الأمم المتحدة

A/CN.9/630/Add.2

الجمعية العامة

Distr.: General
26 April 2007
Arabic
Original: English

لجنة الأمم المتحدة للقانون التجاري الدولي
الدورة الأربعون
فيينا، ٢٥ حزيران/يونيه - ١٢ تموز/يوليه ٢٠٠٧

الأعمال التي يمكن الاضطلاع بها مستقبلاً في مجال التجارة الإلكترونية

وثيقة مرجعية شاملة عن العناصر اللازمة لإنشاء إطار قانوني مؤات للتجارة الإلكترونية: نموذج فصل عن استخدام طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي

مذكّرة من الأمانة*

إضافة

يحتوي مرفق هذه المذكّرة على جزء (الجزء الأول، الفصل ثانيا، القسمين ألف وباء) من نموذج فصل من وثيقة مرجعية شاملة يتناول المسائل القانونية ذات الصلة باستخدام طرائق التوثيق والتوقيع الإلكترونية على الصعيد الدولي.

* تأخّرت أمانة لجنة الأمم المتحدة للقانون التجاري الدولي في تقديم هذه الوثيقة بسبب نقص الموظفين.

070607 V.07-82825 (A)

المرفق

المحتويات

	الفقرات	الصفحة
الجزء الأول- طرائق التوقيع والتوثيق الإلكترونية	١-٤٦	٣
ثانيا- المعاملة القانونية للتوثيق الإلكتروني والتوقيعات الإلكترونية	١-٤٦	٣
ألف- النهج الخاص بالتكنولوجيا في النصوص التشريعية	٥-١٩	٤
١- نهج الحد الأدنى	٦-١٢	٥
٢- نهج التكنولوجيا المحدّدة	١٣-١٥	٩
٣- نهج المستويين أو الشقّين	١٦-١٩	١٢
باء- القيمة الإثباتية في طرائق التوقيع والتوثيق الإلكترونية	٢٠-٤٦	١٤
١- "التوثيق" والإسناد العام للسجلات الإلكترونية	٢١-٢٩	١٤
٢- القدرة على الوفاء بمقتضيات التوقيع القانونية	٣٠-٣٥	٢٠
٣- الجهود المعنية باستحداث مكافئات إلكترونية لأشكال خاصة من التوقيعات	٣٦-٤٦	٢٥

الجزء الأول
طرائق التوقيع والتوثيق الإلكترونية

[...]

ثانيا- المعاملة القانونية للتوثيق الإلكتروني والتوقيعات الإلكترونية

١- بناء الثقة بالتجارة الإلكترونية ذو أهمية كبيرة في تطويرها. 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؛[(1)] أو الاتفاقات التعاقدية.[(2)]

٢- يجري 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 قائمة ومغلقة من المستعملين، كالمؤسسات المالية المشاركة في نظام المدفوعات المشترك بين المصارف، أو بورصات السندات المالية والسلع الأساسية، أو رابطة شركات طيران ووكلاء سفر. وفي هذه الحالات، عادة ما تكون المشاركة في الشبكة محصورة في المؤسسات والشركات التي سبق أن قُبِلت في المجموعة. وقد أنشئت غالبية هذه الشبكات قبل عدة عقود زمنية، وهي تستخدم تكنولوجيا متطورة واكتسبت مستوى عاليا من الخبرة في عمل هذا النظام. وأدّى النمو السريع للتجارة الإلكترونية في العقد الماضي إلى تطوير نماذج شبكية أخرى، مثل سلاسل العرض أو المنصّات الحاسوبية التجارية.

---

(1) انظر، على سبيل المثال، اللجنة الاقتصادية لأوروبا، مركز الأمم المتحدة لتيسير التجارة والمعاملات التجارية الإلكترونية، التوصية رقم ٣٢ المعنونة "صكوك التنظيم الرقابي الذاتي في مجال التجارة الإلكترونية (مدونات قواعد السلوك)" (ECE/TRADE/277)، والمتاحة في الموقع الشبكي http://www.unece.org/cefact/recommendations/rec_index.htm، الذي تم الدخول إليه في ٢٨ آذار/مارس ٢٠٠٧.

(2) تهدف الكثير من المبادرات على المستويين الوطني والدولي إلى وضع عقود نموذجية. انظر، على سبيل المثال، 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) والمتاحتين في الموقع الشبكي http://www.unece.org/cefact/recommendations/rec_index.htm، الذي تم الدخول إليه في ٢٨ آذار/مارس ٢٠٠٧.

٣- ومع أن هذه المجموعات الجديدة قد نُظّمت أصلا في بنية تتمحور حول التوصيلات المباشرة من حاسوب إلى آخر، كما كان الحال بالنسبة إلى معظم 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 التجاريين"، وهي مصممة 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.[3] وفي حدود الحرية التعاقدية بمقتضى القانون الواجب تطبيقه، عادة ما تكون هذه القواعد والاتفاقات ذاتية الإنفاذ.

٤- غير أنه 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 يستخدمها الأطراف تحددها القواعد القانونية الواجب تطبيقها على شكل قواعد تحوّطية بشأن التقصير أو قواعد 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

٥- اتخذت التشريعات واللوائح التنظيمية الخاصة بالتوثيق الإلكتروني أشكالا عديدة مختلفة على المستويين الدولي والداخلي. ويمكن تحديد ثلاثة نهوج رئيسية للتعامل مع

(3) وللاطلاع 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.

تكنولوجيات التوقيع والتوثيق: (أ) نهج الحد الأدنى؛ و(ب) نهج التكنولوجيا المحدّدة؛ و(ج) نهج المستويين أو الشقين.[4]

١- نهج الحد الأدنى

٦- تعترف بعض الولايات القضائية بجميع التكنولوجيات التي تستخدم في التوقيع الإلكتروني، تبعا لسياسة عامة بشأن الحياد التكنولوجي.[5] 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، وتلبي كذلك بعض متطلبات قابلية التعويل ذات الحياد إزاء التكنولوجيا.

٧- ويقدّم قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية[6] مجموعة المعايير التشريعية الأوسع انتشارا لإرساء نظير وظيفي عام بين التوقيعات الإلكترونية والخطية. وتنص الفقرة ١ من المادة ٧ من القانون النموذجي على ما يلي:

"(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."

٨- 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 الوظيفيتين بالشكل

(4) 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*، المجلد ٧، العدد ٢، (٢٠٠١) الصفحة ٢٣٤ وما بعدها.

(5) على سبيل المثال أستراليا ونيوزيلندا.

(6) انظر الحاشية [...] [منشورات الأمم المتحدة، رقم المبيع A.99.V.4].

الإلكتروني على أنها تلبي شرطا من الشروط القانونية للتوقيع الإلكتروني. ولذلك، فإن القانون النموذجي محايد تكنولوجيا؛ أي أنه 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 ويساعد 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.

٩- وقد أُدرِج هذا المبدأ العام في قوانين الكثير من البلدان. ذلك أن مبدأ الحياد التكنولوجي يتيح المجال أيضا لاستيعاب التطورات التكنولوجية المستقبلية. إضافة إلى ذلك، يبرز هذا النهج حرية الأطراف في اختيار التكنولوجيا المناسبة لاحتياجاتهم. وبالتالي، فإن الأمر يتوقف على قدرة الأطراف على تحديد مستوى الأمن الكافي لاتصالاتهم. وقد يؤدي ذلك إلى تجنب التعقد المفرط من الناحية التكنولوجية وما يرتبط به من تكاليف.[7]

١٠- وباستثناء أوروبا حيث تأثرت التشريعات أساسا بالتوجيهات الإدارية الصادرة عن الاتحاد الأوروبي،[8] فإن معظم البلدان التي وضعت تشريعات في مجال التجارة الإلكترونية استخدمت القانون النموذجي بشأن التجارة الإلكترونية كنموذج لها.[9] كما اتُخِذ القانون

---

(7) S. Mason, "Electronic signatures in practice", *Journal of High Technology Law*، المجلد الرابع، العدد ٢ (٢٠٠٦)، الصفحة ١٥٣.

