا لكي تكون صحيحة. كما تقبّلت محاكم في الولايات المتحدة الاعتراف التشريعي بالتوقيعات الإلكترونية، حيث أجازت استخدامها أيضا في أوضاع ليست متوخّاة صراحة في اللوائح التنفيذية للقوانين، كما في مسألة الأوامر القضائية.[١٢٣] والأهم من ذلك في السياقات التعاقدية هو أن المحاكم قدَّرت أيضا كفاية التوثيق على ضوء التعاملات فيما بين الأطراف، بدلا من استخدام معيار صارم لكل الأوضاع. وهكذا، فإنه في الأحوال التي استخدمت فيها الأطراف البريد الإلكتروني بانتظام في مفاوضاتها، رأت المحاكم أن اسم المنشئ المطبوع على رسالة مرسلة بالبريد الإلكتروني يفي بمقتضيات التوقيع القانونية.[١٢٤] واعتُبر اختيار الشخص عن قصد طبع اسمه في ختام كل الرسائل الإلكترونية" توثيقا صحيحا.[١٢٥] واستعداد محاكم الولايات المتحدة للقبول بأن رسائل البريد الإلكتروني والأسماء المطبوعة فيها هي وسائل كافية للوفاء بمقتضيات الكتابة[١٢٦] إنما يتّبع تفسيرا متحررا لمفهوم "التوقيع" يُفهم منه أنه يشمل "أي رمز نفذه أو اعتمده الطرف بقصد توثيق نص مكتوب"، بحيث أن "الاسم المطبوع على مستند أو ترويسته يكفي للوفاء باقتضاء التوقيع"،[١٢٧] في ظروف معيّنة. أما عندما لا تنكر الأطراف أنها كتبت أو

---

(١٢١) Germany, Landesgericht (Land Court) Bonn, Case No. 2 O 450/00, 7 August 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht,* JurPC Web-Dok. No. 136/2002، متاح في الموقع الشبكي http://www.jurpc.de/rechtspr/20020136.htm (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

(١٢٢) Germany, Oberlandesgericht (Court of Appeal) Köln, Case No. 19 U 16/02, 6 September 2002, JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht, JurPC Web-Dok. No. 364/2002، متاح في الموقع الشبكي http://www.jurpc.de/rechtspr/20020364.htm (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

(١٢٣) *Department of Agriculture and Consumer Services v. Haire*, Fourth District Court of Appeal of Florida, Case Nos. 4D02-2584 and 4D02-3315, 15 January 2003.

(١٢٤) *Cloud Corporation v. Hasbro, Inc.*, United States Court of Appeals for the Seventh Circuit, 26 December 2002, Federal Reporter, 3rd series, vol. 314, p. 296.

(١٢٥) *Jonathan P. Shattuck v. David K. Klotzbach,* Superior Court of Massachusetts, 11 December 2001, 2001 Mass. Super. LEXIS 642.

(١٢٦) *Central Illinois Light Company v. Consolidation Coal Company*, United States District Court for the Central District of Illinois, Peoria Division, 30 December 2002, Federal Supplement, 2nd Series, vol. 235, p. 916.

(١٢٧) المرجع نفسه، صفحة ٩١٩: "يمكن استخدام المستندات والفواتير ورسائل البريد الإلكتروني الداخلية للوفاء بمقتضيات قانون الاحتيالات في القانون التجاري الموحد لولاية إلينوي". إلا أنه في القضية الواقعية، رأت المحكمة أن العقد المزعوم لا تتوفر فيه مقتضيات قانون الاحتيالات؛ لا لأن الرسائل الإلكترونية في حدّ ذاتها لم تستطع أن تسجل على نحو صحيح شروط العقد، ولكن لأنه لم يكن هناك ما يفيد بأن محرّري رسائل البريد الإلكتروني والأشخاص المذكورين فيها هم من مستخدمي المدعى عليه.

تلقت رسائل بالبريد الإلكتروني، فإن مقتضيات التوقيع القانونية تكون قد استوفيت إذ إن المحاكم "قد اعترفت منذ زمن طويل بأن التوقيع الملزم يمكن أن يأخذ شكل أي علامة أو دلالة يعتقد الطرف الذي سيُلزَم بأنها مناسبة"، شريطة أن تكون لدى المحرّر "النيّة في أن يلزم نفسه".[١٢٨]

١٠٨- وقد اتبعت محاكم في المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية نهجا مماثلا، حيث رأت عموما أن شكل التوقيع أقل دلالة من الوظيفة التي يؤديها. ومن ثم تنظر المحاكم في مدى ملاءمة الواسطة المستخدمة لإسناد سجل لشخص معيَّن، وكذلك لتبيان نية ذلك الشخص فيما يتعلق بذلك السجل، ولذلك يجوز أن تعدّ رسائل البريد الإلكتروني "مستندات"، كما يجوز أن تكون الأسماء المطبوعة على الرسائل الإلكترونية "توقيعات".[١٢٩] وقد أعلنت بعض المحاكم أنه "لا ريب عندها في أنه إذا أنشأ طرف مستندا إلكترونيا وأرسله عومل ذلك الشخص على أنه قد وقّعه، تماما مثلما يُعامل قانونا لو وقَّع على نسخة ورقية من المستند نفسه" وأن "المستند الذي يُنشَأ إلكترونيا لا يختلف عن النسخة الورقية".[١٣٠] وقد رفضت المحاكم أحيانا الاحتجاج بأن رسائل البريد الإلكتروني تشكل عقودا موقّعة لأغراض قانون الاحتيالات، وذلك أساسا لعدم وجود نيّة في الالتزام بالتوقيع. غير أنه لا توجد سابقة فيما يبدو رفضت فيها المحاكم مسبقا قدرة رسائل البريد الإلكتروني والأسماء المطبوعة فيها على الوفاء بمقتضيات الكتابة والتوقيع القانونية. وارتئي في بعض الحالات أن مقتضيات قانون الاحتيالات لم تُستوفَ لأن رسائل البريد الإلكتروني المعنية لم تبيّن إلا مفاوضات جارية لا اتفاقا نهائيا، وذلك مثلا لأن أحد الأطراف تصوّر أثناء المفاوضات أن عقدا ملزما سوف يُبرم بعد توقيع "مذكرة معاملة" وليس قبل ذلك.[١٣١] وفي قضايا أخرى أشارت المحاكم إلى أنها ربما كانت تميل إلى أن تقبل أن يُعتبر توقيعا "اسمُ المنشئ أو حروفه الأولى" في "نهاية رسالة البريد الإلكتروني" أو في "أي مكان آخر في متن رسالة البريد الإلكتروني"، إلا أنها رأت أن "إدراج عنوان الشخص في البريد الإلكتروني تلقائيا بعد إرسال المستند من قِبل]مقدِّم خدمات الإنترنت[المرسل أو المتلقّي أو كليهما" "لا يُقصد به أن يكون توقيعا".[١٣٢] ومع أن المحاكم البريطانية تُفسّر فيما يبدو مقتضيات الكتابة المنصوص عليها في قانون الاحتيالات تفسيرا أشدّ صرامة من نظيراتها في الولايات المتحدة، فهي تميل عموما إلى أن تجيز استخدام أي نوع من طرائق التوقيع أو التوثيق الإلكترونية، حتى خارج نطاق أي تفويض قانوني معيّن، ما دامت الطريقة المعنية تؤدي وظائف التوقيع الخطّي نفسها.[١٣٣]

---

[١٢٨] *Roger Edwards, LLC v. Fiddes & Son, Ltd.*, United States District Court for the District of Maine, 14 February 2003, Federal Supplement, 2nd Series, vol. 245, p. 251.

[١٢٩] *Hall v. Cognos Limited* (Hull Industrial Tribunal, Case No. 1803325/97) (unreported).

[١٣٠] *Mehta v. J. Pereira Fernandes S.A.* [2006] EWHC 813 (Ch), (United Kingdom, England and Wales High Court, Chancery Division), [2006] 2 Lloyd's Rep 244 (United Kingdom, England and Wales, Lloyd's List Law Reports).

[١٣١] *Pretty Pictures Sarl v. Quixote Films Ltd.*, 30 January 2003 ([2003] EWHC 311 (QB), (United Kingdom, England and Wales High Court, Law Reports Queen's Bench, [2003] All ER (D) 303 (January)) (United Kingdom, All England Direct Law Reports (Digests)).

[١٣٢] *Mehta v. J. Pereira Fernandes S.A.* ....

[١٣٣] *Mehta v. J. Pereira Fernandes S.A.* ..., No. 25، "تجدر ملاحظة أن رأي اللجنة القانونية فيما يتعلق بـ[توجيه الاتحاد الأوروبي بشأن التجارة الإلكترونية (2000/31/EC)] هو أنه لا تلزم أي تغييرات ذات شأن فيما يتعلق بقوانين تقضي بوجوب التوقيعات لأنه يمكن اختبار ما إذا كانت تلك المقتضيات قد استوفيت، وذلك بطريقة عملية هي الاستفسار عما إذا كان سلوك الموقّع المفترض يدل على نيّة التوثيق لشخص متعقل. . . . وهكذا، كما سبق أن قُلت، إذا طبع أحد الأطراف أو وكيل الطرف الذي يرسل رسالة بريد إلكتروني اسمه أو اسم أصيله في حدود ما يقضي به أو يسمح به قانون الدعوى في متن رسالة البريد الإلكتروني، يكفي ذلك في رأيي ليكون توقيعا لأغراض [قانون الاحتيالات]".

١٠٩- وتميل المحاكم في الولايات القضائية للبلدان التي تأخذ بالقانون المدني عموما إلى اتباع نهج أكثر تقييدا، ويحتمل أن يكون السبب هو أن مفهوم "المستند" في كثير من تلك البلدان يدل ضمنا في الأحوال الاعتيادية على استخدام شكل ما من التوثيق فيكاد يتعذّر من ثمّ الفصل بينه وبين "التوقيع". فالمحاكم في فرنسا، مثلا، كانت ممانعة لقبول الوسائل الإلكترونية لتعيين الهوية على أنها مكافئة للتوقيعات الخطّية، إلى حين اعتماد تشريع يعترف صراحة بصحة التوقيعات الإلكترونية.[١٣٤] وثمة اتجاه أكثر تحررا تتسم به القرارات التي تقبل تقديم الشكاوى الإدارية إلكترونيا وذلك لغرض التقيد بأجل محدد بموجب القانون، على الأقل ما دامت تؤكّد في وقت لاحق بمراسلات عادية.[١٣٥]

١١٠- وعلى العكس من النهج التقييدي الذي تتبعه المحاكم الألمانية بشأن إسناد رسائل البيانات في سياق تكوين العقود، كانت هذه المحاكم متحرّرة فيما يبدو في قبولها طرائق تعيين الهوية باعتبارها مكافئة للتوقيعات الخطّية في إجراءات المحاكم. فقد دار نقاش في ألمانيا حول ازدياد استخدام الصور الممسوحة إلكترونيا عن توقيع المحامي لتوثيق نسخ حاسوبية طبق الأصل تحتوي على عرائض استئناف مرسلة مباشرة من محطة حاسوب بواسطة جهاز توصيل معدّل كاشف (مودم) إلى آلة الفاكس الخاصة بالمحكمة. وفي قضايا سابقة، رأت محاكم الاستئناف[١٣٦] والمحكمة الاتحادية[١٣٧] أن الصورة الممسوحة إلكترونيا لتوقيع خطي لا تفي بمقتضيات التوقيع المطبّقة حاليا، ولا تقدّم أي إثبات لهوية الشخص. ويمكن تصور إلحاق تعيين الهوية بـ"توقيع إلكتروني متقدم" على النحو المعرّف في القانون الألماني. غير أن على المشرِّع لا المحاكم عموما وضع شروط التكافؤ بين الكتابة والخطابات غير المادية المرسَلة بوسائط نقل البيانات.[١٣٨] ولكن، نُقض هذا الفهم لاحقا نظرا لإجماع رأي محاكم اتحادية أخرى قبلت تسليم دفوع إجرائية معينة بواسطة إبلاغ إلكتروني لرسالة بيانات مرفقة بصورة ممسوحة إلكترونيا للتوقيع.[١٣٩]

---

[١٣٤] رفضت محكمة النقض في فرنسا قبول عريضة استئناف كانت موقّعة إلكترونيا، نظرا لوجود ارتياب بشأن هوية الشخص الذي أنشأ التوقيع، وكان طلب الاستئناف قد وقّع إلكترونيا قبل نفاذ قانون ١٣ آذار/ مارس ٢٠٠٠، الذي اعترف بالمفعول القانوني للتوقيعات الإلكترونية (Cour de cassation, Deuxième chamber civile, 30 avril 2003, Sté Chalets Boisson c/ M. X.)، النص متاح في الموقع الشبكي www.juriscom.net/jpt/visu.php?ID=239، وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨.

[١٣٥] France, Conseil d'État, 28 December 2001, No. 235784, *Élections municipales d'Entre-Deux-Monts* (النسخة الأصلية متاحة لدى الأمانة).

[١٣٦] على سبيل المثال، قضية لدى محكمة الاستئناف في ألمانيا Oberlandesgericht (Court of Appeal) Karlsruhe, Case No. 14 U 202/96, 14 November 1997, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht,* JurPC Web-Dok. No. 09/1998، النص متاح في الموقع الشبكي www.jurpc.de/rechtspr/19980009.htm (وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٣٧] Germany, Bundesgerichtshof (Federal Court of Justice), Case No. XI ZR 367/97, 29 September 1998 *JurPC – Internet-Zeitschrift für Rechtsinformatik und Informationsrecht,* JurPC Web-Dok No. 05/1999، النص متاح في الموقع الشبكي http://www.jurpc.de/rechtspr/19990005.htm (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٣٨] المرجع نفسه.

[١٣٩] عند البت في قضية أحيلت من المحكمة الاتحادية في ألمانيا إلى الغرفة المشتركة للمحاكم الاتحادية العليا في ألمانيا، لاحظت الغرفة المشتركة أن مقتضيات الشكل في إجراءات المحاكم ليست غاية في حد ذاتها. فالغرض منها هو ضمان تحديد مضمون الرسالة وهوية الشخص الذي صدرت منه على نحو يكفي للاعتماد عليه. ولاحظت الغرفة المشتركة التطور الحاصل في تطبيق مقتضيات الشكل عمليا بحيث تستوعب تطورات تكنولوجية سابقة، مثل التلكس أو الفاكس. ورأت الغرفة المشتركة أن قبول تسليم دفوع إجرائية معينة بوسائل الاتصال الإلكتروني مع صورة ممسوحة إلكترونيا عن التوقيع يكون متمشيا مع روح قانون السوابق القائم (Gemeinsamer Senat der obersten Gerichtsh?fe des Bundes, GmS-OGB 1/98, 5 April 2000, *JurPC-Internet Zeitschrift für Rechtsinformatik und Informationsrecht,* JurPC WebDok No.160/2000، النص متاح في الموقع الشبكي http://www.jurpc.de/rechtspr/20000160.htm (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

١١١- ومما تجدر ملاحظته أن هناك محاكم حتى في بعض الولايات القضائية الخاضعة للقانون المدني، التي اعتمدت تشريعات تؤيّد استخدام توقيعات رقمية تستند إلى مرافق المفاتيح العمومية (PKI)، مثل كولومبيا،[١٤٠] قد اتّبعت نهجا متحررا مماثلا، وأكدت، على سبيل المثال، جواز قبول إجراءات قضائية تتمّ كليا بواسطة اتصالات إلكترونية. وارتئي أن المستندات المتبادلة أثناء تلك الإجراءات صحيحة حتى إن لم تكن موقّعة بتوقيع رقمي، حيث إن الاتصالات الإلكترونية تستخدم طرائق تتيح المجال لتعيين هوية الأطراف.[١٤١]

١١٢- ولكنْ، لا تزال السوابق القضائية المتعلقة بالتوقيعات الإلكترونية نادرة، والعدد القليل من قرارات المحاكم الصادرة في هذا الصدد حتى الآن لا يوفر أساسا كافيا لاستخلاص استنتاجات ثابتة. ومع ذلك، يكشف استعراض مختصر لما يوجد من سوابق عدّة اتجاهات متّبعة. فالنهج التشريعي المتّبع إزاء التوقيعات الإلكترونية والتوثيق الإلكتروني يبدو أنه أثّر على موقف المحاكم بشأن هذه المسألة. ويحتمل أن التركيز التشريعي على "التوقيعات" الإلكترونية، من دون وجود قاعدة عامة مصاحبة لذلك بشأن الإسناد، قد أدى إلى إفراط في توجيه الانتباه إلى وظيفة تعيين الهوية التي تؤديها طرائق التوثيق. وقد أحدث ذلك في بعض البلدان قدرا من انعدام الثقة حيال أي طرائق للتوثيق لا تفي بالتعريف القانوني لماهية "التوقيع" الإلكتروني. ولذلك، ليس من المؤكد أن المحاكم ذاتها التي اتّبعت نهجا متحررا في سياق دعاوى الاستئناف القضائية أو الإدارية سوف تكون متحررة بنفس القدر فيما يتعلق بمقتضيات التوقيع بخصوص إثبات صحة العقود، فبينما قد يواجه أحد الطرفين فعلا، في سياق تعاقدي، مخاطرة خرق الاتفاق من جانب الطرف الآخر، فإنه في سياق الإجراءات المدنية عادة ما يكون الطرف الذي يستخدم توقيعات أو سجلات إلكترونية هو المهتم بتأكيد موافقته على السجل ومضمونه.

٣- الجهود المبذولة من أجل استحداث مكافئات إلكترونية لأشكال خاصة من التوقيعات

(أ) التطبيقات الدولية: مذكرات التصديق الإلكترونية

١١٣- اجتمعت لجنة خاصة في لاهاي من ٢٨ تشرين الأول/ أكتوبر إلى ٤ تشرين الثاني/ نوفمبر ٢٠٠٣ لاستعراض التطبيق العملي لاتفاقية لاهاي اللاغية لشرط التصديق القانوني على الوثائق العامة الأجنبية (اتفاقية لاهاي بشأن مذكرات التصديق)، واتفاقية لاهاي بشأن خدمة تبليغ الوثائق القضائية وغير القضائية في الخارج فيما يتعلق بالمسائل المدنية أو التجارية[١٤٢] (اتفاقية لاهاي بشأن خدمة التبليغ)، والاتفاقية المتعلقة

---

[١٤٠] اعتمدت كولومبيا، مثلا، قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، بما فيه الأحكام العامة للمادة ٧، لكنها أنشأت قرينة قانونية للصحة فيما يتعلق بالتوقيعات الإلكترونية فقط (*قانون التجارة الإلكترونية*، (المادة ٢٨)).

[١٤١] كولومبيا، Juzgado Segundo Promiscuo Municipal Rovira Tolima, *Juan Carlos Samper v. Jaime Tapias*, 21 July 2003, Rad. 73-624-40-89-002-2003-053-00: في هذه القضية، انتهت المحكمة إلى أن العملية المنفّذة بواسطة وسائل إلكترونية صحيحة رغم أن رسائل البريد الإلكتروني لم تكن موقّعة رقميا، وذلك للأسباب التالية: *(أ)* أمكن تعيين هوية مرسل رسائل البيانات تماما؛ *(ب)* وافق مرسل رسائل البيانات على مضمون رسائل البيانات المرسلة وأكده؛ *(ج)* حفظت رسائل البيانات في أمان في المحكمة؛ *(د)* أمكن استعراض الرسائل في أي وقت (النص متاح في الموقع الشبكي http://www.camara-e.net/_upload/80403-0-7-diaz082003.pdf-، وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٤٢] الأمم المتحدة، *مجموعة المعاهدات*، المجلد ٦٥٨، الرقم ٩٤٣٢.

بالحصول على الأدلة خارج البلد في المسائل المدنية أو التجارية، (اتفاقية لاهاي بشأن الحصول على الأدلة).[١٤٣] وحضر اجتماع اللجنة الخاصة بشأن التطبيق العملي للاتفاقيات بشأن مذكرات التصديق وخدمة التبليغ والحصول على الأدلة ١١٦ مندوبا يمثلون ٥٧ دولة من الدول الأعضاء والدول الأطراف في واحدة أو أكثر من الاتفاقيات قيد الاستعراض والدول التي لها صفة مراقب. وشدّدت اللجنة الخاصة على أن الاتفاقيات الثلاث تطبق في بيئة خاضعة لتطورات تقنية مهمة. ومع أنه لم يكن بالإمكان توقع هذا التطور حينَ اعتماد الاتفاقيات الثلاث، فقد أكدت اللجنة الخاصة أن التكنولوجيات الحديثة جزء لا يتجزأ من مجتمع اليوم وأن استعمالها أمر واقع.[١٤٤] وفي هذا الصدد، لاحظت اللجنة الخاصة أن روح ونص الاتفاقيات المذكورة لا يشكلان عقبة أمام استخدام التكنولوجيا الحديثة وأنه يمكن زيادة تحسين تطبيقها وتنفيذها بالاعتماد على تلك التكنولوجيا.[١٤٥] وأوصت اللجنة الخاصة بأن تتعاون الدول الأطراف في تلك الاتفاقيات مع المكتب الدائم لمؤتمر لاهاي للقانون الدولي الخاص على وضع تقنيات لتطبيق مذكرات تصديق إلكترونية "مع مراعاة جملة أمور منها قانونا الأونسيترال النموذجيان بشأن التجارة الإلكترونية وبشأن التوقيعات الإلكترونية، اللذان يستندان كلاهما إلى مبدأي عدم التمييز والتكافؤ الوظيفي".[١٤٦] وفي نيسان/ أبريل ٢٠٠٦، أطلق المكتب الدائم لمؤتمر لاهاي للقانون الدولي الخاص ورابطة الكتاب العدول الوطنية في الولايات المتحدة البرنامج الرائد الخاص بمذكرات التصديق الإلكترونية (e-APP). وفي إطار هذا البرنامج الرائد، يعمل مؤتمر لاهاي والرابطة، إلى جانب أي دولة مهتمة، من أجل ترويج نماذج من البرامجيات الحاسوبية والمساعدة في تطبيقها، لأجل: *(أ)* إصدار واستخدام مذكرات التصديق الإلكترونية و*(ب)* تشغيل سجلات إلكترونية خاصة بمذكرات التصديق الإلكترونية.[١٤٧] ويتناول البرنامج الرائد صيغتين منفصلتين، ولكن متطابقتين في نهاية الأمر، من مذكرات التصديق الإلكترونية. وكلتا الطريقتين تحمي المستند الأساسي وشهادة التصديق الإلكترونية من التعديلات غير المأذون بها، غير أن كلا منهما تمثل صلة وصل مختلفة فيما يتعلق بالمتلقي.

١١٤- فبمقتضى الطريقة الأولى، يمكن أن تضيف السلطة المختصة في صيغة معيّنة شهادة التصديق باعتبارها الصفحة الأخيرة من المستند العام الأساسي (ينص البرنامج الرائد على تبادل المستندات في صيغة الوثيقة المحمولة (بي-دي-أف) (PDF). فالمتلقي يفتح الملف ويجد شهادة التصديق الإلكترونية مدرجة باعتبارها الصفحة الأخيرة من المستند. وفي حال اختيار هذه الصيغة، فإن المستند العام الأساسي وشهادة التصديق الإلكترونية يشكلان مستندا متصلا واحدا أو بعبارة أخرى ملفا إلكترونيا واحدا. ويمكن للمرء مع ذلك أن يطبع صفحة أو أكثر من هذا الملف الوحيد، بحيث يتسنى طبع شهادة التصديق الإلكترونية على حدة.[١٤٨]

---

[١٤٣] المرجع نفسه، المجلد ٨٤٧، الرقم ١٢١٤٠.

[١٤٤] مؤتمر لاهاي للقانون الدولي الخاص، "Conclusions and recommendations adopted by the Special Commission on the Practical Operation of the Hague Apostille, Evidence and Service Conventions: 28 October to 4 November 2003" para.4 (متاح على الموقع الشبكي http://hcch.e-vision.nl/upload/ wop/lse_concl_e.pdf، وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٤٥] مؤتمر لاهاي للقانون الدولي الخاص، "Conclusions and recommendations adopted by the Special Commission ...".

[١٤٦] مؤتمر لاهاي للقانون الدولي الخاص، "Conclusions and recommendations adopted by the Special Commission ..." , para.24.

[١٤٧] "Electronic Apostille Pilot Program (e-APP): memorandum on some of the technical aspects underlying the suggested model for the issuance of electronic apostilles (e-apostilles)" Christophe Bernasconi and Rich Hansberger (متاح على الموقع الشبكي http://www.hcch.net/upload/ wop/genaff_pd18e2007.pdf ، وقد اطلع عليه في ٢٦ أيار/ مايو ٢٠٠٨).

[١٤٨] "Electronic Apostille Pilot Program ..." para. 18",

١١٥- أما الطريقة الثانية فتقتضي إلحاق المستند العام الأساسي كملف منفصل بشهادة التصديق الإلكترونية. وحتى في هذه الحالة، فإن المتلقي يتلقى ملفا واحدا بصيغة "بي-دي-أف"، إلا أن المستعمل عند فتح الملف يرى أولا شهادة التصديق الإلكتروني، ويمكنه بعد ذلك أن يفتح المستند العام الأساسي الملحق بتلك الشهادة ليطلع عليه كملف منفصل بصيغة "بي-دي-أف". وارتئ أن هذه الطريقة توفر لمتلقي المستند المصدَّق عليه وسيطا أكثر بداهة (وهي الطريقة التي اعتمدتها، على سبيل المثال، وزارة الخارجية في الولايات المتحدة فيما يتعلق بطلباتها الإلكترونية بشأن إيداع براءات الاختراع وباعتبارها نموذجا لمذكرات التصديق الإلكترونية). والغاية من إرفاق المستند العام الأساسي كملف بشهادة التصديق الإلكترونية أن يتبيَّن للمتلقي بوضوح شديد عندما يفتح المستند أولَ الأمر أنه بصدد مذكرة تصديق. ومن هنا يمكنه أن يفتح بعد ذلك المستند العام الأساسي للاطلاع على محتوياته."[١٤٩]

١١٦- ويقتضي أي من النموذجين أن يتضمن تطبيق مذكرات التصديق إصدار شهادات في شكل إلكتروني توقعها السلطة المختصة المناسبة توقيعا رقميا لأغراض اتفاقية لاهاي بشأن مذكّرات التصديق. وتحتفظ كل سلطة مختصة إضافةً إلى ذلك بسجل في شكل إلكتروني يتيح التحقق من الشهادات الصادرة لتأييد مذكرات التصديق.[١٥٠]

١١٧- وفي البلدان التي ألغت مقتضيات التصديق القانوني أو تقديم مذكرات التصديق، يمكن وضع نظم يُمنح بواسطتها الاعتراف القانوني بالتسجيلات الأجنبية الموثّقة توثيقا عدليا بناء على التحقق من طرائق التوقيع أو التوثيق الإلكترونية التي استعملها الكاتب العدل الأصلي. ويجب على مستعمل المستند (وهو عادة كاتب عدل آخر) أن يتحقق من التوقيع الإلكتروني للكاتب العدل الأصلي بطريقة بسيطة وسريعة. ويمكن القيام بذلك عن طريق الإنترنت بالدخول إلى موقع الجهة التي تقدم خدمات التصديق إلى الكاتب العدل الأصلي، وهي عادة ما تكون، في أوروبا على الأقل، هي الغرفة الوطنية التي ينتمي إليها الكاتب العدل. وهناك مسألة ذات صلة بهذا الموضوع، وهي التحقق من صلاحية الكاتب العدل الأصلي لتوثيق المستندات بمقتضى النظام القانوني الذي يعمل في إطاره. ومن أجل تيسير هذه العملية وتجنب الحاجة إلى استشارة هيئة الإشراف الأجنبية المكلفة بالترخيص للكتاب العدول، إن وجدت، اقتُرح أن تقتصر جهات تقديم خدمات التصديق المنشأة تحت إشراف غرف الكتاب العدول على إصدار الشهادات للكتاب العدول المأذون لهم في ذلك الوقت بمزاولة وظيفة الكاتب العدل بحيث يترتب تلقائيا على أي تعليق أو إلغاء لصلاحية الكاتب العدل منع التحقق من توقيع الكاتب العدل.[١٥١]

---

[١٤٩] "Electronic Apostille Pilot Program ..." para. 19,

[١٥٠] للاطلاع على مزيد من المعلومات عن تطبيق مذكرات التصديق، انظر الموقع الشبكي للبرنامج الرائد الخاص بمذكرات التصديق الإلكترونية (e-APP)، في العنوان التالي: http://www.e-app.info/ (اطلع عليه في ٦ حزيران/يونيه ٢٠٠٨).

[١٥١] "La signature électronique transfrontalière des notaires: une réalit européenne" *La semaine juridique (édition notariale et immobilière)*, No. 39, 24 September 2004, p. 1447. Ugo Bechini and Bernard Reynis.

(ب) التطبيقات الداخلية: الأختام والتوثيق العدلي والإشهاد

١١٨- لقد ألغت بعض الولايات القضائية اقتضاءَ الأختام بناء على أن الخَتم لم يعد مناسبا اليوم، ثم حلّ محله توقيع مصدّق عليه بالإشهاد (أي بشهادة شاهد).[١٥٢] وتوجد في ولايات قضائية أخرى تشريعات تسمح بالتوقيعات الإلكترونية الآمنة تلبية لاقتضاء المهر بختم. فمثلا، توجد لدى إيرلندا أحكام محددة خاصة بالتوقيعات الإلكترونية الآمنة، مع ما يناسبها من التصديق، تُستخدم بدلا من الأختام، رهنا بموافقة الشخص المعني أو الهيئة العمومية المعنية، أي من يلزم أن يعطى لـه المستند الممهور بالختم، أو مَن هو مسموح بأن يُعطى لــه.[١٥٣] وتنص كندا على أن المقتضيات بشأن وجود خاتم الشخص المعني المنصوص عليها بموجب قوانين اتحادية معيّنة، إنما تُستوفى بتوقيع إلكتروني آمن يعرّف التوقيع الإلكتروني الآمن بأنه خاتم ذلك الشخص.[١٥٤]

١١٩- كما أطلق عدد من البلدان مبادرات تتوخّى استخدام المستندات والتوقيعات الإلكترونية في المعاملات العقارية التي تنطوي على سندات عقارية. والنموذج المستخدم في فكتوريا، أستراليا، يتوخى استخدام تكنولوجيا التوقيعات الرقمية الآمنة عبر الإنترنت ببطاقات رقمية تصدرها هيئة تصديق. وفي المملكة المتحدة، يتوخى النموذج أن يقوم محامو الإجراءات بإنشاء السندات العقارية نيابة عن موكليهم عبر الإنترنت. وفي بعض التشريعات يُعترف بإمكانية استخدام "أختام إلكترونية" كبديل لـلأختام اليدوية، مع ترك التفاصيل التقنية عن شكل الخاتم الإلكتروني ليُبتَّ فيها منفصلة.[١٥٥]

١٢٠- وأمّا قانون الولايات المتحدة الموحَّد لتسجيل الأملاك العقارية إلكترونيا،[١٥٦] فهو ينص صراحة على أن من غير الضروري أن يكون التوقيع الإلكتروني مصحوبا بصورة مادية أو إلكترونية لدمغة أو شارة أو خاتم. فالمطلوب أساسا هو المعلومات المبيَّنة على الخاتم لا الخاتم نفسه. كما ينص ذلك القانون على أن التوقيع الإلكتروني يفي بأغراض أي تشريع أو لائحة تنظيمية أو معيار يقتضي دمغة أو بصمة أو ختما

---

[١٥٢] مثلا، قانون الملكية في المملكة المتحدة، Law of Property (Miscellaneous Provisions) Act 1989، الذي نَفّذ تقرير لجنة إصلاح القانون، Law Reform Commission Report on "Deeds and escrows" (Law Com. No. 143, 1987).

