A

الأمم المتحدة

Distr.
LIMITED

A/CN.9/WG.IV/WP.71
31 December 1996
ARABIC
ORIGINAL: ENGLISH

الجمعية العامة

لجنة الأمم المتحدة للقانون التجاري الدولي
الفريق العامل المعني بالتجارة الإلكترونية
الدورة الحادية والثلاثون
نيويورك، ١٨-٢٨ شباط/ فبراير ١٩٩٧

تخطيط الأعمال المقبلة في مجال التجارة الإلكترونية التوقيعات الرقمية، وسلطات التصديق، وما يتصل بذلك من مسائل قانونية

مذكرة من الأمانة

المحتويات

مقدمة

١ - بعد أن اعتمدت اللجنة قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية شرعت، في دورتها التاسعة والعشرين، في مناقشة الأعمال المقبلة في مجال التجارة الإلكترونية، على أساس مداولات أولية أجراها فريق العمل المعني بالتبادل الإلكتروني للبيانات في دورته الثلاثين (A/CN.9/421، الفقرات ١٠٩-١١٩). واتفق بوجه عام على أنه ينبغي للأونسيترال أن تواصل عملها من أجل إعداد معايير قانونية من شأنها أن تضفي قابلية التنبؤ على التجارة الإلكترونية، ومن ثم تعزيز التجارة في جميع المناطق.

٢ - وقدمت اقتراحات جديدة بشأن مواضيع وأولويات ممكنة للأعمال المقبلة. وتمثل اقتراح في أن تشرع اللجنة في إعداد قواعد بشأن التوقيعات الرقمية. وذكر أن إنشاء قوانين بشأن التوقيعات الرقمية، الى جانب قوانين تعترف بنشاط سلطات التصديق أو أشخاص آخرين يرخص لهم بإصدار شهادات إلكترونية أو أشكال أخرى من التأمين على منشأ وإسناد الرسائل التي تحمل "توقيعات" رقمية، يعتبر في بلدان كثيرة أمراً جوهرياً بالنسبة لتنمية التجارة الخارجية. كما ذكر أن القدرة على الاعتماد على التوقيعات الرقمية ستفتح الأبواب أمام نمو التعاقد عبر الوسائل الإلكترونية بشأن الحقوق في السلع وغيرها من المصالح وبشأن إمكانية نقل هذه الحقوق. وفي كثير من الولايات القضائية يجري الآن إعداد قوانين جديدة لتنظيم التوقيعات الرقمية. وقد ذكر أن إعداد هذه القوانين قد بدت عليه منذ الآن دلائل الافتقار الى الوحدة. فإذا قررت اللجنة أن تضطلع بعمل في هذا المجال فسوف تتاح لها فرصة إضفاء التناسق على القوانين الجديدة أو على الأقل إقرار مبادئ مشتركة في مجال التوقيعات الإلكترونية وبالتالي توفير بنية أساسية دولية لهذا النشاط التجاري.

٣ - وحظي هذا الاقتراح بتأييد شديد وإن كان قد رئي بوجه عام أنه إذا قررت اللجنة الاضطلاع بعمل في مجال التوقيعات الرقمية من خلال فريقها العامل المعني بالتبادل الإلكتروني للبيانات، فإنه ينبغي لها أن تخول الفريق العامل صلاحية دقيقة. كما رئي أنه بالنظر الى استحالة إقدام اللجنة على إعداد معايير تقنية، ينبغي لها أن تحرص على ألا تقحم نفسها في المسائل التقنية للتوقيعات الرقمية. وذكر أن الفريق العامل قد سلم في دورته الثلاثين بإمكانية الحاجة الى الاضطلاع بعمل فيما يتعلق بسلطات التصديق، وبأن هذا العمل ربما يحتاج الى أن ينفذ في سياق موضوعي هيئات التسجيل ومقدمي الخدمات. ومن جهة أخرى رأى الفريق العامل أيضا أنه ينبغي ألا يتطرق الى أي اعتبارات تقنية بصدد ملاءمة استخدام أي قواعد معينة (A/CN.9/421، الفقرة ١١١). وأعرب عن انشغال باحتمال تجاوز العمل في مجال التوقيعات الرقمية نطاق القانون التجاري وتطرقه الى مسائل عامة تعني القانون المدني أو القانون الإداري. وذكر في الرد على ذلك أن هذا ينطبق أيضا على أحكام القانون النموذجي وأن اللجنة ينبغي لها ألا تخشى إعداد قواعد مفيدة بحجة أن مثل هذه القواعد ربما تكون نافعة أيضا خارج مجال العلاقات التجارية.

٤ - وتمثل اقتراح آخر، قدم على أساس المداولات الأولية التي أجراها الفريق العامل، في أن الأعمال المقبلة ينبغي أن تركز على مقدمي الخدمات: وذكرت المسائل التالية باعتبارها مسائل يمكن النظر فيها بصدد مقدمي الخدمات: المعايير الدنيا للأداء في حالة عدم إبرام اتفاق بين الأطراف؛ نطاق افتراض المخاطر من جانب الأطراف النهائيين؛ تأثير هذه القواعد أو الاتفاقات في أطراف ثالثة؛ توزيع مخاطر نشاط المتطفلين وغيره من الأنشطة غير المأذونة؛ المدى الذي يمكن أن تذهب إليه الضمانات الإلزامية، إن وجدت، أو غيرها من الالتزامات في حالة تقديم خدمات ذات قيمة مضافة (انظر A/CN.9/421، الفقرة ١١٦).