(8) وبخاصة التوجيه الإداري الصادر عن البرلمان الأوروبي ومجلس أوروبا 1999/93/EC بشأن إطار مجتمعي للتوقيعات الإلكترونية (انظر الحاشية [...]) [الجريدة الرسمية للجماعات الأوروبية، العدد L.13]. ويلي التوجيه بشأن التوقيعات الإلكترونية توجيه آخر أكثر شمولا، 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 (توجيه إداري بشأن التجارة الإلكترونية) (الجريدة الرسمية للجماعات الأوروبية، العدد L.178، تاريخ ١٧ تموز/يوليه ٢٠٠٠)، المتعلق بمختلف جوانب توفير خدمات تكنولوجيا المعلومات وبعض مسائل التعاقد الإلكتروني.

(9) 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؛ وأستراليا، قانون المعاملات الإلكترونية، ١٩٩٩؛ وإكوادور، *Ley de comercio electrónico, firmas electrónicas y mensajes de datos* (قانون التجارة الإلكترونية والتوقيعات الإلكترونية ورسائل البيانات) (٢٠٠٢)؛ وإيرلندا، قانون التجارة الإلكترونية، ٢٠٠٠؛ وباكستان، قانون المعاملات الإلكترونية، ٢٠٠٢؛ وبنما، *Ley de firma digital* (قانون التوقيع الرقمي) (٢٠٠١)؛ وتايلند، قانون المعاملات الإلكترونية (٢٠٠١)؛ والجمهورية الدومينيكية، *Ley sobre comercio electrónico, documentos y firmas digitales* (قانون بشأن التجارة الإلكترونية) (٢٠٠٢)؛ وجنوب أفريقيا، قانون الاتصالات والمعاملات الإلكترونية (٢٠٠٢)؛ وسري لانكا،

النموذجي أساسا لمواءمة التشريعات الداخلية الخاصة بالتجارة الإلكترونية في البلدان المنظَّمة على أساس اتحادي (فيدرالي)، مثل كند[10] والولايات المتحدة الأمريكية.[11] وقد حافظت

قانون المعاملات الإلكترونية (٢٠٠٦)؛ وسلوفينيا، قانون التجارة الإلكترونية والتوقيع الإلكتروني (٢٠٠٠)؛ وسنغافورة، قانون المعاملات الإلكترونية (١٩٩٨)؛ وجمهورية كوريا، القانون الإطاري للتجارة الإلكترونية (٢٠٠١)؛ والصين، قانون التوقيعات الإلكترونية الذي صدر عام ٢٠٠٤؛ وفرنسا، *Loi 2000-230 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique* (قانون ٢٠٠٠-٢٣٠ بشأن تكييف قانون الإثبات على تكنولوجيات المعلومات والمتعلق بالتوقيع الإلكتروني) (٢٠٠٠)؛ والفلبين، قانون التجارة الإلكترونية (٢٠٠٠)؛ وفنزويلا (جمهورية - البوليفارية)، *Ley sobre mensajes de datos y firmas electrónicas* (قانون رسائل البيانات والتوقيعات الإلكترونية) (٢٠٠١)؛ وفييت نام، قانون المعاملات الإلكترونية (٢٠٠٦)؛ وكولومبيا، *Ley sobre mensajes de datos y firmas electrónicas* (قانون التوقيعات الإلكترونية الرقمية) (٢٠٠٢)؛ والمكسيك، *Decreto por el que se reforman y adicionan diversas disposiciones del código civil para el distrito federal en materia federal, del Código federal de procedimientos civilies, del Código de comercio y de la Ley federal de protección al consumidor* (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)؛ وموريشيوس، قانون المعاملات الإلكترونية لعام ٢٠٠٠؛ ونيوزيلندا، قانون المعاملات الإلكترونية لعام ٢٠٠٢؛ والهند، قانون تكنولوجيا المعلومات، ٢٠٠٠. كما اعتُمد القانون النموذجي في أقاليم تابعة لتاج المملكة المتحدة لبريطانيا العظمى وايرلندا 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 وايرلندا 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، الصين (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.

(10) 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، الذي تم الدخول إليه في ١٢ نيسان/أبريل ٢٠٠٧). 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 كوبيك تشريعا خاصا (قانون إنشاء إطار قانوني لتكنولوجيا المعلومات (٢٠٠١))، ومع أنه أوسع نطاقا ومختلف جدا من حيث الصياغة، فهو يحقّق 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.nccusl.org/nccusl/uniformact_factsheets/ uniformacts-fs-ueta.asp، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧.

البلدان التي اشترعت القانون النموذجي، إلا بعض الاستثناءات القليلة جدا،[12] على نهج الحياد التكنولوجي، و لم تنص في قانونها على تكنولوجيا معينة و لم تبد أي تفضيل لتكنولوجيا معيّنة. ويتبع قانون الأونسيترال النموذجي للتوقيعات الإلكترونية،[13] الذي اعتمد في عام ٢٠٠١، واتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية[14] وهي أحدث عهدا منه (التي اعتمدتها الجمعية العامة في ٢٣ تشرين الثاني/نوفمبر ٢٠٠٥، وفُتح باب التوقيع عليها منذ ١٦ كانون الثاني/يناير ٢٠٠٦) النهج نفسه، مع أن قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية يحتوي على بعض النصوص الإضافية (انظر الفقرات [...]-[...] أدناه).

١١- 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.

١٢- 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،

(11) 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 شبكي http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧). 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، ديلاوير، فلوريدا، كارولاينا الجنوبية، كارولاينا الشمالية، كاليفورنيا، كانزاس، كناتيكت، كنتاكي، كولورادو، لوا، لويزيانا، ماريلاند، ماساشوستس، مشيغان، مينيسوتا، نبراسكا، نيفادا، نيوجيرزي، نيومكسيكو، نيوهامبشاير، هاواي، وايومنغ، ويسكنسن. ومن المرجح أن تعتمد ولايات أخرى تشريعات تنفيذ في المستقبل القريب، بما في ذلك ولاية إلينوي التي اشترعت قانون الأونسيترال النموذجي من خلال قانون أمن التجارة الإلكترونية (١٩٨٨). 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، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧.

(12) إكوادور، بنما، الجمهورية الدومينيكية، جنوب أفريقيا، كولومبيا، موريشيوس، الهند.

(13) انظر الحاشية [...] [منشورات الأمم المتحدة، رقم المبيع A.02.V.8].

(14) انظر الحاشية [...] [قرار الجمعية العامة، ٦٠/٢١، المرفق].

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

١٣- يثير الاهتمام بتعزيز حياد الوسائط مسائل هامة أخرى. فاستحالة ضمان الأمن المطلق ضد 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.[15] 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 الحاسوبية ونظم المعلومات. بيد أنه قد يكون من الأنسب، من منظور قانون الأعمال التجارية الخاص،

(15) قانون يوتا للتوقيع الرقمي، الذي اعتُمد عام ١٩٩٥، هو أحد الأمثلة الأولى على ذلك لكنه أُلغي اعتبارا من ١ أيار/مايو ٢٠٠٦ .بموجب قانونَ الولاية رقم ٢٠، المتاح في الموقع الشبكي http://www.le.state.ut.us/~2006/htmdoc/sbillhtm/sb0020.htm، الذي تم الدخول إليه في ٢٨ آذار/مارس ٢٠٠٧.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 قوانين الأرجنتين Ley de firma digital (2001) and Decreto No. 2628/2002 (Reglamentación de la Ley de firma digital)؛ وإستونيا (قانون التوقيعات الرقمية لسنة 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 بشأن التوقيعات الإلكترونية وخدمات التوثيق (٢٠٠١)؛ وليتوانيا، قانون التوقيعات الإلكترونية (٢٠٠٠)؛ وماليزيا، قانون التوقيعات الرقمية لسنة ١٩٩٧؛ وبولندا، قانون التوقيعات الإلكترونية (٢٠٠١)؛ والاتحاد الروسي، قانون التوقيعات الإلكترونية الرقمية (٢٠٠٢).