[١٥٣] إيرلندا، قانون التجارة الإلكترونية (Electronic Commerce Act, section 16.) ولكن، عندما يلزم إعطاء المستند المراد ختمه لهيئة عمومية أو لشخص يتصرف نيابة عن هيئة عمومية، أو يُسمح بأن يعطى لهذه الهيئة أو لهذا الشخص، يجوز مع ذلك للهيئة العمومية التي توافق على استخدام توقيع إلكتروني أن تطلب أن يكون وفقا لتكنولوجيا معلومات معينة ولمقتضيات إجرائية معينة.

[١٥٤] كندا، قانون حماية المعلومات الشخصية والمستندات الإلكترونية (٢٠٠٠)، Personal Information Protection and Electronic Documents Act (2000), part 2, section 39. والقانونان الاتحاديان المشار إليهما هما القانون الاتحادي للأملاك العقارية والأملاك المنقولة، واللوائح الاتحادية للأملاك العقارية Federal Real Property and Federal Immovables Act وFederal Real Property Regulations.

[١٥٥] توجد أمثلة على المقتضيات المتعلقة بإثبات صحة مستندات من جانب ممتهنين مرخصين أو مسجلين، مثل قانون المهن الهندسية والجيوعلمية (مانيتوبا، كندا)، Engineering and Geoscientific Professions Act (Manitoba, Canada)، الذي يعرِّف الخاتم الإلكتروني "بأنه شكل إثبات الهوية الذي تصدره الرابطة لأي من أعضائها ليُستخدم في إثبات صحة المستندات إلكترونيا في شكل قابل للقراءة حاسوبيا (انظر http://apegm.mb.ca/keydocs/act/index.html اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٥٦] أعد مؤتمر الولايات الوطني للمأمورين القضائيين بشأن قوانين موحدة للولايات (National Conference of Commissioners on Uniform State Laws)، قانون الولايات الموحَّد لتسجيل الأملاك إلكترونيا (Uniform Real Property Electronic Recording Act of the United States)، وهو متاح في الموقع الشبكي http://www.law.upenn.edu/bll/ulc/urpera/URPERA_Final_Apr05-1.htm، (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨). وقد اعتمد في ولايات أريزونا وأركانساس وديلاوير ومقاطعة كولومبيا، وكونيتيكات وفلوريدا وأيداهو وإيلينوي وكانساس ومينيسوتا ونيفادا ونيومكسيكو وكارولينا الشمالية وكارولينا الجنوبية وتينيسي وتكساس وفرجينيا وواشنطن وويسكنسن (انظر الموقع الشبكي http://www.nccusl.org، اطلع عليه في ٢٠ آذار/ مارس ٢٠٠٨).

لشخص أو كيان اعتباري. وهذه العلامات المادية غير قابلة للتطبيق على مستند إلكتروني كليا. ومع ذلك، يقضي هذا القانون بأن تكون المعلومات التي كانت ستتضمنها الدمغة أو الشارة أو الختم مرفقةً بالمستند أو التوقيع أو مرتبطة بهما منطقيا بطريقة إلكترونية.[١٥٧] وبذلك لا تكون دمغة أو شارة التوثيق العدلي اللازمة بموجب قوانين بعض الولايات لازمة للتوثيق العدلي الإلكتروني بموجب هذا القانون. ولا لزوم أيضا لدمغة أو شارة كيان اعتباري خلافا لما تقتضيه قوانين بعض الولايات لإثبات تصرّف قام به موظف مسؤول في كيان اعتباري.

١٢١- وليس من الشائع استخدام الأختام في المستندات الخاصة في الولايات القضائية الآخذة بالقانون المدني، وإن كان معظم تلك الولايات القضائية يستخدم التوثيق العدلي على نطاق واسع كوسيلة للتأكد من هوية الأشخاص وصحة المستندات. وفي عدة ولايات قضائية خاضعة للقانون المدني اعتمد الكتاب العدول بالفعل تكنولوجيات المعلومات والاتصالات كأداة اعتيادية في عملهم. وفي كثير من البلدان، أنشأت غرف الكتاب العدول هيئات لتقديم خدمات التصديق تتولى إصدار شهادات تصديق تدعم استخدام التوقيعات الإلكترونية (وهي عادة توقيعات رقمية) من جانب الكتاب العدول الأعضاء فيها وفي بعض الأحيان من جانب عموم الناس.

١٢٢- ففي إيطاليا، أذنت هيئة تكنولوجيا المعلومات في الحكومة لمجلس الكتاب العدول في ١٢ أيلول/ سبتمبر ٢٠٠٢ بأن يقدم خدمات التصديق للكتاب العدول الإيطاليين، الذين يمكن التحقق من توقيعاتهم الرقمية على الإنترنت.[١٥٨] وعلاوة على ذلك، فإن الكتاب العدول الإيطاليين بصدد الانتقال التام نحو استخدام التكنولوجيات الإلكترونية لإرسال التسجيلات إلى السجلات العمومية. ففيما يتعلق بنقل المذكرات والنظم الأساسية وتعديلاتها إلى السجلات التجارية، على سبيل المثال، استُبعدت المستندات الورقية استبعادا تاما. وأُحرز أيضا تقدم ملحوظ فيما يتعلق بالإرسال الإلكتروني لتسجيلات الصفقات المتعلقة بأملاك عقارية، رغم أن المستندات الورقية لا تزال مستعملة، لأسباب تعزى حسبما يُزعم إلى التأخر في الأخذ بتكنولوجيات الاتصالات الإلكترونية في نظام المحاكم. وتقدم هذه الخدمات بدعم من هيئة أنشأها المجلس والصندوق الوطني للكتاب العدول في عام ١٩٩٧ خصيصا لأغراض تجهيز خدمات تكنولوجيا المعلومات والاتصالات المقدمة للكتاب العدول الإيطاليين.[١٥٩] ويستخدم نظام مماثل في إسبانيا حيث أنشأ المجلس العام للكتاب العدول هيئته الخاصة بالتصديق وحيث استحدث الكتاب العدول نظاما للإيداع الإلكتروني للتسجيلات في السجلات التجارية.[١٦٠]

١٢٣- وفي فرنسا، يسمح النص المنقّح للمادة ١٣١٧ من القانون المدني، على سبيل المثال، بتدوين "السندات الصحيحة" بالوسائل الإلكترونية وفق شروط يحددها مجلس الدولة. وأنشأ مجلس الكتاب العدول الأعلى الفرنسي نظاما للتصديق على التوقيعات الرقمية التي يستخدمها الكتاب العدول الفرنسيون.[١٦١] وتصدِّق على النظام الذي يستخدمه الكتاب العدول الفرنسيون هيئة أنشأتها عدة وكالات تابعة للحكومة الفرنسية بهدف تقديم خدمات التصديق. ورغم أن الكتاب العدول الفرنسيين لا يستخدمون

[١٥٧] وهي معايير مماثلة للمعايير الراسخة في قانون الولايات المتحدة الموحد للمعاملات الإلكترونية.

[١٥٨] انظر http://ca.notariato.it (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٥٩] انظر الباب "Servizi Notartel" في الموقع www.notariato.it (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٦٠] انظر http://www.notariado.org/n_tecno (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٦١] "La signature électronique notariale certifiée", *La revue fiscale notariale,* No. 10, October 2007, Alerte 53.

حتى الآن الإرسال الإلكتروني للتسجيلات بنفس القدر الذي يستخدمه الكتاب العدول الإيطاليون والإسبان، فإن استحداث التطبيق الحاسوبي لنقل المستندات عن بعد (Télé@actes) في أيار/ مايو ٢٠٠٦ لا بد أن يمكّن الكتاب العدول من تبادل سندات الملكية مع مكاتب تسجيل الرهن العقاري في شكل إلكتروني تام. ويجري الاضطلاع أيضا بأعمال ترمي إلى تحويل النسخ الورقية لسندات الملكية العقارية إلى الشكل الرقمي.

١٢٤- وفي ألمانيا، أتاح القانون الاتحادي لعام ١٩٩٣ بشأن تعجيل إجراءات التسجيل[١٦٢] إمكانية تنفيذ مقتضيات التسجيل القانونية العقارية والتجارية وغيرها في الشكل الإلكتروني. واستفادت الإدارات القضائية دون الوطنية من هذه الإمكانية بدرجات متفاوتة ومن خلال نهوج تقنية مختلفة.[١٦٣] وتمكن الكتاب العدول الألمان بفضل استحداث نظام تسجيل إلكتروني من تبادل المعلومات مباشرة مع نظم التسجيل بوسائل الاتصالات الإلكترونية. ومن أجل ضمان اتسام التسجيلات الإلكترونية الموثقة توثيقا عدليا بنفس القدر من الموثوقية الذي تتسم به التسجيلات الورقية الموثقة توثيقا عدليا، أنشأ الكتاب العدول الألمان هيئة لتقديم خدمات التصديق وفقا لمقتضيات القانون الألماني للتوقيعات الإلكترونية. ومنحت الهيئة الألمانية لتنظيم الاتصالات رخصة لمقدم خدمات التصديق في ١٥ كانون الأول/ ديسمبر ٢٠٠٠. وكما هو الحال بالفعل في بلدان أخرى، فإن نظام التصديق الذي أنشأه الكتاب العدول الألمان هو نظام مستند إلى مَرفِق مفاتيح عمومية (PKI) يستخدم تكنولوجيا التوقيع الرقمي. ولا تقتصر الشهادات التي تصدرها هيئة تقديم خدمات التصديق التابعة لغرفة الكتاب العدول الاتحادية على التصديق على المفتاح العمومي الذي استخدمه الكاتب العدل للتوقيع على المستندات، بل هي تصدِّق أيضا على صلاحية الموقِّع بصفته كاتبا عدلا محلَّفا. وبمقتضى النظام الألماني، تُستَخدَم التوقيعات الرقمية لتوثيق التسجيلات وقت إنشائها وكذلك عند كل استنساخ لها. وفي المبادئ التوجيهية الصادرة عن غرفة الكتاب العدول الاتحادية، ورد تذكير الكتاب العدول بضرورة كفالة إرسال المستندات الإلكترونية بطريقة آمنة، وذلك بألاّ يستخدموا على سبيل المثال إلا التوصيلات الآمنة المستندة إلى بروتوكول التشفير الآمن (SSL).[١٦٤] ومن أجل تيسير تجهيز التسجيلات الإلكترونية في نظم التسجيل أو استخدام الزبائن لها، يُلزم الكتاب العدول الألمان بإعداد المستندات في صيغة معيارية (لغة التوسيم الموسعة، أو اختصارا XML).[١٦٥] وتقتضي القواعد الألمانية المتعلقة بإصدار التسجيلات الإلكترونية الصحيحة مستويين من التوثيق من جانب الكاتب العدل، وذلك بأن تُوصَل جميعُ التسجيلات الإلكترونية، مشفوعة بمرفقاتها والملفات المحتوية على التوقيع الرقمي للكاتب العدل، وتُحفَظ معاً في صيغة ملف مضغوط (ZIP)، ثم يوثَّق الملف المضغوط مرة أخرى بواسطة التوقيع الرقمي للكاتب العدل.

١٢٥- وهناك أيضا استخدام متزايد للمكافئات الإلكترونية للصكوك الموثقة توثيقا عدليا في النمسا. والنظام النمساوي للتوثيق العدلي الإلكتروني شبيه عموما بالنظام الألماني من حيث سماته الأساسية. غير أن إحدى السمات الخاصة للنظام النمساوي تتمثل في إنشاء سجل إلكتروني مركزي (محفوظات المستندات

---

[١٦٢] Germany Bundesgesetztblatt, part I, 20 December 1993, p. 2182.

[١٦٣] انظر المعلومات المتعلقة بمدى تطبيق غرفة الكتاب العدول الاتحادية للسجلات الإلكترونية في ألمانيا في الموقع التالي http://www.bnotk.de/Service/Elektronischer_Rechtsverkehr/Registerelektronisierung.html (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٦٤] انظر "*Empfehlungen zur sicheren Nutzung des Internet*", Rundschreiben 13/2004 der Bundesnotarkammer vom 12.03.2004، متاح في الموقع الشبكي http://www.bnotk.de/Service/Rundschreiben/RS.2004.13.sichere.Internetnutzung.html (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٦٥] انظر *"Hinweise und Anwendungsempfehlungen für den elektronischen Handels-, Genossenschafts- und Partnerschaftsregisterverkehr"* Rundschreiben 25/2006 der Bundesnotarkammer vom 07.12.2006، متاح في الموقع الشبكي http://www.bnotk.de/Service/Empfehlungen+Hinweise/RS25-06_El-Handelsregisterverkehr.html (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

الإلكترونية) ("cyberDOC") لحفظ المستندات بأمان في شكل إلكتروني. فهناك شركة مستقلة اشتركت في إنشائها غرفة الكتاب العدول الخاضعين للقانون المدني النمساوية وشركة سيمنس، وهي توفر للكتاب العدول محفوظات إلكترونية تتضمن وظائف توثيقية.[١٦٦] والكتاب العدول النمساويون ملزمون بموجب القانون بتسجيل وتخزين جميع سندات التوثيق العدلي المنشأة بعد ١ كانون الثاني/ يناير ٢٠٠٠ في هذا النظام الخاص بالمحفوظات.

١٢٦- وفي حين أن وظيفة الكاتب العدل المتعلقة بتوثيق التوقيعات يمكن بوجه عام تكرارها في بيئة إلكترونية باستخدام طرائق التوثيق والتوقيع الإلكترونية، فإن هناك وظائف أخرى تتطلب حلولا أوسع نطاقا. ويجب عادة أن تذكر الصكوك الموثقة توثيقا عدليا، حسب الاقتضاء، تاريخ إنشائها وتاريخ تسجيلها وتاريخ توقيعها أو استنساخها. وارتئ أن مجرد استخدام التقنيات الآلية يمكن أن يكون بديلا عن التاريخ المصدّق عليه من كاتب عدل.[١٦٧]

١٢٧- ولكنّ الأهمَّ من ذلك هو إجراءات حفظ التسجيلات الإلكترونية للصكوك الموثقة توثيقا عدليا. فالقانون يُلزم الكتاب العدول عادة بحفظ سجل للمستندات التي يتلقونها أو يصدرونها. ويطرح استنساخ هذا السجلَ العام في بيئة إلكترونية عددا من التحديات. وهناك مشكلة أخرى—أكبر من ذلك— تكمن في خطر عدم التوافق التقني بين مختلف البرامجيات والمعدات التي قد يستخدمها الكتاب العدول لهذا الغرض. فبسبب التطور السريع لتكنولوجيات المعلومات والاتصالات، تتعاظم الحاجة إلى نقل البيانات من صيغة أو من واسطة إلى أخرى. غير أن قابلية قراءة البيانات المنقولة إلى صيغ ووسائط جديدة غير مضمونة في كل الأحوال. وهذا يستدعي استحداث إجراءات رقابية تتيح التحقق من سلامة محتويات السجل قبل النقل وبعده. وكما سبقت الإشارة إلى ذلك، فإن تكنولوجيا التشفير المستندة إلى مرافق المفاتيح العمومية (PKI) لا تضمن بالضرورة مقروئية التوقيعات الرقمية نفسها مع مرور الوقت (انظر الفقرة ٥١ أعلاه). وهذا يتطلب إدارة متأنية لعملية النقل وربما تأكيد التوثيق المستخدم في الأصل. وقد تبين أن من الأفضل، لضمان الاتساق وقابلية الاستخدام التبادلي، أن يُعهد بهذه الوظيفة إلى طرف آخر موثوق به لا إلى كل كاتب من الكتاب العدول.[١٦٨]

١٢٨- وهذا، على سبيل المثال، هو النموذج الذي اختاره المشرعون الفرنسيون آخرَ الأمر. فالإصلاح الذي أجري حديثا للقواعد المنظِّمة للتسجيلات الموثقة توثيقا عدليا يحدِّد عموما شروط التكافؤ الوظيفي بين الصكوك الورقية الموثّقة توثيقا عدليا والسجلات الإلكترونية.[١٦٩] ومن الأحكام المتعلقة أساسا بأمن المعلومات ما نصت عليه القواعد الجديدة من إنشاء نظام محفوظات مركزي للسندات الموثقة توثيقا عدليا في الشكل الإلكتروني يكفل حفظ السجلات الإلكترونية بطريقة تصون سلامتها؛ وعدم إتاحة الوصول إليها إلا للكتاب العدول الذين ينشؤونها؛ ونقلها إلى صيغ جديدة حسبما تقتضيه الضرورات التقنية دون تغيير محتواها؛ وتمكين الكاتب العدل من تدوين معلومات لاحقة دون تغيير المحتوى الأصلي لتلك السجلات.

---

[١٦٦] انظر Österreichische Notariatskammer (Austrian Chamber of Civil Law Notaries)، (غرفة الكتاب العدول الخاضعين للقانون المدني النمساوية)، متاح في الموقع الشبكي http://www.notar.at، تحت العنوان "Cyberdoc"، (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٦٧] Didier Froger, "Les contraintes du formalisme et de l'archivage de l'acte notarié établi sur support dématérialisé", La semaine juridique (édition notariale et immobilière), No. 11, 12 March 2004, p. 1130.

[١٦٨] Didier Froger, "Les contraintes du Formalisme ..."

[١٦٩] France. "Décret n 2005-973 du 10 août 2005 modifiant le décret n 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires", Journal Officiel, 11 August 2005, p. 96.

١٢٩- ورغم التقدم الحاصل في السنوات الأخيرة، لا تزال بعض الشكوك تحوم حول كيفية التوفيق بين القواعد الجديدة التي تجيز المكافئ الإلكتروني للصكوك الورقية الموثّقة توثيقا عدليا والعناصر الجوهرية للصكوك الصحيحة، ولا سيما الحاجة إلى حضور الأطراف شخصيا أمام الكاتب العدل.[١٧٠] وعلى افتراض أن الحضور الشخصي لا غنى عنه لإنشاء تسجيل قانوني صحيح، فإن التحدي يكمن في إجراء تعديلات محتملة على الأشكال الحالية لتتلاءم مع تكنولوجيات المستقبل.[١٧١] وذُكر في هذه الصدد أن علم التشفير لا يحل محل الرموز الملموسة للسلطة العمومية ورضا الأطراف.[١٧٢] ولذا تشترط بعض القواعد أن يكون الأطراف والشهود قادرين على رؤية صورة من توقيعهم فعليا على الشاشة؛ كذلك، يجب أن تظهر صورة من ختم الكاتب العدل على جميع الصكوك.[١٧٣]

١٣٠- وفي الولايات المتحدة، توجد ثلاثة تشريعات رئيسية ذات صلة بالتوثيق العدلي الإلكتروني، وهي: القانون الموحَّد للمعاملات الإلكترونية (Uniform Electronic Transactions Act)،[١٧٤] وقانون التوقيعات الإلكترونية في التجارة العالمية والوطنية (Electronic Signatures in Global and National Commerce Act (E-sign))[١٧٥] *والقانون* الموحّد لتسجيل الأملاك العقارية إلكترونيا (Uniform Real Property Electronic Recording Act).[١٧٦] وهي تنص مجتمعة على أن الشروط القانونية التي تقضي بتوثيق مستند أو توقيع مقترن بمستند توثيقا عدليا أو الاعتراف به أو التحقّق منه أو الشهادة عليه أو إنشائه مع القسم تُستوفى إذا أُرفق بالمستند أو التوقيع أو ارتبط به منطقيا التوقيعُ الإلكتروني للشخص المأذون له بالقيام بتلك الأفعال، إلى جانب كل المعلومات الأخرى التي يقضي بإدراجها أي قانون آخر واجب التطبيق. ومنذ ذلك الحين وضع عدد من الولايات نظما للتوثيق العدلي بالوسائل الإلكترونية. فعلى سبيل المثال، أنشأت إدارة شؤون ولاية بنسلفانيا (Pennsylvania Department of State)، إلى جانب فريق خاص من مكاتب التسجيل العقاري على مستوى المقاطعات، برنامج التسجيل العدلي الإلكتروني واستخدام الأختام العدلية الإلكترونية، الذي يتيح للكتاب العدول أن يقوموا بالتوثيق العدلي الآني وأن يرسلوا بواسطة الاتصال الحاسوبي المباشر المأمون أختاما عدلية إلكترونية جرى التحقق منها. ويهدف نظام التوثيق العدلي الإلكتروني هذا إلى تبسيط المعاملات التجارية بين الموظفين الحكوميين والمؤسسات التجارية وإلى زيادة حماية عامة الناس من التزوير والاحتيال، مع المحافظة في الوقت نفسه على مقومات التوثيق العدلي الأساسية. ويستخدم هذا النظام خدمات التصديق الرقمي التي يوفرها مقدم خدمات تجارية.[١٧٧]

١٣١- ويجب على الكتاب العدول الذين يهتمون بالمشاركة في هذه المبادرة الخاصة بالتوثيق العدلي الإلكتروني تقديم طلباتهم إلى مكتب التفويضات والانتخابات والتشريع التابع للولاية للحصول على صفة

---

(١٧٠) Pierre-Yves Gautier and Xavier Linant de Bellefonds, "De l'écrit électronique et des signatures qui s'y attachent", La semaine juridique *(édition générale),* No. 24, 14 June 2000, I 236, sects. 8-10.

(١٧١) Pierre Catala, "Le formalisme et les nouvelles technologies", *Répertoire du notariat Defrénois,* No. 20, 2000, pp. 897-910.

(١٧٢) Luc Grynbaum, "Un acte authentique électronique pour les notaires", Communication Commerce électronique, No. 10, October 2005, com. 156.

(١٧٣) Decree No. 71-941, as amended by decree No. 2005-973, art. 17, para. 3, (انظر الحاشية ١٦٩).

(١٧٤) انظر الحاشية ٩٠.

(١٧٥) وهو مدوَّن في قانون الولايات المتحدة، العنوان ١٥، الفصل ٩٦، الأبواب ٧٠٠١-٧٠٣١، United States Code, title 15, chapter 96, sections 7001-7031.

(١٧٦) انظر الحاشية ١٥٦.

(١٧٧) Anthony Garritano, "National e-notary standards in progress", *Mortgage Servicing News* (New York), vol. 10, No. 2, 1 March 2006, p. 11.

كاتب عدل مأذون له بالتوثيق الإلكتروني. ويجب على الكاتب العدل أن يحصل، مقابل دفع رسوم، على شهادة رقمية في شكل ختم عدلي إلكتروني من هيئة التصديق المعتمدة على المستوى الاتحادي يوافق عليها مكتب الإدارة وأمين كومنولث ولاية بنسلفانيا ويختارها مكتب التسجيل العقاري المشارك في مبادرة التوثيق العدلي الإلكتروني. وقبل الحصول على الشهادة الرقمية، يجب على الكاتب العدل المأذون له بالتوثيق الإلكتروني المثول شخصيا أمام أي مكتب من مكاتب التسجيل العقاري المشاركة في مبادرة التوثيق العدلي الإلكتروني وأن يقدم إلى مكتب التسجيل العقاري خطاب الموافقة من إدارة شؤون الولاية وأدلة مرضية تثبت هويته. ويجب على الكاتب العدل المأذون لـه بالتوثيق الإلكتروني أن يكفل عند كل توثيق إلكتروني أن تكون المعلومات التالية مرفقةً أو مرتبطة منطقيا بالتوقيع الإلكتروني أو التسجيل الإلكتروني الذي يجري تـوثـيـقـه تـوثـيـقـا عـدليا أو الاعتراف به أو التحقق منه: الاسم الكامل للكاتب العدل المأذون له بالتوثيق الإلكتروني مشفوعا بعبارة "الكاتب العدل العمومي"، واسم البلدية والمقاطعة التي يوجد فيه مكتب لذلك الكاتب العدل وتاريخ انتهاء مدة تفويضه. ويجب أن يكفل الكاتب العدل المأذون له بالتوثيق الإلكتروني حضور الشخص الذي يُجرَى التوثيقُ العدلي الإلكتروني لأجله حضورا شخصيا أمامه عند إجراء كل توثيق عدلي إلكتروني. واستنادا إلى إدارة شؤون ولاية بنسلفانيا، لا تزال العناصر الأساسية للتوثيق العدلي، ومنها حضور مُوقّعي المستند شخصيا أمام الكاتب العدل، واجبة التطبيق. غير أن الكاتب العدل يثبت رقميا المعلومات المحددة لهويته، لا في مستند ورقي مختوم عليه بختم عدلي مطاطي، بل في مستند يتمثل في بيانات إلكترونية موجودة في شكل قابل للقراءة حاسوبيا.[١٧٨]

١٣٢- وكما هو الحال إجمالا في الولايات القضائية الآخذة بالقانون المدني، جرت بعض المناقشات في الولايات القضائية الخاضعة للقانون العام حول قدرة الوسائل الإلكترونية على محاكاة وظيفة طرائق التوثيق الـعـدلي والـتـوثـيـق الـتـقـليدية. وما دام التوثيق العدلي ينحصر أساسا في تأكيد سلامة المستندات وهوية الموقعين، فليس هناك فيما يبدو صعوبة مستعصية في استخدام الاتصالات الإلكترونية كمكافئ للمستندات الورقية. غير أن الوضع يصبح أقل وضوحا عندما يتم التصديق على صحة مستند أو تسجيل بواسطة تأكيد كاتب عدل لحضور شخص عند إنشاء المستند أو التسجيل.[١٧٩]

١٣٣- وقيل إن إجراءات الشهادة التقليدية، مثل الإشهاد، التي يمكن استخدامها فيما يتصل بإعداد الكاتب العدل سندا عموميا، ولكن يمكن استخدامها أيضا بشكل مستقل عن ذلك، ليست قابلة كليا للتكيف مع عملية توقيع المستندات إلكترونيا، حيث إنه لا يوجد أي ضمان على أن صورة المستند التي تظهر على الشاشة هي في الواقع المستند نفسه الذي سوف يُمهر عليه التوقيع الإلكتروني. فكل ما يستطيع أن يراه

---

[١٧٨] انظر http://www.dos.state.pa.us/dos/site/default.asp، تحت العنوان "Notaries", "Electronic Notarization" (اطلع عليه في ٥ حزيران/ يونيه ٢٠٠٨).

[١٧٩] "بفضل التكنولوجيا التي أصبحت تتيح الآن عقد 'اجتماعات عن بعد' بين الأطراف في مدن مختلفة، أو حتى في دول مختلفة، يرجح أن تتسع في المستقبل تعاريف "الحضور الشخصي" المنصوص عليها في القوانين التشريعية حيث يمكن أن يشهد كاتب عدل في لوس أنجلس على توقيع تلفزيوني يضعه شخص يوجد في لندن. ويبدو أن التفاعل الصوتي بين الكاتب العدل والموقّع الغائب والحصول الآني على الصورة المرئية للموقّع هما شرطان لازمان لهذه التوثيقات العدلية الإلكترونية البعيدة. ومع ذلك، وفي حين يمكن تصور هذه الصكوك العدلية الإلكترونية، حيث يكون الكاتب العدل في موقع والمدلي باعتراف أو إقرار في موقع آخر، على الأقل دون التفاعل الصوتي، كما يدل على ذلك استعمال البريد الإلكتروني على نطاق واسع، فإن التفاعل المرئي شرط لا غنى عنه فيما يبدو. وإلا فكيف للكاتب العدل أن يتأكد أن موقّعا بعيدا ليس مكرها بصورة سافرة على التوقيع، وأن يسجل صورة مرئية تثبت أن المرسل ليس محتالا يستخدم مفتاحا خاصا مسروقا. وكما أن محكمة نيبراسكا العليا في عام ١٩٨٤ (قضية كريستينسين ضد أرانات (Christensen v. Arant) قد أكدت أن مجرد الاتصال الصوتي من خلال باب واصل لا يكفي دليلا على الحضور الشخصي بالمعنى القانوني التقليدي، كذلك من المرجح أن مجرد الاتصال الإلكتروني من خلال واسطة غير مرئية لن يكفي دليلا على الحضور الشخصي بالمعنى القانوني المستقبلي" (Charles N. Faerber, "Being there: the importance of physical presence to the notary", The John Marshall Law Review, vol. 31, spring 1998, pp. 749-776).