٥ - ورأى كثيرون أن من المناسب أن تدرس الأونسيترال العلاقة بين مقدمي الخدمات والمنتفعين بها والأطراف الثالثة. وقيل إن من الأهمية بمكان توجيه تلك الجهود نحو إعداد قواعد ومعايير دولية للسلوك التجاري الميداني، قصد دعم التجارة من خلال الوسائل الإلكترونية دون أن يكون الهدف هو إنشاء نظام تقنيني لمقدمي الخدمات أو أي قواعد أخرى يمكن أن تترتب عليها تكاليف لا تتحملها التطبيقات السوقية للتبادل الإلكتروني للبيانات (انظر A/CN.9/421، الفقرة ١١٧). غير أنه رئي أيضا أن موضوع مقدمي الخدمات قد يكون مفرط الاتساع ويشمل من المواقف الواقعية المختلفة ما تتسنى معاملته كبند عمل وحيد. واتفق عموماً على أن المسائل المتعلقة بمقدمي الخدمات يمكن تناولها على نحو ملائم في سياق كل مجال عمل جديد يتطرق إليه الفريق العامل.

٦ - وكان هناك اقتراح آخر مؤداه أن اللجنة ينبغي لها أن تبدأ العمل في إعداد قواعد عامة جديدة تدعو إليها الحاجة لتوضيح الكيفية التي يمكن بها تأدية الوظائف التعاقدية التقليدية من خلال التجارة الإلكترونية. وقيل إن دواعي انعدام اليقين كثيرة فيما يتعلق بما يعنيه مصطلحا "الأداء"، و"التسليم" وغيرهما من المصطلحات في سياق التجارة الإلكترونية حيث يمكن أن تحدث العروض وقبولها وتسليم المنتجات على شبكة حاسوبية مفتوحة عبر العالم. وكان من شأن النمو السريع التجارة القائمة على الحواسيب وكذلك نمو المعاملات التي تجرى من خلال الإنترنيت وغيرها من النظم، أن أضفيا أولوية على هذا الموضوع. واقترح أن تجري الأمانة دراسة تبين نطاق هذا العمل؛ فإذا قررت اللجنة بعد فحصها هذه الدراسة أن تواصل هذه المهمة، فسيكون من الخيارات المتاحة إدراج تلك القواعد في فرع "الأحكام الخاصة" بقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية.

٧ - وتمثل اقتراح آخر في أن اللجنة ينبغي لها أن تركز انتباهها على مسألة الإدراج بالإشارة. وذكر أن الفريق العامل كان قد اتفق على أن من الملائم تناول هذا الموضوع في سياق أعم يشمل مسألتي هيئات التسجيل ومقدمي الخدمات (A/CN.9/421، الفقرة ١١٤). واتفقت اللجنة عموما على أن هذه المسألة يمكن أن تعالج في سياق بحث موضوع سلطات التصديق.

٨ - وبعد المناقشة، وافقت اللجنة على أن من المناسب إدراج مسألتي التوقيعات الرقمية وسلطات التصديق في جدول أعمال اللجنة شريطة أن تغتنم هذه الفرصة لتناول مواضيع أخرى اقترحها الفريق العامل للأعمال المقبلة. واتفق أيضا بصدد تخويل الفريق العامل ولاية أدق على أن القواعد الموحدة المزمع إعدادها ينبغي أن تتناول مسائل يذكر منها: الأساس القانوني الذي تنهض عليه عمليات التصديق، بما في ذلك التكنولوجيا الناشئة في مجالي التوثيق الرقمي والتصديق الرقمي؛ وانطباق عملية التصديق؛ وتوزيع المخاطر والمسؤوليات على المنتفعين ومقدمي الخدمات والأطراف الثالثة في سياق استخدام تقنيات التصديق؛ والمسائل المحددة المتعلقة بالتصديق من خلال استخدام هيئات التسجيل؛ والإدراج بالإشارة.

٩ - وطلبت اللجنة الى الأمانة أن تعد دراسة أساسية لمسائل التوقيعات الرقمية ومقدمي الخدمات بالاستناد الى تحليل القوانين التي يجري إعدادها في بلدان مختلفة. وينبغي للفريق العامل أن يبحث، على أساس تلك الدراسة، استصواب وجدوى إعداد قواعد موحدة بشأن المواضيع آنفة الذكر. واتفق على أن العمل الذي يعتزم الفريق العامل القيام به في دورته الحادية والثلاثين يمكن أن يشمل مشاريع قواعد بشأن بعض جوانب المواضيع آنفة الذكر. وطلب الى الفريق العامل أن يزود اللجنة بقدر كاف من العناصر يمكنها من اتخاذ قرار مستنير بشأن نطاق القواعد الموحدة المزمع إعدادها. وبالنظر الى اتساع نطاق الأنشطة التي يتناولها قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية والتي ستتناولها الأعمال المقبلة في مجال التجارة الإلكترونية، تقرر تعديل اسم الفريق العامل المعني بالتبادل الإلكتروني للمعلومات بجعله "الفريق العامل المعني بالتجارة الإلكترونية".[1]

١٠ - وتحتوي هذه المذكرة على دراسة لمسألة التوقيعات الرقمية والمسائل المتصلة بها. وقد أعدت على ضوء قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية ومع مراعاة ما اعتمد مؤخرا من نصوص تشريعية وما يجري إعداده من تلك النصوص في بلدان كثيرة. واستعين في إعداد هذه الدراسة فضلا عن ذلك بأعمال منظمات أخرى يخص منها بالذكر **الممارسات الدولية الموحدة في مجالي التوثيق والتصديق** الذي تعده الغرفة التجارية الدولية في الوقت الحاضر، **والخطوط التوجيهية للتوقيعات الرقمية** التي نشرتها رابطة المحامين الأمريكيين، كما تتجلى في تلك الدراسة النتائج التي أسفر عنها اجتماع فريق خبراء مخصص ضم خبراء في مجال التوقيعات الرقمية وأعضاء في أمانة الأونسيترال.

١١ - وعملاً بالتعليمات التي صدرت مؤخراً بشأن توخي مزيد من الاقتصاد في إعداد وثائق الأمم المتحدة والحيلولة دون تضخمها، جاءت الملاحظات على مشاريع الأحكام موجزة بقدر الإمكان على أن يقدم شفويا المزيد من الإيضاحات.