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، التي يتطلب فيها 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".

١٤- 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."[16] 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.[17] 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 مستوى من الأمن يوازي المستوى الذي توفره بعض التقنيات المحددة، 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.

---

(16) Stewart Baker and Matthew Yeo, in collaboration with the secretariat of the International Telecommunication Union, "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، الذي تم الدخول إليه في ١٢ نيسان/أبريل ٢٠٠٧.

(17) غير أنه بالنظر إلى أن مرفق المفاتيح العمومية بات الآن ناضجا وراسخا بما فيه الكفاية، فإن بعض هذه الشواغل قد لا توجد الآن بالحدة التي كانت عليها من قبل.

١٥- 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 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)؛[18]

(ب) **تدخّل حكومي محدود**. قد تقرر الحكومة تأسيس 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؛[19]

(ج) **عملية تقودها الحكومة**. قد تقرّر الحكومة إنشاء مؤسسة مركزية حصرية لتقديم خدمات التوثيق. كما يمكن إنشاء مؤسسات لتقديم خدمات التوثيق ذات أغراض خاصة بموافقة الحكومة.[20] وتمثّل نظم إدارة شؤون الهوية (انظر الفقرات [...]-[...] أعلاه) طريقة أخرى قد تتولى الحكومات من خلالها توجيه عملية التوقيع الرقمي على نحو

(18) 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.

(19) المرجع نفسه، حيث تُذكر سنغافورة كمثال.

(20) المرجع نفسه، حيث تُذكر كل من الصين وماليزيا كمثالين.

غير مباشر. وقد قامت بعض الحكومات من قبلُ بمباشرة برامج خاصة بإصدار وثائق هوية مقروءة آليا لمواطنيها ("وثائق هوية إلكترونية") مزوّدة بخصائص وظيفية للتوقيع الإلكتروني.

٣- نهج المستويين أو الشقّين

١٦- في هذا النهج، تضع التشريعات عتبة منخفضة من المقتضيات لكي تحظى طرائق التوثيق الإلكتروني بحد أدنى معيّن من الوضع القانوني، وتمنح بعض طرائق التوثيق الإلكترونية مفعولا قانونيا أكبر (يشار إليها على نحو متفاوت بأنها توقيعات إلكترونية أو شهادات تصديق مستوفية الشروط مأمونة أو متقدّمة أو معزّزة).[21] وعلى المستوى الأساسي، تمنح التشريعات التي تعتمد نظاما من مستويين عموما 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 بشأنها أن تمتثل لمقتضيات محدّدة قد ترتبط بتكنولوجيا معيّنة. وحاليا، يعرّف هذا النوع من التشريعات عادة هذه التوقيعات المأمونة بالنسبة إلى تكنولوجيا مرافق المفاتيح العمومية.

١٧- ويجري اختيار هذا النهج في الأحوال النمطية 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 (أكانت نماذج ذاتية التنظيم الرقابي، أو نماذج الاعتماد الطوعي أو مخططا تديره الحكومة)، في الأكثر بالطريقة نفسها المتبعة في النهج الخاص بالتكنولوجيا المحدّدة (انظر الفقرتين [...]-[...] 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 بأنهم يمكن أن يعتبروا من مصدِري الشهادات "المأمونة" أو "المستوفية الشروط".

(21) Aalberts and van der Hof, *Digital Signature Blindness*... (انظر الحاشية [...])، الفقرة ٣-٢-٢.

١٨- وكانت سنغافورة[22] والاتحاد الأوروبي[23] أول الولايات القضائية التي سنّت تشريعات لاعتماد نهج المستويين. ثم تبعهما عدد من الولايات القضائية الأخرى.[24] ويتيح قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية المشترعة إقامة نظام من مرحلتين من خلال عدد من اللوائح التنظيمية وإن كان لا يروّج له فعلا.[25]

---

(22) 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 التوقيع "(أ) 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 المرتبط بسجل إلكتروني يرتبط به بطريقة من شأنها أن تبطل التوقيع الإلكتروني عند حصول أي تغيير في السجل")، وهي 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 القانون فإن التوقيعات الإلكترونية المدعومة بشهادة جديرة بالثقة تمتثل لأحكام الباب ٢٠ من القانون، تعتبر تلقائيا "توقيعات إلكترونية مأمونة".

(23) على غرار قانون المعاملات الإلكترونية في سنغافورة، يميز التوجيه الإداري الصادر عن الاتحاد الأوروبي بشأن التوقيعات الإلكترونية [انظر الحاشية [...]] 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"توقيع إلكتروني متقدّم" (بحسب التعريف الوارد في الفقرة ٢من 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) متصل ببيانات 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 الشروط أصدرها مقدّم خدمات تصديق معتَمد، أو لم يُنشأ من خلال أداة مأمونة لإنشاء التوقيعات." لكن المعلن هو أن التوقيعات الإلكترونية المتقدمة "التي تستند إلى شهادة تصديق مستوفية الشروط والتي أُنشئت بواسطة أداة مأمونة لإنشاء التوقيعات وحدها": "(أ) تستوفي الشروط القانونية للتوقيع فيما يخص البياناتَ 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).

(24) موريشيوس وباكستان على سبيل المثال. انظر الحاشية [٩] أعلاه للحصول على تفاصيل القوانين النظامية ذات الصلة.

(25) تنص الفقرة ٣ من المادة ٦ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية (انظر الحاشية [...])، 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.

١٩- وبالنسبة للمستوى الثاني 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).[26] علاوة على ذلك، اقتُرِح 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 اضطرابا مع المقتضيات القانونية الوطنية.

باء- القيمة الإثباتية في طرائق التوقيع والتوثيق الإلكترونية

٢٠- 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 وطرائق التوقيع والتوثيق الورقية. ومع أن قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لاقى قبولا واسعا، وأن عددا متزايدا من الدول أخذ يستخدمه كأساس لتشريعاتها الخاصة بالتجارة الإلكترونية، فإنه لا يمكن بعدُ الافتراض بأن مبادئ هذا القانون النموذجي قد بلغت درجة التطبيق الشامل. فالموقف الذي اتخذته مختلف الولايات القضائية فيما يتعلق بالتوقيعات الإلكترونية والتوثيق الإلكتروني يعكس نمطيا النهج العام للولاية القضائية إزاء اشتراطات الكتابة والقيمة الإثباتية في السجلات الإلكترونية.

١- "التوثيق" والإسناد العام للسجلات الإلكترونية

٢١- ينطوي استخدام الطرائق الإلكترونية للتوثيق على اثنين من الجوانب لهما صلة بهذه المناقشة. الجانب الأول يتعلق بالمسألة العامة لإسناد رسالة إلى منشئها المفترَض. وأما الجانب الثاني فيتعلق بمدى مناسبة طريقة تعيين الهوية التي يستخدمها الأطراف لغرض تلبية مقتضيات الشكل المحدّدة، خصوصا مقتضيات التوقيع القانونية. ومما له صلة أيضا بالموضوع المفاهيم القانونية التي تدلّ ضمنا على وجود توقيع خطي، مثلما هو الحال بالنسبة لمفهوم "المستند" في بعض النظم القانونية. وحتى إذا ما جاز الجمع بين هذين الجانبين في كثير من الأحيان أو إذا

(26) Baker and Yeo, "Background and issues concerning authentication…"، (انظر الحاشية [١٦]).