الشاهد والموقِّع هو تمثيل قابل لأن يقرأه إنسان على شاشة الحاسوب لما يُدعى بأنه موجود في نظام المعلومات. فعندما يرى الشاهدُ الموقعَ يضغط على لوحة المفاتيح فإنّ الشاهد لا يعلم يقينا ما الذي يحدث فعلا. ولذلك لا يمكن ضمان أن المعروض على الشاشة يقابل محتـويات نظام المعلومات وأن نقـرات الموقِّع على المفاتيح تقابل نواياه إلا إذا سبق أن جرى إقرار نظام المعلومات لأجل إحـداث مسار موثوق به بمعايير تقييم موثوق بها.[١٨٠]

١٣٤- غير أن التوقيع الإلكتروني الآمن يستطيع أن يؤدي وظيفة مماثلة للشاهد المصدّق بالإشهاد، وذلك بتعيين هوية الشخص الذي يزعم أنه يوقِّع السند. فباستخدام توقيع إلكتروني آمن من دون شاهد بشري يمكن التحقّق من صحة التوقيع وهوية الشخص صاحب التوقيع وسلامة المستند وربما حتى تاريخ ووقت التوقيع. وبهذا المعنى قد يفوق التوقيع الإلكتروني الآمن التوقيع الخطي العادي من حيث مرتبة التصنيف. ويحتمل أن تكون مزايا وجود شاهد فعلي، إضافة إلى ذلك، للمصادقة بالإشهاد على توقيع رقمي آمن ضئيلة إلى أدنى حد إلا إذا كان هناك ارتياب في طبيعة عملية التوقيع الطوعية.[١٨١]

١٣٥- ولم تـذهب الـتشـريـعـات الـقـائمة إلى حد الاستعاضة كليا عن مقتضيات الإشهاد بالتوقيعات الإلكترونية، وإنما تسمح فقط للشاهد بأن يستخدم توقيعا إلكترونيا. وينص قانون نيوزيلندا للمعاملات الإلكترونية (Electronic Transactions Act) على أن توقيع الشاهد الإلكتروني يفي بالاقتضاء القانوني بوجوب الشهادة من قِبل شاهد على توقيع أو ختم. ولم تحدَّد التكنولوجيا المراد استخدامها في إنشاء التوقيع الإلكتروني، لكن هذه التكنولوجيا يجب أن تستبين على نحو واف هوية الشاهد وتبيّن على نحو واف أخذ شهادة شاهد على التوقيع أو الختم؛ كما يجب أن يتسنّى التعويل عليها بالقدر المناسب للغرض الذي استلزم توقيع الشاهد والظروف المحيطة بذلك".[١٨٢]

١٣٦- وينص القانون الكندي لحماية المعلومات الشخصية والمستندات الإلكترونية على أن المقتضيات الواردة في القانون الاتحادي بشأن إشهاد شاهد على توقيع إنما تُستوفى فيما يتعلق بمستند إلكتروني إذا وقَّع كل موقِّع وكل شاهد على المستند الإلكتروني بتوقيعه الإلكتروني الآمن.[١٨٣] ويجوز الإدلاء في شكل إلكتروني بإفادة لازمة بموجب قوانين اتحادية معينة تقرّ أو تشهد بأن أي معلومات مقدمة من الشخص الذي يدلي بالإفادة هي صادقةٌ أو دقيقة أو كاملة إذا وقّع عليها الشخص بتوقيعه الإلكتروني الآمن.[١٨٤] كما يجوز الإدلاء بإفادة يقضي القانون الاتحادي بالإدلاء بها بعد أداء قَسَم أو إقرار رسمي في شكل إلكتروني إذا وقّع

---

[١٨٠] هذا هو ما يشار إليه في المؤلفات بمشكلة "What you see is what you sign" (WYSIWYS) (ما تراه هو الذي توقِّع عليه). وللاطلاع على بحث يتناول أجهزة التحكم في العرض الموثوق منها، انظر أيضا V. Liu and others, "Visually sealed and digitally signed documents", Association of Computing Machinery, ACM *International Conference Proceedings Series,* vol. 56, *Proceedings of the Twenty-seventh Australasian Conference on Computer Science,* vol. 26 (Dunedin, New Zealand, 2004) p. 287؛ وكذلك.

[١٨١] انظر المناقشة الواردة في الاستعراض المشترك بين هيئة تنمية المعلومات والاتصالات ومكتب النائب العام في سنغافورة لقانون المعاملات الإلكترونية: *Joint IDA-AGC Review of Electronic Transactions Act Stage II: Exclusions under Section 4 of the ETA,* consultation paper LRRD No. 2/2004 (Singapore, 2004), parts 5 and 8, متـاحة في الموقع الشبكي www.agc.gov.sg، الباب "Publications" (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٨٢] نيوزيلندا، قانون المعاملات الإلكترونية لسنة ٢٠٠٢ (انظر الحاشية ٨٨)، الباب ٢٣.

[١٨٣] Canada, Personal Information Protection and Electronic Documents Act (2000), part 2, sect. 46.

[١٨٤] Canada, Personal Information Protection ..., section 45.

عليها الشخص الذي أدلى بها مستخدما توقيعه الإلكتروني الآمن وإذا وقَّعها الشخص الذي أدلى بها أمامه والمأذون له بقبول الإفادات المدلى بها بعد أداء قَسَم أو إقرار رسمي بتوقيع ذلك الشخص الإلكتروني الآمن.[١٨٥] وهناك بديل اقتُرح لأجل توفير المزيد من الضمان، وهو أن ينفِّذ التوقيعَ الإلكتروني اختصاصيٌّ مهني يكون مؤتمنا أو أن ينفَّذ ذلك التوقيع في حضوره، مثل محام أو موثّق عدلي.[١٨٦]

[١٨٥] Canada, Personal Information Protection ..., section 44.

[١٨٦] سيحتاج كتبة سندات نقل الملكية العقارية إلى توقيعات إلكترونية وإلى توثيق إلكتروني من هيئة تصديق معترف بها. وقد يحتاج البائعون والمشترون إلى تفويض كتبة سندات نقل الملكية العقارية بالتوقيع بتفويض خطي. انظر: "E-conveyancing: the strategy for the implementation of e-conveyancing in England and Wales" (United Kingdom, Land Registry, 2005) (نقل الملكية العقارية إلكترونيا: استراتيجية تنفيذ نقل الملكية العقارية إلكترونيا في انكلترا وويلز). النص متاح في الموقع الشبكي http://www.landregistry.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc، وقد اطلع عليه في ٧ نيسان/ أبريل ٢٠٠٧. ومن المقرّر أن ينفّذ هذا المشروع على مراحل من عام ٢٠٠٦ إلى عام ٢٠٠٩.

الجزء الثاني

استخـــدام طـــرائق التوقـــيع والتوثيـق الإلكترونيـة عـبر الحـدود

المحتــويات

الصفحة

أولا- الاعتراف القانوني بطرائق التوثيق والتوقيع الإلكترونية الأجنبية

١٣٧- إن جوانب عدم التوافق القانوني وجوانب عدم التوافق التقني هما المصدران الرئيسيان للصعوبات المعترضة في استخدام طرائق التوقيع والتوثيق الإلكترونية عبر الحدود، وخصوصا عندما يُقصد اعتبارها بديلا عن توقيع صحيح من الناحية القانونية. أما جوانب عدم التوافق التقني فهي تمسّ بقابلية التشغيل البيني لنظم التوثيق. وأما جوانب عدم التوافق القانوني فهي قد تنشأ لأن القوانين في الولايات القضائية المختلفة تفرض مقتضيات مختلفة فيما يتعلق باستخدام طرائق التوقيع والتوثيق الإلكترونية وبصحّتها.

ألف- تأثير القوانين الداخلية على الصعيد الدولي

١٣٨- عندما تسمح القوانين الداخلية باستخدام طرائق توثيق إلكترونية متكافئة مع طرائق التوثيق الورقية، قد يكون هناك عدم اتساق في المعايير المستند إليها لإقرار صحّة تلك المكافئات الإلكترونية. فعلى سبيل المثال، إذا كان القانون لا يعترف إلاّ بالتوقيعات الرقمية، فإن الأشكال الأخرى من التوقيعات الإلكترونية لن تكون مقبولة. وهناك جوانب أخرى من عدم الاتساق في معايير الاعتراف بطرائق التوثيق والتوقيع الإلكترونية قد لا تحول دون استخدامها عبر الحدود من حيث المبدأ، ولكنّ ما يترتّب على ضرورة الامتثال للمقتضيات التي تفرضها الولايات القضائية المتباينة من تكلفة وانعدامٍ في اليُسر قد يقلّل من مكاسب السرعة والكفاءة المتوقّعة من استخدام الاتصالات الإلكترونية.

١٣٩- ومن ثم فإن الأقسام التالية تبحث في تأثير النهوج القانونية المتباينة في تناول مسألة التكنولوجيا على تنامي الاعتراف عبر الحدود في هذا الصدد. وهي تلخّص أيضا التوافق في الآراء الناشئ على الصعيد الدولي بشأن التدابير التي يمكن أن تيسّر استعمال طرائق التوقيع والتوثيق الإلكترونية على الصعيد الدولي.

١- *العقبات الدولية التي يحدثها تنازع النهوج الداخلية*

١٤٠- النهوج المحايدة تكنولوجيا، وبخاصة تلك التي تتضمّن "اختبار قابلية التعويل" بشأن الطريقة المستخدمة، تميل إلى تسوية مشكلة وجود جوانب من عدم التوافق القانوني. ومن بين الصكوك القانونية الدولية التي تعتمد هذا النهج قانونُ الأونسيترال النموذجي بشأن التجارة الإلكترونية (الفقرة (١) *(ب)* من المادة ٧ منه) واتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية (الفقرة ٣ من

المادة ٩ منها) وبمقتضى هذا النهج، فإن طريقة التوقيع أو التوثيق الإلكترونية التي يمكن أن تعيّن هويّة الموقِّع وأن تبيّن نيّة الموقِّع فيما يتعلق بالمعلومات التي يحتوي عليها الخطاب الإلكتروني، من شأنها أن تستوفي مقتضيات التوقيع، شريطة أن تفي بعدّة معايير. وعلى ضوء جميع الظروف المحيطة، بما في ذلك أيُّ اتفاق بين منشئ رسالة البيانات والمرسَلة إليه تلك الرسالة، فإن طريقة التوقيع أو التوثيق يجب أن تُظهر أنها جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أُنشئت أو أُرسلت من أجله رسالة البيانات. وعلى نحو بديل، يجب أن تُظهر تلك الطريقة، إما هي بذاتها وإما مقترنة بدليل إثبات آخر، أنها استوفت هذه الأغراض.

١٤١- ويمكن القول إن نهج الحد الأدنى من الشروط ييسّر استخدام طرائق التوثيق والتوقيع الإلكترونية عبر الحدود، لأن أيّ طريقة من طرائق التوقيع أو التوثيق الإلكترونية يصحّ استخدامها في إطار هذا النهج للتوقيع على عقد أو خطاب أو توثيقه، ما دامت تلك الطريقة تفي بالشروط العامة المشار إليها أعلاه. غير أن من تبعات هذا النهج أن تلك الشروط لا يتسنى إثباتها عادة إلاّ لاحقا، وليس ثـمّة من ضمان بأن المحكمة سوف تعترف باستخدام أي طريقة معيّنة من هذه الطرائق.

١٤٢- لكنّ استخدام طرائق التوثيق والتوقيع الإلكترونية عبر الحدود يطرح إشكالا حقيقيا في النظم التي تستلزم أو تحبّذ استخدام تكنولوجيا معيّنة. وتزداد هذه المشكلة تعقُّدا من حيث علاقتها المباشرة بمستوى التنظيم الرقابي الحكومي لاستخدام طرائق التوقيع والتوثيق الإلكترونية ودرجة اليقين القانوني التي يسندها القانون إلى أي طريقة أو تكنولوجيا محدّدة. وأسباب ذلك بسيطة: ذلك أنّه عندما لا يسند القانون أي قيمة أو قرينة قانونية معيّنة إلى أنواع معيّنة من التوقيع أو التوثيق الإلكتروني، بل يقتصر على النص على تكافؤها العام مع التوقيعات بخط اليد أو التوثيق بالوسيلة الورقية، فإن التعويل على توقيع إلكتروني ينطوي على المخاطر نفسها التي يُحتمل أن تتأتّى من التعويل على توقيع بخط اليد بمقتضى القانون الساري. وأما عندما يسند القانون مزيدا من القرائن القانونية إلى توقيع إلكتروني معيّن (أي التوقيعات التي تُعتبر عادة "مأمونة" أو "متقدّمة")، فإن مستوى المخاطر المتزايد ينتقل من طرف إلى آخر. وأحد الافتراضات الأساسية في أي تشريع خاص بتكنولوجيا محدّدة هو أن ذلك الانتقال العام في المخاطر القانونية المستنتج مسبقا من الجائز تسويغه بمستوى العوليّة التي تتيحها تكنولوجيا بعينها، لدى الامتثال لمعايير وإجراءات معيّنة. وأما الجانب السلبي في هذا النهج فهو أنّه عندما يُستَنَدُ في العوليّة مسبقا على استعمال تكنولوجيا معيّنة (ضمن جملة من الشروط الأخرى)، فإن جميع التكنولوجيات الأخرى—أو حتى تلك التكنولوجيا ذاتها إذا ما استُعملت بشروط مختلفة اختلافا طفيفا—أصبحت مسبقا أيضا غير جديرة بالتعويل عليها، أو على أقل تقدير أصبحت موضع شُبهة مسبقا بأنها غير جديرة بالتعويل عليها.

١٤٣- ولذا فإن تنازع التشريعات الوطنية الخاصة بتكنولوجيات محدّدة قد يحبط، بدلا من أن يشجّع، استعمال التوقيعات الإلكترونية في التجارة الدولية. وهذا يمكن أن يحدث بطريقتين متمايزتين ولكن مترابطتين ترابطا وثيقا.

١٤٤- فأولا، إذا كانت التوقيعات الإلكترونية، وكذلك مقدِّمو خدمات التصديق الذين يوثّقونها، عرضةً لتنازع المقتضيات القانونية والتقنية في ولايات قضائية مختلفة، فإن ذلك قد يحبط استخدام التوقيعات الإلكترونية أو يحول دون اللجوء إليها في كثير من المعاملات المالية عبر الحدود، إن لم يستطع التوقيع الإلكتروني أن يفي بمقتضيات مختلف الولايات القضائية في آن واحد.

١٤٥- وثانيا، يمكن أن يؤدي التشريع الخاص بتكنولوجيا محدّدة، وخصوصا التشريع الذي يقرّ استعمال التوقيعات الرقمية، وهذه أيضا هي حالة النهج الثنائي، إلى ظهور خليط معقّد من المعايير التقنية ومقتضيات الترخيص المتنازعة، مما يجعل استعمال التوقيعات الإلكترونية عبر الحدود أمرا صعبا جدا.

كذلك فإن وجود نظام يفرض فيه كل بلد معاييره قد يؤدّي أيضا إلى منع الأطراف من إبرام اتفاقات بشأن الاعتراف المتبادل والتصديق المقابل.[١٨٧] وهناك حقا مشكلة كبيرة باقية فيما يتعلق، على الخصوص، بالتوقيعات الرقمية، وهي مشكلة الاعتراف بها عبر الحدود. وقد لاحظت الفرقة العاملة المعنية بأمن وخصوصية المعلومات (WPSIP)، التابعة لمنظمة التعاون والتنمية في الميدان الاقتصادي (OECD) (يُشار إليها فيما يلي بالفرقة العاملة)، أنّه بالرغم من كون النهج الذي يأخذ به معظم الولايات القضائية يبدو نهجا غير تمييزي، فإن الاختلافات في المقتضيات المحلية سوف تستمر في توليد مشاكل فيما يتعلق بقابلية التشغيل البيني.[١٨٨] ولأغراض هذه الدراسة، قد تكون مواطن الضعف التالية التي لاحظتها الفرقة العاملة وثيقة الصلة بالموضوع:

(أ) *قابلية التشغيل البيني*. لقد تَبيّن أن التحدّيات والقيود المعترضة في قابلية التشغيل البيني سائدة. فعلى المستوى التقني، مع أن هناك كثرة وافرة من المعايير، فإن عدم وجود معايير مشتركة "أساسية" بشأن بعض التكنولوجيات قد ذُكر في عداد المشاكل المصادفة. وعلى المستوى القانوني/ مستوى السياسة العامة، ذُكر أن الصعوبة في فهم المعنيين الرئيسيين إطارَ الثقة الخاص بكل منهم، بما في ذلك إسناد المسؤولية والتعويض، هي كلها في عداد العوامل التي تعوق التقدّم في هذا الصدد. ووفقا لرأي الفرقة العاملة، فإن هذا مجال "يبدو أنه يتطلّب دراسة وتمحيصا أكثر دقة بغية العمل ربما على تطوير أدوات مشتركة تساعد الولايات القضائية في بلوغ مستوى قابلية التشغيل البيني المرغوب فيه من أجل إقرار تطبيق أو نظام معيّن"؛

(ب) *الاعتراف بخدمات التوثيق الأجنبية*. كان محور التركيز في الجهود المبذولة، وفقا لرأي الفرقة العاملة، ينصبّ على إنشاء خدمات داخلية. ومن ثم فإن آليات الاعتراف بخدمات التوثيق الأجنبية "ليست مطوّرة جيدا عموما". وبناء على هذا الأساس، تقترح الفرقة العاملة أن ذلك "يبدو مجالا قد يكون من المفيد القيام بمزيد من العمل فيه. ولمّا كان أي عمل في هذا المجال من شأنه أن يكون شديد الصلة بالموضوع الأعم وهو قابلية التشغيل البيني، فإنه يمكن دمج الموضوعين معا"؛

(ج) *قبول مستندات الاعتماد*.[١٨٩] في بعض الحالات ذُكر أن قبول مستندات الاعتماد الصادرة عن كيانات أخرى يُعدّ حاجزا يعرقل قابلية التشغيل البيني. ومن ثم، ترى الفرقة العاملة أن يُنظر بعين الاعتبار إلى إمكانية وضع مجموعة من أفضل الممارسات أو من المبادئ التوجيهية بشأن إصدار مستندات الاعتماد لأغراض التوثيق. وقد يكون العمل جاريا من قبل في عدّة ولايات قضائية بخصوص هذه المسألة، مما يمكن أن يسهم بمدخلات مفيدة لأي مبادرات تقوم بها الفرقة العاملة في هذا الصدد؛

---

[١٨٧] Baker and Yeo, "Background and issues concerning authentication ...".

[١٨٨] الفرقة العاملة المعنية بأمن وخصوصية المعلومات، التابعة لمنظمة التعاون والتنمية في الميدان الاقتصادي *The Use of Authentication across Borders in OECD Countries* (DSTI/ICCP/REG (2005)4/FINAL)، النص متاح على الموقع الشبكي: http://www.oecd.org/dataoecd/1/10/35809749.pdf، (اطُّلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٨٩] مستند الاعتماد هو علامة رمزية تُعطى لإثبات خضوع فرد بعينه أو جهاز محدّد لعملية توثيق. ومستندات الاعتماد المخصّصة للمستعمل أساسية جدا لأغراض التوثيق. وأما مستندات الاعتماد التي يحملها الأفراد فقد تكون كافية لبعض أشكال التوثيق. ومن الأمثلة على ذلك رخصة سياقة صالحة، أو رقم الضمان الاجتماعي الشخصي، أو أي رقم آخر خاص بتعيين الهوية، أو ما يسمّى "البطاقات الذكية" (Centre for Democracy and Technology مركز الديمقراطية والتكنولوجيا، "Privacy principles for authentication systems") النص متاح على الموقع الشبكي: http://www.cdt.org/privacy/authenticaation/030513interim.shtml، (اطُّلع عليه في ٥ حزيران/ يونيه ٢٠٠٨)).

(د) *طائفة متنوّعة من طرائق التوثيق المستخدمة*. وجدت الفرقة العاملة أن هناك في كل الدول الأعضاء في منظمة التعاون والتنمية في الميدان الاقتصادي طائفة متنوعة من الحلول الخاصة بالتوثيق التي يجري استخدامها. وتتدرج تلك الطرائق من كلمات السر، من ناحية، إلى العلامات الرمزية والتوقيعات الرقميّة والقياسات البيومترية، من الناحية الأخرى. وتبعا للتطبيق المعتمد، وكذلك مقتضياته، يمكن أن تُستخدم تلك الطرائق منفردة أو مجتمعة. وفي حين أن كثيرين قد يرون في ذلك سمة إيجابية، فإن المعلومات التي جُمعت في الدراسة الاستقصائية التي أجرتها الفرقة العاملة تشير إلى أن طائفة الإمكانيات واسعة جدا مما قد يجعل مقدّمي خدمات التطبيق ومستعمليها في حيرة كبيرة بحيث يتعذر عليهم إدراك الطريقة المناسبة لمقتضياتهم. ووفقا لرأي الفرقة العاملة، فإن ذلك يلمح إلى إمكانية تحقيق بعض النفع من استحداث أداة مرجعية من أجل تقييم مختلف طرائق التوثيق، والدرجة التي تبلغها خصائصها الإسنادية في معالجة المقتضيات المحددة من جانب مقدّمي خدمات التطبيق أو مستعمليها.

١٤٦- ويمكن أن ترتفع درجة الثقة في استخدام طرائق التوقيع والتوثيق الإلكترونية في المعاملات الدولية بازدياد عدد الدول التي تعتمد اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية، وتنفيذ نهجها المحايد تكنولوجيا المتبع بشأن التوقيعات الإلكترونية والتوثيق الإلكتروني. غير أنه ليس من الواقعي أن يتوقّع المرء أن يؤدّي ذلك إلى اجتناب كلي للحاجة إلى حل متوائم من أجل معالجة مسألة عدم توافق المعايير القانونية والتقنية. فقد تعمد بلدان كثيرة مع ذلك إلى فرض استخدام طرائق توثيق محددة في أنواع معيّنة من المعاملات. كما أن بعض البلدان قد يرتئي أن الحاجة تقتضي توفير توجيهات ملموسة أكثر دقّةً بشأن تقييم إمكانية التعويل على طرائق التوقيع والتوثيق، وخصوصا الأجنبية منها، ومدى تكافؤها مع الطرائق المستخدمة، أو المعروفة على أقل تقدير، في البلد.

٢- التوافق الناشئ في الآراء

١٤٧- إن التباين في السياسات العامة الذي ظهر على الصعيد الدولي ربما يعود إلى مجموعة من العوامل، ولكن بدرجات مختلفة. فكما لوحظ من قبلُ (انظر الفقرات ٢-٦ أعلاه)، يميل بعض البلدان إلى فرض مقتضيات بشأن الشكل أشدّ صرامة وخصوصية فيما يتعلق بالتوقيعات والمستندات، في حين يركّز بعضها الآخر على نية الطرف الموقّع، ويسمح باتباع طائفة واسعة من الطرائق من أجل إثبات صحة التوقيعات. وهذه الاختلافات العامة عادة ما تتجسّد في تشريعات محددة تتناول طرائق التوثيق والتوقيع الإلكترونية (انظر الفقرات ٨٣-١١٢ أعلاه). ويتأتّى مصدر إضافي من مصادر انعدام الاتساق من تفاوت درجة التدخل الحكومي في الجوانب التقنية من طرائق التوثيق والتوقيع الإلكترونية. فبعض البلدان تنزع إلى القيام بدور مباشر في تحديد المعايير القياسية بشأن التكنولوجيات الجديدة، ربما اعتقادا منها بأن ذلك من شأنه أن يُضفي مزية تنافسية على الصناعة المحلية.[١٩٠]

١٤٨- كما إن السياسات العامة المتباينة قد تعكس أيضا افتراضات مختلفة بشأن الكيفية التي ستنشأ بها تكنولوجيات التوثيق. فوفقا لأحد السيناريوهات، وهو ما يسمى "أنموذج التوثيق العالمي"،[١٩١] يتمثل الغرض الرئيسي من تكنولوجيات التوثيق في التحقّق من هويات ومميزات أشخاص لا توجد علاقة سابقة بينهم ولا يكون استخدامهم المشترك للتكنولوجيا موضع اتفاق تعاقدي. ولذا فإن تكنولوجيا التوثيق أو

[١٩٠] Baker and Yeo, "Background and issues concerning authorization ..."

[١٩١] Baker and Yeo, "Background and issues concerning authorization ..."

التوقيع المستخدمة ينبغي أن تثبت هوية الشخص المعني أو مميزاته الأخرى لعدد من الأشخاص يُحتمل أن يكون غير محدود ومن أجل عدد من الأغراض يُحتمل أن يكون غير محدود أيضا. ويشدّد هذا النموذج على أهمية المعايير التقنية وعلى المقتضيات العملياتية الخاصة بمقدّمي خدمات التصديق عندما تكون هناك أطراف ثالثة مؤتمنة مشمولة. والسيناريو الآخر، وهو ما يُسمى "أنموذج التوثيق المقيَّد بالتزام"، يرى أن الغرض الرئيسي من استخدام تكنولوجيات التوثيق والتوقيع هو التحقق من هويات ومميزات أشخاص يستخدمون التكنولوجيا على نحو مشترك بمقتضى اتفاقات تعاقدية.[١٩٢] ولذلك فإن تكنولوجيا التوثيق المستخدمة ينبغي أن تثبت هوية حامل شهادة التصديق أو مميزاته الأخرى، من أجل مجموعة محددة من الأغراض فحسب، وضمن جماعة معيّنة من الأطراف التي يُحتمل أن تكون أطرافا معوِّلة، وكذلك خاضعة لأحكام وشروط مشتركة بشأن استخدام التكنولوجيا. وفي إطار هذا النموذج، ينصبّ التركيز على الاعتراف القانوني بالاتفاقات التعاقدية.

١٤٩- وعلى الرغم من هذه التباينات، والتي لا يزال بعضها سائدا، فإن النتائج التي خلصت إليها الفرقة العاملة[١٩٣] تشير إلى أن هناك الآن فيما يبدو توافقا متناميا في الآراء على الصعيد الدولي بشأن المبادئ الأساسية التي ينبغي أن تحكم التجارة الإلكترونية، وخصوصا التوقيع الإلكتروني. والنتائج المستخلصة التالية مثيرة للاهتمام على وجه الخصوص بشأن الدراسة الحالية:

(أ) *النهج غير التمييزي تجاه التوقيعات والخدمات "الأجنبية"*. لا تُنكر الأطر التشريعية المفعول القانوني للتوقيعات الناشئة من دوائر خدمات قائمة في بلدان أخرى، ما دامت هذه التوقيعات قد أُنشئت بمقتضى الشروط نفسها المنصوص عليها بشأن المفعول القانوني على الصعيد الداخلي. وبناء على هذا الأساس، يبدو أن هذا النهج غير تمييزي، ما دامت المقتضيات المحلية، أو ما يكافئها من المقتضيات، مستوفاة. وهذا يتسق مع النتائج المستخلصة في دراسات استقصائية سابقة بشأن التوثيق قامت بها الفرقة العاملة؛

(ب) *الحياد تكنولوجيا*. مع أن كل المجيبين على الدراسة الاستقصائية تقريبا قد بيّنوا أن الأطر التشريعية والتنظيمية بشأن خدمات التوثيق والتوقيعات الإلكترونية في بلدانهم محايدة تكنولوجيا، فقد بيّنت الأغلبية أنه عندما يتعلق الأمر بتطبيقات بيئة الحكومة الإلكترونية، أو عندما يلزم توفير أقصى حد من اليقين القانوني في التوقيع الإلكتروني، يُنَصّ تحديدا على استخدام مرفق المفاتيح العمومية (PKI). وبناء على هذا الأساس، فإنه بالرغم من كون الأطر التشريعية قد تكون محايدة تكنولوجيا، يبدو أن القرارات المتعلقة بالسياسة العامة تقتضي النص على تحديد التكنولوجيا التي ينبغي استخدامها؛

(ج) *مدى انتشار استخدام مرفق المفاتيح العمومية*. وفقا لرأي الفرقة العاملة، يبدو أن استعمال مرفق المفاتيح العمومية هو طريقة التوثيق التي تحظى بالاختيار عندما يلزم توفير دليل إثبات قوي بشأن هوية المستعمل ودرجة عالية من اليقين القانوني بخصوص التوقيع الإلكتروني. وهو يُستخدم في أوساط معينة تضم "جماعات ذات اهتمامات مشتركة"، حيث يبدو أن جميع مستعملي هذا المرفق لديهم شكل ما من العلاقة التجارية السابقة. كما إن استعمال 'البطاقات الذكية' بالاستعانة بمرفق المفاتيح العمومية، وكذلك دمج وظائف التصديق الرقمي في صلب البرامجية التطبيقية، قد جعلا استعمال هذه الطريقة أقل تعقُّدا على المستعملين. غير أن من المسلّم به عموما أن استعمال مرفق المفاتيح العمومية ليس لازما من أجل جميع التطبيقات، ومن ثم ينبغي أن يكون اختيار طريقة التوثيق بناء على أساس ملاءمتها للأغراض التي سوف تُستعمل من أجلها.

---

[١٩٢] Baker and Yeo, "Background and issues concerning authorization ...".

[١٩٣] Organization for Economic Cooperation and Development, *The Use of Authentication across Borders in OECD Countries ....*

١٥٠- علاوة على ذلك، وجدت الفرقة العاملة أن الأطر التنظيمية في جميع البلدان المشمولة في الدراسة الاستقصائية تتضمن شكلا ما من أشكال الإطار التشريعي أو التنظيمي القائم لتوفير الشروط اللازمة للمفعول القانوني للتوقيعات الإلكترونية على الصعيد الداخلي. وقد وجدت الفرقة العاملة أنه في حين قد تختلف التفاصيل التشريعية فيما بين الولايات القضائية المختلفة، يمكن مع ذلك، فيما يبدو، تبيّن وجود نهج متسق في هذا الصدد، من حيث أن معظم القوانين الداخلية يستند إلى أطر قائمة، دولية أو عابرة للحدود الوطنية (أي قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، والتوجيه الإداري 1999/93/EC الصادر عن البرلمان الأوروبي وعن المجلس بشأن إطار خاص بالجماعة الأوروبية بشأن التوقيعات الرقمية[١٩٤]).

١٥١- وقد أُعيد تبيان البنود الجوهرية في هذا التوافق الناشئ في الآراء في التوصية بشأن التوثيق الإلكتروني التي اعتمدها مجلس منظمة التعاون والتنمية في الميدان الاقتصادي في ١٢ حزيران/ يونيه ٢٠٠٧، والتي تدعو الدول إلى أمور عدّة، منها ما يلي:

(أ) العمل في سبيل إرساء نهوج محايدة تجاه التكنولوجيا المستخدمة من أجل التوثيق الإلكتروني الفعّال داخليا وعبر الحدود لهوية الأشخاص والكيانات؛

(ب) العناية بتطوير منتجات وخدمات توثيق إلكتروني تجسّد ممارسات سليمة في الأعمال التجارية، والعناية بتوفيرها واستخدامها، بما في ذلك إقرار ضمانات تقنية وغير تقنية تلبّي احتياجات المشاركين، وخصوصا فيما يتعلق بأمن معلوماتهم وهوياتهم وخصوصيتها؛

(ج) التشجيع، في إطار القطاعين الخاص والعام كليهما، على تحقيق التواؤم القانوني والتجاري وقابلية التشغيل البيني لمخططات التوثيق، بغية تسهيل التفاعلات والمعاملات على الخط الحاسوبي المباشر عبر القطاعات وعبر الولايات القضائية، وبغية ضمان إتاحة الإمكانية لانتشار منتجات وخدمات التوثيق على الصعيدين الوطني والدولي؛[١٩٥]

(د) القيام بخطوات لزيادة وعي المشاركين كافة، بمن فيهم أولئك الذين يعملون في اقتصادات الدول غير الأعضاء، بمنافع استعمال طرائق التوثيق الإلكتروني على الصعيدين الوطني والدولي.

١٥٢- وهذه البنود الموصى بها متّسقة بقدر كبير مع مجمَل النهج الذي اتخذته الأونسيترال في مجال التجارة الإلكترونية (أي التسهيل بدلا من التنظيم الرقابي، والحياد تجاه التكنولوجيا، واحترام حرية التعاقد، وعدم التمييز). غير أن هناك عدة مسائل قانونية تحتاج إلى معالجة من أجل تسهيل استعمال طرائق التوثيق والتوقيع الإلكترونية في سياق دولي أو عابر للحدود.

---

[١٩٤] *Official Journal of the European Communities,* L 13/12, 19 January 2000.