---

(١) الوثائق الرسمية للجمعية العامة، الدورة الحادية والخمسون، الملحق رقم ١٧ (A/51/17)، الفقرات ٢١٦-٢٢٤.

أولا - ملاحظات عامة بشأن التوقيعات الرقمية

ألف - وظائف التوقيعات

١٢ - تستند المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية الى الاعتراف بوظائف التوقيع في بيئة ورقية. وعند إعداد القانون النموذجي، ناقش الفريق العامل الوظائف التالية التي جرت التوقيعات الخطية على أدائها: تحديد هوية شخص ما؛ إضفاء اليقين على قيام ذلك الشخص بنفسه بفعل التوقيع؛ قرن ذلك الشخص بمحتوى المستند الموقّع. وذكر أنه يمكن للتوقيع أن يؤدي، فضلا عن ذلك، طائفة متنوعة من الوظائف تبعا لطبيعة المستند الموقّع. من ذلك مثلا أن التوقيع قد يشهد بنية الطرف أن يلتزم بمحتوى العقد الموقّع؛ أو بنية الشخص أن يصدق على صدور نص ما عن شخص معين؛ أو بنية شخص أن يقرن نفسه بمحتوى نص كتبه شخص آخر؛ أو بحقيقة أن شخصا ما كان في مكان ما في وقت معين.

١٣ - وفي بيئة إلكترونية، لا يمكن التمييز بين أصل الرسالة وصورتها، والرسالة لا تحمل أي توقيع خطي وهي ليست مدونة على ورق. وإمكانية الغش كبيرة نظراً لسهولة اعتراض المعلومات المتوافرة في شكل إلكتروني وتغييرها دون أن يكتشف ذلك وللسرعة التي يمكن بها تجهيز معاملات متعددة. والغرض من تقنيات مختلفة متوافرة في الأسواق في الوقت الحاضر أو ما زالت قيد التطوير، هو إتاحة الوسائل التقنية التي يمكن بها أن يؤدّى في بيئة إلكترونية بعض أو جميع الوظائف التي تعرّف بأنها من خصائص التوقيعات الخطية. وهذه التقنيات يمكن أن يشار إليها بصورة عامة بعبارة "توقيعات إلكترونية".

باء - التوقيعات الرقمية وغيرها من التوقيعات الإلكترونية

١٤ - عند مناقشة استصواب وجدوى إعداد قواعد قانونية موحدة التوقيعات الرقمية، وبغية مساعدة اللجنة في دراستها لنطاق هذه القواعد الموحدة الممكنة، قد يرغب الفريق العامل في بحث مختلف التقنيات التي يجري استعمالها حالياً أو ما زالت قيد التطوير ويتمثل الغرض منها في توفير معادِلات وظيفية للتوقيعات الخطية، كما قد يرغب في بحث أنواع أخرى من آليات التوثيق المستخدمة في بيئة ورقية.

١ - التوقيعات الإلكترونية المعتمدة على تقنيات أخرى غير الترميز بالمفتاح العام

١٥ - من الجدير بالذكر أنه توجد، الى جانب "التوقيعات الرقمية" القائمة على ترميز المفتاح العام الذي يشكل الموضوع الرئيسي لهذه المذكرة، أدوات أخرى مختلفة كثيراً ما يشار إليها بعبارة آليات "التوقيع الإلكتروني" وتستخدم في الوقت الحاضر أو ينظر في أمر استخدامها مستقبلا بهدف أداء وظيفة أو عدد من الوظائف الآنفة الذكر التي تؤديها التوقيعات الخطية. ومن أمثلة ذلك تقنيات معينة تعتمد على التوثيق القائم على واحدة من أدوات الإحصاء الحيوي قائمة على التوقيعات الخطية، وفيها يوقع الموقع يدويا باستخدام قلم خاص إما على شاشة الحاسوب أو على لوح رقمي. وعندئذ يُحال التوقيع الخطي بواسطة الحاسوب ويخزن كمجموعة من القيم الرقمية التي يمكن أن تضاف الى رسالة البيانات ويستطيع متلقيها أن يعرضها على شاشة الحاسوب لأغراض التوثيق. ويفترض هذا النظام من نظم التوثيق أن عينات من التوقيع الخطي قد سبق تحليلها وتخزينها بواسطة أداة الإحصاء الحيوي.

١٦ - وقد يرغب الفريق العامل في أن يناقش ما إذا كان ينبغي توسيع نطاق عمله لكي يشمل التوقيعات الإلكترونية بوجه عام علما بأن هذا العمل سوف يتطلب من الأمانة أن تجري بحوثا إضافية عن المتضمنات التقنية والقانونية لاستخدام أدوات "التوقيع" المعتمدة على تقنيات أخرى غير ترميز المفتاح العام. وبالنظر الى توافر قدر كاف من المعلومات الأولية عن المتضمنات القانونية للتوقيعات الرقمية، والى وجود مشاريع قوانين بشأن الموضوع في عدد من البلدان، فإن هذه المذكرة تركز على المسائل المتعلقة بالتوقيعات الرقمية المعتمدة على ترميز المفتاح العام.

١٧ - وعند مناقشة استصواب وجدوى إعداد قواعد موحدة تنطبق على التوقيعات الرقمية وغيرها من أشكال التوقيع الإلكتروني، قد يرغب الفريق العامل في أن ينظر فيما إذا كانت الأونسيترال ينبغي أن تحاول تطوير قواعد موحدة على

مستوى وسط بين المستوى العالي من العمومية الذي بلغه القانون النموذجي وبين قواعد أكثر تحديداً تتناول تقنية واحدة أو أكثر من تقنيات معينة. وأياً كان الأمر فإنه عملا بمبدأ حياد الرسائل الذي أخذ به في القانون النموذجي، ينبغي القواعد الموحدة المزمع إعدادها – إن هي ركزت على التوقيعات الرقمية، ألا تثني عن استخدام طرق بديلة.