تعذر التمييز بينهما تماما، حسب الظروف، فقد تجدي محاولة تحليلهما منفصلين، إذ يبدو أن المحاكم تتجه إلى استنتاجات مختلفة حسب الوظيفة المرتبطة بطريقة التوثيق.

٢٢- يتناول 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،[27] التي تحدّد التزامات مرسل أمر الدفع. والمقصود من المادة ١٣ من القانون النموذجي بشأن التجارة الإلكترونية هو أن تُطبّق متى 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 لإدعاء بتزوير توقيع المنشئ المفترض. وأما في بيئة إلكترونية، فيمكن أن يكون شخص غير مأذون له هو الذي أرسل الرسالة، ولكن التوثيق بشيفرة أو بالترميز أو بوسائل مشابهة لذلك من شأنه أن يكون دقيقا. والغرض من المادة ١٣ ليس إسناد مرجعية تحرير رسالة بيانات لطرف 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 المزعوم.

٢٣- والفقرة ١ من المادة ١٣ من القانون النموذجي بشأن التجارة الإلكترونية تذكِّر بالمبدأ القابل بأن المنشئ ملزم برسالة البيانات إذا كان هو الذي أرسلها فعلا. وتشير الفقرة ٢ إلى وضع أرسل فيه الرسالة شخص غير المنشئ وكانت لديه صلاحية التصرّف نيابة عن المنشئ. وأما الفقرة ٣ فتعالج نوعين من الأوضاع حيث يمكن للمرسل إليه أن يعوّل على اعتبار رسالة البيانات صادرة عن المنشئ: وذلك أولا في أوضاع طبَّق فيها المرسل إليه على نحو سليم إجراء للتوثيق سبق أن وافق عليه المنشئ؛ وثانيا، في أوضاع كانت فيها رسالة البيانات ناتجة من تصرفات شخص كانت متاحة له بحكم علاقته بالمنشئ سبل الوصول إلى الإجراءات التي يتبعها المنشئ للتوثيق.

٢٤- وقد اعتمد عدد من البلدان القاعدة الواردة في المادة ١٣ من القانون النموذجي بشأن التجارة الإلكترونية، بما فيها افتراض الإسناد المنصوص عليه في الفقرة ٣ من هذه المادة.[28] وتشير بعض البلدان صراحة إلى استخدام الشيفرات أو كلمات السر أو غير ذلك

(27) منشورات الأمم المتحدة، رقم المبيع A.99.V.11، المتاحة في الموقع الشبكي: http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf.

(28) انظر كولومبيا *(art. 17)*؛ وإكوادور (المادة ١٥)؛ وموريشيوس *((2) sect. 12 ,*؛ والفلبين *((sect. 18, para. (3)*؛ وجمهورية كوريا *((art. 7, para 2. (2)*؛ وسنغافورة *((3) sect. 13* ؛ وتايلند *(sect. 16)*؛ وفنزويلا (جمهورية-البوليفارية) *(art. 9)*. وترد أيضا القواعد نفسها في قوانين جيرسي التابعة للتاج البريطاني

من وسائل تعيين الهوية كعوامل توجد قرينة تدل على هوية المؤلِّف (المحرّر).[29] 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.[30]

٢٥- 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.[31] وإضافة إلى ذلك، لم يدرج عدد من البلدان التي نفّذت القانون النموذجي بشأن التجارة الإلكترونية أي حكم محدد يستند إلى المادة ١٣.[32] وكان الافتراض في تلك البلدان أنه ليست هناك حاجة إلى قواعد محددة، وأنه من الأفضل أن تُترك مسألة الإسناد لمعالجتها بطرق الإثبات العادية، بالطريقة نفسها التي يعالج بها إسناد المستندات الورقية: أي "الشخص الذي يريد أن يعوّل على أي توقيع يعرِّض نفسه لمخاطرة في عدم صحة التوقيع، ولا تتغير هذه القاعدة بالنسبة للتوقيع الإلكتروني."[33]

٢٦- لكن بلدانا أخرى فضَّلت أن تدرج أحكام القانون النموذجي للتجارة الإلكترونية الخاصة بالإسناد منفصلة عن الأحكام الخاصة بالتوقيعات الإلكترونية. ويستند هذا النهج إلى

(art. 8)، والأراضي البريطانية عبر البحار برمودا *(sect. 16, para. 2)*، وجزر تركس وكايوكس *(sect. 14)*. وللحصول على تفاصيل عن القوانين النظامية ذات الصلة، انظر الحاشية [٩] أعلاه.

(29) المكسيك (انظر الحاشية [٩] أعلاه)، الفقرة أولا، من المادة ٩٠.

(30) مثلا، ينص قانون الولايات المتحدة الموحّد بشأن المعاملات الإلكترونية في الباب ٩ (أ) على أن السجل الإلكتروني أو التوقيع الإلكتروني "ينسب إلى الشخص إذا كان من فعل هذا 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". وينص علاوة على ذلك 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".

(31) أستراليا (الباب ١٥، الفقرة ١)؛ والهند بالأسلوب نفسه أساسا (الباب ١١)؛ وباكستان (الباب ١٣، الباب الفرعي ٢)؛ وسلوفينيا (المادة ٥)؛ وإقليم جزيرة مان التابع للتاج البريطاني (الباب ٢)؛ ومنطقة هونغ كونغ الإدارية الخاصة التابعة للصين (الباب ١٨). وللاطلاع على تفاصيل مختلف القوانين انظر الحاشية [٩] أعلاه.

(32) مثلا، ايرلندا وجنوب أفريقيا وفرنسا وكندا ونيوزيلندا.

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

الفهم القائل بأن الإسناد في سياق مستندي يخدم غرضا رئيسيا هو توفير أساس لقدر معقول من التعويل، وقد يتضمّن أساليب أكثر اتساعا من تلك التي تُستخدم بشكل أكثر ضيقا 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".[34] ومثل هذه القاعدة العامة بشأن الإسناد لا تؤثر في استخدام التوقيع كوسيلة لإسناد السجل لشخص، وإنما تستند إلى التسليم بأن "التوقيع ليس هو الطريقة الوحيدة للإسناد".[35] ولذلك، وفقا للتعليق على قانون الولايات المتحدة:

"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 وسيلة لإثبات الإسناد مفيدا نظرا للأهمية الفريدة التي تتسم بها إجراءات الأمن في البيئة الإلكترونية. وفي إجراءات

(34) الولايات المتحدة، القانون الموحد بشأن المعاملات الإلكترونية (١٩٩٩) (Uniform Electronic Commerce Act) (انظر الحاشية [١١]، الباب ٩). تقدم الفقرة ١ من التعليقات الرسمية على الباب ٩ الأمثلة التالية التي يمكن أن يسند فيها كل من السجل الإلكتروني والتوقيع الإلكتروني لشخص: "يطبع الشخص اسمه كجزء من طلب شراء بالبريد الإلكتروني"؛ أو "يطبع مستخدم الشخص، بموجب تفويض، اسم الشخص كجزء من طلب شراء بالبريد الإلكتروني"؛ أو "الحاسوب الخاص بالشخص، المبرمج لطلب سلع عند تلقي معلومات خاصة بقائمة جرد ضمن حدود معينة، يصدر طلب شراء يتضمن اسم الشخص وغير ذلك من معلومات تعيين الهوية كجزء من الطلب".

(35) المرجع نفسه. 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 الفاكس. 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."