[١٩٥] *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication* (Paris, June 2007)، النص متاح في الموقع الشبكي http://www.oecd.org/dataoecd/32/45/38921342.pdf (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

باء- معايير بشأن الاعتراف بطرائق التوثيق والتوقيع الإلكترونية الأجنبية

١٥٣- مثلما ذُكر أعلاه، فإن إحدى العقبات الرئيسية التي ما فتئت تعرقل استخدام التوقيعات الإلكترونية والتوثيق الإلكتروني عبر الحدود هي عدم قابلية التشغيل البيني، من جراء التنازع أو التباين في المعايير أو عدم الاتساق في تنفيذها. وقد أُنشئت منتديات مختلفة من أجل الترويج لمرفق مفاتيح عمومية قابل للتشغيل البيني وقائم على معايير، باعتباره أساسا تستند إليه المعاملات المأمونة في تطبيقات التجارة الإلكترونية. وتشمل تلك المنتديات منظمات حكومية دولية[١٩٦] ومنظمات مختلطة بين القطاع العام والقطاع الخاص،[١٩٧] على الصعيد العالمي[١٩٨] أو الإقليمي.

١٥٤- ويهدف بعض هذا العمل التقني إلى وضع معايير تقنية بشأن توفير المعلومات الضرورية لتلبية بعض المقتضيات القانونية.[١٩٩] بيد أن هذا العمل المهم يُعنى في الأكثر بالجوانب التقنية لا بالمسائل القانونية،

---

[١٩٦] في منطقة آسيا والمحيط الهادئ، وضع المنتدى التابع لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC) مبادئ توجيهية في هذا الخصوص: "Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction eCommerce" (eSecurity Task Group, APEC Telecommunications and Information Working Group)، كانون الأول/ ديسمبر ٢٠٠٤ (النص متاح في الموقع الشبكي http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf ، (النص الأصلي متاح لدى الأمانة)). والقصد من هذه المبادئ التوجيهية تقديم المساعدة في استحداث مخططات يمكن أن تكون قابلة للتشغيل البيني وفي استعراض للمخططات القائمة. وتشمل هذه المبادئ التوجيهية أصناف أو أنواع شهادات التصديق المستخدمة في مضمار التجارة الإلكترونية عبر الحدود الوطنية فقط. وليس القصد من هذه المبادئ التوجيهية معالجة شهادات تصديق أخرى، وكذلك لا يُقصد منها تقييد المخططات بحيث تقتصر على إصدار شهادات التصديق المشمولة بهذه المبادئ التوجيهية فحسب.

[١٩٧] ضمن الاتحاد الأوروبي، استحدثت هيئة المعايير القياسية الخاصة بتكنولوجيا المعلومات والاتصالات (ICT)، في عام ١٩٩٩، المبادرة الأوروبية بشأن التوحيد القياسي للتوقيعات الإلكترونية (EESSI)، من أجل التنسيق بين أنشطة التوحيد القياسي دعما لتنفيذ التوجيه الإداري 1999/93/EC الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية. كما إن هيئة المعايير القياسية المذكورة هي نفسها أُنشئت من خلال مبادرة قامت بها اللجنة الأوروبية للتوحيد القياسي (CEN)، التي أنشأتها منظمات وطنية معنية بالمعايير القياسية ومنظمتان غير ربحيتين: هما اللجنة الأوروبية للتوحيد القياسي الكهربائي-التقني (CENELEC) والمعهد الأوروبي لمعايير الاتصالات السلكية واللاسلكية (ETSI). وقد طوّر هذا المعهد معايير قياسية شتى من أجل تعزيز قابلية التشغيل البيني بين مختلف النظم، ولكن تنفيذها لا يزال بطيئا، بسبب تعقّدها المزعوم (Paolo Balboni, "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication" Information and Communications Technology Law, vol. 13, No. 3 (2004), pp 211-242).

[١٩٨] على سبيل المثال، أُسست منظمة الارتقاء بمعايير نظم المعلومات البنيوية (OASIS) في عام ١٩٩٣، وهي اتحاد مؤسسات دولي غير هادف إلى الربح، من أجل تشجيع وضع معايير قياسية خاصة بالأعمال التجارية الإلكترونية والتقريب بينها واعتمادها. وقد أنشأت هذه المنظمة لجنة تقنية لمرفق المفاتيح العمومية، تضم مستعملي هذا المرفق وبائعيه وخبراءه، من أجل معالجة المسائل ذات الصلة بنشر تكنولوجيا شهادات التصديق الرقمية. ووضعت اللجنة التقنية للمرفق التابعة لهذه المنظمة خطة عمل تتوخّى فيها عدة أمور ومنها إعداد لمحات خصائص أو مبادئ توجيهية محددة تبيّن كيف ينبغي استخدام هذه المعايير في تطبيقات معيّنة تحقيقا لقابلية المرفق للتشغيل البيني؛ واستحداث معايير جديدة، عند الحاجة؛ وتوفير اختبارات خاصة بقابلية التشغيل البيني، وتنظيم أحداث الاختبارات (OASIS, PKI Technical Committee, "PKI action plan"، (شباط/ فبراير ٢٠٠٤)، النص متاح على الموقع الشبكي http://www.oasis-open.org/committees/pki/ pkiactionplan.pdf، (اطُلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[١٩٩] على سبيل المثال، استحدث المعهد الأوروبي لمعايير الاتصالات السلكية واللاسلكية (ETSI) معيارا قياسيا (TS 102 231) بشأن تنفيذ إقامة بنية غير هرمية التنظيم من أجل القيام بعدة أمور، منها معالجة مسائل الاعتراف التبادلي بالنطاقات الشبكية المخصصة لمرفق المفاتيح العمومية، وبالتالي صحة شهادات التصديق. وأساسا، يحدد المعيار التقني المشار إليه الصادر عن المعهد المذكور ما يلزم من أجل توفير المعلومات عن وضعية مقدّم خدمات التصديق (الذي يسمى "مقدّم خدمات الثقة"). وهو يعتمد صيغة شكلية لقائمة موقّعة، هي "قائمة وضعية خدمات الثقة" كأساس لعرض هذه المعلومات. وتلبي قائمة وضعية خدمات الثقة التي حددها المعهد الاشتراط الخاص بتقديم دليل يثبت ما إذا كان مقدّم خدمات الثقة يعمل، أو قد عمل، بموافقة من أي نظام معترف به، إما في وقت تقديم الخدمات، وإما في الوقت الذي جرت فيه معاملة تعوّل على تلك الخدمات. وبغية استيفاء ذلك الاشتراط، يجب أن تحتوي قائمة وضعية خدمات الثقة معلومات يمكن من خلالها التثبّت مما إذا كانت خدمات مقدّم خدمات التصديق معلومة، في وقت إجراء المعاملة، من جانب مشغّل النظام، وإذا كان ذلك كذلك فما هي وضعية الخدمة حينذاك (أي ما إذا كانت موافقا عليها، أو معلّقة أو ملغاة أو مطعونا فيها). ولذا فإن قائمة وضعية خدمات الثقة المتوخاة في المعيار التقني المشار إليه الصادر عن المعهد المذكور يجب ألا تقتصر فيما تتضمنه من بيانات على وضعية الخدمة في الوقت الراهن، بل أن تتضمّن أيضا بيانات عن تاريخ وضعيتها. ومن ثم فإن القائمة تجمع بين قائمة الخدمات الصحيحة ("القائمة البيضاء") وقائمة الخدمات الملغاة أو المطعون فيها ("القائمة السوداء") (انظر الموقع الشبكي http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231 v010201p&RGW.doc، وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

وهو يتجاوز نطاق هذه الدراسة. ولذا فإن المناقشة الواردة في الأقسام التالية تركّز على المقتضيات القانونية الشكلية والمضمونية الخاصة بالاعتراف بالتوقيعات الإلكترونية عبر الحدود.

١- مكان المنشأ والمعاملة بالمثل والتثبت من الصحة محليا

١٥٥- مكان المنشأ لا يزال عاملا تقليديا في منح الوثائق أو الصكوك الأجنبية اعترافا قانونيا. وهذا يكون عادة على أساس المعاملة بالمثل، وذلك لكي تُعطى التوقيعات وشهادات التصديق الصادرة في بلد ما مفعولا داخليا، بحيث تُعطى التوقيعات وشهادات التصديق الداخلية مفعولا قانونيا في البلد الآخر. وثمة إمكانية أخرى وهي إخضاع المفعول القانوني الداخلي الذي ينطوي عليه التوقيع الأجنبي وشهادة التصديق الأجنبية لشكل ما من أشكال التثبت من الصحة أو الإقرار بواسطة مقدّم خدمات تصديق داخلي أو سلطة تصديق داخلية أو هيئة تنظيم رقابي داخلية. من الجائز الجمع بين هذه النهوج.[٢٠٠]

١٥٦- وليس شائعا أن تنكر القوانين الداخلية صراحة الاعتراف القانوني بأي توقيعات أو شهادات تصديق أجنبية، مما قد يؤكّد ظهور طابعها غير التمييزي. ولكن، في الممارسة العملية يُحتمل أن ينطوي كثير من أنظمة الاعتراف على تأثير تمييزي ما، حتى وإن كان غير مقصود. فعلى سبيل المثال، يحظر التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية عموما التمييز تجاه شهادات التصديق الأجنبية المستوفية للشروط (أي التوقيعات الرقمية المستندة إلى مرفق المفاتيح العمومية). غير أن هذا التوجيه الإداري يعمل في المقام الأول لصالح شهادات التصديق الصادرة عن مقدّمي خدمات التصديق الموجودين داخل أقاليم الدول الأعضاء في الاتحاد الأوروبي. وأما مقدّم خدمات التصديق الموجود في بلد من غير الاتحاد الأوروبي فلديه ثلاثة خيارات للحصول على الاعتراف بشهادة التصديق الصادرة عنه في الاتحاد الأوروبي، وهي: استيفاء مقتضيات التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية، والحصول على اعتماد بمقتضى مخطط موجود في دولة عضو؛ أو إنشاء علاقة تصديق مقابل مع مقدّم خدمات تصديق مستقر في دولة عضو في الاتحاد الأوروبي؛ أو القيام بعمله تحت مظلة اعتراف عام يُوفر على مستوى اتفاق دولي.[٢٠١] والطريقة التي يتبعها التوجيه الإداري الصادر عن الاتحاد الأوروبي في تنظيم الجوانب الدولية تشير إلى أن ضمان الشروط الخاصة بتوفير سبل الوصول إلى الأسواق في الخارج لمقدِّمي خدمات التصديق التابعين للاتحاد الأوروبي، هو واحد من الأهداف المنشودة التي يسعى التوجيه الإداري إلى تحقيقها.[٢٠٢] ومن خلال الجمع بين مقتضى التكافؤ المضموني مع معايير الاتحاد الأوروبي والمقتضى الإضافي

[٢٠٠] في الأرجنتين، مثلا، يُعترف بشهادات التصديق الأجنبية والتوقيعات الإلكترونية الأجنبية في حال وجود اتفاق على المعاملة بالمثل بين الأرجنتين وبلد المنشأ الذي تتبع له سلطة التصديق الأجنبية، أو في حال وجود إقرار من جانب سلطة تصديق مرخّصة في الأرجنتين وموثّقة من جانب السلطة الإنفاذية (انظر *قانون التوقيعات الرقمية* (٢٠٠١)، المادة ١٦).

[٢٠١] فعلا، بمقتضى المادة ٧ من التوجيه الإداري، يجب على الدول الأعضاء في الاتحاد الأوروبي فقط أن تضمن أن شهادات التصديق الصادرة عن مقدّم خدمات تصديق في بلد ثالث معترف بها باعتبارها مكافئة قانونيا لشهادات التصديق الصادرة عن مقدّم خدمات تصديق موجود ضمن الجماعة الأوروبية وذلك *(أ)* إذا كان مقدّم خدمات التصديق "يستوفي المقتضيات المنصوص عليها في هذا التوجيه، وإذا كان معتمدا بمقتضى مخطط اعتماد طوعي قائم في دولة عضو"؛ أو *(ب)* إذا كان مقدّم خدمات التصديق الموجود ضمن الجماعة والذي يستوفي المقتضيات المنصوص عليها في التوجيه الإداري "يضمن" شهادة التصديق؛ أو *(ج)* إذا كانت شهادة التصديق أو كان مقدّم خدمات التصديق "معترفا بهما بمقتضى اتفاق ثنائي أو متعدّد الأطراف بين الجماعة وبلدان ثالثة أو منظمات دولية".

[٢٠٢] الشاغل المتعلق بتأمين سبل وصول مقدِّمي خدمات التصديق الأوروبيين إلى الأسواق الأجنبية واضح من صياغة الفقرة ٣ من المادة ٧ من التوجيه الإداري، التي تنص على أنه "حينما تعلم المفوضية بأي صعوبات تواجه الأنشطة التي تضطلع بها الجماعة من حيث سبل الوصول إلى الأسواق في بلدان ثالثة، يجوز لها، إذا اقتضت الضرورة، أن تقدّم مقترحات إلى المجلس التماسا لتكليف مناسب من أجل التفاوض على حقوق مشابهة بشأن المشاريع التي تضطلع بها الجماعة في تلك البلدان الثالثة".

بشأن الاعتماد وفقا لمخطط قائم في دولة عضو، فإن التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية يشترط بالفعل على مقدّمي خدمات التصديق الأجانب الامتثال للنظام الأصلي الذي يتبعون له والنظام المطبّق في الاتحاد الأوروبي على حد سواء، وهو عبارة عن معيار أعلى مستوى مما هو مطلوب من مقدّمي خدمات التصديق المعتمدين في دولة عضو في الاتحاد الأوروبي.[٢٠٣]

١٥٧- وقد جرى تنفيذ المادة ٧ من التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية ولكن مع بعض التغييرات.[٢٠٤] فإيرلندا ومالطة، على سبيل المثال، تعترفان بالتوقيعات الرقمية الأجنبية (شهادات التصديق المستوفية للشروط، بمقتضى مصطلحات الاتحاد الأوروبي) باعتبارها مكافئة للتوقيعات الداخلية، ما دامت المقتضيات القانونية الأخرى مستوفاة. وفي حالات أخرى، يخضع هذا الاعتراف للتحقق الداخلي (النمسا، لكسمبرغ) أو لقرار يصدر عن سلطة داخلية (الجمهورية التشيكية، إستونيا، بولندا). وهذه النزعة نحو الإصرار على شكل ما من أشكال التحقّق الداخلي، والتي يسوّغها عادة شاغل مشروع بشأن مستوى قابلية التعويل على شهادات التصديق الأجنبية، يؤدي في الممارسة العملية إلى نظام ينطوي على تمييز تجاه شهادات التصديق الأجنبية على أساس المنشأ الجغرافي الصادرة منه.

٢- التكافؤ المضموني

١٥٨- اتساقا مع تقليد قديم العهد، أحجمت الأونسيترال عن إقرار الاعتبارات الجغرافية عند اقتراح عوامل للاعتراف بشهادات التصديق الأجنبية والتوقيعات الإلكترونية الأجنبية. فالفقرة ١ من المادة ١٢ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية تنص صراحة على أنه لدى تقرير ما إذا كانت شهادة التصديق سارية المفعول قانونيا، أو ما إذا كان التوقيع الإلكتروني كذلك، أو تقرير مدى كونهما كذلك، لا يُولى أي اعتبار للموضع الجغرافي الذي تصدر فيه الشهادة أو يُنشأ أو يُستخدم فيه التوقيع الإلكتروني أو للموضع الجغرافي لمكان عمل المصدر أو الموقّع.

١٥٩- والقصد من الفقرة ١ من المادة ١٢ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية هو تبيان المبدأ الأساسي الذي مفاده أنّ مكان المنشأ، في حد ذاته، لا ينبغي بأي حال من الأحوال أن يكون عاملا في تقرير ما إذا كان ينبغي الاعتراف بما يمكن أن يكون لشهادات التصديق أو التوقيعات الإلكترونية الأجنبية من مفعول قانوني، وتقرير إلى أي مدى ينبغي ذلك، فتقرير ما إذا كان يمكن أن تنطوي شهادة التصديق أو التوقيع الإلكتروني على مفعول قانوني، وتقرير مداه، ينبغي أن يعتمدا على قابلية التعويل عليهما من الناحية التقنية، لا على المكان الذي صدرت منه شهادة التصديق أو التوقيع الإلكتروني. وهناك أحكام غير تمييزية مماثلة للمادة ١٢ من القانون النموذجي بشأن التوقيعات الإلكترونية يمكن العثور عليها أيضا في بعض الأنظمة الداخلية، مثل قانون الولايات المتحدة بشأن التوقيعات الإلكترونية في التجارة العالمية والوطنية لعام ٢٠٠٠.[٢٠٥] فهذه الأحكام تنص على أن مكان المنشأ، في حد ذاته، لا ينبغي أن يكون عاملا في تقرير ما إذا كان ينبغي الاعتراف بأن شهادات التصديق أو التوقيعات الإلكترونية الأجنبية يمكن أن

---

(٢٠٣) Jos Dumortier and others, "The legal and market aspects of electronic signatures", study for the European Commission Directorate General Information Society, Katholieke Universiteit Leuven, 2003, p. 58.

(٢٠٤) Jos Dumortier and others, "The legal and market aspects of electronic signatures"..., pp. 92-94.

(٢٠٥) United States Code, title 15, chapter 96, section 7031 (Principles governing the use of electronic signatures in international transactions).

تنطوي على مفعول قانوني، ومدى ذلك المفعول، في دولة مشترعة. فهي تعترف بأن المفعول القانوني لشهادة التصديق أو للتوقيع الإلكتروني ينبغي أن يتوقف على قابلية التعويل عليهما تقنيا.[٢٠٦]

١٦٠- وبدلا من العوامل الجغرافية، يقرر القانون النموذجي اختبارا للتكافؤ المضموني بين مستويات قابلية التعويل التي تتيحها شهادات التصديق والتوقيعات المعنية. ووفقا لذلك، فإن شهادة التصديق الأجنبية إذا ما كانت تتيح مستوى من التكافؤ الجوهري من حيث قابلية التعويل عليها باعتبارها شهادة تصديق صادرة في الدولة المشترعة، وجب أن يكون لها المفعول القانوني نفسه. ومن المنطلق ذاته، يجب أن يكون للتوقيع الإلكتروني المُنشَأ أو المُستخدَم خارج البلد المفعول القانوني نفسه باعتباره توقيعا إلكترونيا منشأ أو مستخدما داخل البلد إذا أتاح مستوى من التكافؤ الجوهري من حيث قابلية التعويل عليه. كما إن التكافؤ بين مستويات قابلية التعويل التي تتيحها شهادات التصديق والتوقيعات الداخلية والأجنبية يجب تقريرها وفقا للمعايير الدولية المعترف بها وأيّ عوامل أخرى وثيقة الصلة بالموضوع، بما في ذلك اتفاق الأطراف على استخدام أنواع معينة من التوقيعات أو شهادات التصديق الإلكترونية، ما لم يتعذر أن يكون الاتفاق صحيحا أو ساري المفعول بمقتضى القانون المطبّق.

١٦١- لكن القانون النموذجي لا يقتضي إبرام ترتيبات بشأن المعاملة بالمثل ولا يروج لذلك. والواقع أن القانون النموذجي لا يحتوي على أي اقتراح محدد بشأن الأساليب القانونية التي يمكن بها للدولة المشترعة أن تعترف مسبقا بقابلية التعويل على الشهادات والتوقيعات التي تمتثل لقانون بلد أجنبي (مثلا إعلان من طرف واحد أو معاهدة).[٢٠٧] والطرائق التي يمكن اتباعها بغية تحقيق تلك النتيجة، التي ذُكرت أثناء إعداد القانون النموذجي، تشمل، على سبيل المثال، الاعتراف التلقائي بالتوقيعات التي تمتثل لقوانين دولة أخرى إذا كانت قوانين الدولة الأجنبية تقتضي مستوى من قابلية التعويل متكافئا على الأقل مع المستوى المطلوب بخصوص التوقيعات الداخلية المكافئة. والأساليب القانونية الأخرى التي يتسنى من خلالها لدولة مشترعة أن تعترف مسبقا بقابلية التعويل على شهادات التصديق والتوقيعات الأجنبية يمكن أن تشمل إصدار إعلانات من جانب واحد أو إبرام معاهدات.[٢٠٨]

[٢٠٦] قانون *الأونسيترال النموذجي بشأن التوقيعات الإلكترونية* . . . ، الجزء الثاني، الفقرة ٨٣.

[٢٠٧] المرجع نفسه، الفقرة ١٥٧.

[٢٠٨] انظر تقرير الفريق العامل المعني بالتجارة الإلكترونية عن أعمال دورته السابعة والثلاثين (A/CN.9/483)، الفقرتين ٣٩ و٤٢.

ثانيا- طرائق ومعايير إنشاء تكافؤ قانوني

١٦٢- كما هو مبيّن أعلاه، وجدت الدراسة الاستقصائية التي قامت بها الفرقة العاملة المعنية بأمن وخصوصية المعلومات، التابعة لمنظمة التعاون والتنمية في الميدان الاقتصادي، أن مُعظم الأطر التشريعية غير تمييزية من حيث المبدأ، على الأقل تُجاه التوقيعات الإلكترونية الأجنبية وكذلك التوثيق الإلكتروني الأجنبي، شريطة أن تُستوفى فيهما المقتضيات المحلية أو ما يكافئها، بمعنى أنها لا تُنكر نفاذ مفعول التوقيعات القانوني فيما يتعلق بالخدمات الصادرة أصلا من بلدان أخرى، شريطة أن تكون تلك التوقيعات قد أُنشئت بمقتضى الشروط نفسها المطبّقة على التوقيعات المعترَف بها بمقتضى القانون الداخلي.[٢٠٩] غير أن فرقة العمل لاحظت أيضا أن آليات الاعتراف بخدمات التوثيق الأجنبية ليست متطوّرة على نحو جيد عموما، وحدّدت ذلك باعتباره مجالاً قد يكون من المفيد الاضطلاع فيه بعمل مستقبلا. ونظرا إلى أن أي عمل في هذا المجال من شأنه أن يكون وثيق الصلة بموضوع أعمّ وهو قابلية التشغيل البيني، اقترحت الفرقة العاملة الجمع بين هذين الموضوعين. كما اقترحت الفرقة العاملة أن توضع مجموعة من أفضل الممارسات المتّبعة أو من المبادئ التوجيهية في هذا الخصوص. وفي آونة أحدث عهدا، لاحظت منظمة التعاون المذكورة أن آليات الاعتراف بخدمات التوثيق الأجنبية قد تطورت، ولكن الخبرة في تطبيقاتها عبر الولايات القضائية لا تزال محدودة. علاوة على ذلك، فإن الولايات القضائية تحتاج إلى بعض الوسائل لتقييم إطار الثقة لدى شركائها في هذا الميدان. ومع أن منظمة التعاون المذكورة أعربت عن الأمل في أن تُوفِّرَ مبادئها التوجيهية والإطار الذي تتيحه مساعدة في هذا الصدد، فقد بيّنت أن من اللازم القيام بعمل أكثر شمولا بشأن هذه المسألة.[٢١٠] ويتناول القسمان التاليان بالمناقشة موضوع الترتيبات والآليات القانونية بشأن قابلية التشغيل البيني على الصعيد الدولي، والعوامل التي تحدّد التكافؤ بين أنظمة المسؤولية. وهما يركّزان في المقام الأول على المسائل الناشئة عن استعمال طرائق التوقيع والتوثيق الإلكترونية على الصعيد الدولي المدعّمة بشهادات تصديق صادرة عن مقدّم خدمات تصديق هو طرف ثالث موثوق به، وخصوصا التوقيعات الرقمية في إطار مرفق مفاتيح عمومية (PKI)، وذلك لأن من الأرجح نشوء صعوبات قانونية فيما يتعلق باستخدام طرائق التوقيع والتوثيق الإلكترونية عبر الحدود مما يقتضي إشراك أطراف ثالثة في عملية التوقيع والتوثيق.

ألف- أنواع الاعتراف المتبادل وآلياته

١٦٣- إن العبء الإضافي الذي تلقيه على عاتق مقدّمي خدمات التصديق الأجانب المقتضياتُ الداخلية ذات الصلة بالتكنولوجيا يمكن أن يصبح حاجزا يعرقل التجارة الدولية.[٢١١] وعلى سبيل المثال، فإن القوانين ذات الصلة بالوسائل التي تتّبعها السلطات الوطنية في منح الموافقة على الاعتراف بالتوقيعات الإلكترونية

---

(٢٠٩) Organization for Economic Cooperation and Development, The Use of Authentication across Borders in OECD Countries...

(٢١٠) ECD Recommendation on Electronic Authentication ..., p. 27.

(٢١١) Alliance for Global Business, "A discussion paper on trade-related aspects of electronic commerce in response to the WTO's e-commerce work programme", April 1999, p. 29 (النص متاح في الموقع الشبكي http://www.biac.org/statements/iccp/AGBtoWTO April1999.pdf، وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

الأجنبية وشهادات التصديق الإلكترونية الأجنبية يمكن أن تنطوي على تمييز جائر تجاه منشآت الأعمال التجارية الأجنبية. وحتى الآن، يُلاحظ أن كل هيئة تشريعية نظرت في هذه المسألة أدرجت في قوانينها بعض المقتضيات ذات الصلة بالمعايير التي ينبغي أن يتقيّد بها مقدّم خدمات التصديق الأجنبي، ومن ثم فإن هذه المسألة ذات صلة لا تنفصم بالقضية الأوسع نطاقا الخاصة بتضارب المعايير الوطنية. وفي الوقت نفسه، فإن التشريع قد يفرض أيضا قيودا جغرافية أو إجرائية أخرى تحول دون الاعتراف بالتوقيعات الإلكترونية عبر الحدود.

١٦٤- وفي حال عدم وجود مرفق مفاتيح عمومية دولي، يمكن أن ينشأ عدد من دواعي القلق بخصوص الاعتراف بشهادات التصديق من جانب سلطات التصديق في البلدان الأجنبية. وكثيرا ما يتم الاعتراف بشهادات التصديق الأجنبية بواسطة طريقة تسمّى "التصديق المتبادل". وفي تلك الحالة، من الضروري أن تعترف سلطات التصديق المتكافئة جوهريا (أو سلطات التصديق الراغبة في أن تأخذ على عاتقها بعض المخاطر المعيّنة بخصوص شهادات التصديق الصادرة عن سلطات تصديق أخرى) بالخدمات التي يقدّمها كل منها، وذلك لكي يستطيع المستعملون التابعون لكل منها أن يتواصلوا فيما بينهم بمزيد من الكفاءة وبقدر أكبر من الشعور بالأمان في الجدارة بالثقة الَتي تتّسم بها الشهادات التي تصدر عنها. وقد تنشأ مسائل قانونية بخصوص التصديق المتبادل أو الربط التسلسلي بين الشهادات عندما تتعدّد السياسات العامة الأمنية المشمولة في هذا المجال، ومن ذلك مثلاً مسألة تحديد الطرف الذي تسبّب سوء تصرّفه في وقوع خسارة، والطرف الذي عَوَّل المستعمِل على إفاداته.

١- الاعتراف المتبادل

١٦٥- الاعتراف المتبادل هو ترتيب بشأن التشغيل البيني يستطيع في إطاره الطرف المعوِّل في منطقة مرفق مفاتيح عمومية أن يستعمل معلومات صادرة عن سلطة مرجعية في منطقة مرفق مفاتيح عمومية آخر بغية توثيق شخص في منطقة مرفق المفاتيح العمومية الآخر.[٢١٢] ويكون هذا عادة نتيجة لعملية ترخيص أو اعتماد رسمية في منطقة مرفق المفاتيح العمومية الآخر، أو لعملية تدقيق رسمية أُجريت بشأن مقدّم خدمات التصديق الممثِّل لمنطقة مرفق المفاتيح العمومية.[٢١٣] وأما التبعة التي تترتّب على ما إذا كان من الجائز الثقة بمنطقة مرفق مفاتيح عمومية أجنبي فتقع على كاهل الطرف المعوِّل أو مالك التطبيق الحاسوبي أو الخدمة الإلكترونية، لا على كاهل مقدّم خدمات تصديق يثق فيه على نحو مباشر الطرفُ المعوِّل.

١٦٦- ويحدث الاعتراف المتبادل عادة على مستوى مرفق المفاتيح العمومية، لا على مستوى مقدّم خدمات التصديق المعني بمفرده. ومن ثم، عندما يعترف مرفق مفاتيح عمومية بمرفق مفاتيح مثيل آخر، فهو يعترف تلقائيا بأي مقدّمي خدمات تصديق معتَمدين في إطار مخطط مرافق المفاتيح العمومية. وهذا الاعتراف يستند على الأرجح إلى تقييم عملية اعتماد مرفق المفاتيح العمومية الآخر، لا إلى تقييم كل مقدّم خدمات تصديق بمفرده معتَمد لدى مرفق المفاتيح العمومية الآخر. وفي الأحوال التي تصدر فيها مرافقُ المفاتيح العمومية أصنافا متعدّدة الدرجات من شهادات التصديق، فإن عملية الاعتراف المتبادَل تشتمل على تحديد صنف من شهادات التصديق التي يمكن القبول بها لغرض استخدامها في المنطقتين، وكذلك على الاستناد في التقييم إلى ذلك الصنف من الشهادات.

---

[٢١٢] مفهوم الاعتراف المتبادل استحدثته في عام ٢٠٠٠ المجموعة المكلّفة بمهمة معالجة التوثيق الإلكتروني التابعة للفريق العامل بشأن الاتصالات عن بُعد والمعلومات، التابع لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ (APECTEL Working Group)، انظر منشور (APEC) رقم ٢٠٢-TC-01.2، (APEC, 2002) *Electronic authentication: issues relating to its selection and use*، متاح على الموقع الشبكي http://www.apec.org/apec/publications/all_publications/telecommunications.html (اطُّلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[٢١٣] تعريف يستند إلى عمل المجموعة المكلّفة بمهمة معالجة التوثيق الإلكتروني، التابعة للفريق العامل بشأن الاتصالات عن بُعد والمعلومات، التابع لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC).

١٦٧- كما إن الاعتراف المتبادل يستتبع بالضرورة مسائل تتعلق بقابلية التشغيل البيني من الناحية التقنية على مستوى التطبيق فقط، أي أن البرامجية التطبيقية يجب أن تكون قادرة على معالجة شهادة التصديق الأجنبية، والدخول إلى النظام الدليلي الحاسوبي لمنطقة مرفق المفاتيح العمومية الأجنبي من أجل التثبّت من صحة وضعية شهادة التصديق الأجنبية. وينبغي أن يُلاحظ من حيث الممارسة العملية أن مقدّمي خدمات التصديق يصدرون شهادات تصديق على درجات مختلفة من قابلية التعويل، وفقا للأغراض التي يعتزم زبائنهم استعمال الشهادات من أجلها. وقد تنتج عن الشهادات والتوقيعات الإلكترونية، في الداخل والخارج معا، آثار قانونية مختلفة تتوقّف على درجة قابلية كل منها للتعويل عليها. ففي بعض البلدان، على سبيل المثال، قد تترتّب آثار قانونية في ظروف معيّنة حتى على الشهادات التي يُشار إليها أحيانا بوصفها "متدنّية الدرجة" أو "متدنّية القيمة" (مثلا، عندما يكون الطرفان قد اتفقا تعاقديا على استخدام مستندات من هذا القبيل) (انظر الفقرات ٢٠٢-٢١٠ أدناه). ولذا فإن التكافؤ المراد إنشاؤه هو بين الشهادات المتقارنة وظيفيا.