٢ – التوقيعات الرقمية المعتمدة على الترميز بالمفتاح العام[٢]

(أ) المفاهيم والمصطلحات التقنية

'١' الترميز

١٨ – تُنشأ التوقيعات الرقمية ويُتثبت من صحتها باستخدام الترميز، فرع الرياضيات التطبيقية الذي يعنى بتحويل الرسائل الى صيغ غير مفهومة ثم إعادتها الى صيغتها الأصلية. وتستخدم التوقيعات الرقمية ما يعرف باسم "ترميز المفتاح العام" الذي كثيراً ما ينهض على استخدام دوال خوارزمية لإنتاج "مفتاحين" مختلفين ولكنهما مترابطان رياضيا (والمفاتيح أعداد ضخمة يُحصل عليها باستخدام سلسلة من الصيغ الرياضية المطبقة على أعداد أولية). ويُستخدم أحد هذين المفتاحين في إنشاء توقيع رقمي أو في تحويل بيانات الى صيغة غير مفهومة في ظاهرها، ويستخدم المفتاح الثاني للتثبت من صحة توقيع رقمي أو إعادة رسالة البيانات الى صيغتها الأصلية. وكثيراً ما يشار الى أجهزة وبرامجيات الحاسوب التي تستخدم مثل هذين المفتاحين بعبارة جامعة هي "نظم ترميز" (cryptosystems) أو بعبارة أكثر تحديداً هي "نظم ترميز غير متناظرة" « asymmetric cryptosystems » حيث تعتمد على خوارزميات غير متناظرة.

١٩ – وعلى حين أن استخدام الترميز هو أحد السمات الرئيسية للتوقيعات الرقمية، فإن مجرد حقيقة أن التوقيع الرقمي يستخدم لتوثيق رسالة تحتوي على معلومات مقدمة في صيغة رقمية ينبغي ألا يُخلَط بينها وبين استخدام أعم للترميز لأغراض الحفاظ على السرية. وترميز الحفاظ على السرية هو طريقة تستخدم لترميز رسالة إلكترونية بحيث لا يتمكن من قراءتها أحد غير منشئ الرسالة والمرسَل إليه. وفي عدد من البلدان يقيد القانون استخدام الترميز لأغراض الحفاظ على السرية 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 نظراً لأن التوقيع الرقمي المرَمّز قد لا يكون سوى إضافة الى رسالة غير مرمّزة. وقد يرغب الفريق العامل في دراسة المدى الذي يمكن أن تذهب إليه قواعد موحدة ممكنة بشأن التوقيعات الرقمية في الاعتراف باستخدام الترميز لأغراض التوثيق باعتباره أمرا متميزاً عن استخدامه لأغراض الحفاظ على السرية.

٢٠ – ويمكن القول، على سبيل توضيح الأسباب التي من أجلها يمكن أن تدعو الحاجة الى قواعد مختلفة حيث يستخدم الترميز لأغراض الحفاظ على السرية وحيث لا يستخدم إلا في سياق التوقيعات الرقمية، بأنه حيث يستخدم الترميز لأغراض الحفاظ على سرية الرسائل، من المهم في ظل ظروف كثيرة أن توجد طريقة لاسترداد الرسائل المرمّزة في حالة ضياع المفتاح الخاص وكان للرسالة المرمّزة قيمة هامة، قانونية أو مالية أو محاسبية عامة. فهذه التكنولوجيا، عندما تطبق كما ينبغي، تتيح لمُصدر زوج المفاتيح أن يستبقي المفتاح المفقود أو ينشئه من جديد. ومن جهة أخرى قد لا تكون هناك حاجة الى استبقاء أو إعادة إنشاء مفتاح خاص يستخدم في إنشاء توقيعات رقمية، ومن الممكن أن يقلل امتلاك القدرة التقنية على تحقيق ذلك من الثقة التي يوليها المنتفعون والجمهور عموماً للنظام في مجموعه.

'٢' مفاتيح الترميز العامة والخاصة

٢١ – المفاتيح المتكاملة التي تستخدم في التوقيعات الرقمية أطلق عليها اعتباطياً "المفتاح الخاص"، وهو المفتاح الذي لا يستخدمه إلا الموقّع في إنشاء توقيع رقمي، و"المفتاح العام" الذي يكون عادة معروفاً على نطاق أوسع ويستخدمه طرف معتمِد

---

(٢) استُند في عرض كثير من عناصر وصف أداء نظام التوقيع الرقمي في هذا الفرع الى **الخطوط التوجيهية للتوقيع الرقمي**، الصادرة عن رابطة المحامين الأمريكيين، الصفحات من ٨ الى ١٧.

في التثبت من صحة التوقيع الرقمي[٣]. وإذا احتاج عدد كبير من الناس الى التثبت من صحة التوقيع الرقمي للموقّع، تعين إتاحة المفتاح العام لهم جميعاً أو توزيعه عليهم بنشره مثلا في قاعدة بيانات مباشرة أو في أي دليل عام بحيث يسهل الوصول إليه. وعلى الرغم من أن زوج المفاتيح مترابطان رياضيا، فإنه إذا صُمِّم ونُفِّذ نظام ترميز بطريقة مأمونة استحال عمليا اشتقاق مفتاح خاص انطلاقا من معرفة المفتاح العام. وتنبني أكثر الخوارزميات شيوعاً في الترميز باستخدام المفتاح العام والمفتاح الخاص على سمة هامة من سمات الأعداد الأولية: فما أن تضرب تلك الأعداد في بعضها البعض لإنتاج عدد جديد حتى يستحيل عمليا معرفة أي عددين أوليين أنشآ ذلك الرقم الجديد الأكبر[٤]. وهكذا فعلى الرغم من أن كثيراً من الناس قد يعرفون المفتاح العام لموقّع معين ويستخدمونه في التثبت من صحة توقيعاته، فإنه لا يمكنهم أن يكتشفوا المفتاح الخاص للموقّع ويستخدموه في تزييف توقيعات رقمية.