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 إجراءً أمنياً 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 أنه ينبغي أن تمنح أشكال أخرى من إثبات الإسناد قدرا أدنى من المفعول الاقناعي. 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."[36]

٢٧- من المهم أيضا التذكّر أن قرينة الإسناد لا تحل وحدها محل تطبيق القواعد القانونية التي تحكم التوقيعات حيثما كان التوقيع لازما لصحة فعل أو لإثباته. ومتى تقرر أنه يمكن إسناد سجل أو توقيع إلى طرف معيّن، "يجب تقرير مفعول السجل أو التوقيع على ضوء السياق والظروف المحيطة، بما في ذلك اتفاق الأطراف، إن وجد"، وكذلك "المقتضيات القانونية الأخرى المأخوذة بعين الاعتبار على ضوء السياق".[37]

٢٨- 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.[38] فقد رفضت محاكم في الولايات المتحدة دعاوى تحتج بأن رسائل البريد الإلكتروني غير مقبولة كدليل إثبات لأنها أدلة إثبات غير موثقة وشفوية.[39] 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

(36) المرجع نفسه، التعليقات الرسمية على الباب ٩.

(37) المرجع نفسه، الفقرة ٦ من التعليقات الرسمية على الباب ٩.

(38) الولايات المتحدة، قضية *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.

(39) الولايات المتحدة، قضية *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.

الـذاتي".[40] وتمـيل المحـاكم إلى أن تـأخذ في الاعتـبار كـل أدلـة الإثـبات المتاحة، ولا تـرفض السجلات الإلكترونية على أنها أدلة ظاهرية غير كافية.

٢٩- أمـا في البلدان الـتي لم تعتمد القـانون النموذجي بشأن التجارة الإلكترونية، فيبدو أنه لا توجـد أحكام تشريعية محددة تعالج مسألة الإسناد بأسلوب مماثل. وفي تلك البلدان عادة ما يكـون الإسـناد واقعـة تتوقّف عـلى الاعـتراف القـانوني بالتوقيعات الإلكترونـية والافتراضـات المتصـلة بالسـجلات الموثّقـة بـأنواع معينة من التوقيعات الإلكترونية. وقد دعت شواغل تتعلق بمخاطـر التلاعـب في السـجلات الإلكترونـية، مـثلا، إلى عـدم الـتفات المحـاكم في بعـض تلـك البلدان إلى قـيمة رسـائل البـريد الإلكـتروني كدليل إثبات في الإجـراءات القضائية، بسبب أن رسـائل البـريد الإلكتروني لا توفر ضمانات كافية على سلامتها.[41] وتوجد أمثلة أخرى على نهـوج أكـثر تقييدا بشـأن القـيمة الإثباتية في السـجلات الإلكترونـية والإسناد في قضايا حديثة العهـد كانـت تـتعلق بالمـزادات عـبر الإنترنـت، طبّقـت فـيها المحـاكم معـيارا عـالي المسـتوى بخصـوص إسناد رسـائل البيانات. وكانـت هـذه القضـايا متعلقة غالبا بدعـاوى إخـلال بعقد بسـبب عـدم تسـديد ثمـن سـلع زُعـم أنهـا مشـتراة في مـزادات عـلى الإنترنـت. وتمسّك المدّعون بـأن المدّعـى عليهـم كانوا هـم الطرف المشتري، حيث إن أعلى عرض لشراء السلع كان موثقا بكـلمة سـر المدّعـى عليه وأُرسـل مـن عـنوان البـريد الإلكـتروني الخـاص بـالمدّعى عليه. ورأت المحـاكم أن هـذه العناصـر لا تكفـي للوصـول إلى اسـتنتاج راسـخ بـأن المدّعـى عليه هـو الـذي شـارك فعـلا في المـزاد وقـدم العـرض الفائز لشـراء السـلع. واسـتخدمت المحـاكم حججا مختلفة لتسـويغ هذا الموقف. فمثلا، قيل إن كلمات السر لا يُعوّل عليها لأنه يمكن لأي شخص يعلم كـلمة سـر المدّعـى عليه أن يسـتخدم عـنوان المدّعـى عليه في البـريد الإلكـتروني مـن أي مكان وأن يشـارك في المـزاد مسـتخدما اسـم المدّعـى عليه،[42] وهـي مخاطـرة رأت بعـض المحاكم أنها

(40) الولايات المتحدة، قضية *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.

(41) ألمانيا، قضية 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, available at http://www.jurpc.de/rechtspr/20020332.htm, accessed on 11 September 2003.

(42) ألمانيا، قضية 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, available at http://www.jurpc.de/rechtspr/20020071.htm, accessed on 25 August 2003; see also 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, available at http://www.jurpc.de/rechtspr/20040074.htm, accessed on 2 February 2007.

"شديدة الاحتمال جدا"، 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.[43] 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 وسط معين، حيث إنه لا توجد قرينة قانونية على أنه يمكن إسناد الرسائل المرسلة عبر موقع على شبكة الإنترنت باللجوء إلى كلمة سر أحد الأشخاص لدخول هذا الموقع، إلى ذلك الشخص.[44] 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.[45]

٢- القدرة على الوفاء بمقتضيات التوقيع القانونية

٣٠- اتجهت المحاكم في بعض البلدان إلى تفسير مقتضيات التوقيع بأسلوب متحرّر. وكانت هذه هي الحال عادة في بعض الولايات القضائية للقانون العام، كما سبق بيانه، (انظر المقدمة، الفقرات [...] - [...])، فيما يتعلق بمقتضيات قانون الاحتيالات، الذي يقضي بأنه يجب أن تكون معاملات معيَّنة 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.[46] وما هو أهم من ذلك في السياقات التعاقدية هو أن المحاكم قدَّرت أيضا كفاية التوثيق على ضوء التعاملات فيما بين الأطراف، بدلا من

(43) ألمانيا، قضية 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, available at http://www.jurpc.de/rechtspr/20020291.htm, accessed on 25 August 2003.

(44) ألمانيا، قضية 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, available at http://www.jurpc.de/rechtspr/20020136.htm, accessed on 25 August 2003.

(45) ألمانيا، قضية 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, available at http://www.jurpc.de/rechtspr/20020364.htm, accessed on 25 August 2003.

(46) الولايات المتحدة، قضية *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.

استخدام معيار صارم لكل الأوضاع. وهكذا، فانه 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.[47] واعتُبر "اختيار الشخص عن قصد طبع اسمه في ختام كل الرسائل الإلكترونية" توثيقا صحيحا.[48] واستعداد محاكم الولايات المتحدة إلى القبول بأن رسائل البريد الإلكتروني والأسماء المطبوعة فيها وسائل كافية للوفاء بمقتضيات الكتابة[49] إنما يتّبع تفسيرا متحررا لمفهوم "التوقيع"، الذي 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"،[50] في ظروف معيّنة. وفي الأحوال التي لا ينكر فيها الأطراف كتابة الرسائل أو تلقيها بالبريد الإلكتروني، تُستوفى إذ ذاك مقتضيات التوقيع القانونية، حيث إن المحاكم "قد اعترفت منذ أجل 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".[51]

٣١- وقد اتبعت محاكم في المملكة المتحدة لبريطانيا العظمى وايرلندا الشمالية نهجا مماثلا، حيث رأت عموما أن شكل التوقيع أقل دلالة من الوظيفة التي يؤديها. ومن ثم تنظر المحاكم في مدى ملاءمة الوسط المستخدم لإسناد سجل لشخص معيَّن، وكذلك لتبيان قصد ذلك الشخص بالنسبة للسجل، ولذلك يجوز أن تعدّ رسائل البريد الإلكتروني "مستندات"، كما

(47) الولايات المتحدة، قضية *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.

(48) الولايات المتحدة، قضية *Jonathan P. Shattuck v. David K. Klotzbach*, Superior Court of Massachusetts, 11 December 2001, 2001 Mass. Super. LEXIS 642.