١٦٨- وكما قيل أعلاه، فإن القرار بشأن الثقة بشهادة أجنبية، في الاعتراف المتبادل، إنما يقع على عاتق الطرف المعوِّل، لا على عاتق مقدّم خدمات التصديق إليه. وهو لا يقتضي بالضرورة وجود عقد أو اتفاق بين نطاقي مرفقي مفاتيح عمومية. وكذلك ليس من الضروري توافر تصنيف تفصيلي للسياسات العامة الناظمة لشهادات التصديق[٢١٤] وبيانات الممارسات المتّبعة في هذه الشهادات،[٢١٥] إذ إن الطرف المعوِّل يقرّر ما إذا كان سيقبل بالشهادة الأجنبية استنادا إلى ما إذا كانت الشهادة صادرة عن مقدّم خدمات تصديق أجنبي جدير بالثقة. ويُعتبر مقدّم خدمات التصديق جديرا بالثقة إذا كان مرخّصا لـه بالعمل أو معتمدا من جانب هيئة ترخيص أو اعتماد رسمية، أو إذا ما كان قد خضع لتدقيق من جانب طرف ثالث مستقل موثوق به. ومن ثم فإن الطرف المعوِّل يتخذ قراره أحاديا بناءً على معلومات دقيقة بالاستناد إلى السياسات العامة المنصوص عليها في بيان السياسة العامة الناظمة للشهادات أو بيان الممارسة المتّبعة في الشهادات في نطاق مرفق المفاتيح العمومية الأجنبي.

٢- التصديق المتبادل فيما بين مرافق المفاتيح العمومية

١٦٩- يشير مفهوم التصديق المتبادل إلى الممارسة المتّبعة في الاعتراف بالمفتاح العمومي الصادر عن مقدّم خدمات تصديق آخر بدرجة متفق عليها من الثقة، بموجب عقد مبرم عادةً. ويؤدّي ذلك بصفة أساسية إلى اندماج نطاقي مرفقي مفاتيح عمومية (كليا أو جزئيا) ضمن نطاق أكبر حجما. وفيما يخص المستعملين الذين يتعاملون مع مقدّم خدمات تصديق واحد منهما، يُعتبر المستعملون الذين يتعاملون مع مقدّم خدمات التصديق الآخر موقّعين فحسبُ ضمن مرفق المفاتيح العمومية الموسّع.

١٧٠- وينطوي التصديق المتبادل على توافر قابلية التشغيل البيني من الناحية التقنية والمواءمة في السياسات العامة الناظمة لشهادات التصديق وبيانات الممارسات المتّبعة في الشهادات أيضا. ذلك أنّ المواءمة في السياسات العامة، والتي تكون في صيغة مواءمة بين السياسات العامة الناظمة للشهادات وبيانات الممارسات المتّبعة في إصدار الشهادات، ضرورية لضمان التوافق بين نطاقات مرافق المفاتيح العمومية من حيث عملياتها ذات الصلة بإدارة شهادات التصديق (أي ذات الصلة بإصدار الشهادات وتعليقها وإلغائها) وإلى تقيّدها بمقتضيات عملياتية وأمنية متشابهة على حدّ سواء. كما إن مقدار الشمول في المسؤولية وثيق الصلة بهذا الخصوص أيضا. وهذه الخطوة على درجة عالية من التعقّد، إذ إن هذه المستندات تكون عادة ضخمة الحجم وتتناول طائفة واسعة من المسائل.

---

[٢١٤] السياسة العامة الناظمة لشهادات التصديق هي مجموعة مسمّاة من القواعد تبيّن قابلية تطبيق شهادة ما على مجموعة معيّنة و/أو صنف معيّن من التطبيقات الإلكترونية التي تشتمل على مقتضيات أمان مشتركة فيما بينها.

[٢١٥] بيان الممارسات المتّبعة في شهادات التصديق هو بيان يوضّح الممارسات التي يتّبعها مقدّم خدمات تصديق في إصدار شهادات التصديق.

١٧١- والتصديق المتبادل ملائم في الأكثر لنماذج منشآت الأعمال التجارية المغلقة نسبيا، وذلك مثلا إذا كان نطاقا مرفقي المفاتيح العمومية كلاهما يتشاركان في مجموعة من التطبيقات والخدمات الإلكترونية، كالبريد الإلكتروني أو التطبيقات الخاصة بالشؤون المالية. كما إن توافر النظم المتوافقة تقنيا وعملياتيا والسياسات العامة المتطابقة والبنى القانونية نفسها من شأنها كلها أن تيسّر بدرجة كبيرة التصديق المتبادل.

١٧٢- وأما التصديق الأحادي الجانب (حيث يثق نطاق مرفق مفاتيح عمومية واحد في آخر ولكن ليس العكس بالعكس) فليس أسلوبا شائعا. ذلك أن نطاق مرفق المفاتيح العمومية الواثق يجب عليه أن يضمن من جانب واحد أن سياساته العامة متوافقة مع السياسات العامة لدى نطاق مرفق المفاتيح العمومية الموثوق به. ويبدو أن اللجوء إلى هذا الأسلوب مقصور على التطبيقات والخدمات في الأحوال التي تكون فيها الثقة اللازمة للمعاملة التجارية المشمولة فيها أحادية الجانب، وذلك مثلا في تطبيق يكون فيه على التاجر أن يثبت هويته للزبون قبل أن يقدّم الأخير معلومات محاطة بالسرّية.

باء- التكافؤ في معايير السلوك وأنظمة المسؤولية

١٧٣- إن معرفة ما إذا كان استخدام طرائق التوقيع والتوثيق الإلكترونية على الصعيد الدولي يستند إلى مخطط للاعتراف المتبادل أو التصديق المتبادل، أو إلى قرار بالاعتراف بمرفق مفاتيح عمومية بأجمعه أو بواحد أو أكثر من مقدّمي خدمات التصديق الأجانب، أو بإرساء مستويات متكافئة بين أصناف شهادات التصديق الصادرة في إطار مرافق مفاتيح عمومية مختلفة، هي معرفة تقوم على افتراض مسبق بأن تقديرا للتكافؤ بين ممارسات التصديق الداخلية والأجنبية وكذلك شهادات التصديق نفسها قد تم.[٢١٦] ومن وجهة نظر قانونية، يقتضي ذلك إجراء تقدير للتكافؤ بين ثلاثة عناصر رئيسية، هي: التكافؤ في القيمة القانونية؛ والتكافؤ في الواجبات القانونية؛ والتكافؤ في المسؤولية.

١٧٤- أما التكافؤ في القيمة القانونية فيعني أن يُسنَد إلى شهادة تصديق أجنبية أو توقيع أجنبي المفعولُ القانوني نفسه المسنَد إلى مكافئ داخلي لهما. والمفعول القانوني الداخلي الناتج عن ذلك إنما يُقرّر بصفة أساسية بناءً على القيمة التي يسندها القانون الداخلي إلى طرائق التوقيع والتوثيق الإلكترونية، وقد نُوقش ذلك من قبلُ (انظر الفقرات ١٠٧-١١٢ أعلاه). وأما الاعتراف بالتكافؤ في الواجبات القانونية وأنظمة المسؤولية فيترتّب عليه استنتاج بأن الواجبات المفروضة على الأطراف العاملة في إطار نظام مرفق مفاتيح عمومية تقابل من حيث الجوهر الواجبات الموجودة بمقتضى النظام الداخلي، وأن المسؤولية عن الإخلال بتلك الواجبات هي نفسها من حيث الجوهر أيضا.

١٧٥- لكن هذه المسؤولية في سياق التوقيعات الإلكترونية قد تثير مسائل مختلفة تبعا لاختلاف التكنولوجيا المستخدمة والبنية التحتية التي يقوم عليها التصديق. وقد تطرأ مسائل معقّدة، وبخاصة في الحالات التي يوفّر فيها التصديقَ طرفٌ ثالثٌ مخصّص لهذا العمل، مثل مقدّم خدمات تصديق. وفي حالة من هذا القبيل، سوف يكون هناك بصفة أساسية ثلاثة أطراف مشمولة، أيْ مقدّم خدمات التصديق، والموقّع، والطرف الثالث المعوِّل. ويمكن أن يصبح كل منهم مسؤولاً، أو قد يفقد الحق في تأكيد مسؤولية

---

[٢١٦] على سبيل المثال، استحدث الفريق العامل المعني بالسياسة العامة بشأن التصديق، التابع للهيئة المكلّفة بالسياسة العامة بشأن مرفق المفاتيح العمومية الاتحادي في الولايات المتحدة (United States Federal Public Key Infrastructure Policy Authority, Certificate Policy Working Group) منهجية بخصوص تقديم رأي اجتهادي بشأن التكافؤ بين عناصر السياسة العامة (بناءً على الإطار المحدّد في الاستمارة RFC" 2527" (طلب تقديم تعليقات ("Request for Comments." وقد تُستخدم هذه المنهجية عند تصنيف مرافق المفاتيح العمومية المختلفة أو تصنيف مرفق مفاتيح عمومية بناءً على هذه المبادئ التوجيهية (انظر الموقع الشبكي http://www.cio.gov/fpkipa، وقد اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

الطرف الآخر، وذلك بمقدار ما تسبّب أفعالهم أو حالات امتناعهم عن الفعل من ضرر لأي من الأطراف، أو بمقدار ما تخالف تلك الأفعال والامتناعات واجباتهم الصريحة أو الضمنية. وقد اعتُمدت نهوج تشريعية متنوّعة بخصوص المسؤولية فيما يتعلق باستخدام التوقيعات الرقمية:

(أ) *عدم وجود أحكام محدّدة بشأن معايير السلوك أو المسؤولية.* قد يكون واحد من الخيارات المتاحة أن يمسك القانون عن معالجة هذه المسألة. ففي الولايات المتحدة الأمريكية، لا ينص قانون التوقيعات الإلكترونيةَ في التجارة العالمية والوطنية لعام ٢٠٠٠[٢١٧] على أحكام بخصوص مسؤولية أي من الأطراف المشمولة في خدمة التصديق. وعموما يمكن القول إن هذا النهج قد اعتُمد في أكثر الولايات القضائية الأخرى التي تأخذ بنهج يكتفي بالحدّ الأدنى من المقتضيات في معالجة التوقيعات الإلكترونية، كما في أستراليا؛[٢١٨]

(ب) *معايير السلوك وقواعد المسؤولية لمقدّمي خدمات التصديق فقط.* يتجه نهج آخر إلى الاقتصار في القانون على النص على مسؤولية مقدّم خدمات التصديق فقط. وهذه هي الحالة بمقتضى التوجيه الإداري الصادر عن الاتحاد الأوروبي 1999/93/EC بشأن إطار التوقيعات الإلكترونية في الجماعة الأوروبية،[٢١٩] والذي يفيد البند ٢٢ منه بأنّ "مقدّمي خدمات التصديق الذين يقدّمون خدمات التصديق للعموم يخضعون للقواعد الوطنية بشأن المسؤولية"، حسبما يرد بإجمال في المادة ٦ من التوجيه الإداري. ومما هو جدير بالملاحظة أن المادة ٦ لا تطبّق إلاّ على "التوقيعات المستوفية الشروط"، مما يعني، في الوقت الحالي، التوقيعات الرقمية المستندة إلى مرافق المفاتيح العمومية فقط؛[٢٢٠]

(ج) *معايير السلوك وقواعد المسؤولية للموقّعين ومقدّمي خدمات التصديق.* في بعض الولايات القضائية، ينص القانون على أحكام بشأن مسؤولية كل من الموقّع ومقدّم خدمات التصديق، لكنه لا يقرّر معيارا بشأن واجب العناية على الطرف المعوِّل. وهذه هي الحالة في الصين، بمقتضى قانون التوقيعات الإلكترونية الصادر عام ٢٠٠٥. وهذه هي الحالة أيضا في سنغافورة بمقتضى قانون المعاملات الإلكترونية لعام ١٩٩٨؛

(د) *معايير السلوك وقواعد المسؤولية لجميع الأطراف.* أخيرا، قد ينص القانون على معايير سلوك وعلى أساس للمسؤولية بشأن جميع الأطراف المشمولة. وهذا النهج معتَمد في قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، الذي يبيّن الواجبات فيما يخص سلوك الموقّع (المادة ٨)، وسلوك مقدّم خدمات التصديق (المادة ٩)، وسلوك الطرف المعوِّل (المادة ١١). ويمكن القول إن القانون النموذجي يبيّن المعايير التي يُستنَد إليها في تقييم سلوك أولئك الأطراف. غير أنه يدع المجال للقانون الداخلي لكي يقرّر عواقب عدم التمكّن من الوفاء بالواجبات المختلفة والأساس اللازم للمسؤولية، وهي عواقب قد تلحق بمختلف الأطراف المشمولة في تشغيل نظم التوقيع الإلكتروني.

---

[٢١٧] United States Code, title 15, chapter 96, section 7031.

[٢١٨] يُعتقد، على سبيل المثال، بأن آليات القانون الخاص التي يجيزها القانون الأسترالي، كالاستبعادات التعاقدية وكذلك التنازلات عن بعض الحقوق وأشكال التبرّؤ من المسؤولية، والقيود المفروضة على إعمالها بموجب القانون العام، تلائم التنظيم الرقابي للمسؤولية على نحو أفضل من الأحكام القانونية التشريعية (انظر Mark Sneddon, *Legal liability and e-transactions: a scoping study for the National Electronic Authentication Council* (National Office for the Information Economy، كانبيرا، ٢٠٠٠)، الصفحات ٤٣-٤٧) دراسة متاحة على الموقع الشبكي http://unpan1.un.org/intradoc/ groups/public/documents/APCITY/ UNPAN014676.pdf، (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[٢١٩] *Official Journal of the European Communities,* L 13/12, 19 January 2000.

[٢٢٠] التشريعات المعتمدة في الاتحاد الأوروبي تتّبع هذا النهج، ومنها على سبيل المثال القوانين التالية في ألمانيا والنمسا والمملكة المتحدة: German law on electronic signature (SignaturGesetz – SigG) and the related ordinance (SigV), 2001, the Austrian Federal Electronic Signature Law (SigG) and the United Kingdom of Great Britain and Northern Ireland Electronic Signature Regulation 2002, section 4.

١٧٦- وقد تكون الاختلافات في الأنظمة الداخلية الخاصة بالمسؤولية عقبة تعرقل الاعتراف بالتوقيعات الإلكترونية عبر الحدود الوطنية. وهناك سببان رئيسيان يؤدّيان إلى ذلك. أولهما أن مقدّمي خدمات التصديق قد يحجمون عن الاعتراف بالشهادات الأجنبية أو المفاتيح الصادرة عن مقدّمي خدمات تصديق أجانب، ممّن قد تكون قواعد المسؤولية أو معايير واجب العناية التي يطبّقونها أدنى مستوى من قواعدهم ومعاييرهم. وثانيهما أن مستعملي طرائق التوقيع والتوثيق الإلكترونية هم أيضا قد يخشون من أن يؤدّي انخفاض مستوى حدود المسؤولية أو معايير واجب العناية التي يطبّقها مقدّم خدمات تصديق أجنبي إلى الحدّ من سبل الانتصاف المتاحة لهم، على سبيل المثال، في حالة حدوث تزوير أو تعويل زائف. ولهذين السببين ذاتهما، عادة ما يعمد القانون في الحالات التي ينص فيها التشريع على أحكام بشأن استخدام طرائق التوقيع والتوثيق الإلكترونية، أو على الأنشطة التي يضطلع بها مقدّمو خدمات التصديق، إلى إخضاع الاعتراف بشهادات التصديق الأجنبية أو بمقدّمي خدمات التصديق الأجانب إلى شكل من أشكال التقييم لتقدير مدى التكافؤ الجوهري مع قابلية التعويل التي تتيحها شهادات التصديق الداخلية ويتيحها مقدمو خدمات التصديق الداخليون. ومن ثم فإن معايير واجب العناية ومستويات المسؤولية التي يخضع لها مختلف الأطراف تكوّن أساس القياس القانوني الرئيسي الذي يُقاس بناءً عليه هذا التكافؤ. علاوة على ذلك، فإن مقدرة مقدّم خدمات التصديق على الحدّ من مسؤوليته أو التبرّؤ منها سوف يكون لها أيضا تأثير في مستوى التكافؤ الذي يُتاح لشهادات التصديق التي يصدرها.

١- أساس المسؤولية في إطار مرفق المفاتيح العمومية

١٧٧- توزيع المسؤولية في إطار مرفق مفاتيح عمومية يتم أساسا بطريقتين: أي بواسطة أحكام تعاقدية، أو بموجب القانون (قانون سوابق، أو قانون تشريعي، أو كليهما). وفي العادة، تكون العلاقات بين مقدّم خدمات التصديق والموقّع ذات طبيعة تعاقدية، ولذلك فإن المسؤولية، في تلك الأحوال، سوف تستند إلى حدوث إخلال بالالتزامات التعاقدية لأي من هذين الطرفين. وأما العلاقات بين الموقّع وطرف ثالث فسوف تتوقّف على طبيعة تعاملهما معا في أي واقعة ملموسة. وقد تكون، أو قد لا تكون، مستندة إلى عقد مبرم. وأخيرا، فإن العلاقات بين مقدّم خدمات التصديق والطرف الثالث المعوِّل لن تكون في أكثر الحالات قائمة على عقد مبرم.[٢٢١] وبمقتضى أكثر النظم القانونية، سوف يترتّب على أساس المسؤولية (سواء بحكم العقد أو بجريرة المضرّة) عواقب جسيمة وخطيرة الشأن تلحق بنظام المسؤولية، وخصوصا فيما يتعلق بالعناصر التالية: *(أ)* درجة الخطأ اللازمة لكي تستوجب مسؤولية الطرف المعني (أي بعبارة أخرى، ما هو "معيار واجب العناية" الذي يلتزم به طرف تجاه الطرف الآخر)؛ و*(ب)* الأطراف التي قد تطالب بتعويضات عن الأضرار، ومقدار التعويضات التي يمكن أن تحصِّلها عن الأضرار؛ و*(ج)* ما إذا كان الطرف الذي يقع على عاتقه الخطأ قادرا على الحدّ من مسؤوليته أو على التبرّؤ منها، ومدى مقدرته على ذلك.

١٧٨- ويُستخلص مما ورد أعلاه أن معايير المسؤولية لن تتباين من بلد إلى آخر فحسب، بل إنها سوف تتباين أيضا، ضمن البلد الواحد، تبعا لطبيعة العلاقة بين الطرف الذي يُعتبر مسؤولا عن الضرر والطرف

---

[٢٢١] تناول ستيفن هيندلانغ (Steffen Hindelang) في مناقشة تفصيلية مسألة إمكانية إنشاء علاقة تعاقدية بين مقدّم خدمات التصديق والطرف الثالث في إطار القانون الإنكليزي، فخلص إلى استنتاج سلبي "No remedy for disappointed trust: the liability regim for certification authorities towards third parties outwith the EC Directive in England and Germany compared", *Journal of Information, Law and Technology*, No. 1, 2002) النص متاح على الموقع الشبكي http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/hindelang، (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨). غير أن هناك ولايات قضائية من الجائز فيها نشوء علاقة تعاقدية من هذا النحو.

الذي لحقه الضرر. علاوة على ذلك، فقد يكون لعدّة قواعد ونظريات قانونية مختلفة تأثير في جانب أو آخر من جوانب المسؤولية في إطار نظام مسؤولية تعاقدي أو خاضع للقانون العام أو للقانون التشريعي، مما يقلّل أحيانا من الفوارق بين النظامين. لكن هذه الدراسة لا يسعها أن تقدّم تحليلا تفصيليا كاملا لهذه المسائل العامة؛ بل إنها سوف تركّز على المسائل التي تُثار على وجه التحديد في سياق مرفق مفاتيح عمومية، وسوف تتناول بالنقاش في إيجاز الكيفية التي عالجت بها القوانين الداخلية تلك المسائل.

(أ) معيار واجب العناية

١٧٩- مع أن النظم القانونية المختلفة تستخدم نظما ونظريات مختلفة في ترتيب الدرجات بخصوص المسؤولية، فإنه يُفترض لأغراض هذه الدراسة أن مسؤولية الأطراف المشمولة في إطار مرفق للمفاتيح العمومية من شأنها أن تستند بصفة أساسية إلى ثلاثة معايير ممكنة، هي: الإهمال أو الخطأ العادي؛ والإهمال المفترض (أو الخطأ الذي يكون عبء إثباته معكوسا)؛ والمسؤولية المطلقة.[٢٢٢]

'١' *الإهمال العادي*

١٨٠- بمقتضى هذا المعيار العام، يكون أي شخص ملزما قانونا بتقديم تعويض لغيره من الأشخاص عن أيّ عواقب سلبية تنجم عن تصرفاته، شريطة أن تكون العلاقة بالشخص الآخر من النوع الذي يقتضي بحكم القانون واجبَ العناية. علاوة على ذلك، فإن معيار واجب العناية اللازم عموما يُقصد به "العناية المعقولة"، والتي يمكن تعريفها ببساطة بأنها تلك الدرجة من العناية التي يمارسها شخص لديه قدر عادي من الحذر والمعرفة والتبصّر في الظروف نفسها أو في ظروف مشابهة. وفي الولايات القضائية التي تطبّق القانون العام، كثيرا ما يُشار إلى هذا المعيار بتعبير معيار "الشخص العاقل"، في حين أنه كثيرا ما يُشار إليه في عدد من الولايات القضائية التي تطبّق القانون المدني بتعبير معيار "أب أسرة صالح". وبالنظر إلى معيار العناية المعقولة من منظور الأعمال التجارية تحديدا، فإنه يشير إلى درجة العناية التي من شأن أي شخص حصيف وكفء على نحو عادي، يقوم بعمل أو مشروع تجاري من فرع الأعمال نفسه، أن يمارسها في ظروف مشابهة. وفي الأحوال التي تستند فيها المسؤولية عموما إلى معيار الإهمال العادي، فإن على الطرف المتضرّر أن يبيّن أن الضرر سبّبه إخلال الطرف الآخر بالتزاماته.

١٨١- ومعيار واجب العناية المعقولة (أو معيار الإهمال العادي) هو المعيار العام بشأن واجب العناية المتوخّى في قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية. ويُطبّق هذا المعيار الخاص بالعناية على مقدّمي خدمات التصديق بخصوص إصدار شهادات التصديق أو إلغائها وإفشاء المعلومات.[٢٢٣] وقد يُستخدَم عدد من العوامل في تقدير مدى امتثال مقدّم خدمات التصديق لمعيار واجب العناية العام المتعلق

---

[٢٢٢] للاطّلاع على مناقشة لنظام المسؤولية في هذا السياق، انظر Balboni, "Liability of certification service providers ..."، الصفحات ٢٣٢ وما بعدها.

[٢٢٣] تنص الفقرة ١ من المادة ٩ من القانون النموذجي على ما يلي: حيثما يوفّر مقدّم خدمات التصديق خدمات لتأييد توقيع إلكتروني يجوز استخدامه لإعطاء مفعول قانوني بصفته توقيعا، يتعيّن على مقدّم خدمات التصديق المشار إليه: [. . .] "(ب) أن يولي قدرا معقولا من العناية لضمان دقّة واكتمال كل ما يقدّمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها، أو مدرجة في الشهادة؛ (ج) أن يوفّر وسائل يكون الوصول إليها متيسّرا بقدر معقول وتمكّن الطرف المعوِّل من التأكّد من الشهادة مما يلي: " [. . .]؛ "(د) أن يوفّر وسائل يكون الوصول إليها متيسّرا بقدر معقول وتمكّن الطرف المعوّل من التأكّد، عند الاقتضاء، من الشهادة أو من سواها، مما يلي: [. . .]."

به.[٢٢٤] ويطبّق المعيار نفسه أيضا على الموقّعين بخصوص الحيلولة دون استخدام أدوات إنشاء التوقيعات على نحو غير مأذون به، وكذلك بخصوص تأمين حفظ هذه الأدوات.[٢٢٥] والقانون النموذجي يمدّد نطاق معيار العناية المعقولة العام نفسه ليشمل الطرف المعوِّل، والذي يُتوقّع منه أن يقوم بخطوات معقولة من أجل التحقّق من جدارة توقيع إلكتروني بالتعويل عليه، وكذلك من صحة شهادة التصديق أو من تعليقها أو إلغائها، وأن يراعي أي تقييد بشأن الشهادة.[٢٢٦]

١٨٢- لكنّ قلة من البلدان، وهي عادة الدول التي اشترعت قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، قد اعتمدت معيار "العناية المعقولة" العام فيما يخص سلوك مقدّم خدمات التصديق.[٢٢٧] وفي بعض البلدان، يبدو أن مقدّم خدمات التصديق سوف "يُلزم على الأرجح بمعيار العناية المعقولة العام"، مع أن مقدّمي خدمات التصديق، بحكم طبيعتهم، سوف يكونون أطرافا من ذوي المهارات المتخصصة يضع فيهم الأشخاص العاديون ثقتهم بقدر يتجاوز الثقة التي تُولى للمشاركين العاديين في أنشطة السوق، "مما قد يؤدي في نهاية المطاف إلى نشوء وضعية مهنية خاصة بهم، أو إلى إخضاعهم إلى درجة أعلى من واجب العناية تستوجب منهم أن يفعلوا ما هو معقول بالنظر إلى مهاراتهم المتخصصة".[٢٢٨] ويبدو فعلا، حسبما ترد مناقشته أدناه (انظر الفقرة ١٨٩)، أن هذه هي الحال في أكثر البلدان.

١٨٣- وأما فيما يخصّ الموقّع، فإن بعض الولايات القضائية التي اعتمدت قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية تنص على أحكام بشأن تطبيق معيار "العناية المعقولة" العام.[٢٢٩] وفي مختلف البلدان، يشتمل القانون على قائمة مستفيضة إلى حد ما بالالتزامات الإيجابية من دون وصف معيار العناية

---

[٢٢٤] *القانون النموذجي بشأن التوقيعات الإلكترونية* . . . . تبيّن الفقرة ١٤٦ من دليل الاشتراع أنه "لدى تقدير مسؤولية مقدّم خدمات التصديق، ينبغي أن توضع في الاعتبار العوامل التالية، على سبيل المثال لا الحصر: *(أ)* تكلفة الحصول على الشهادة؛ *(ب)* طبيعة المعلومات التي يجري التصديق عليها؛ *(ج)* وجود ومدى أي قيد على الغرض الذي يمكن أن تُستخدم الشهادة من أجله؛ *(د)* وجود أي بيان يحدّ من نطاق أو مدى مسؤولية مقدّم خدمات التصديق؛ *(هـ)* أي سلوك إسهامي من جانب الطرف المعوّل. ولدى إعداد القانون النموذجي، اتفق عموما على أنه، عندما تُحدّد في الدولة المشترعة الخسارة التي يمكن استردادها، ينبغي إيلاء الاعتبار للقواعد الناظمة لحدود المسؤولية في الدولة التي يوجد فيها مقدّم خدمات التصديق أو في أي دولة أخرى يُطبّق قانونها بموجب قاعدة تنازع القوانين ذات الصلة."

[٢٢٥] تبيّن المادة ٨ من القانون النموذجي أنه "حيثما أمكن استخدام بيانات إنشاء التوقيع لإنشاء توقيع ذي مفعول قانوني، يتعيّن على كل موقّع: *(أ)* أن يولي قدرا معقولا من العناية لاجتناب استخدام بيانات إنشاء توقيعه استخداما غير مأذون به؛ *(ب)* أن يبادر، دون تأخر لا مُسوّغ له، إلى استخدام الوسائل التي يوفّرها مقدّم خدمات التصديق [. . .]، أو خلافا لذلك، إلى بذل جهود معقولة لإشعار أي شخص يجوز للموقّع أن يتوقّع منه على وجه معقول أن يعوّل على التوقيع الإلكتروني أو أن يقدّم خدمات تأييدا للتوقيع الإلكتروني، وذلك في حالة: '١' معرفة الموقّع بأن بيانات إنشاء التوقيع تعرّضت لما يثير الشبهة؛ أو '٢' كون الظروف المعروفة لدى الموقّع تؤدي إلى نشوء احتمال قوي بتعرّض بيانات إنشاء التوقيع لما يثير الشبهة". إضافة إلى ذلك، يجب على الموقّع "أن يولي قدرا معقولا من العناية . . . ، لضمان دقة واكتمال كل ما يقدّمه الموقّع من تأكيدات مادية ذات صلة بالشهادة طيلة دورة سريانها، أو يُتوخى إدراجها في الشهادة".

[٢٢٦] المادة ١١، الفقرات الفرعية *(أ)* و*(ب)* '١'، و*(ب)* '٢'.

[٢٢٧] على سبيل المثال، جزر كايمان، قانون المعاملات الإلكترونية، ٢٠٠٠، الفرع ٢٨؛ وتايلند، قانون المعاملات الإلكترونية (٢٠٠١)، الفرع ٢٨.

[٢٢٨] Thomas J. Smedinghoff، "Certification authority: liability issues"، دراسة أعدّها من أجل رابطة المصرفيين الأمريكيين، شباط/ فبراير ١٩٩٨ القسم ١-١، وهي متاحة على الموقع الشبكي http://www.bakernet.com/ecommerce/ca-liability-analysis.pdf، (اطلع عليه في ٦ حزيران/ يونيه ٢٠٠٨).

[٢٢٩] على سبيل المثال، تايلند، قانون المعاملات الإلكترونية (٢٠٠١)، الفرع ٢٧.