٢٢ - وجدير بالذكر مع ذلك أن مفهوم ترميز المفتاح العام لا يقتضي ضمناً بالضرورة استخدام الخوارزميات الآنفة الذكر المبنية على الأعداد الأولية. ذلك أنه توجد في الوقت الراهن تقنيات رياضية تستخدم أو قيد التطوير، يذكر منها نظم الترميز القائمة على المنحنيات الناقصية، التي كثيراً ما يقال عنها إنها تتيح درجة عالية من الأمان من خلال استخدام أطوال مفاتيح مخفضة الى حد كبير. وقد يرغب الفريق العامل، عند مناقشته المسائل المتعلقة بترميز المفتاح، في أن يعرف الى أي مدى يؤخذ بتقنية ترميز المفتاح العام في التجارة الدولية في الوقت الحاضر. وفي الوقت نفسه قد يرغب الفريق العامل في اتخاذ موقف محايد تقنيا يضع في الاعتبار التكنولوجيا الراهنة دون أن يستبعد حدوث تغيرات في تقنيات الحساب التي تستخدم في إنتاج أزواج المفاتيح. وفضلا عن ذلك فإن هذا الانفتاح على التطورات التقنية في صناعة الحواسيب سيكون متسقا مع قرار اللجنة بأنه يستحيل على الأونسيترال أن تقدم على إعداد معايير تقنية وبأنه ينبغي الحرص على ألا تتورط في المسائل التقنية المتعلقة بالتوقيعات الرقمية (انظر الفقرة ٣ أعلاه).

'٣' "دالة التشويش"

٢٣ - والى جانب عملية إنتاج المفاتيح توجد عملية أساسية أخرى يشار إليها عموما بعبارة "دالة التشويش" (hash function) وتستخدم في إنشاء التوقيعات الرقمية وفي التثبت من صحتها. ودالة التشويش عملية رياضية مبنية على خوارزمية تنشئ صورة رقمية أو شكلا مركزاً من الرسالة كثيراً ما يشار إليها بعبارة "خلاصة رسالة" (message digest) أو "بصمة رسالة" (message fingerpoint) تتخذ شكل "قيمة تشويش" (hash value) أو "نتيجة تشويش" (hash result) ذات طول موحد يكون عادة أصغر كثيراً من الرسالة ولكنه يخصها وحدها الى حد كبير. وأي تغيير يطرأ على الرسالة تترتب عليه دائماً نتيجة تشويش مختلفة عندما تستخدم نفس دالة التشويش. وفي حالة دالة تشويش مأمونة، تعرف أحيانا باسم دالة تشويش ذات اتجاه واحد، يستحيل عملياً اشتقاق الرسالة الأصلية عند معرفة قيمة التشويش العائدة إليها. وعلى ذلك فإن دوال التشويش تمكن من تشغيل البرنامج الحاسوبي المعد لإنشاء التوقيعات الرقمية بمقادير أصغر من البيانات التي يمكن التنبؤ بها، ومن تحقيق ارتباط إثباتي قوي مع محتوى الرسالة الأصلية، والتوصل بذلك الى توفير الأدلة على أنه لم يطرأ على الرسالة أي تعديل منذ أن وقعت رقميا.

---

(٣) ينتظر من مستعمل مفتاح خاص أن يحافظ على سرية ذلك المفتاح الخاص. ومن الجدير بالذكر أن المستعمل الفرد ليس بحاجة الى أن يعرف المفتاح الخاص. والمرجح هو أن يحفظ ذلك المفتاح الخاص على بطاقة ذكية أو أن يكون الوصول إليه من خلال رقم هوية شخصي أو، في الحالات المثلى، من خلال أداة حيوية قياسية لإثبات الهوية، كأن يكون ذلك مثلا من خلال التعرف على بصمة الإبهام.

(٤) تشير بعض المعايير الموجودة، مثل "الخطوط التوجيهية للتوقيعات الرقمية" الصادر عن رابطة المحامين الأمريكيين الى مفهوم "الاستحالة الحسابية" (computational infeasibility) لوصف عدم قابلية العملية للعكس، أي الأمل في استحالة اشتقاق المفتاح الخاص السري العائد الى مستعمله من المفتاح العام لذلك المستعمل. و"الاستحالة الحسابية" مفهوم نسبي يستند الى قيمة البيانات المحمية، وتكلفة العمليات الحسابية 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 المقبل (الخطوط التوجيهية للتوقيعات الرقمية، رابطة المحامين الأمريكيين، ص ٩، الملاحظة ٢٣).

'٤' التوقيع الرقمي

٢٤ - قبل التوقيع على مستند أو على أي معلومات أخرى، يتعين على الموقّع أن يرسم بدقة حدود ما يريد التوقيع عليه. والمعلومات المراد توقيعها والتي حددت على هذا النحو يمكن الإشارة إليها بعبارة "الرسالة". ثم تتولى دالة تشويش في البرنامج الحاسوبي للموقّع حساب نتيجة تشويش تنفرد بها عملياً تلك الرسالة. وعندئذ يحول البرنامج الحاسوبي الموقّع نتيجة التشويش الى توقيع رقمي مع استخدام المفتاح الخاص للموقع. وبذلك يكون التوقيع الرقمي الناتج عن ذلك توقيعا تنفرد به الرسالة والمفتاح الخاص الذي استخدم في إنشائها.

٢٥ - ونموذجيا، يلحق التوقيع الرقمي (نتيجة تشويش للرسالة موقع عليها رقميا) ويخزن أو ينقل مع رسالته. غير أن من الممكن أيضا إرساله أو خزنه على أنه عنصر بيانات منفصل ما دام مرتبطا برسالته على نحو يمكن التعويل عليه. وبالنظر الى أن التوقيع الرقمي إنما يخص رسالته دون سواها، فإنه لا تكون له أي فائدة إذا انفصل عن رسالته بصفة دائمة.