(49) الولايات المتحدة، قضية *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.

(50) المرجع نفسه، صفحة ٩١٩: "يمكن استخدام المستندات الداخلية والفواتير ورسائل البريد الإلكتروني للوفاء بقانون الاحتيالات في القانون التجاري الموحد لولاية الينوي" Illinois [Uniform Commercial Code]. إلا أنه في القضية الواقعية، رأت المحكمة أن العقد المزعوم عاجز عن الوفاء بمقتضيات 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 المتهم.

(51) الولايات المتحدة، قضية *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.

يجوز أن تكون الأسماء المطبوعة على الرسائل الإلكترونية "توقيعات".[52] وقد أعلنت بعض المحاكم أنه "لا ريب عندها في أنه إذا أنشأ طرف وأرسل مستندا أُنشئ إلكترونيا يُعامل على أنه قد وقّعه، تماما مثلما من شأنه أن يُعامل قانونا لو وقّع على نسخة ورقية من المستند نفسه" وأنه "لا يمكن أن يؤدي إنشاء المستند إلكترونيا مقارنة بنسخة ورقية إلى أي تمييز".[53] وقد رفضت المحاكم أحيانا الاحتجاج بأن رسائل البريد الإلكتروني تشكل عقدا موقّعا لأغراض قانون الاحتيالات، وذلك أساسا لعدم وجود نيّة في الالتزام بالتوقيع. غير أنه لا توجد سابقة فيما يبدو لرفض المحاكم مسبقا قدرة رسائل البريد الإلكتروني والأسماء المطبوعة فيها على الوفاء بمقتضيات الكتابة والتوقيع القانونية. وارتئي في بعض الحالات أن مقتضيات قانون الاحتيالات لم تستوف لأن رسائل البريد الإلكتروني المعنية لم تبيّن إلا مفاوضات جارية لا اتفاق نهائي، وذلك مثلا لأن أحد الأطراف تصوّر أثناء المفاوضات أن عقدا ملزما سوف يُبرم بعد توقيع "مذكرة معاملة" وليس قبل ذلك.[54] وفي قضايا أخرى ألمحت المحاكم بأنها ربما كانت تميل إلى القبول باعتبار "اسم المنشئ أو حروفه الأولى" في "نهاية رسالة البريد الإلكتروني" أو في "أي مكان آخر في متن رسالة البريد الإلكتروني توقيعا"، إلا أنها رأت أن "إدراج عنوان الشخص في البريد الإلكتروني تلقائيا بعد إرسال المستند إما من قِبل [مقدِّم خدمات الإنترنت] المرسل وإما من قِبل المتلقّي أو كليهما" "لا يُقصد به أن يكون توقيعا".[55] 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

(52) الولايات المتحدة، قضية *Hall v. Cognos Limited* (Hull Industrial Tribunal, Case No. 1803325/97) (unreported).

(53) المملكة المتحدة، قضية *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).

(54) المملكة المتحدة، قضية *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)).

(55) قضية *Mehta v. J. Pereira Fernandes S.A.* (انظر الحاشية [٥٥]).

الإلكترونية، حتى خارج نطاق أي تفويض قانوني معيّن، ما دامت الطريقة المعنية تؤدي وظائف التوقيع الخطّي نفسها.[56]

٣٢- وتميل عموما المحاكم في الولايات القضائية للبلدان التي تأخذ بالقانون المدني 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 يتعذَّر من ثمّ الفصل بينه و"التوقيع". إذ إن المحاكم في فرنسا، مثلا، كانت ممانعة لقبول الوسائل الإلكترونية لتعيين الهوية على أنها مكافئة للتوقيعات الخطّية، إلى حين اعتماد تشريع يعترف صراحة بصحة التوقيعات الإلكترونية.[57] وثمة اتجاه أكثر تحررا تأخذ به القرارات التي تقبل تقديم الشكاوى الإدارية إلكترونيا وذلك لغرض الوفاء بموعد محدّد، على الأقل ما دامت تؤكَّد في وقت لاحق بمراسلات عادية.[58]

٣٣- وعلى العكس من النهج التقييدي الذي تتبعه المحاكم الألمانية حاليا 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. ودار 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 (موديم) إلى آلة الفاكس الخاصة بالمحكمة. وفي قضايا

(56) قضية *Mehta* ضد *J. Pereira Fernandes S.A.* (see note [55]), 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 المزعوم 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]".

(57) رفضت محكمة النقض في فرنسا قبول عريضة استئناف كانت موقّعة إلكترونيا، نظرا لوجود ارتياب بشأن هوية الشخص الذي أنشأ التوقيع، وكان قد وقّع الاستئناف 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.*، متاحة في الموقع الشبكي www.juriscom.net/jpt/visu.php?ID=239، الذي تم الدخول إليه في ١٢ أيلول/سبتمبر ٢٠٠٣).

(58) فرنسا، قضية Conseil d'État, 28 décembre 2001, N° 235784, *Élections municipales d'Entre-Deux-Monts*، معلومات متاحة في الموقع الشبكي www.rajf.org/article.php3?id_article=467، الذي تم الدخول إليه في ١٢ أيلول/سبتمبر ٢٠٠٣.

سابقة رأت محاكم الاستئناف[59] والمحكمة الاتحادية *(Bundesgerichtshof)*[60] أن الصورة الممسوحة إلكترونيا عن توقيع 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 أنه على المشرِّع عموما لا المحاكم وضع شروط للتكافؤ بين الكتابة والاتصالات غير الملموسة المرسَلة بوسائط نقل البيانات.[61] 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 عن توقيع.[62]

٣٤- ومما تجدر ملاحظته أن هناك محاكم حتى في بعض الولايات القضائية التي تطبّق القانون المدني، التي اعتمدت تشريعات تؤيّد استخدام توقيعات إلكترونية تستند إلى مرافق المفاتيح العمومية (PKI)، مثل كولومبيا،[63] قد اتّبعت نهجا متحررا مماثلا، وأكدت، على

(59) 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، متاحة في الموقع الشبكي www.jurpc.de/rechtspr/19980009.htm، الذي تم الدخول إليه في ١٢ أيلول/سبتمبر ٢٠٠٣.

(60) ألمانيا، قضية 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، متاحة في الموقع الشبكي http://www.jurpc.de/rechtspr/19990005.htm، الذي تم الدخول إليه في ١٢ أيلول/سبتمبر ٢٠٠٣.

(61) المرجع نفسه.

(62) في قضية أحيلت من المحكمة الاتحادية في ألمانيا Bundesgerichtshof (انظر الحاشية ٦٢ أعلاه)، إلى الغرفة المشتركة للمحاكم الاتحادية العليا في ألمانيا (Gemeinsamer Senat der obersten Gerichtshöfe des Bundes) لاحظت الغرفة المشتركة أن مقتضيات الشكل في إجراءات المحاكم ليست غاية في حد ذاتها. فالغرض منها هو ضمان تحديد يعتمد عليه على نحو واف لمضمون الرسالة وهوية الشخص الذي صدرت منه. ولاحظت الغرفة المشتركة التطور الحاصل في تطبيق مقتضيات الشكل عمليا بحيث تستوعب التطورات التكنولوجية السابقة، 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 الدعوى القائم (Gemeinsamer Senat der obersten Gerichtshöfe des Bundes, GmS-OGB 1/98, 5 April 2000, *JurPC—Internet Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC WebDok No.160/2000)، متاحة في الموقع الشبكي http://www.jurpc.de/rechtspr/ 20000160.htm، الذي تم الدخول إليه في ١٢ أيلول/سبتمبر ٢٠٠٣.