أو تبيان عواقب عدم الامتثال لتلك الالتزامات.[٢٣٠] ولكن، في بعض البلدان يكمل القانون بوضوح صريح تلك القائمة بإعلان عام بشأن مسؤولية الموقّع عن إخلاله.[٢٣١] بل وتعتبر المسؤولية في إحدى الحالات مسؤولية ذات طابع جنائي.[٢٣٢] ويُفترض جدلا بأنه قد لا يكون هناك معيار وحيد بشأن العناية، بل نظام متراتب، مع اعتبار معيار العناية المعقولة العام قاعدة تحوّطية بشأن التزامات الموقّع، وهو معيار يُرفع إلى مستوى معيار ضمان فيما يخص بعض الالتزامات المحدّدة، وهي عادة تلك الالتزامات التي تتعلق بدقة وصدق التأكيدات المقدّمة.[٢٣٣]

١٨٤- وأما الحال فيما يتعلق بالطرف المعوّل فهو غريب، لأن من غير المرجّح أن يتضرّر الموقّع ولا مقدّم خدمات التصديق من جراء فعل أو امتناع عن فعل من جانب الطرف المعوّل. وفي معظم الظروف، إذا ما أخفق الطرف المعوّل في التصرف بالدرجة اللازمة من العناية، فإنه سوف يتحمّل عواقب تصرّفه، لكنه لن يتكبّد أي مسؤولية تجاه مقدّم خدمات التصديق. ولذا فليس مفاجئا أن القوانين الداخلية بشأن التوقيعات الرقمية، لدى معالجة دور الأطراف المعوّلة، قلّما تنص على أكثر من قائمة عامة بشأن واجبات الطرف المعوّل الأساسية. وهذه هي عموما الحالة في الولايات القضائية التي اعتمدت قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، الذي يوصي بالأخذ بمعيار "العناية المعقولة" فيما يتعلق بسلوك الطرف المعوّل.[٢٣٤] لكن هذا الاقتضاء غير منصوص عليه صراحة في بعض الحالات.[٢٣٥] وينبغي أن يُذكر هنا أن واجبات الطرف المعوّل الصريحة أو الضمنية ليست غير ذات صلة فيما يخص مقدّم خدمات التصديق. فإخلال

---

[٢٣٠] على سبيل المثال، الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٢٥؛ وجزر كايمان، قانون المعاملات الإلكترونية، ٢٠٠٠، الفرع ٣١؛ وشيلي، *القانون الخاص بالمستندات الإلكترونية والتوقيع الإلكتروني وخدمات التصديق على التوقيع الإلكتروني (٢٠٠٢)*، المادة ٢٤؛ وإكوادور، *قانون التجارة الإلكترونية والتوقيعات الإلكترونية ورسائل البيانات*، المادة ١٧؛ والهند، *قانون تكنولوجيا المعلومات*، ٢٠٠٠، الفروع ٤٠-٤٢؛ وموريشيوس، قانون المعاملات الإلكترونية ٢٠٠٠، المواد ٣٣-٣٦؛ وبيرو، *قانون التوقيعات وشهادات التصديق الرقمية*، المادة ١٧؛ وتركيا، التشريع المتعلق بالإجراءات والمبادئ ذات الصلة بتنفيذ قانون التوقيعات الإلكترونية (٢٠٠٥)، المادة ١٥؛ وتونس، *القانون الخاص بالمبادلات والتجارة الإلكترونية*، المادة ٢١؛ وفنزويلا (جمهورية-البوليفارية)، *القانون المتعلق برسائل البيانات والتوقيعات الإلكترونية*، المادة ١٩.

[٢٣١] الصين، *قانون التوقيعات الإلكترونية ٢٠٠٤*، المادة ٢٧؛ كولومبيا، *القانون ٥٢٧ بشأن التجارة الإلكترونية*، المادة ٤٠؛ المكسيك، *مدونة القوانين التجارية: المرسوم المتعلق بالتوقيعات الإلكترونية (٢٠٠٣)*، المادة ٩٩؛ الجمهورية الدومينيكية، *القانون المتعلق بالتجارة الإلكترونية والمستندات والتوقيعات الرقمية (٢٠٠٢)*، المادتان ٥٣ و٥٥؛ بنما، *قانون التوقيعات الرقمية (٢٠٠١)*، المادتان ٣٧ و٣٩؛ الاتحاد الروسي، *القانون الاتحادي بشأن التوقيعات الرقمية الإلكترونية (٢٠٠٢)*، البند ١٢؛ فنزويلا (جمهورية-البوليفارية)، القانون *المتعلق برسائل البيانات والتوقيعات الإلكترونية*، المادة ١٩؛ فييت نام، *قانون المعاملات الإلكترونية*، المادة ٢٥.

[٢٣٢] باكستان، تشريع المعاملات الإلكترونية، ٢٠٠٢، الفرع ٣٤.

[٢٣٣] على سبيل المثال، سنغافورة، قانون المعاملات الإلكترونية (الفصل ٨٨). وتنص الفقرة ٢ من الفرع ٣٧ من القانون على أن الموقّع بقبوله شهادة تصديق يصدّق لجميع أولئك الذين يعوّلون على نحو معقول على المعلومات الواردة في الشهادة بأن *(أ)* المكتتب حائز بحق للمفتاح الخصوصي المقابل للمفتاح العمومي المذكور في الشهادة؛ و*(ب)* جميع الإفادات التي قدّمها المكتتب إلى سلطة التصديق وذات الصلة الجوهرية بالمعلومات المذكورة في الشهادة صادقة؛ و*(ج)* جميع المعلومات الواردة في الشهادة التي تندرج في نطاق معرفة المكتتب صادقة. وأما الفقرة ١ من الفرع ٣٩ فهي لا تتوخى سوى مراعاة واجب ممارسة العناية المعقولة في الاحتفاظ بالتحكم بالمفتاح الخصوصي المقابل للمفتاح العمومي المذكور في تلك الشهادة، والحؤول دون إفشائه لشخص غير مأذون له بإنشاء التوقيع الرقمي الخاص بالمكتتب. ويبدو أن هذه هي الحالة أيضا في جمهورية فنزويلا البوليفارية، حيث إن المادة ١٩ من *القانون المتعلق برسائل البيانات والتوقيعات الإلكترونية* تخص صراحة الالتزام باجتناب استخدام أداة إنشاء التوقيع على نحو غير مأذون به بأنه التزام بتوخي "الحرص الواجب"، في حين أن الالتزامات الأخرى يعبّر عنها بتعابير غير قانونية.

[٢٣٤] جزر كايمان، قانون المعاملات الإلكترونية، ٢٠٠٠، الفرع ٢١؛ المكسيك، *مدونة القوانين التجارية: المرسوم المتعلق بالتوقيعات الإلكترونية (٢٠٠٣)*، المادة ١٠٧؛ وتايلند، قانون المعاملات الإلكترونية (٢٠٠١)، الفرع ٣٠.

[٢٣٥] تركيا، تشريع الإجراءات والمبادئ الخاصة بتنفيذ قانون التوقيعات الإلكترونية (٢٠٠٥)، المادة ١٦؛ وفييت نام، قانون المعاملات الإلكترونية، المادة ٢٦.

الطرف المعوّل بواجبه في توخي العناية قد يزوّد مقدّم خدمات التصديق فعلا بدفاع يدرأ به عن نفسه مطالبة من جانب طرف معوّل بشأن المسؤولية عندما يستطيع مقدّم خدمات التصديق، على سبيل المثال، أن يبيّن أن الضرر الذي لحق بالطرف المعوّل كان يمكن اجتنابه أو التخفيف منه لو أن الطرف المعوّل قد اتخذ تدابير معقولة بغية التأكد من صحة شهادة التصديق أو الأغراض التي يمكن استخدامها من أجلها.

'٢' *الإهمال المفترَض*

١٨٥- الإمكانية الثانية هي نظام يستند إلى وقوع خطأ ويكون فيه عبء الإثبات معكوسا. وفي إطار هذا النظام، يُفتَرض وقوع خطأ من جانب طرف عند حصول ضرر من فعل يمكن أن يُعزى إليه. والأساس المنطقي الذي يقوم عليه نظام من هذا القبيل يتجسّد عموما في الافتراض بأن الضرر، في بعض الظروف المعيّنة، لا يمكن وقوعه، في أثناء مجرى الأحداث العادي، إلا بسبب إخفاق طرف ما في الامتثال لالتزاماته أو التقيّد بمعيار سلوك متوقّع منه.

١٨٦- وفي القانون المدني، قد يقع الخطأ المفترض فيما يتعلق بالمسؤولية عن الإخلال بالعقد،[٢٣٦] وكذلك بشأن أحوال مختلفة خاصة بالمسؤولية عن الضرر. ومن الأمثلة على ذلك مختلف أشكال المسؤولية عن أفعال المستخدَمين أو الوكلاء أو صغار الأطفال أو الحيوانات، والمسؤولية الناشئة في سياق بعض الأنشطة التجارية أو الصناعية (الضرر البيئي، والضرر بالممتلكات المجاورة، وحوادث النقل). وأما النظريات التي تسوّغ عكس عبء الإثبات والأحوال المعيّنة التي يُجاز فيها فتختلف من بلد إلى آخر.

١٨٧- وفي الممارسة العملية، يؤدي مثل هذا النظام إلى نتيجة مشابهة لنتيجة المعيار المعزّز بشأن العناية المتوقّعة من المهنيين بمقتضى القانون العام. إذ يجب على المهنيين أن يكون لديهم مقدار أدنى من المعرفة الخاصة والمهارات الضرورية للتصرّف كأعضاء في المهنة المعيّنة، وعليهم واجب التصرّف كما يتصرّف عضو عاقل في المهنة في ظرف معيّن.[٢٣٧] وهذا لا يعني بالضرورة أن عبء الإثبات معكوس، لكنّ الدرجة الأعلى من معيار العناية المتوقّعة من الشخص المهني تعني في الممارسة العملية أن المهنيين يعتبرون قادرين على اجتناب فعل ما يسبّب الأذى للأشخاص الذين يستأجرون خدماتهم أو الذين يأتمنونهم على رعاية مصلحتهم على أي نحو آخر، إذا ما تصرفوا وفقا لتلك المعايير. ولكن، في بعض الظروف المعيّنة يجيز المذهب القانوني

[٢٣٦] الفقرة ١ من الفرع ٢٨٠ من مدونة القوانين المدنية في ألمانيا، على سبيل المثال، تعتبر المدين مسؤولا عن التعويض عن الضرر الناشئ عن الإخلال بالتزام تعاقدي ما لم يكن ذلك المدين مسؤولا عن ذلك الإخلال. والفقرة ١ من المادة ٩٧ من مدونة قوانين الالتزامات في سويسرا تنص على هذا المبدأ بعبارات أوضح من ذلك: إذا لم يحصل الدائن على أداء الدين، يكون المدين مسؤولا عن التعويض عن الضرر الناتج عن ذلك، إلا إذا استطاع أن يثبت أن عدم الأداء لا يُعزى إلى خطأ من جانبه هو. وترد قاعدة مشابهة في المادة ١٢١٨ من مدونة القوانين المدنية في إيطاليا. وبمقتضى القانون الفرنسي، يُفترض دائما وقوع إهمال إذا ما كان العقد ينطوي على وعد له نتيجة معيّنة ما، لكن الإهمال شيء يجب إثباته عندما يكون الهدف من العقد توفير معيار أداء بدلا من تحقيق نتيجة محدّدة (انظر Gérard Légier, "Responsabilité contractuelle", *Répertoire de droit civil Dalloz,* August 1989, No. 58-68).

[٢٣٧] W. Page Keeton and others, *Prosser and Keeton on the Law of Torts,* 5th ed., (Saint Paul, Minnesota, West Publishing Co., 1984), section 32 at p. 187.

القائل بأن الشيء ينضح بما فيه (res ipsa loquitur) للمحاكم بأن تفترض، في حال عدم وجود ما يثبت العكس، أن وقوع الضرر في 'أثناء مجرى الأمور الاعتيادي' لا يكون ممكنا إلا من جراء إخفاق شخص ما في توخّي العناية المعقولة.[٢٣٨]

١٨٨- وإذا ما طُبّقت هذه القاعدة على أنشطة مقدّمي خدمات التصديق، فإن من شأن ذلك أن يعني أنه حينما يلحق ضرر بطرف معوِّل أو موقِّع، نتيجة لاستعمال توقيع إلكتروني أو شهادة تصديق إلكتروني، وعندما يمكن عزو ذلك الضرر إلى إخفاق من جانب مقدّم خدمات التصديق في التصرّف وفقا لالتزاماته التعاقدية أو القانونية، يُفترض إذ ذاك أن مقدّم خدمات التصديق كان مُهمِلا.

١٨٩- ويبدو أن الإهمال المفترَض هو المعيار السائد المتّبع بمقتضى القوانين الداخلية. فعلى سبيل المثال، بمقتضى التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية، يكون مقدّم خدمات التصديق مسؤولا عن التعويض عن الأضرار تجاه أي كيان يعوّل على نحو معقول على شهادة التصديق المستوفية الشروط، ما لم يثبت مقدّم خدمات التصديق بأنه لم يتصرّف بإهمال.[٢٣٩] وبعبارة أخرى، يمكن القول إنّ مسؤولية مقدّم خدمات التصديق عن الضرر تستند إلى معيار الإهمال مع عبء إثبات معكوس: أي أن على مقدّم خدمات التصديق أن يثبت أن تصرفاته لم تنطو على إهمال، وذلك لأنه في أفضل موقف يؤهّله للقيام بذلك، بما لديه من المهارات التقنية وسبل الوصول إلى المعلومات ذات الصلة (وهما شيئان قد لا يمتلكهما الموقّعون ولا الأطراف الثالثة المعوّلة).

١٩٠- وهذه هي الحالة أيضا في إطار قوانين داخلية شتى خارج الاتحاد الأوروبي تنص على قائمة مستفيضة بالواجبات التي ينبغي لمقدّمي خدمات التصديق أن يراعوها، وهي تخضعهم عموما للمسؤولية عن أي خسارة يسبّبها إخفاقهم في الامتثال لالتزاماتهم بمقتضى القوانين التشريعية.[٢٤٠] وليس من الواضح

---

[٢٣٨] "لا بدّ أن يكون هناك دليل معقول على حصول إهمال. ولكن، عندما يُبيَّن أن الشيء المعني خاضع لإدارة المدّعى عليه أو مستخدميه، وأن الحادث هو حادث لا يقع، في أثناء مجرى الأمور الاعتيادي، إذا ما حرص الذين يتولون الإدارة على توخي العناية على نحو صحيح، فإن ذلك يمثّل دليل إثبات معقولا، في حال عدم وجود توضيح من جانب المدّعى عليهم، على أن الحادث وقع من جراء انعدام العناية." (C. J. Erle in Scott v. *The London and St. Katherine's Docks Co.*, Ex. Ch., 3 H & C 596, 601, 159 Eng. Rep. 665, 667 (1865)).

[٢٣٩] *الجريدة الرسمية للجماعات الأوروبية* (*Official Journal of the European Communities,* L 13/12). المادة ٦ من التوجيه الإداري تنص على معيار حد أدنى من المسؤولية. وهذا من شأنه أن يتيح الإمكانية للدول المشترعة أن تعزز مسؤولية مقدّم خدمات التصديق، وذلك على سبيل المثال بتطبيق نظام المسؤولية المطلقة أو توسيع نطاق المسؤولية ليشمل شهادات التصديق المستوفية الشروط. غير أن ذلك لم يحدث حتى الآن ولا يُرجّح أن يحدث لأن من شأنه أن يضع مقدّمي خدمات التصديق التابعين لأحد البلدان في موقف غير مؤات مقارنة بغيرهم من مقدّمي خدمات التصديق التابعين لبلدان الاتحاد الأوروبي (Balboni "Liability of certification service providers ..."، الصفحة ٢٢٢.

[٢٤٠] الأرجنتين، *قانون التوقيعات الرقمية*، (٢٠٠١)، المادة ٣٨؛ شيلي، *القانون الخاص بالمستندات الإلكترونية والتوقيع الإلكتروني وخدمات التصديق على التوقيع الإلكتروني* (٢٠٠٢)، المادة ١٤؛ إكوادور، *قانون التجارة الإلكترونية والتوقيعات الإلكترونية ورسائل البيانات*، المادة ٣١؛ بنما، *قانون التوقيعات الرقمية* (٢٠٠١)، المادة ٥١؛ تونس، *القانون الخاص بالمبادلات والتجارة الإلكترونية*، المادة ٢٢.

تماما ما إذا كانت هذه القوانين كلها تلجأ فعلا إلى عكس عبء الإثبات، لكن عددا منها ينص بالفعل نصا صريحا تماما على الأخذ بهذا العكس، إما عموما،[٢٤١] وإما فيما يتعلق بالتزامات محدّدة.[٢٤٢]

١٩١- وهناك من يرى أنّ تفضيل الأخذ بنظام يقوم على الخطأ المفترض هو نتيجة لدواعي القلق من أن المسؤولية التي تستند إلى معيار الإهمال العادي لن تكون منصفة للطرف المعوّل، الذي قد تعوزه المعرفة التكنولوجية وكذلك سبل الوصول إلى المعلومات ذات الصلة، لكي يفي بعبء إظهار إهمال مقدّم خدمات التصديق.

'٣' *المسؤولية المطلقة*

١٩٢- قاعدة المسؤولية المطلقة أو "المسؤولية الموضوعية" هي قاعدة تُستخدم في نظم قانونية مختلفة من أجل عزو المسؤولية إلى شخص ما (عادة ما يكون هذا الشخص من صانعي أو متعهدي منتجات أو معدّات يُحتمل أن تكون خطرة أو مؤذية) من دون العثور على ما يدلّ على وقوع خطأ أو إخلال بواجب توخي العناية. ويُعتبر الشخص مسؤولا عن الضرر لسبب بسيط يعزى إلى طرحه منتجاً معيباً في السوق أو إلى سوء صنعه لقطعة من المعدّات. وبما أن هذه المسؤولية تُفترض من واقعة حدوث الخسارة أو الضرر فحسب، فليس ثمة من حاجة إلى إثبات العناصر القانونية الإفرادية اللازمة لإثبات تصرّف كالإهمال أو الإخلال بضمان أو السلوك العمدي.

١٩٣- كما إن قاعدة المسؤولية المطلقة هي قاعدة استثنائية بمقتضى أكثر النظم القانونية، ولا تُفترض في الأحوال الاعتيادية، في حال عدم وجود عبارة قانونية واضحة. وفي سياق طرائق التوقيع والتوثيق الإلكترونية، قد تؤدي المسؤولية المطلقة إلى إلقاء عبء مفرط على عاتق مقدّم خدمات التصديق، مما من شأنه أيضا أن يعوق صلاحية الصناعة للاستمرار تجاريا في مرحلة مبكرة من مسار تطورها. وفي الوقت الحالي، لا يبدو أن هناك بلدا يفرض مسؤولية مطلقة لا على مقدّم خدمات التصديق ولا على أي أطراف أخرى مشمولة في عملية إنشاء التوقيعات الإلكترونية. وصحيح أنه في البلدان التي تنص قوانينها على فهرس بالالتزامات الإيجابية على مقدّمي خدمات التصديق، عادة ما يكون معيار واجب العناية المفروض على مقدّمي خدمات التصديق عاليا جدا، ويقترب في بعض الحالات من نظام المسؤولية المطلقة، لكن مقدّم خدمات التصديق يستطيع مع ذلك إبراء ذمته من المسؤولية إذا استطاع أن يبيّن أنه تصرّف متوخّيا الحرص اللازم في عمله.[٢٤٣]

---

[٢٤١] الصين، قانون التوقيعات الإلكترونية، الصادر عام ٢٠٠٤، المادة ٢٨: "إذا تكبّد صاحب توقيع إلكتروني أو شخص يعوّل على توقيع إلكتروني خسارة نتيجة للتعويل على خدمة تصديق التوقيع الإلكتروني المقدّمة من مقدّم خدمات تصديق إلكتروني، أثناء قيامه بأنشطة مدنية، وإذا أخفق مقدّم خدمة التصديق الإلكتروني في تقديم دليل يثبت أن مقدّم الخدمة لم يرتكب خطأ، فعلى مقدّم خدمة التصديق الإلكتروني أن يتحمّل إذ ذاك المسؤولية عن التعويض عن الأضرار"؛ انظر أيضا تركيا، قانون التوقيعات الإلكترونية ٢٠٠٤، المادة ١٣: "يتحمّل مقدمو خدمات التصديق الإلكتروني المسؤولية عن التعويض عن الأضرار التي تتكبّدها أطراف ثالثة نتيجة لانتهاك أحكام هذا القانون أو الإعلانات القانونية التي تنشر وفقا لهذا القانون. ولا تقع المسؤولية التعويضية عن الأضرار على عاتق مقدّم خدمات التصديق الإلكتروني إذا أثبت عدم حدوث إهمال من جانبه."

[٢٤٢] "لا يتحمّل مقدّم خدمات التصديق المأذون له بالعمل المسؤولية عن الأغلاط في المعلومات الواردة في شهادة تصديق معتمدة عندما *(أ)* تكون المعلومات مقدّمة من الشخص المبيّنة هويته في الشهادة المعتمدة أو بالنيابة عنه؛ و*(ب)* يستطيع مقدّم خدمات التصديق أن يثبت أنه اتخذ جميع التدابير المعقولة عمليا بغية التحقق من تلك المعلومات (بربادوس، الفصل ٣٠٨ باء من قانون المعاملات الإلكترونية (١٩٩٨)، الفرع ٢٠)"؛ انظر أيضا برمودا، قانون المعاملات الإلكترونية، ١٩٩٩، الفرع ٢٣، الفقرة ٢ *(ب)*.

[٢٤٣] على سبيل المثال، في إكوادور وبنما وشيلي.

(ب) الأطراف التي يحق لها أن تطالب بتعويضات عن الأضرار ومقدار التعويضات الممكن تحصيلها

١٩٤- إحدى المسائل المهمّة في تعيين مدى مسؤولية مقدّمي خدمات التصديق والموقِّعين أيضا تتعلق بفئة الأشخاص الذين قد يحق لهم أن يطالبوا بتعويض عن الضرر الذي يسبّبه إخلال من جانب أي طرف بالتزاماته التعاقدية أو القانونية. والقضية الأخرى ذات الصلة بتلك المسألة تتعلق بمدى الالتزام بالتعويض وبأنواع الأضرار التي ينبغي التعويض عنها.

١٩٥- فالمسؤولية التعاقدية تترتّب عموما على الإخلال بالتزام تعاقدي. وفي سياق مرفق المفاتيح العمومية، يوجد عادة عقد بين الموقّع ومقدّم خدمات التصديق. ومن ثم فإن عواقب الإخلال من جانب أي واحد منهما بالتزاماته التعاقدية تجاه الآخر تقرّرها عبارات العقد، كما تحكمها القوانين الواجب تطبيقها على العقود. وفيما يخص التوقيعات وشهادات التصديق الإلكترونية، عادة ما تنشأ المسؤولية خارج إطار علاقة تعاقدية محدّدة بوضوح عندما يتكبّد شخص ما ضررا أثناء التعويل المعقول على المعلومات المقدّمة إما من مقدّم خدمات التصديق وإما من الموقّع، والتي تبيّن أنها زائفة أو غير دقيقة. وفي العادة، لا يبرم الطرف الثالث المعوِّل عقدا مع مقدّم خدمات التصديق، وقد لا يتعامل مع مقدّم خدمات التصديق على الإطلاق، ما عدا فيما يتعلق بالتعويل على الشهادة. وهذا يمكن أن يثير أسئلة صعبة لا تحظى بالإجابة الكاملة في بعض الولايات القضائية.

١٩٦- وفي إطار معظم نظم القانون المدني، يمكن أن يُفترَض أن مقدّم خدمات التصديق من شأنه أن يكون مسؤولا عن التعويض عن خسارة يتكبّدها الطرف المعوِّل نتيجة للتعويل على معلومات غير دقيقة أو زائفة، حتى من دون وجود أحكام محدّدة في هذا الخصوص في تشريعات محدّدة تعالج موضوع التوقيعات الإلكترونية. وفي عدّة ولايات قضائية، قد تُستخلص هذه المسؤولية من الحكم العام بشأن المسؤولية عن الضرر الذي اعتُمد في معظم تقنينات القانون المدني المدوّنة،[٢٤٤] مع بعض الاستثناءات القليلة.[٢٤٥] ففي بعض الولايات القضائية، يمكن إجراء قياس بين ما يقوم به مقدّم خدمات التصديق وما يقوم به الكتّاب العدول، الذين يعتبرون عموما مسؤولين عن الضرر الذي يسبّبه وقوع إهمال في أدائهم واجباتهم.

١٩٧- وأما في الولايات القضائية القائمة على القانون العام، قد لا يكون الوضع واضحا تماما. ذلك أنه في حال ارتكاب مضارّة في أداء الأفعال التي يحكمها عقد ما، كانت الولايات القضائية القائمة على القانون العام تلجأ تقليديا إلى اقتضاء وجود صلة تعاقد من نحو ما بين فاعل المضرّة والطرف المتضرّر. ولكن، بما أن الطرف الثالث المعوّل لا يبرم عقدا مع مقدّم خدمات التصديق، وقد لا يتعامل مع مقدّم خدمات التصديق على الإطلاق، باستثناء ما يتعلق بالتعويل على التصديق الزائف، فقد يصعب في بعض الولايات القضائية

---

[٢٤٤] المادة ١٣٨٢ من مدونة القوانين المدنية الفرنسية تنص على أنه أيا كان التصرف البشري الذي يسبّب ضررا لشخص آخر فإن الذي وقع الضرر من جراء خطئه يُلزَم بالتعويض عنه. وهذه القاعدة العامة بشأن المسؤولية قد استُلهمت منها أحكام مشابهة في عدّة بلدان أخرى، ومنها مثلا المادة ٢٠٤٣ من مدونة القوانين المدنية في إيطاليا، والمادة ٤٨٣ من مدونة القوانين المدنية في البرتغال.

[٢٤٥] تحتوي مدونة القوانين المدنية الألمانية على ثلاثة أحكام عامة (في الفروع ٨٢٣ أولا، و٨٢٣ ثانيا، و٨٢٦)، وعلى بعض من القواعد المحدّدة التي تعالج عددا من حالات المضارّة الضيقة التحديد على الأرجح. والحكم الرئيسي هو في الفرع ٨٢٣ أولا، والذي يختلف عن المدونة الفرنسية من حيث إنه يشير صراحة إلى إيذاء شخص آخر في حياته أو بدنه أو صحته أو حريته أو ممتلكاته أو في أي حق له من حقوقه.

القائمة على القانون العام (في حال عدم وجود حكم قانوني صريح) على الطرف المعوّل أن يثبت سببا لرفع دعوى على مقدّم خدمات التصديق.[٢٤٦] فإذا لم تكن هناك صلة تعاقد، فإن أي سبب لرفع دعوى بناءً على المضرّة بمقتضى القانون العام من شأنه أن يتطلّب تبيان حدوث إخلال بواجب العناية يدين به فاعل المضرّة تجاه الطرف المتضرّر. وليس واضحا كليا ما إذا كان يوجد واجب من هذا النحو على مقدّم خدمات التصديق إزاء جميع الأطراف المعوِّلة المحتمَلَة. وعلى العموم، يُحجِم القانون العام عن إخضاع شخص "للمسؤولية عن دفع تعويض بمقدار غير محدّد طوال فترة غير محدّدة من الزمن، لفئة غير محدّدة"[٢٤٧] بسبب بيان خاطئ ناجم عن إهمال، ما لم تكن الكلمات التي نُطق بها بإهمال "قد قيلت بلفظها مباشرة، مع معرفة أو ملاحظة أنها سوف يُتصرّف بناء عليها، لشخص ما يلتزم المتكلّم تجاهه بعلاقة واجب من نحو ما، بحكم منصب عام أو عقد أو غير ذلك، بأن يتصرّف بعناية فيما لو تصرّف فعلا."[٢٤٨]

١٩٨- وفي هذه الحالة، تتمثل المسألة الأساسية في تحديد طائفة الأشخاص الذين يدين لهم مقدّم خدمات التصديق (أو الموقّع فيما يتعلق بذلك) بواجب العناية. وهناك أساسا ثلاثة معايير قد تُستخدم في تحديد تلك الطائفة من الأشخاص الذين يجوز لهم في حال من هذا القبيل أن يؤكدوا حسب الأصول الصحيحة ما لهم من مطالبات على مقدّم خدمات التصديق، وهي:[٢٤٩]

(أ) *معيار إمكانية التوقّع*. هذا أوسع معايير المسؤولية نطاقا. وبناء على هذا المعيار، سوف يكون الموقّع أو مقدّم خدمات التصديق مسؤولا عن التعويض عن الضرر تجاه أي شخص كان تعويله على البيانات الزائفة يمكن توقّعه على نحو معقول؛

(ب) *المعيار القائم على النيّة والمعرفة*. هذا معيار أضيق نطاقا من سابقه، يقصر المسؤولية على الخسارة التي يتكبّدها واحد من مجموعة الأشخاص الذين ينوي الشخص المعني أن يقدّم لهم معلومات لكي يستفيدوا ويسترشدوا بها، أو يعرف أن متلقيها ينوي تقديمها؛

(ج) *معيار الصلة القانونية*. هذا أكثر المعايير تقييدا، فهو يقتضي إنشاء واجب يُؤدّى للزبون فحسب، أو لشخص تربطه بمقدّم المعلومات صلة محددة.

١٩٩- لكن قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لا يسعى إلى الإحاطة الشاملة بجميع الأشخاص الذين قد يندرجون ضمن فئة الأطراف المعوِّلة، والتي يمكن أن تشمل "أي شخص له علاقة تعاقدية بالموقّع أو مقدّم خدمات التصديق أو ليست له علاقة تعاقدية بهما".[٢٥٠] وعلى نحو مماثل، يقتضي التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية أن يعتبر مقدّم خدمات

---

[٢٤٦] على سبيل المثال، فيما يتعلق بالقانون العام الإنكليزي، يستنتج أحد المؤلفين بأنه "في حال عدم وجود تشريع، فإن مسؤولية [مقدّم خدمات التصديق] تجاه [الطرف الثالث] بعيدة عن اليقين، ومع ذلك فإنه يمكن التكهّن بأن [الطرف الثالث] يتكبّد خسارة نتيجة إهماله. علاوة على ذلك، فإن من الصعب أن يرى المرء كيف يستطيع [الطرف الثالث] أن يحمي نفسه. فإذا لم تكن هناك مسؤولية عن الضرر، فإنه يمكن الاحتجاج بأن هناك ثغرة واضحة على الأقل. وقد يسدّ القانون العام الثغرات، لكن العملية الإجرائية لا تتسم باليقين ولا يُعوّل عليها" (Paul Todd, E-Commerce Law (Abingdon, Oxon, Cavendish Publishing Limited (2005), pp. 149-150). وقد تم التوصل إلى استنتاجات مشابهة بخصوص القانون الأسترالي، انظر Sneddon, *Legal liability and e-transactions* ...، *الصفحة* ١٥.

[٢٤٧] Judge Cardozo in *Ultramares Corporation v. George A. Touche et al*, Court of Appeals of New York 6 January, 1931, 174 N.E. 441, p. 445.

[٢٤٨] Judge Cardozo in *Ultramares Corporation v. George A. Touche et al* ..., p. 447.

[٢٤٩] Smedinghoff, "Certification authority: liability issues" ..., sect. 4.3.1.

[٢٥٠] *قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية* . . . ، الفقرة ١٥٠.