'٥' التثبت من صحة التوقيع الرقمي

٢٦ - التثبت من صحة التوقيع الرقمي عملية تدقيق للتوقيع الرقمي بالرجوع الى الرسالة الأصلية والى مفتاح عام معين الابت فيما إذا كان ذلك التوقيع الرقمي قد أنشئ لتلك الرسالة ذاتها باستخدام المفتاح الخاص المناظر المفتاح العام المذكور. ويتم التثبت من صحة توقيع رقمي بحساب نتيجة تشويش جديدة الرسالة الأصلية بواسطة نفس دالة التشويش التي استخدمت لإنشاء التوقيع الرقمي. ثم يدقق الشخص المحقق، باستخدام المفتاح العام ونتيجة التشويش الجديدة، فيما إذا كان التوقيع الرقمي قد أنشئ باستخدام المفتاح الخاص المناظر وما إذا كانت نتيجة التشويش المحسوبة مجدداً تطابق نتيجة التشويش الأصلية التي حُوِّلت الى التوقيع الرقمي أثناء عملية التوقيع.

٢٧ - ويؤكد برنامج التثبت الحاسوبي "صحة" التوقيع الرقمي عندما: (١) يكون المفتاح الخاص للموقّع قد استخدم لتوقيع الرسالة رقميا، ومعروف أن ذلك هو الذي سيحدث إذا استخدم المفتاح العام للموقّع في التثبت من صحة التوقيع نظراً لأن المفتاح العام الموقّع لا يشهد بصحة توقيع رقمي ما لم يكن ذلك التوقيع قد أنشأه المفتاح الخاص الموقّع؛ و (٢) عندما تكون الرسالة لم يطرأ عليها أي تغيير، ومعروف أن ذلك هو الذي سيحدث إذا كانت نتيجة التشويش المحسوبة بمعرفة الشخص المحقق مطابقة لنتيجة التشويش المستخرجة من التوقيع الرقمي أثناء عملية التثبت من صحته.

(ب) البنية الأساسية المفتاح العام وسلطات التصديق

٢٨ - للتثبت من صحة توقيع رقمي يجب أن يمكّن الشخص المحقق من الوصول الى المفتاح العام الموقّع وأن يُضْمَن له تناظره مع المفتاح الخاص الموقّع. ومن جهة أخرى فإن زوج المفاتيح العام والخاص ليس له اقتران ذاتي بأي شخص معين إذ هو مجرد زوج من الأرقام، ويلزم توافر آلية إضافية لقرن شخص أو كيان معين بزوج المفاتيح قرنا يعول عليه. وإذا كان لترميز المفتاح العام أن يحقق الأغراض المقصودة منه، تعين إيجاد طريقة لإرسال مفاتيح لطائفة متنوعة من الأشخاص كثير منهم غير معروفين لدى المرسل حيث لم تنشأ وتنمى علاقة ثقة بين الأطراف. ولكي تنشأ علاقة كهذه، يجب أن تتوافر لدى الأطراف المعنية درجة عالية من الثقة فيما يصدر من مفاتيح عامة وخاصة.

٢٩ - وقد يتوافر مستوى الثقة المطلوب بين الأطراف الذين يثقون بعضهم ببعض ويكونون قد تعاملوا فيما بينهم على امتداد فترة طويلة من الزمن وتجري الاتصالات بينهم على نظام مغلق ويعملون داخل مجموعة مغلقة ولديهم القدرة على تنظيم معاملاتهم تعاقديا كأن يكون بينهم مثلا اتفاق شراكة تجارية. وفي معاملة لا تضم سوى طرفين، يمكن لكل منهما أن يبلغ الآخر (عبر قناة مأمونة نسبيا، مثل رسول خاص أو هاتف مأمون) المفتاح العام من زوج المفاتيح الذي يستخدمه كل منهما. ومن جهة أخرى لن يكفل نفس مستوى الثقة إذا كانت الأطراف لا تتعامل فيما بينها إلا نادراً، ويجرون اتصالاتهم على نظام مفتوح (مثل الشبكة العالمية التي توفرها الإنترنيت)، ولا يعملون في إطار مجموعة مغلقة أو تنفيذاً لاتفاقات شراكات تجارية أو وفقا لقانون ينظم ما بينهم من علاقات.

٣٠ - وعلاوة على ذلك فبالنظر الى أن الترميز بالمفتاح العام تكنولوجية رياضية معقدة ينبغي أن تتوافر لجميع مستعمليها ثقة في مهارة الأطراف التي تصدر المفاتيح العامة والخاصة وفي معارفهم وفيما يتخذونه من ترتيبات أمان.(٥)

٣١ - وقد يصدر موقّع مرتقب بيانا عاما يذكر فيه أن التوقيعات التي يمكن التثبت من صحتها بمفتاح عام معين ينبغي أن تعامل على أنها ناشئة من ذلك الموقّع. غير أن الأطراف الأخرى قد لا تكون على استعداد لقبول البيان ولا سيما حيث لم يكن قد أبرم عقد سابق يقر بما لا يدع مجالا للشك الأثر القانوني لذلك البيان المنشور. فالطرف الذي يعتمد على مثل هذا البيان المنشور على نظام مفتوح ودون سند يدعمه، سيكون عرضة لمخاطرة كبيرة نتيجة لوضعه ثقته، في غفلة منه، في شخص محتال، أو نتيجة لاضطراره الى دحض إنكار زائف لتوقيع رقمي (وهي مسألة كثيراً ما يشار إليها بعبارة "عدم التنصل") إذا تبين أن معاملة ما ليست في صالح الموقّع المدّعَى.