(63) مثل كولومبيا، التي اعتمدت قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، بما فيه الأحكام العامة للمادة ٧، وإنما أنشأت قرينة قانونية للوثاقة فيما يتعلق بالتوقيعات الإلكترونية فقط (*Ley de comercio electrónico*، المادة ٢٨).

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.(64)

٣٥- 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. فيبدو أن النهج التشريعي المتّبع إزاء التوقيعات الإلكترونية والتوثيق الإلكتروني قد 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 لما هو "التوقيع" الإلكتروني. ولذلك ليس من المؤكد أن المحاكم ذاتها التي اتّبعت نهجا متحررا في سياق دعاوى الاستئناف القضائية أو الإدارية سوف تكون متحررة بقدر متساو فيما يتعلق بمقتضيات التوقيع بخصوص إثبات صحة العقود. ففي الواقع، في حين أنه في سياق تعاقدي قد يواجه أحد الطرفين 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 المعنية باستحداث مكافئات إلكترونية لأشكال خاصة من التوقيعات

(أ) مذكرات التصديق (Apostilles)*

٣٦- قيل إن روح ونص اتفاقية لاهاي اللاغية لشرط التصديق القانوني على الوثائق العامة الأجنبية، المبرمة في لاهاي في ٥ تشرين الأول/أكتوبر ١٩٦١، لا يشكلان عقبة أمام

* سيتم التوسع في هذا القسم في النسخة النهائية من الوثيقة المرجعية الشاملة.

(64) كولومبيا، قضية *Juan Carlos Samper* ضد Juzgado Segundo Promiscuo Municipal Rovira Tolima, *Jaime Tapias*, 21 julio 2003, Rad. 73-624-40-89-002-2003-053-00. رأت المحكمة أن العملية المنفّذة بواسطة وسائل إلكترونية صحيحة رغم أن رسائل البريد الإلكتروني لم تكن موقّعة رقميا، وذلك لأن (أ) كان يتسنى 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) كان يمكن استعراض الرسائل في أي وقت (متاحة في الموقع الشبكي http://www.camara-e.net/_upload/80403--0-7-diaz082003.pdf، الذي تم الدخول إليه في ٢ شباط/فبراير ٢٠٠٧).

استخدام التكنولوجيا الحديثة.[65] وقد أيّد المنتدى الدولي الأول بشأن التوثيق الإلكتروني والتصديقات الإلكترونية ذلك الاستنتاج، ولاحظ أنه يمكن زيادة تحسين تطبيق الاتفاقية وتنفيذها بالاعتماد على تلك التكنولوجيات.[66] ومن شأن تقديم تفسير للاتفاقية في ضوء مبدأ التكافؤ الوظيفي أن يسمح للسلطات المختصة بأن تحفظ سجلات إلكترونية، وكذلك بأن تصدر مذكرات تصديق إلكترونية، بغية مواصلة تعزيز المساعدة القانونية الدولية والخدمات الحكومية.

٣٧- وفي نيسان/أبريل ٢٠٠٦، أطلق مؤتمر لاهاي للقانون الدولي الخاص ورابطة الموثقين الوطنية في الولايات المتحدة البرنامج الرائد الخاص بالتصديق الوافي الإلكتروني (e-APP). وفي إطار هذا البرنامج الرائد يعمل مؤتمر لاهاي والرابطة، إلى جانب أي دولة مهتمة، من أجل تطوير نماذج من البرامجيات الحاسوبية وترويجها والمساعدة في تنفيذها، لأجل: (أ) إصدار واستخدام مذكرات التصديق الوافي الإلكترونية و(ب) تشغيل سجلات إلكترونية خاصة بمذكرات التصديق الوافي الإلكترونية.[67]

(ب) الأختام

٣٨- ألغت فعلا بعض الولايات القضائية من قبلُ اقتضاء الأختام بناء على أن الخَتم لم يعد مناسبا اليوم، وقد حلّ محله توقيع مصدّق عليه بالإشهاد (أي بشهادة شاهد).[68] وتوجد في ولايات قضائية أخرى تشريعات تسمح بالتوقيعات الإلكترونية الآمنة تلبية لاقتضاء المهر بختم. فمثلا، توجد لدى ايرلندا أحكام محددة خاصة بالتوقيعات الإلكترونية الآمنة، مع ما

---

(65) 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" (The Hague, 2003).

(66) الاستنتاجات المعتمدة في المنتدى الدولي الأول بشأن التوثيق الإلكتروني والتصديقات الإلكترونية، المعقود في ٣٠ و٣١ أيار/مايو ٢٠٠٥، لاس فيغاس، الولايات المتحدة، متاحة في الموقع الشبكي http://www.hcch.net/upload/concl_forum.pdf، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧.

(67) صُمّم البرنامج الرائد للتصديق الوافي الإلكتروني لاستخدام تكنولوجيا موجودة فعلا وشائعة الاستخدام. والتكنولوجيا المقترحة تستند إلى صيغة الوثيقة المحمولة (صيغة PDF) المدمجة فيها لغة الترميز الموسعة (XML). ويمكن الحصول على معلومات إضافية من الموقع الشبكي http://hcch.e-vision.nl/index_en.php?act=text.display&tid=37، تحت عنوان "Second International Forum on e-Notarization and e-Apostilles" (المنتدى الدولي الثاني المعقود في واشنطن العاصمة، ٢٧-٢٩ أيار/مايو ٢٠٠٦).

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

يناسبها من التصديق، تُستخدم بدلا من الأختام، رهنا بموافقة الشخص المعني أو الهيئة العمومية المعنية، أي من يلزم أن يعطى له المستند الممهور بالختم، أو مَن هو مسموح بأن يُعطى له.(69) وتنص كندا على أن المقتضيات بشأن وجود خاتم الشخص المعني المنصوص عليها بموجب بعض القوانين الاتحادية المعيّنة، إنما تستوفى بتوقيع إلكتروني آمن يعرّف التوقيع الإلكتروني الآمن على أنه خاتم ذلك الشخص.(70)

٣٩- كما أطلقت عدة بلدان مبادرات تتوخّى استخدام المستندات والتوقيعات الإلكترونية في المعاملات العقارية التي تنطوي على سندات عقارية. والنموذج المستخدم في فكتوريا، أستراليا، يتوخى استخدام تكنولوجيا التوقيعات 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 لـ"الأختام اليدوية"، مع ترك التفاصيل التقنية عن شكل الخاتم الإلكتروني ليُبتَّ فيها منفصلة.(71)

٤٠- وينص صراحة قانون الولايات المتحدة الموحَّد لتسجيل الأملاك العقارية (United States Uniform Real Property Electronic Recording Act).(72) على أنه لا يلزم أن يكون

---

(69) ايرلندا، قانون التجارة الإلكترونية، Electronic Commerce Act, section 16، إلا أنه في الأحوال التي يلزم فيها إعطاء المستند الممهور 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.

(70) 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 والقانون الاتحادي للأملاك المنقولة، واللوائح الاتحادية للأملاك العقارية (Federal Real Property and Federal Immovables Act وFederal Real Property Regulations).

(71) 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 يعرَّف الخاتم الإلكتروني "بأنه شكل إثبات الهوية الذي تصدره الرابطة لأي من أعضائها ليُستخدم في اثبات صحة المستندات إلكترونيا في شكل قابل للقراءة حاسوبيا (انظر http://apegm.mb.ca/keydocs/act/index.html، الذي تم الدخول إليه في ٤ نيسان/أبريل ٢٠٠٧).