التصديق مسؤولا عن التعويض عن وقوع أضرار تجاه "أي كيان أو شخص اعتباري أو طبيعي يعوّل على نحو معقول" على شهادة التصديق المستوفية الشروط. والواضح أن التوجيه الإداري الصادر عن الاتحاد الأوروبي يستند إلى وجود مخطط خاص بمرافق المفاتيح العمومية، لأنه لا يطبّق إلا في حالات التوقيعات الرقمية (شهادات التصديق المستوفية الشروط). ومفهوم الكيان يُفسّر عادة بأنه يشير إلى الأطراف الثالثة المعوّلة، وقد أخذت بتنفيذ التوجيه الإداري بهذا المعنى جميع الدول ما عدا اثنتين منها.[٢٥١]

٢٠٠- وعلى غرار قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، لا يضيّق التوجيه الإداري الصادر عن الاتحاد الأوروبي فئات الأشخاص الذين يجوز أن يكونوا مستوفي الشروط لاعتبارهم من الأطراف المعوّلة. ولذلك فقد رُئي بأنه حتى في إطار القانون العام "من البديهي فيما يتعلق بتقديم خدمات التصديق أن يكون مقدّمو خدمات التصديق ملزمين بواجب توخي العناية تجاه كل من قد يُعوِّل على شهادات التصديق الصادرة عنهم في اتخاذ قراره بشأن القبول بتوقيع إلكتروني معيّن في معاملة معيّنة، لأن الغرض الجوهري الذي تصدر من أجله الشهادة هو التشجيع على ذلك التعويل".[٢٥٢]

٢٠١- وهناك جانب آخر يثير الاهتمام يتعلق بطبيعة الخسارة التي يمكن استردادها من موقّع أو مقدّم خدمات تصديق. ففي بعض الولايات القضائية القائمة على القانون العام، مثلا، تعتبر المطالبات بالتعويض عن الخسارات الاقتصادية المحض الناجمة عن عيوب في المنتجات، غير قابلة لتحصيلها بناء على المضرّة التقصيرية. غير أن هناك حالات من الاحتيال المتعمَّد، أو حتى حالات من سوء الإفادة الناجم عن إهمال في بعض الولايات القضائية القائمة على القانون العام، تعتبر استثناءات من قاعدة الخسارة الاقتصادية.[٢٥٣] ومن المثير للاهتمام أن يلاحظ في هذا الصدد أن اللوائح التنظيمية للتوقيعات الإلكترونية لعام ٢٠٠٢ في المملكة المتحدة لم تستنسخ أحكام المسؤولية الواردة في التوجيه الإداري بشأن التوقيعات الإلكترونية الصادر عن الاتحاد الأوروبي. ولذا فإن هناك قواعد معيارية بشأن المسؤولية تُطبّق فيما يتعلق، في هذه الحالة، باختبار مدى قُرب احتمال وقوع الضرر.[٢٥٤] وأما مقدار التعويضات التي يمكن تحصيلها عن الأضرار، فهي مسألة تُترك عادة لتقريرها بمقتضى القوانين العامة بشأن العقود أو بشأن المضارّة. وبعض القوانين يقتضي صراحة من مقدّمي خدمات التصديق أن يحصلوا على تأمين على المسؤولية عن الأضرار، أو أن يعلنوا لجميع الموقّعين المحتملين، ضمن ما يقدمونه لهم من معلومات، عن الكفالات المالية بشأن مسؤوليتهم المحتملة عن الأضرار.[٢٥٥]

(ج) القدرة على الحدّ من المسؤولية أو التنصّل منها تعاقديا

٢٠٢- من المتوقّع من مقدّمي خدمات التصديق أن يسعوا بقدر الإمكان عادة إلى الحد من مسؤوليتهم التعاقدية أو مسؤوليتهم عن المضرّة التقصيرية تجاه الأطراف الموقّعة والمعوّلة. أما فيما يخص الموقّع، فستكون البنود التقييدية مدرجة عادة ضمن عدّة عناصر من وثائق العقد، ومنها مثلا بيانات الممارسة المتّبعة في عملية التصديق. وتلك البيانات قد تفرض حدا أعلى للمسؤولية بحسب الحوادث العرضية، أو بحسب سلسلة

---

[٢٥١] الاستثناءان هما الدانمرك وهنغاريا، Balboni, "Liability of certification service providers ..."، الصفحة ٢٢٠.

[٢٥٢] Lorna Brazell, Electronic Signatures: *Law and Regulation* (London, Sweet and Maxwell, 2004), p. 187.

[٢٥٣] Smedinghoff, "Certification authority: liability issues" ..., section 4.5.

[٢٥٤] Dumortier and others, "The legal and market aspects of electronic signatures" ..., p. 215.

[٢٥٥] تركيا، قانون التوقيعات الإلكترونية، ٢٠٠٤، المادة ١٣؛ الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٢١ *(أ)* (١)؛ انظر أيضا المكسيك، *مدونة القوانين التجارية: المرسوم المتعلق بالتوقيعات الإلكترونية (٢٠٠٣)*، المادة ١٠٤ (ثالثا).

الحوادث العرضية، أو بحسب الفترة الزمنية، وقد تستبعد فئات معيّنة من الأضرار. ويمكن أن يتمثّل أسلوب آخر في تضمين شهادات التصديق الحد الأقصى من قيمة المعاملة التي يجوز استخدام الشهادة من أجلها، أو قصر استخدام الشهادة على أغراض معيّنة فقط.[٢٥٦]

٢٠٣- وفي حين يعترف معظم النظم القانونية، عموما، بحق الأطراف في العقد في اللجوء إلى الحد من المسؤولية أو استبعادها من خلال الأحكام التعاقدية، فإن هذا الحق يخضع عادة إلى قيود وشروط مختلفة. ففي معظم الولايات القضائية القائمة على القانون المدني، مثلا، يعتبر اللجوء إلى استبعاد كلي لمسؤولية شخص ما عن خطأ من جانبه، غير مسموح به،[٢٥٧] أو يكون خاضعا لتقييدات واضحة.[٢٥٨] علاوة على ذلك، إذا كانت شروط العقد لم يتم التفاوض عليها بحرية، بل فرضها أحد الأطراف أو قرّرها مسبقا ("عقود الإذعان")، فقد يتبيّن أن بعض الأنواع من البنود التقييدية تعتبر "تعسفية" ومن ثم باطلة.

٢٠٤- وأما في الولايات القضائية التي تطبّق القانون العام، فقد تُستخلص نتيجة مشابهة من نظريات مختلفة. ففي الولايات المتحدة، على سبيل المثال، تلجأ المحاكم عموما إلى عدم إنفاذ أحكام تعاقدية يتبيّن أنها "منافية للضمير". ومع أن هذا المفهوم يعتمد عادة على تقرير الظروف المعيّنة المحيطة بالقضية، فإنه يشير عموما إلى شروط العقد "التي لا يضعها أي إنسان عاقل، وغير متوهّم، من ناحية، ولا يقبلها أي إنسان منصف وأمين، من ناحية أخرى"،[٢٥٩] والتي تتميز "بعدم وجود خيار مجدٍ من جانب أحد الطرفين إضافة إلى كون أحكام العقد محابية على نحو غير معقول للطرف الآخر".[٢٦٠] وعلى نحو مماثل لمعالجة مفهوم "عقد الإذعان" في القانون المدني، طُبّق هذا المذهب للحيلولة دون اللجوء إلى "الممارسات التجارية غير المستقيمة" من جانب أطراف لديها تفوّق في القدرة على المساومة.[٢٦١] وليس كل شرط تعاقدي ينحو هذا المنحى باطلا. ولكن مع أن المحاكم تعمد عموما إلى إنفاذ شكل نموذجي ما من عقود الإذعان، التي تنعدم فيها القدرة على المساومة بخصوص الشروط، حتى في عقود المستهلكين، فإنه يحدث أحيانا أن تمتنع المحكمة عن إنفاذ بند في عقد نموذجي إذا ما أدى إدراجه في العقد إلى مفاجأة مجحفة.[٢٦٢]

---

(٢٥٦) Smedinghoff, "Certification authority: liability issues" ..., section 5.2.5.4; and Hindelang, "No remedy for disappointed trust ...", section 4.1.1.

(٢٥٧) في فرنسا، يمكن من حيث المبدأ استبعاد المسؤولية الناجمة عن إخلال بالعقد. ولكن من حيث الممارسة العملية، تميل المحاكم إلى إبطال تلك البنود حيثما يتبيّن أن البند المعني قد يحل الطرف من عواقب إخلال بالتزام تعاقدي "جوهري" (انظر Légier, "Responsabilité contractuelle"، العددين ٢٦٢ و٢٦٣).

(٢٥٨) في معظم بلدان القانون المدني، يحظر القانون التنصّل من المسؤولية الناجمة عن إهمال أو إخلال جسيم بواجب تفرضه قاعدة من قواعد السياسة العامة. ولدى بعض البلدان قواعد صريحة في هذا الشأن، ومن ذلك مثلا المادة ١٠٠ ثانيا من مدونة قوانين الالتزامات في سويسرا، والمادة ١٢٢٩ من مدونة القوانين المدنية في إيطاليا. وهناك بلدان أخرى، مثل البرتغال، ليس لديها قواعد قانونية مشابهة، لكنها تحقّق النتيجة نفسها أساسا، مثل إيطاليا (انظر Pinto Monteiro, *Cláusulas Limitativas e de Exclusão de Responsabilidade Civil* (Coimbra, Faculdade de Direito de Coimbra, 1985)، الصفحة ٢١٧.

(٢٥٩) *First Financial Ins. Co. v. Purolator Security, Inc.*, 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), citing Hume v. U.S., 132 U.S. 406, 410 (1975), cited in Smedinghoff, "Certification authority: liability issues" ..., section 5.2.5.4.

(٢٦٠) *First Financial Ins. Co. v. Purolator Security, Inc* ..., citing Williams v. Walker-Thomas Furniture Co., 350 F.2d 315, 320 (D.C. 1965), cited in Smedinghoff, "Certification authority: liability issues" ..., section 5.2.5.4.

(٢٦١) *First Financial Ins. Co. v. Purolator Security, Inc*., 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), cited in Smedinghoff, "Certification authority: liability issues" ..., section 5.2.5.4.

(٢٦٢) Raymond T. Nimmer, *Information Law,* section 11.12[4][a], at 11-37, cited in Smedinghoff, "Certification authority liability issues" ..., section 5.2.5.4.

٢٠٥- وأخيرا، فإن من الجائز، في نظامي القانون المدني والقانون العام كليهما، أن تعمد قواعد حماية المستهلكين إلى تقليص قدرة مقدّم خدمات التصديق بدرجة كبيرة على الحد من مسؤوليته عن الضرر تجاه الموقّع، وذلك في الظروف التي يؤدّي فيها تقييد هذه المسؤولية إلى حرمان الموقّع فعلا من حق أو من سبيل انتصاف يعترف بهما القانون الواجب تطبيقه.

٢٠٦- وأما الإمكانية المتاحة لمقدّم خدمات التصديق لكي يحد من مسؤوليته المحتملة تجاه الطرف المعوّل فمن شأنها أن تكون في معظم الحالات خاضعة لقيود أكبر كثيرا من ذلك. وما عدا نماذج الأعمال التجارية المغلقة التي يكون من اللازم فيها للطرف المعوّل أن يتقيّد بشروط العقد،[٢٦٣] فإن الطرف المعوّل كثيرا جدا ما لا يكون ملزما بموجب عقد تجاه مقدّم خدمات التصديق أو حتى تجاه الموقّع. ومن ثم، فبقدر ما تكون لدى الطرف المعوّل مطالبة بشأن مضارّة تقصيرية تجاه مقدّم خدمات التصديق أو الموقّع، قد لا تكون لدى هذين الطرفين أي وسيلة للحد من مسؤوليتهما فعلا، لأن من شأن ذلك أن يتطلب، بمقتضى معظم النظم القانونية، توجيه إشعار واف بالغرض إلى الطرف المعوّل بخصوص تقييد المسؤولية. كما إن عدم معرفة هوية الطرف المعوّل قبل وقوع الضرر قد يمنع مقدّم خدمات التصديق (وهناك من يقول إن ذلك قد يمنع الموقّع في حالات أكثر) من اللجوء إلى تهيئة نظام فعال لغرض الحد من مسؤوليته. وهذه المشكلة عادة ما تظهر في النظم المفتوحة حيث يتفاعل الغرباء من دون اتصال مسبق، وهي تترك الموقّع معرّضا لعواقب يُحتمل أن تكون وخيمة عليه.[٢٦٤] وهذه الحال يرتئي الكثيرون، وخصوصا ممثلي صناعة التصديق، أنها عائق خطير الشأن أمام اتساع نطاق استخدام طرائق التوقيع والتوثيق الإلكترونية، باعتبار الصعوبة التي يلقاها مقدّمو خدمات التصديق في تقدير مدى تعرّضهم للمسؤولية.

٢٠٧- وقد حدت الرغبة في توضيح القانون في هذا الشأن بعدد من البلدان إلى الاعتراف صراحة بحق مقدّمي خدمات التصديق في الحد من مسؤوليتهم. فعلى سبيل المثال، يُلزم التوجيه الإداري الصادر عن الاتحاد الأوروبي الدول الأعضاء في الاتحاد الأوروبي بضمان جواز أن يبيّن مقدّم خدمات التصديق في شهادة تصديق مستوفية الشروط "التقييدات على استخدام تلك الشهادة" ما دامت تلك التقييدات "معترفا بها لدى أطراف ثالثة".[٢٦٥] وهذه التقييدات قد تكون عادة من فئتين: فقد تكون هناك قيود تحد من أنواع المعاملات التي يجوز استخدام شهادات معيّنة أو أصناف معيّنة من الشهادات؛ وقد تكون هناك أيضا قيود تحد من قيمة المعاملات التي يجوز من أجلها استخدام الشهادة المعيّنة أو الصنف المعيّن من الشهادات بخصوصها. وبمقتضى أي من هاتين الفرضيتين، فإن مقدّم خدمات التصديق يُعفى صراحة من المسؤولية "عن الضرر الناجم عن استخدام شهادة تصديق مستوفية الشروط تتجاوز نطاق التقييدات المفروضة عليها"[٢٦٦] علاوة على ذلك، فإن التوجيه الإداري الصادر عن الاتحاد الأوروبي يكلّف الدول الأعضاء في الاتحاد بمهمة ضمان

---

[٢٦٣] كما هو متوخّى بشأن اتحاد التوثيق الإلكتروني: E-Authentication Federation administered by the General Services Administration of the United States Government (انظر E-Authentication Federation, Interim Legal Document Suite, version 4.0.7، متاحة على الموقع الشبكي http://www.cio.gov/eauthentication/، وقد اطلع عليه في ٨ شباط/ فبراير ٢٠٠٧).

[٢٦٤] Sneddon p. 18 "*Legal liability and e-transactions* ...",

[٢٦٥] European Union directive on electronic signatures, article 6, paragraph 3.

[٢٦٦] European Union directive on electronic signatures ...

"جواز أن يبيّن مقدّم خدمات التصديق في الشهادة المستوفية الشروط حدا يفرضه على قيمة المعاملة التي يمكن استخدام الشهادة من أجلها، شريطة أن يكون ذلك الحد معترفا به لدى أطراف ثالثة".[٢٦٧] وفي تلك الحالة، لا يكون مقدّم خدمات التصديق مسؤولا عن التعويض عن الضرر الناتج عن تجاوز هذا الحد الأقصى.[٢٦٨]

٢٠٨- لكنّ التوجيه الإداري الصادر عن الاتحاد الأوروبي لا يضع حدا أعلى للمسؤولية التعويضية التي يجوز أن يتكبّدها مقدّم خدمات التصديق. غير أن التوجيه الإداري يتيح المجال بالفعل لمقدّم خدمات التصديق لكي يحد من القيمة القصوى بحسب المعاملة التي يجوز استخدام الشهادة من أجلها، معفيا بذلك مقدّم خدمات التصديق من المسؤولية التعويضية التي تتجاوز حد القيمة الأعلى.[٢٦٩] وعلى سبيل الممارسة المتّبعة في الأعمال التجارية، كثيرا ما يلجأ أيضا مقدّمو خدمات التصديق إلى اعتماد حد أعلى إجمالي بشأن مسؤوليتهم التعويضية، بناء على أساس تعاقدي.

٢٠٩- وهناك عدّة قوانين داخلية أخرى تؤيّد تلك الممارسات التعاقدية بالاعتراف بحد للمسؤولية التي يتحمّلها مقدّم خدمات التصديق تجاه أي طرف يُحتمل أن يلحق به ضرر. وفي العادة، تسمح هذه القوانين بوضع تقييدات حسبما هو محدّد في بيان الممارسة المتّبعة الصادر عن مقدّم خدمات التصديق، وفي بعض الحالات تعفي هذه القوانين صراحة مقدّم خدمات التصديق من المسؤولية إذا ما استُخدمت شهادة ما لغرض يختلف عن الغرض الذي صدرت من أجله.[٢٧٠] علاوة على ذلك، تعترف بعض القوانين بحق مقدّمي خدمات التصديق في إصدار شهادات تصديق من أصناف مختلفة وفي وضع مستويات تعويل مختلفة مُوصى بها،[٢٧١] مما يتيح عادة مستويات مختلفة من التقييد (ومن الأمان) تبعا للأجرة المدفوعة. غير أن بعض القوانين الأخرى تحظر صراحة فرض أي قيود تحدّ من المسؤولية غير ما هو ناتج عن القيود المفروضة على استخدام الشهادات أو قيمتها.[٢٧٢]

٢١٠- أما البلدان التي أخذت بنهج الحد الأدنى من الشروط، فقد اعتبرت أن التدخّل التشريعي في هذا الخصوص غير مرغوب فيه عموما، وفضّلت أن تترك هذه المسألة للأطراف لكي تقرّرها بموجب عقد.[٢٧٣]

---

[٢٦٧] European Union directive on electronic signatures, article 6, paragraph 4.

[٢٦٨] European Union directive on electronic signatures ...

[٢٦٩] Dumortier and others "The legal and market aspects of electronic signatures"..., p. 55؛ انظر أيضا Hindelang "No remedy for disappointed trust ..." section 4.1.1؛ أما بالبوني ("Liability of certification service providers ..."), p. 230 فهو يذهب إلى أبعد من ذلك، إذ يفيد بأنه "بمقتضى المادة ٦ (٤)، لا يجوز سوى الحد من قيمة المعاملة [. . .]، وهذا لا علاقة له بالمبلغ المحتمل للتعويض الذي يمكن أن يترتب على تلك المعاملة".

[٢٧٠] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٣٩؛ بربادوس، الفصل ٣٠٨ باء من قانون المعاملات الإلكترونية (١٩٩٨)، الباب ٢٠، الفقرتان ٣ و٤؛ برمودا، قانون المعاملات الإلكترونية، ١٩٩٩، الباب ٢٣، الفقرتان ٣ و٤؛ شيلي، *القانون الخاص بالمستندات الإلكترونية والتوقيعات الإلكترونية وخدمات التصديق على التوقيعات الإلكترونية (٢٠٠٢)*، المادة ١٤؛ فييت نام، القانون المتعلق بالمعاملات الإلكترونية، المادة ٢٩، الفقرتان ٧ و٨ (هذا القانون الأخير لا يتضمن إعفاء صريحا من المسؤولية).

[٢٧١] سنغافورة، قانون المعاملات الإلكترونية (الفصل ٨٨) لعام ١٩٨٨، البابان ٤٤ و٤٥؛ موريشيوس، قانون المعاملات الإلكترونية لعام ٢٠٠٠، المادتان ٣٨ و٣٩.

[٢٧٢] تركيا، قانون التوقيعات الإلكترونية لعام ٢٠٠٤، المادة ١٣.

[٢٧٣] انظر بخصوص أستراليا Sneddon, Legal liability and e-transactions (see note [11]), pp. 44-47; and for the United States, Smedinghoff, "Certification authority: liability issues" ..., section 5.2.51.

٢- حالات خاصة للمسؤولية في إطار مرفق للمفاتيح العمومية

٢١١- لقد ظلت المناقشات حول المسؤولية فيما يتصل باستخدام طرائق التوقيع والتوثيق الإلكترونية منصبّة بشكل رئيسي على أساس مسؤولية مقدّمي خدمات التصديق وسمات تلك المسؤولية. ومن المسلم به عموما أن الواجب الأساسي لمقدّم خدمات التصديق هو أن يستخدم نظما وإجراءات وموارد بشرية جديرة بالثقة وأن يتصرّف وفقا للتأكيدات التي يقدمها بشأن سياساته وممارساته.[٢٧٤] وإضافة إلى ذلك، يتوقع من مقدّم خدمات التصديق أن يولي قدرا معقولا من العناية لضمان دقة واكتمال كل ما يقدّمه من تأكيدات جوهرية ذات صلة بالشهادة. وربما تُعرّض هذه الأنشطة كلّها مقدّم خدمات التصديق لدرجات متفاوتة من المسؤولية حسب القانون الواجب التطبيق. وتبين الفقرات التالية الحالات التي تنطوي على احتمال تعرض مقدّم خدمات التصديق لقدر أكبر من المسؤولية وتوجز الطرائق التي تتناول بها القوانين الداخلية تلك المسؤولية.

(أ) عدم إصدار الشهادة أو التأخر في إصدارها

٢١٢- يُصدر مقدّم خدمات التصديق الشهادات عادة بناء على طلبات يقدمها الموقّعون المرشحون. وإذا ما استوفى الطلب المعايير التي وضعها مقدّم خدمات التصديق، جاز لمقدّم خدمات التصديق أن يصدر الشهادة. وقد يحصل أن يستوفي مقدّمُ الطلب المعايير، إلا أن طلبه يرفض أو يؤخر إصداره رغم ذلك، إما بسبب ارتكاب مقدّم خدمات التصديق خطأ فحسب، أو لأن مرافق تقديم الطلبات الخاصة بمقدّم خدمات التصديق لم تكن متاحة عمدا أو عرضا، أو لأن مقدّم خدمات التصديق يرغب، لدوافع خفية، في تأخير إصدار شهادة لمقدّم الطلب أو يرفض إصدارها. ويجوز لمقدّمي الطلبات الذين ترفض طلباتهم أو تؤخر في ظروف من هذا القبيل أن يقدموا مطالبات تجاه مقدّم خدمات التصديق.[٢٧٥]

٢١٣- وإذا كانت ثمة سوق تنافسية لخدمات التصديق، فربما لا يكون هناك ضرر حقيقي يلحق بمقدّم الطلب إذا ما رفض أحد مقدّمي خدمات التصديق إصدار الشهادة، سواء عرضا أم عمدا. ولكن، في ظل عدم وجود تنافس حقيقي، فربما ينجم عن رفض مقدّم خدمات التصديق إصدار الشهادة أو تأخير إصدارها ضرر خطير عندما لا يتمكن مقدّم الطلب المرفوض من المشاركة في عمل تجاري بعينه بدون الشهادة. وحتى إن كانت ثمة بدائل تنافسية متاحة، فيمكن تصور خسائر تتصل بمعاملات محددة وتنجم عن الظروف التي تُطلب فيها شهادة فيما يتعلق بمعاملة معينة ولا تكون الشهادة متاحة، نتيجة للتأخير أو الرفض، في الوقت المناسب لإجراء المعاملة المعتزمة، مما يضطر مقدّم الطلب إلى التراجع عن المعاملة المربحة.[٢٧٦]

---

[٢٧٤] قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية . . . ، الفقرتان الفرعيتان ١ *(أ)* و١ *(ب)* من المادة ٩.

[٢٧٥] "Certification authority: liability issues" Smedinghoff ..., section 3.2.1.

[٢٧٦] "Certification authority: liability issues" Smedinghoff ..., section 3.2.1.

٢١٤- ولا يُرجح أن ينشأ مثل هذا السيناريو في سياق دولي، لأن معظم الموقّعين يسعون على الأرجح إلى الحصول على خدمات التصديق من مقدّمي خدمات تصديق في بلدانهم.

(ب) الإهمال لدى إصدار الشهادة

٢١٥- الوظيفة الرئيسية للشهادة هي ربط هوية الموقّع بمفتاح عمومي. وبناء على ذلك، تكون المهمة الرئيسية لمقدّم خدمات التصديق هي التحقق، وفقا لممارساته المعلنة، من أن مقدّم الطلب هو الموقّع المزعوم وأنه يسيطر على المفتاح الخصوصي المقابل للمفتاح العمومي المدرج في الشهادة. وعدم القيام بذلك يمكن أن يعرّض مقدّم خدمات التصديق لمسؤولية محتملة تجاه الموقّع أو تجاه طرف ثالث يعوِّل على الشهادة.

٢١٦- وربما يلحق ضرر بالموقّع، على سبيل المثال، بسبب إصدار الشهادة خطأ لمحتال يستخدم هوية مختلسة. وربما يتآمر مستخدَمو مقدّم خدمات التصديق أو المتعاقدون معه على إصدار شهادات خاطئة باستخدام مفتاح التوقيع الخاص بمقدّم خدمات التصديق بخصوص طلبات غير سليمة يقدمها المحتال. وربما يصدر أولئك الأشخاص بإهمال شهادة خاطئة، إما من خلال عدم القيام بإجراءات التحقق التي أعلن عنها مقدّم خدمات التصديق لدى استعراض طلب المحتال، أو باستخدام مفتاح التوقيع الخاص بمقدّم خدمات التصديق لإنشاء شهادة لم يوافق على إصدارها. وأخيرا، ربما يقوم الجاني بانتحال شخصية الموقّع باستخدام وثائق هوية مزورة، ولكنها تبدو أصلية، وإقناع مقدّم خدمات التصديق، رغم توخي الحرص والامتثال دون إهمال لسياساته المنشورة، بإصدار شهادة للمحتال.[٢٧٧]

٢١٧- ويمكن أن يكون لإصدار شهادة خطأ لشخص محتال آثار خطيرة. فالأطراف المعوّلة التي تُجري مع المحتال معاملات بالاتصال الحاسوبي المباشر قد تعوّل على البيانات غير الصحيحة في الشهادة المصدرة خطأ وتقوم، نتيجة لذلك التعويل، بشحن بضاعة أو تحويل أموال أو تقديم ائتمان أو الاضطلاع بمعاملات أخرى معتقدة أنها تتعامل مع الطرف المنتحلة شخصيته. وعند اكتشاف الاحتيال، ربما تكون الأطراف المعوّلة قد تكبدت خسارة فادحة. وفي هذه الحالة، يوجد طرفان متضرران: الطرف المعوّل الذي تعرض للاحتيال بالشهادة المصدرة خطأ، والشخص الذي انتحلت شخصيته في تلك الشهادة. وسيكون لكليهما مطالبات تجاه مقدّم خدمات التصديق. وثمة سيناريو آخر قد ينجم عن إصدار شهادة بإهمال لشخص وهمي، وفي هذه الحالة لا يتكبد الضرر سوى الطرف المعوّل.[٢٧٨]

٢١٨- وتنص المادة ٩ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية على جملة أمور منها أن يولي مقدّم خدمات التصديق قدرا معقولا من العناية لضمان دقة واكتمال كل ما يقدّمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها، أو مدرجة في الشهادة. وقد نُقل هذا الواجب العام حرفيا

[٢٧٧] "Certification authority: liability issues" Smedinghoff ..., section 3.2.1.

[٢٧٨] "Certification authority: liability issues" (Smedinghoff ..., section 3.2.1.

إلى التشريعات الداخلية لعدة بلدان تنفذ القانون النموذجي،[٢٧٩] رغم أنّ معيار القدر المعقول من العناية يبدو أنه رفع في بعض البلدان إلى معيار ضمان أعلى.[٢٨٠]

٢١٩- والنظام الذي أنشأه التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية يلزم الدول الأعضاء في الاتحاد الأوروبي بأن تضمن، "كحد أدنى"، أن يكون مقدّم خدمات التصديق، لدى إصدار شهادة باعتبارها شهادة مستوفية الشروط للجمهور، أو بضمان شهادة من هذا القبيل للجمهور، مسؤولا عن الضرر الذي يلحق بأي كيان أو شخص قانوني أو طبيعي يعوّل على نحو معقول على تلك الشهادة: *(أ)* فيما يتعلق بدقة جميع المعلومات الواردة في الشهادة المستوفية الشروط، وقت إصدارها، وفيما يتعلق باحتواء تلك الشهادة على كل التفاصيل المشترط توافرها فيها؛ *(ب)* وعن ضمان أن يكون الموقّع المعرف في الشهادة المستوفية الشروط، وقت إصدارها، حائزا لبيانات إنشاء التوقيع المقابلة لبيانات التحقق من التوقيع الواردة في الشهادة أو المعرّفة فيها؛ *(ج)* وعن ضمان إمكانية استخدام بيانات إنشاء التوقيع وبيانات التحقق من التوقيع على نحو تكاملي في الحالات التي ينشئ فيها مقدّم خدمات التصديق كلا النوعين؛ ما لم يثبت مقدّم خدمات التصديق أنه لم يتصرف بإهمال.[٢٨١]

٢٢٠- وتتفق قوانين داخلية أخرى عموما على إلزام مقدّمي خدمات التصديق بالتحقق من دقة المعلومات التي تصدر الشهادات بناء عليها. وفي بعض البلدان، يحمَّل مقدّم خدمات التصديق عموما المسؤولية تجاه أي شخص يعول على نحو معقول على الشهادة عن دقة جميع المعلومات الواردة في الشهادة المعتمدة اعتبارا من التاريخ الذي تُصدر فيه،[٢٨٢] أو أن يكفل دقتها،[٢٨٣] رغم أنه يجوز لمقدّم خدمات التصديق في بعض تلك البلدان أن يتحفظ على هذا الضمان ببيان مناسب في الشهادة.[٢٨٤] غير أن بعض القوانين تبرئ صراحة ذمة مقدّم خدمات التصديق من المسؤولية عما يقدمه الموقّع من معلومات غير دقيقة، رهنا بالتحقق وفقا لبيان ممارسة التصديق، شريطة أن يكون بمقدور مقدّم خدمات التصديق أن يثبت أنه قد اتخذ جميع التدابير المعقولة للتحقق من المعلومات.[٢٨٥]

---

[٢٧٩] على سبيل المثال، تايلند، قانون المعاملات الإلكترونية (٢٠٠١)، الفقرة (٢) من الباب ٢٨، وجزر كايمان (وهي إقليم وراء البحار تابع للمملكة المتحدة)، قانون المعاملات الإلكترونية لسنة ٢٠٠٠، الباب ٢٨ *(ب)*.

[٢٨٠] على سبيل المثال، الصين، قانون التوقيعات الإلكترونية، المادة ٢٢: "يضمن مقدّمو خدمات التصديق أن تكون محتويات شهادات التوقيع الإلكتروني كاملة ودقيقة خلال فترة سريانها، ويضمنون أن يكون بإمكان الأطراف المعوّلة على التوقيعات الإلكترونية التحقق من محتويات شهادات التوقيع الإلكتروني المسجلة وغيرها من المسائل ذات الصلة أو فهم تلك المحتويات والمسائل"، التشديد مضاف.