٣٢ - ويتمثل أحد حلول هذه المشاكل في استخدام واحد أو أكثر من الأطراف الثالثة الموثوقة في الربط بين موقّع معروف الهوية أو بين اسم الموقّع وبين مفتاح عام معين. ويشار الى هذا الطرف الثالث الموثوق عموماً بعبارة "سلطة التصديق" في معظم المعايير والخطوط التوجيهية التقنية. وفي عدد من البلدان تنظم سلطات التصديق هذه في ترتيب تدرجي فتصبح ما يطلق عليه في أحيان كثيرة عبارة البنية الأساسية للمفتاح العام (ب م ع).

'١' البنية الأساسية للمفتاح العام (ب م ع)

٣٣ - يعد إنشاء بنية أساسية للمفتاح العام وسيلة لتوفير الثقة بأن: (١) المفتاح العام لمستعمل ما لم يُعبَث به وأنه يناظر بالفعل المفتاح الخاص لذلك المستعمل؛ (٢) تقنيات الترميز المستخدمة تقنيات سليمة؛ (٣) الكيانات التي تصدر مفاتيح الترميز يمكن التعويل عليها في الحفاظ على المفاتيح العامة والخاصة وفي إعادة إنشائها، وأن هذه المفاتيح يمكن استخدامها في أغراض الحفاظ على السرية حيث يكون استخدام هذه التقنية أمراً مرخصاً به؛ (٤) مختلف نظم الترميز قابلة للتشغيل المتبادل فيما بينها. ولتوفير الثقة المذكورة أعلاه، بوسع البنية الأساسية المفتاح العام أن تقدم عدداً من الخدمات يذكر من بينها ما يلي: (١) إدارة مفاتيح الترميز المستعملة لأغراض التوقيع الرقمي؛ (٢) التصديق على أن مفتاحاً عاماً يناظر مفتاحاً خاصاً؛ (٣) توفير مفاتيح للمستعملين النهائيين؛ (٤) البت في أي المستعملين سيمنحون أي امتيازات في النظام؛ (٥) نشر دليل مأمون بالمفاتيح العامة أو بالشهادات؛ (٦) إدارة البطاقات الشخصية (كالبطاقات الذكية مثلا) التي يمكنها تحديد هوية المستعمل بمعلومات هوية شخصية فريدة أو أن تنتج وتخزن المفاتيح الخاصة العائدة الى أفراد؛ (٧) تدقيق هوية المستعملين النهائيين وتزويدهم بالخدمات؛ (٨) توفير خدمات "عدم التنصل"؛ (٩) توفير خدمات ختم الوقت؛ إدارة مفاتيح الترميز المستخدمة لأغراض الحفاظ على السرية حيث يكون استخدام هذه التقنية أمراً مرخصاً به.

٣٤ - وكثيراً ما تكون البنية الأساسية للمفتاح العام (ب م ع) قائمة على مستويات سلطة تدرّجية مختلفة. ومن أمثلة ذلك أن النماذج التي يجري النظر فيها في بلدان معينة لإنشاء بنى أساسية (ب م ع) ترد بها إشارات الى المستويات التالية: (١) "سلطة رئيسية" (root authority) فريدة يمكن أن تصدق على تكنولوجيا وممارسات جميع الأطراف المرخص لهم بإصدار أزواج مفاتيح ترميز أو شهادات تتعلق باستخدام تلك الأزواج من المفاتيح؛ كما يمكن أن تسجل ما دونها من سلطات التصديق؛(٦) (٢) سلطات تصديق متعددة تحتل مكانة أدنى من مكانة السلطة الرئيسية ويمكنها أن تصدق على أن المفتاح العام لمستعمل ما إنما يناظر المفتاح الخاص لذلك المستعمل (أي أنه لم يُعبَث به)؛ (٣) سلطات تسجيل محلية متعددة تحتل مكانة أدنى من مكانة سلطات التصديق وتتلقى طلبات من مستعملي أزواج من مفاتيح الترميز أو شهادات تتعلق باستخدام تلك الأزواج من المفاتيح، للحصول على براهين لإثبات هوية مستعملين محتملين أو تدقيق تلك الهوية. وفي بلدان معينة، يعتزم قيام محررو العقود بدور سلطات التسجيل المحلية أو بمساندة تلك السلطات في مهمتها.

---

(٥) في المواقف التي يتولى فيها المستعملون أنفسهم إصدار مفاتيح الترميز العامة والخاصة، قد يتعين قيام سلطات التصديق على المفاتيح العامة بتوفير هذه الثقة.

(٦) أما مسألة ما إذا كان لدى الحكومة القدرة التقنية على الاحتفاظ بالمفاتيح الخاصة للحفاظ على السرية أو على إعادة إنشاء تلك المفاتيح فيمكن تناولها على مستوى السلطة الرئيسية.