(72) 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، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧. وقد اعتمد في ولايات أريزونا وديلاوير ومنطقة كولومبيا وكانساس وكارولينا

التوقيع الإلكتروني مصحوبا بصورة مادية أو إلكترونية لدمغة أو شارة أو خاتم. فالمطلوب أساسا هو المعلومات المبيَّنة على الخاتم لا الخاتم نفسه. كما ينص على أن التوقيع الإلكتروني يفي بأغراض أي تشريع أو لائحة تنظيمية أو معيار يقتضي دمغة أو بصمة أو ختما لشخص ما أو كيان اعتباري. وهذه العلامات المادية غير قابلة للتطبيق على مستند إلكتروني كليا. ومع ذلك يقضي هذا القانون بأنه يجب أن تكون المعلومات التي كانت ستكون متضمنة خلافا لذلك في الدمغة أو الشارة أو الختم مرفقة بالمستند أو التوقيع أو مرتبطة بهما منطقيا على نحو إلكتروني.[73] وبذلك لا تكون دمغة أو شارة التوثيق العدلي اللازمة بموجب قوانين بعض الولايات لازمة للتوثيق العدلي الإلكتروني بموجب هذا القانون. كما أنه لا لزوم لدمغة أو شارة كيان اعتبارية كما قد يكون لازما خلافا لذلك بموجب قوانين بعض الولايات لإثبات تصرّف قام به موظف مسؤول في كيان اعتباري.

(ج) التوثيق العدلي*

٤١- هناك ثلاثة تشريعات رئيسية في الولايات المتحدة تتناول موضوع التوثيق، هي: القانون الموحد للمعاملات الإلكترونية (Uniform Electronic Transactions Act)، وقانون التوقيعات الإلكترونية في التجارة العالمية والوطنية (Electronic Signatures in Global and National Commerce Act (E-sign))[74] والقانون الموحّد لتسجيل الأملاك العقارية (Uniform Real Property Electronic Recording Act)،[75] وهي تنص مجتمعة على أن مقتضيات التوثيق العدلي لمستند أو توقيع يرتبط بمستند، أو الاعتراف به أو التحقّق منه أو الشهادة عليه أو إنشائه بعد أداء القَسَم تُستوفى إذا أُرفق بالمستند أو التوقيع أو ارتبط به منطقيا التوقيع الإلكتروني للشخص المأذون له القيام بتلك الأفعال، إلى جانب كل المعلومات الأخرى التي يقضي بإدراجها أي قانون آخر واجب التطبيق.

الشمالية وتكساس وفرجينيا ووسكنسن (انظر الموقع الشبكي http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-urpera.asp، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧).

(73) أي معايير مماثلة للمعايير الراسخة في قانون الولايات المتحدة الموحد للمعاملات الإلكترونية.

* سيتم التوسّع في هذا القسم في النسخة النهائية من الوثيقة المرجعية الشاملة.

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

(75) انظر الحاشية [٧٤].

٤٢- ويوجد في النمسا نظام محفوظات المستندات الإلكترونية "cyberDOC"، وهي شركة مستقلة شاركت في إنشائها غرفة الموثّقين العدليين التابعين للقانون المدني النمساوية وشركة سيمنز، توفر للموثّقين العدليين نظام محفوظات إلكترونية يتضمن وظائف توثيقية.(76) والموثّقون العدليون النمساويون ملزمون بموجب القانون بتسجيل جميع سندات التوثيق العدلي المنشأة بعد ١ كانون الثاني/يناير ٢٠٠٠ وتخزينها في هذا النظام الخاص بالمحفوظات.

(د) الإشهاد

٤٣- قيل إن إجراءات الشهادة التقليدية، مثل الإشهاد، 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 الشاهد والموقِّع هو تمثيل قابل لأن يقرأه إنسان على شاشة الحاسوب لما يُدعى بأنه موجود في الذاكرة الحاسوبية. وعندما يرى الشاهد الموقّع وهو يضغط على لوحة المفاتيح لا يعلم الشاهد يقينا ما الذي يحدث فعلا. ولذلك لا يمكن ضمان أن المعروض على الشاشة يقابل محتويات ذاكرة الحاسوب وأن نقرات الموقِّع على المفاتيح تقابل نواياه إلا إذا سبق أن جرى تقييم الحاسوب لأجل إحداث مسار موثوق به بمعايير تقييم موثوق بها.(77)

٤٤- 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 وثاقة 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

---

(76) انظر Österreichische Notariatskammer (Austrian Chamber of Civil Law Notaries) (غرفة الموثقين العدليين التابعين للقانون المدني النمساوية)، متاحة في الموقع الشبكي http://www.notar.at/de/portal/einrichtungen/cyberdocgmbhcokg/، الذي تم الدخول إليه في ٧ شباط/فبراير ٢٠٠٧.

(77) هذا هو ما يشار إليه في المؤلفات بمشكلة (WYSIWYS) "What you see is what you sign" (ما تراه هو الذي توقّع عليه). انظر 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، وآخرون، صفحة ٢٨٨، وكذلك للاطلاع على بحث يتناول أجهزة التحكم في العرض الموثوق منها (انظر أيضا للاطلاع على مناقشة أجهزة التحكم في العرض الموثوق منها).

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.[78]

٤٥- ولم تذهب التشريعات القائمة 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، ما دامت "تعين على نحو واف هوية الشاهد وتبيّن على نحو واف أخذ شهادة شاهد على التوقيع أو الختم"؛ و"يعوّل عليها بالقدر المناسب للغرض الذي استلزم توقيع الشاهد والظروف المحيطة بذلك".[79]

٤٦- وينص القانون الكندي لحماية المعلومات الشخصية والمستندات الإلكترونية (Personal Information Protection and Electronic Documents Act) 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.[80] ويجوز الإدلاء في شكل إلكتروني بإفادة لازمة بموجب قوانين اتحادية معينة تقرّ أو تشهد بأن أي معلومات مقدمة من الشخص الذي يدلي بالإفادة صادقة أو دقيقة أو كاملة، إذا وقّع عليها الشخص بتوقيعه الإلكتروني الآمن.[81] كما يجوز الإدلاء بإفادة يلزم بموجب القانون الاتحادي الإدلاء بها بعد أداء قَسَم أو إقرار رسمي في شكل إلكتروني إذا وقّع عليها الشخص الذي أدلى بها بتوقيعه الإلكتروني الآمن وإذا وقَّعها الشخص الذي أدلى بالإفادة أمامه والمأذون له بقبول الإفادات المدلى بها بعد أداء قَسَم أو إقرار رسمي بتوقيع ذلك

---

(78) 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، متاحة في الموقع الشبكي "Publications" ,www.agc.gov.sg.

(79) نيوزيلندا، قانون المعاملات التجارية لسنة ٢٠٠٢ (انظر الحاشية [٩])، الباب ٢٣، متاحة في الموقع الشبكي http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes، الذي تم الدخول إليه في ٤ نيسان/أبريل ٢٠٠٧.

(80) كندا، قانون حماية المعلومات الشخصية والمستندات الإلكترونية (انظر الحاشية [٧٢])، الجزء الثاني، الباب ٤٦.

(81) المصدر نفسه، الباب ٤٥.

الشخص الإلكتروني الآمن.[82] وهناك بديل اقتُرح لأجل توفير المزيد من الضمان، وهو أن ينفّذ التوقيع الإلكتروني اختصاصي مهني يكون مؤتمنا أو أن ينفَّذ في حضوره، مثل محام أو موثّق عدلي.[83]

---

(82) المصدر نفسه، الباب ٤٤.

(83) سيحتاج كتبة سندات نقل الملكية العقارية إلى توقيعات إلكترونية وإلى توثيق إلكتروني من هيئة توثيق معترف بها. وقد يحتاج البائعون والمشترون أن يفوضوا 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). متاح في الموقع الشبكي http://www.landregistry.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc، الذي تم الدخول إليه في ٧ نيسان/أبريل ٢٠٠٧. ومن المقرّر أن ينفّذ هذا المشروع على مراحل من عام ٢٠٠٦ إلى عام ٢٠٠٩.