[٢٨١] التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية...، الفقرة ١ من المادة ٦.

[٢٨٢] بربادوس، الفصل ٣٠٨ باء من قانون المعاملات الإلكترونية (١٩٩٨)، الفقرة ١ *(أ)* من الباب ٢٠؛ برمودا، قانون المعاملات الإلكترونية لسنة ١٩٩٩، الباب ٢٣؛ هونغ كونغ (المنطقة الإدارية الخاصة التابعة للصين)، قانون المعاملات الإلكترونية، الباب ٣٩؛ الهند، قانون تكنولوجيا المعلومات لسنة ٢٠٠٠، الباب ٣٦ *(هـ)*؛ موريشيوس، قانون المعاملات الإلكترونية لسنة ٢٠٠٠، الفقرة ٢ *(د)* من الباب ٢٧؛ سنغافورة، قانون المعاملات الإلكترونية، الباب الفرعي ٢ *(أ)* و*(ج)* من الباب ٢٩ والباب الفرعي (١) من الباب ٣٠.

[٢٨٣] تونس، *القانون الخاص بالمبادلات والتجارة الإلكترونية*، الفصل ١٨؛ فييت نام، *قانون بشأن المعاملات الإلكترونية*، المادة ٣١ *(د)*.

[٢٨٤] مثل بربادوس وبرمودا وسنغافورة وموريشيوس ومنطقة هونغ كونغ الإدارية الخاصة التابعة للصين.

[٢٨٥] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٣٩ *(ج)*.

٢٢١- وفي بلدان أخرى، تتحقق النتيجة نفسها لا بضمان قانوني، ولكن بفرض واجب عام على مقدّمي خدمات التصديق يلزمهم بالتحقق من المعلومات التي يقدمها الموقّع قبل إصدار الشهادة،[٢٨٦] أو بوضع نظم للتحقق من تلك المعلومات.[٢٨٧] وفي بعض الحالات، يوجد التزام بإلغاء الشهادة فورا لدى اكتشاف أن المعلومات التي أصدرت الشهادة بناء عليها غير دقيقة أو زائفة.[٢٨٨] غير أنه في حالات قليلة يسكت القانون بشأن إصدار الشهادات، ولا يطلب من مقدّم خدمات التصديق سوى الامتثال لبيان ممارسة التصديق الصادر عنه[٢٨٩] أو إصدار الشهادة وفقا لما يتفق عليه مع الموقّع.[٢٩٠] ولا يعني ذلك أن القانون لا يتوخى أي مسؤولية تقع على عاتق مقدّمي خدمات التصديق. بل على العكس، تنصّ بعض القوانين بوضوح على مسؤولية مقدّمي خدمات التصديق، باشتراط قيام مقدّم خدمات التصديق بشراء تأمين مناسب للمسؤولية تجاه الأطراف الثالثة يغطي جميع الأضرار التعاقدية وغير التعاقدية التي تلحق بالموقّعين والأطراف الثالثة.[٢٩١]

٢٢٢- وواجب مقدّم خدمات التصديق المتمثل في التحقق من دقة المعلومات المقدّمة يكمله واجب الموقِّع بأن "يولي قدرا معقولا من العناية [. . .] لضمان دقة واكتمال كل ما يقدّمه الموقّع من تأكيدات مادية ذات صلة بالشهادة طيلة دورة سريانها، أو يُتوخّى إدراجها في الشهادة."[٢٩٢] لذلك، يمكن أن يُحمّل الموقّع المسؤولية، إما تجاه مقدّم خدمات التصديق أو تجاه الطرف المعوّل، عن تقديم معلومات زائفة أو غير دقيقة إلى مقدّم خدمات التصديق عند تقديم طلب للحصول على الشهادة. ويصاغ ذلك أحيانا في هيئة واجب عام يقضي بتقديم معلومات دقيقة إلى مقدّم خدمات التصديق،[٢٩٣] أو بتوخي قدر معقول من العناية لضمان صحة المعلومات؛[٢٩٤] وأحيانا يعلن صراحة أن الموقّع مسؤول عن الأضرار التي تنجم عن عدم امتثاله لهذا الشرط المحدد.[٢٩٥]

---

[٢٨٦] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٢١ *(س)*؛ شيلي، *القانون الخاص بالمستندات الإلكترونية والتوقيعات الإلكترونية وخدمات التصديق على التوقيعات الإلكترونية*، المادة ١٢ (ج)؛ المكسيك، *مدونة القوانين التجارية: المرسوم المتعلق بالتوقيعات الإلكترونية (٢٠٠٣)*، المادة ١٠٤ (أولا)؛ فنزويلا (جمهورية - البوليفارية)، *القانون المتعلق برسائل البيانات والتوقيعات الإلكترونية*، المادة ٣٥.

[٢٨٧] إكوادور، *قانون التجارة الإلكترونية والتوقيعات الإلكترونية ورسائل البيانات*، المادة ٣٠ *(د)*.

[٢٨٨] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ١٩ *(هـ)* (٢).

[٢٨٩] بيرو، قانون التوقيعات وشهادات التصديق الرقمية، المادة ٢٩ *(أ)*.

[٢٩٠] كولومبيا، *القانون ٥٢٧ بشأن التجارة الإلكترونية*، المادة ٣٢ *(أ)*؛ الجمهورية الدومينيكية، *القانون المتعلق بالتجارة الإلكترونية والمستندات والتوقيعات الرقمية (٢٠٠٢)*، المادة ٤٠ *(أ)*؛ بنما، *قانون التوقيعات الرقمية (٢٠٠١)*، الفقرة ٧ من المادة ٤٩.

[٢٩١] جمهورية فنزويلا البوليفارية، *القانون المتعلق برسائل البيانات والتوقيعات الإلكترونية*، المادة ٣٢.

[٢٩٢] قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية. . . ، الفقرة الفرعية ١ *(ج)* من المادة ٨.

[٢٩٣] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٢٥؛ شيلي، *القانون الخاص بالمستندات الإلكترونية والتوقيعات الإلكترونية وخدمات التصديق على التوقيعات الإلكترونية*، (٢٠٠٢)، المادة ٢٤؛ المكسيك، *مدونة القوانين التجارية: المرسوم المتعلق بالتوقيعات الإلكترونية (٢٠٠٣)*، المادة ٩٩ (ثالثا).

[٢٩٤] جزر كايمان، قانون المعاملات الإلكترونية لسنة ٢٠٠٠، الباب ٣١ *(ج)*.

[٢٩٥] كولومبيا، *القانون ٥٢٧ بشأن التجارة الإلكترونية*، المادة ٤٠؛ الجمهورية الدومينيكية، *القانون المتعلق بالتجارة الإلكترونية والمستندات والتوقيعات الرقمية (٢٠٠٢)*، المادة ٥٥؛ المكسيك، *مدونة القوانين التجارية: المرسوم المتعلق بالتوقيعات الإلكترونية (٢٠٠٣)*، المادة ٩٩ (ثالثا)؛ بنما، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٣٩.

(ج) استخدام التوقيع على نحو غير مأذون به أو تعرّض بيان ممارسة التصديق لما يثير الشبهة

٢٢٣- هناك جانبان لاستخدام أدوات إنشاء التوقيعات والشهادات استخداما غير مأذون به. فمن ناحية، ربما تكون أداة إنشاء التوقيعات غير محفوظة على نحو سليم أو ربما تتعرض لما يثير الشبهة، مثل استيلاء وكيل للموقع عليها. ومن ناحية أخرى، ربما يتعرض التسلسل الهرمي للتوقيع نفسه الخاص بمقدّم خدمات التصديق لما يثير الشبهة، مثلا إذا فقد مقدّم خدمات التصديق مفتاح التوقيع الخاص به أو فقد المفتاح الرئيسي، أو كُشف ذلك المفتاح لأشخاص غير مأذون لهم أو استخدمه أشخاص من هذا القبيل، أو تعرّض على نحو آخر لما يثير الشبهة.

٢٢٤- وقد يتعرض التسلسل الهرمي للتوقيع لما يثير الشبهة بطرائق مختلفة. فقد يدمر مقدّم خدمات التصديق أو أحد مستخدميه أو المتعاقدين معه المفتاح دون قصد أو يفقد السيطرة عليه، أو قد يتضرر مركز البيانات الذي يحتفظ بالمفتاح الخصوصي بسبب حادث، أو قد يدمَّر مفتاح مقدّم خدمات التصديق عمدا أو يتعرض لما يثير الشبهة من قبل شخص ما لأغراض غير مشروعة (مقتحم خصوصية البيانات مثلا). ويمكن أن تكون عواقب تعرّض التسلسل الهرمي للتوقيع لما يثير الشبهة خطيرة جدا. فعلى سبيل المثال، إذا ما وقع المفتاح الخصوصي أو المفاتيح الرئيسية بين يدي أحد المجرمين، أصبح بإمكان ذلك الشخص أن يولد شهادات زائفة ويستخدمها لانتحال شخصيات موقعين حقيقيين أو وهميين، لغير صالح الأطراف المعوّلة. وإضافة إلى ذلك، فبمجرد اكتشاف الضرر، سيقتضي الأمر إلغاء جميع الشهادات التي يصدرها مقدّم خدمات التصديق، مما يحتمل أن يؤدي إلى مطالبات هائلة من جميع أوساط الموقّعين بسبب الخسارة الناجمة عن ذلك الاستخدام.

٢٢٥- ولم يتناول قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية هذه المسألة. ويمكن الاحتجاج بأن الالتزام العام لمقدّم خدمات التصديق، بموجب القانون النموذجي، بأن "يستخدم [. . .] نظما وإجراءات وموارد بشرية جديرة بالثقة"[٢٩٦] يمكن تفسيره على أنه يفرض واجبا على مقدّم خدمات التصديق بأن يتخذ جميع التدابير اللازمة لمنع تعرض مفتاحه الخاص (ومن ثم التسلسل الهرمي للتوقيعات الخاص به برمته) لما يثير الشبهة. وتنص عدة قوانين داخلية صراحة على هذا الالتزام، وكثيرا ما تقرنه بالتزام مقدّم خدمات التصديق باستخدام نظم جديرة بالثقة.[٢٩٧] ويوجد أحيانا واجب محدد باتخاذ تدابير لتفادي تزوير الشهادات.[٢٩٨] ويقع على عاتق مقدّم خدمات التصديق واجب الامتناع عن إنشاء بيانات التوقيع الخاصة بالموقّعين أو الوصول إليها، ويمكن أن يكون مسؤولا عن أفعال مستخدميه الذين يقومون بذلك عمدا.[٢٩٩] ويُفرض على مقدّم خدمات التصديق واجب أن يطلب إلغاء الشهادة الصادرة عنه، إذا ما تعرضت بيانات إنشاء التوقيع المتعلقة بها لما يثير الشبهة.[٣٠٠]

---

[٢٩٦] الفقرة الفرعية ١ *(و)* من المادة ٩.

[٢٩٧] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٢١ *(ج)* و*(د)*؛ كولومبيا، *القانون ٥٢٧ بشأن التجارة الإلكترونية*، المادة ٣٢ *(ب)*؛ موريشيوس، قانون المعاملات الإلكترونية لسنة ٢٠٠٠، المادة ٢٤؛ بنما، *قانون التوقيعات الإلكترونية (٢٠٠١)*، الفقرة ٥ من المادة ٤٩؛ تايلند، قانون المعاملات الإلكترونية (٢٠٠١)، الفقرة ٦ من الباب ٢٨؛ تونس، *القانون الخاص بالمبادلات والتجارة الإلكترونية*، الفصل ١٣.

[٢٩٨] جمهورية فنزويلا البوليفارية، *القانون المتعلق برسائل البيانات والتوقيعات الإلكترونية*، المادة ٣٥.

[٢٩٩] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٢١ *(ب)*.

[٣٠٠] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٢١ *(ع)*.

٢٢٦- ويشترط على الموقّع أيضا أن يتوخى كل ما يلزم من عناية. ويشترط قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، على سبيل المثال، أن يولي الموقّع "قدرا معقولا من العناية لاجتناب استخدام بيانات إنشاء توقيعه استخداما غير مأذون به".[٣٠١] ويوجد واجب مماثل يرد في معظم القوانين الداخلية، وإن كان ثمة اختلافات بينها. ففي بعض الحالات، يُخضع القانونُ الموقّعَ لالتزام صارم بضمان السيطرة الحصرية على أداة إنشاء التوقيع ومنع استخدامها على أي نحو غير مأذون به،[٣٠٢] أو يحمل الموقّعَ وحدَه المسؤوليةَ عن صون أداة إنشاء التوقيع.[٣٠٣] غير أن هذا الالتزام كثيرا ما يوصف باعتباره واجبا يقتضي فرض سيطرة كافية على أداة إنشاء التوقيع أو اتخاذ تدابير وافية للسيطرة عليها،[٣٠٤] أو التصرف بيقظة لاجتناب أي استخدام غير مأذون به،[٣٠٥] أو توخي قدر معقول من العناية لاجتناب أي استخدام غير مأذون به لأداة التوقيع الخاصة به.[٣٠٦]

(د) عدم تعليق الشهادة أو إلغائها

٢٢٧- يمكن أيضا أن يتحمل مقدّم خدمات التصديق المسؤولية عن عدم إلغاء شهادة تعرضت لما يثير الشبهة أو تعليقها. ولكي يؤدي مرفق التوقيعات الرقمية عمله على نحو سليم ويتمتع بالثقة، من المهم أن تكون ثمة آلية قائمة لكي تقرر آنيا ما إذا كانت شهادة معينة صحيحة، أو ما إذا كانت قد علقت أو ألغيت. فكلما تعرض مفتاح خصوصي لما يثير الشبهة، مثلا، كان إلغاء الشهادة هو الآلية الرئيسية التي يمكن بها للموقّع أن يحمي نفسه إزاء المعاملات الاحتيالية التي يقوم بها المحتالون الذين يحتمل أن يكونوا قد حصلوا على نسخة من مفتاحه الخصوصي.

٢٢٨- ونتيجة لذلك، فالسرعة التي يلغي بها مقدّم خدمات التصديق شهادة أحد الموقّعين أو يعلقها إثر طلب من الموقّع هي أمر بالغ الأهمية. والوقت المنقضي بين طلب الموقّع إلغاء الشهادة والإلغاء الفعلي ونشر إشعار بالإلغاء يمكن أن يتيح لمحتال فرصة إبرام معاملات احتيالية. ومن ثم، إذا أخر مقدّم خدمات التصديق على نحو غير معقول نشر الإلغاء في قائمة خاصة بإلغاء الشهادات، أو لم يقم بذلك، أصبح من المحتمل أن يتكبَّد كل من الموقّع والطرف المعوّل الذي يتعرض للاحتيال خسائر كبيرة بالتعويل على شهادة يزعم أنها صحيحة. وفضلا عن ذلك، يجوز لمقدّمي خدمات التصديق أن يعرضوا، في إطار ما يقدمونه من خدمات

---

[٣٠١] الفقرة الفرعية ١ *(أ)* من المادة ٨.

[٣٠٢] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٢٥ *(أ)*؛ كولومبيا، *القانون ٥٢٧ بشأن التجارة الإلكترونية*، المادة ٣٢ *(ب)*؛ الجمهورية الدومينيكية، *القانون المتعلق بالتجارة الإلكترونية والمستندات والتوقيعات الرقمية (٢٠٠٢)*، المادة ٥٣ (د)؛ بنما، *قانون التوقيعات الإلكترونية (٢٠٠١)*، الفقرة ٤ من المادة ٣٧؛ الاتحاد الروسي، الفقرة ١ من البند ١٢ من القانون الاتحادي بشأن التوقيعات الرقمية (٢٠٠٢)؛ تركيا، المادة ١٥ *(هـ)* من قانون الإجراءات والمبادئ المتعلقة بتنفيذ قانون التوقيعات الإلكترونية (٢٠٠٥).

[٣٠٣] تونس، *القانون الخاص بالمبادلات والتجارة الإلكترونية*، المادة ٢١.

[٣٠٤] شيلي، *القانون الخاص بالمستندات الإلكترونية والتوقيعات الإلكترونية وخدمات التصديق على التوقيعات الإلكترونية (٢٠٠٢)*، المادة ٢٤؛ فييت نام، قانون بشأن المعاملات الإلكترونية، الفقرة ٢ *(أ)* من المادة ٢٥.

[٣٠٥] جمهورية فنزويلا البوليفارية، *القانون المتعلق برسائل البيانات والتوقيعات الإلكترونية*، المادة ١٩.

[٣٠٦] جزر كايمان، قانون المعاملات الإلكترونية لسنة ٢٠٠٠، الباب ٣٩ *(أ)*؛ إكوادور، *قانون التجارة الإلكترونية والتوقيعات الإلكترونية ورسائل البيانات*، المادة ١٧ *(ب)*؛ الهند، قانون تكنولوجيا المعلومات لسنة ٢٠٠٠، الفقرة ١ من الباب ٤٢؛ موريشيوس، قانون المعاملات الإلكترونية لسنة ٢٠٠٠، الفقرة ١ *(أ)* و*(ب)* من الباب ٣٥؛ المكسيك، *مدونة القوانين التجارية: المرسوم المتعلق بالتوقيعات الإلكترونية (٢٠٠٣)*، المادة ٩٩ ثانيا؛ سنغافورة؛ قانون المعاملات الإلكترونية (الفصل ٨٨)، الباب ٣٩؛ تايلند، قانون المعاملات الإلكترونية (٢٠٠١)؛ الفقرة ١ من الباب ٢٧.

للتصديق، الاحتفاظ بمستودعات على الخط الحاسوبي المباشر وقوائم خاصة بإلغاء الشهادات يتيسر وصول الأطراف المعوّلة إليها. والاحتفاظ بقاعدة بيانات من هذا القبيل ينطوي على خطرين رئيسيين: احتمال ألا يكون مستودع المعلومات أو قائمة إلغاء الشهادات دقيقين، وأن يوفرا بالتالي معلومات خاطئة يعوِّل عليها المتلقي لما هو في غير مصلحته؛ واحتمال ألا يكون المستودع أو قائمة إلغاء الشهادات متاحين (مثلا بسبب عطل في النظام)، مما يعيق قدرة الموقّعين والأطراف المعوّلة على إنجاز المعاملات.

٢٢٩- وكما ذُكر أعلاه، يفترض قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية أن مقدّم خدمات التصديق قد يصدر مستويات مختلفة من الشهادات بدرجات متفاوتة من العولية والأمن. وبناء على ذلك، لا يشترط القانون النموذجي أن يتيح مقدّم خدمات التصديق نظام الإلغاء بصفة دائمة، فهو أمر قد لا يكون معقولا تجاريا لبعض أنواع الشهادات المنخفضة القيمة. وبدلا من ذلك، لا يشترط القانون النموذجي على مقدّم خدمات التصديق سوى أن يوفّر وسائل يكون الوصول إليها متيسّرا بقدر معقول تمكن الطرف المعوّل من التأكد بالرجوع إلى الشهادة من أمور منها ما إذا كانت هناك وسائل متاحة للموقّع لتقديم إشعار يفيد بأن بيانات إنشاء التوقيع تعرّضت لما يثير الشبهة وما إذا كانت تتاح خدمة إلغاء آنيّة.[٣٠٧] وعندما تتاح خدمات إلغاء آنية، يُلزم مقدّم خدمات التصديق بضمان توافرها.[٣٠٨]

٢٣٠- والنظام الذي أنشأه إيعاز الاتحاد الأوروبي بشأن التوقيعات الإلكترونية يلزم الدول الأعضاء في الاتحاد الأوروبي بأن تضمن، "كحد أدنى"، أن يكون مقدّم خدمات التصديق الذي أصدر شهادة باعتبارها شهادة مستوفية الشروط للجمهور مسؤولا عن الضرر الذي يلحق بأي كيان أو شخص اعتباري أو طبيعي يعوِّل على نحو معقول على تلك الشهادة فيما يتعلق بعدم تسجيل إلغاء الشهادة، ما لم يثبت مقدّم خدمات التصديق أنه لم يتصرف بإهمال.[٣٠٩] وتلزم بعض القوانين الداخلية مقدّم خدمات التصديق باتخاذ تدابير لمنع تزوير الشهادات[٣١٠] أو لإلغاء شهادة ما فورا لدى اكتشاف أن المعلومات التي أصدرت الشهادة بناء عليها غير دقيقة أو زائفة.[٣١١]

٢٣١- وربما يوجد واجب مماثل يقع على عاتق الموقّع وغيره من الأشخاص المأذون لهم. فقانون الأونسيترال النموذجي بشأن التوقيعات، مثلا، يشترط على الموقّع أن يبادر، دون تأخر لا مسوّغ له إلى استخدام الوسائل التي يوفرها مقدّم خدمات التصديق أو خلافا لذلك، إلى بذل جهود معقولة لإشعار أي شخص يجوز للموقّع أن يتوقّع منه على وجه معقول أن يعوّل على التوقيع الإلكتروني إذا كان الموقّع على معرفة بأن بيانات إنشاء التوقيع تعرّضت لما يثير الشبهة أو إذا كانت الظروف المعروفة لدى الموقِّع تؤدي إلى نشوء احتمال قوي بتعرض بيانات إنشاء التوقيع لما يثير الشبهة.[٣١٢]

---

[٣٠٨] الفقرة الفرعية ١ (هـ) من المادة ٩.

[٣٠٩] التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية...، الفقرة ٢ من المادة ٦؛ انظر أيضا الفقرة (ب) من المرفق الثاني للإيعاز.

[٣١٠] بنما، *قانون التوقيعات الرقمية (٢٠٠١)*، الفقرة ٦ من المادة ٤٩.

[٣١١] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)* المادة ١٩ (هـ) (٢).

[٣١٢] الفقرة الفرعية ١ (ب) '١' و'٢' من المادة ٨.

٢٣٢- وكثيرا ما تؤكد القوانين الوطنية واجب الموقّع بأن يطلب إلغاء الشهادة في أي ظرف يمكن أن تكون فيه سرية بيانات إنشاء التوقيع قد تعرضت لما يثير الشبهة،[٣١٣] رغم أنّ القانون يُلزم الموقّع في بعض الحالات بإبلاغ مقدّم خدمات التصديق فحسب بذلك.[٣١٤] وقد اعتمدت قوانين عدة بلدان الصيغة الواردة في قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، الذي يفرض على الموقّع التزاما بأن يخطر كذلك أي شخص يمكن أن يتوقع حامل أداة التوقيع على نحو معقول أن يعول على التوقيع الإلكتروني أو يقدم خدمات داعمة لـه.[٣١٥] ورغم أن عواقب الإخلال بهذا الواجب قد ترد ضمنا في عدد من النظم القانونية، ففي بعض البلدان يعلن القانون صراحة أن الموقّع مسؤول عن عدم الإبلاغ عن فقدان السيطرة على المفتاح الخصوصي أو عدم طلب إلغاء الشهادة.[٣١٦]

خـاتمـــة

٢٣٣- يمكن أن يكون استخدام طرائق التوثيق والتوقيع الإلكترونية على نطاق واسع خطوة مهمة نحو خفض الوثائق التجارية وما يتصل بها من تكاليف في المعاملات الدولية. وفي حين أن وتيرة التطورات في هذا المجال تحددها بقدر كبير جدا نوعية الحلول التكنولوجية وأمنها، فقد يقدم القانون إسهاما كبيرا صوب تيسير استخدام طرائق التوثيق والتوقيع الإلكترونية.

٢٣٤- وقد اتخذ عدد كبير من البلدان بالفعل تدابير داخلية في هذا الاتجاه باعتماد تشريعات تؤكد القيمة القانونية للخطابات الإلكترونية وتضع معايير لتكافئها مع الخطابات الورقية. وغالبا ما تكون الأحكام التي تنظم طرائق التوثيق والتوقيع الإلكترونية عنصرا مهما في تلك القوانين. وقد أصبح قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية هو المعيار الوحيد الأكثر تأثيرا على التشريعات في هذا المجال وساعد تنفيذه الواسع النطاق على الترويج لقدر كبير من المواءمة على الصعيد الدولي. ومن شأن التصديق على اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية على نطاق واسع أن يتيح قدرا أكبر من المواءمة، بتوفير مجموعة محددة من القواعد للمعاملات الدولية.

---

[٣١٣] الأرجنتين، *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٢٥ *(ج)*؛ كولومبيا، *القانون ٥٢٧ بشأن التجارة الإلكترونية*، المادة ٣٢ *(ب)*؛ الفقرة ٤ من المادة ٣٩؛ الجمهورية الدومينيكية، *القانون المتعلق بالتجارة الإلكترونية والمستندات والتوقيعات الرقمية (٢٠٠٢)*، المادتان ٤٩ و٥٣ *(e)*؛ إكوادور، *قانون التجارة الإلكترونية والتوقيعات الإلكترونية ورسائل البيانات*، المادة ١٧ *(و)*؛ موريشيوس، قانون المعاملات الإلكترونية لسنة ٢٠٠٠، المادة ٣٦؛ بنما، *قانون التوقيعات الرقمية (٢٠٠١)*، الفقرة ٥ من المادة ٣٧؛ سنغافورة؛ قانون المعاملات الإلكترونية (الفصل ٨٨)، الباب ٤٠؛ الاتحاد الروسي، الفقرة ١ من البند ١٢ من القانون الاتحادي بشأن التوقيعات الرقمية (٢٠٠٢).

[٣١٤] الهند، قانون تكنولوجيا المعلومات لسنة ٢٠٠٠، الفقرة ٢ من الباب ٤٢؛ تركيا، المادة ١٥ *(و)* و*(ط)* من قانون الإجراءات والمبادئ المتعلقة بتنفيذ قانون التوقيعات الإلكترونية (٢٠٠٥).

[٣١٥] جزر كايمان، قانون المعاملات الإلكترونية لسنة ٢٠٠٠، الباب ٣١ *(ب)*؛ الصين، قانون التوقيعات الإلكترونية، المادة ١٥؛ تايلند، قانون المعاملات الإلكترونية (٢٠٠١)، الفقرة (٢) من الباب ٢٧؛ فييت نام، قانون بشأن المعاملات الإلكترونية، الفقرة ٢ *(ب)* من المادة ٢٥.

[٣١٦] الصين، قانون التوقيعات الإلكترونية، المادة ٢٧؛ والجمهورية الدومينيكية، *القانون المتعلق بالتجارة الإلكترونية والمستندات والتوقيعات الرقمية (٢٠٠٢)*، المادة ٥٥؛ وإكوادور، *قانون التجارة الإلكترونية والتوقيعات الإلكترونية ورسائل البيانات*، المادة ١٧ *(هـ)*؛ بنما؛ *قانون التوقيعات الرقمية (٢٠٠١)*، المادة ٣٩؛ الاتحاد الروسي، الفقرة ٢ من البند ١٢ من القانون الاتحادي بشأن التوقيعات الرقمية (٢٠٠٢)؛ جمهورية فنزويلا البوليفارية، *القانون المتعلق برسائل البيانات والتوقيعات الإلكترونية*، المادة ٤٠.

٢٣٥- وربما يعود اعتماد معايير الأونسيترال تلك بالفائدة أيضا على استخدم طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي. وعلى وجه الخصوص، ربما تتيح المعايير المرنة للتكافؤ الوظيفي بين التوقيعات الإلكترونية والورقية الواردة في اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية إطارا دوليا مشتركا يتيح لطرائق التوثيق والتوقيع الإلكترونية أن تستوفي اشتراطات الشكل الخاصة بالتوقيعات الأجنبية. غير أنه لا تزال بعض المشاكل قائمة، وخصوصا فيما يتصل باستخدام طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي التي تتطلب تدخل طرف ثالث موثوق به في عملية التوثيق أو التوقيع.

٢٣٦- والمشاكل التي تنشأ في هذا المجال على وجه الخصوص تنجم بقدر كبير جدا عن عدم اتساق المعايير التقنية أو عدم توافق المعدات أو البرامجيات، مما يفضي إلى عدم قابلية التشغيل البيني على الصعيد الدولي. وربما تؤدي الجهود الرامية إلى مواءمة المعايير وتحسين التوافق التقني إلى حل للصعوبات الموجودة في الوقت الحالي. غير أنه توجد أيضا صعوبات قانونية تتعلق باستخدام طرائق التوثيق والتوقيع الإلكترونية، وخصوصا فيما يتصل بالقوانين الداخلية التي تفرض استخدام نوع معين من التكنولوجيا للتوقيعات الإلكترونية أو تفضله، وتكون عادة هي تكنولوجيا التوقيعات الرقمية.

٢٣٧- والقوانين التي تنص على القيمة القانونية للتوقيعات الرقمية لا تضفي عادة ذات القيمة القانونية على التوقيعات التي تؤيدها شهادات أجنبية إلا بقدر ما ترى أنها معادلة للشهادات الداخلية. ويبين الاستعراض الذي أجري في هذه الدراسة أن التقييم السليم للتكافؤ القانوني لا يتطلب مقارنة المعايير التقنية والأمنية المتصلة بتكنولوجيا معينة للتوقيعات فحسب، بل يتطلب أيضا مقارنة القواعد التي من شأنها أن تحكم مسؤولية مختلف الأطراف المعنية. ويتيح قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مجموعة من القواعد المشتركة الأساسية التي تحكم واجبات معينة تقع على عاتق الأطراف المعنية بعملية التوثيق والتوقيع والتي قد يكون لها تأثير على المسؤولية الفردية لكل طرف. كما توجد نصوص إقليمية، مثل التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية، توفر إطارا تشريعيا مماثلا لمسؤولية مقدّمي خدمات التصديق العاملين في المنطقة. غير أن أيا من هذين النصين لا يتناول جميع قضايا المسؤولية الناجمة عن استخدام طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي.

٢٣٨- ومن المهم أن يفهم المشرّعون ومقرّرو السياسات الاختلافات بين نظم المسؤولية الداخلية والعناصر المشتركة بينها، من أجل استحداث أساليب وإجراءات ملائمة للاعتراف بالتوقيعات المدعومة بشهادات أجنبية. وربما توفر القوانين الداخلية لبلدان مختلفة بالفعل ردودا متكافئة بقدر كبير لمختلف الأسئلة المطروحة في هذا المنشور، وذلك على سبيل المثال بسبب ما لديها من تقاليد قانونية مشتركة أو بسبب انتمائها لإطار تكامل إقليمي ما. ويمكن أن تستفيد تلك البلدان من استحداث معايير مشتركة بشأن المسؤولية أو حتى من مواءمة قواعدها الداخلية، من أجل تيسير استخدام طرائق التوثيق والتوقيع الإلكترونية عبر الحدود.

FOR UNITED NATIOMNS USE ONLY

Printed in Austria
V.08-55696—March 2009—520

United Nations publication
ISBN: 978-92-1-633051-4
Sales No. A.09.V.4