٣٥ - وقد يرغب الفريق العامل في إجراء مناقشة عامة حول المسائل المتعلقة بالبنى الأساسية (ب م ع). غير أنه مما يذكر أن مثل هذه المسائل قد لا يكون تنسيقها على الصعيد الدولي أمراً يسيراً. ذلك أن تنظيم بنية أساسية (ب م ع) قد ينطوي على مسائل تقنية متنوعة وعلى مسائل تتعلق بالسياسة العامة وقد يكون من الأصوب ترك أمرها لكل دولة تبت فيه.[٧] وفي هذا الصدد، قد يحتاج الأمر الى اتخاذ قرارات من جانب كل دولة تنظر في إنشاء بنية أساسية (ب م ع) بشأن أمور يذكر منها مثلا: (١) شكل الـ ب م ع وعدد مستويات السلطة التي تضمها؛ (٢) ما إذا كان إصدار أزواج مفاتيح الترميز سيكون قاصراً على سلطات تصديق معينة تنتمي الى الـ ب م ع أو كان من الممكن أن يصدر المستعملون أنفسهم تلك الأزواج من المفاتيح؛ (٣) ما إذا كانت سلطات التصديق التي تشهد بصحة أزواج مفاتيح الترميز ينبغي أن تكون كيانات عامة أو كان من الممكن قيام كيانات خاصة بدور سلطات التصديق؛ (٤) ما إذا كانت عملية السماح لكيان معين بالعمل بمثابة سلطة تصديق ينبغي أن تتخذ شكل ترخيص صريح أو إذن من الدولة، أو كان ينبغي اللجوء الى طرق أخرى لمراقبة جودة سلطات التصديق إن هي سمح لها بالعمل دون الحصول على ترخيص محدد؛ (٥) المدى الذي يمكن الذهاب إليه في الترخيص باستخدام الترميز في أغراض الحفاظ على السرية؛ (٦) ما إذا كانت السلطات الحكومية ينبغي أن تحتفظ بحق الوصول الى المعلومات المرمزة عبر آلية "تعليق الأيلولة" (key escrow) أو بوسيلة أخرى. وقد يرغب الفريق العامل في أن يوصي بأن لا تدرج المسائل الآنفة الذكر في الأعمال المقبلة للجنة فيما يتعلق بالتوقيعات الرقمية.

'٢' سلطات التصديق

٣٦ - للربط بين زوج من المفاتيح وبين موقّع مرتقب، تصدر سلطة تصديق شهادة هي عبارة عن سجل إلكتروني يتضمن مفتاحاً عاماً الى جانب اسم المشترك في الشهادة باعتباره "موضوع" الشهادة، وقد يؤكد أن الموقع المرتقب المحددة هويته في الشهادة يحمل المفتاح الخاص المناظر. ومن بين الوظائف الرئيسية للشهادة ربط مفتاح عام بحامل معين. وبوسع "متلقي" الشهادة الراغب في الاعتماد على توقيع رقمي أنشأه حامل المفتاح الخاص المسمى في الشهادة أن يستعمل المفتاح العام المدرج في الشهادة للتثبت من أن التوقيع الرقمي أنشئ باستخدام المفتاح الخاص المناظر. فإذا نجح هذا التثبت، أعطي الشخص المحقق تأكيدا بأن التوقيع الرقمي أنشأه حامل المفتاح العام المدرج اسمه في الشهادة وبأن الرسالة المناظرة لم تعدّل منذ أن وقعت رقمياً.

٣٧ - ولتأمين وثاقة الشهادة فيما يتعلق بمحتواها وبمصدرها كليهما، توقعها رقميا سلطة التصديق. ويمكن التثبت من صحة التوقيع الرقمي لسلطة التصديق المصدرة على الشهادة باستخدام المفتاح العام العائد الى سلطة التصديق المدرجة في شهادة أخرى صادرة عن سلطة تصديق (ربما كانت - وإن لم يكن بالضرورة - أعلى منها مستوى في النظام التدرجي)، وتلك الشهادة الأخرى يمكن بدورها أن توثق باستخدام المفتاح العام المدرج في شهادة غير هذه وتلك، وهكذا دواليك الى أن يطمئن الشخص المعتمد على التوقيع الرقمي بما فيه الكفاية الى صحة التوقيع. وفي كل من هذه الحالات، يجب على سلطة التصديق المصدرة للشهادة أن توقع رقميا على شهادتها أثناء الفترة التشغيلية للشهادة الأخرى المستخدمة في التثبت من صحة التوقيع الرقمي لسلطة التصديق.

٣٨ - والتوقيع الرقمي المناظر لرسالة، سواء أنشأه حامل زوج من المفاتيح لتوثيق رسالة، أو أنشأته سلطة تصديق لتوثيق شهادتها، ينبغي عموما أن يختم زمنيا على نحو يعول عليه، وذلك لكي يتاح للشخص المحقق أن يعرف بما لا يدع مجالا للشك ما إذا كان التوقيع الرقمي قد أنشئ أثناء "الفترة التشغيلية" المذكورة في الشهادة، وذلك شرط من شروط التثبت من صحة توقيع رقمي.

٣٩ - ولتيسير توافر مفتاح عام ومناظرته لحامل معين من أجل استخدامهما للتثبت من الصحة يمكن نشر الشهادة في مستودع أو إتاحة الاطلاع عليها بوسائل أخرى. ونموذجيا، تكون المستودعات قواعد بيانات مباشرة عن الشهادات ومعلومات أخرى متاحة للاسترجاع والاستخدام في التثبت من صحة التوقيعات الرقمية. وتبعاً لأسلوب التنفيذ، يمكن أن

---

(٧) ومن جهة أخرى ففي سياق التصديق المتبادل عبر الحدود (cross-cerfification) ستدعو الحاجة الى التشغيل المتبادل على الصعيد العالمي الى أن تكون الـ ب م ع المنشأة في مختلف البلدان قادرة على التخاطب فيما بينها.

يتحقق استرجاع شهادة بطريقة آلية، وذلك بجعل برنامج التثبت من الصحة يستفسر من المستودع مباشرة من أجل الحصول على الشهادات حسب الحاجة.

٤٠ - وربما يتبين أن الشهادة لا يعول عليها حال صدورها كما يحدث في المواقف التي يدّعي فيها حامل الشهادة لنفسه أمام سلطة التصديق هوية غير هويته. وفي ظروف أخرى ربما يمكن التعويل على الشهادة حين صدورها ولكنها تفقد عولها بعد ذلك. فإذا لحق بالمفتاح الخاص "عيب" ما، كأن يفقد حامل المفتاح الخاص سيطرته عليه فتفقد الشهادة جدارتها بالثقة أو عولها، وعندئذ قد تعمد سلطة التصديق (بناء على طلب حامل المفتاح أو حتى بدون موافقته) الى تعليق الشهادة (بوقف فترة التشغيل مؤقتا) أو الى إلغائها (إبطالها بصفة دائمة). وفور تعليق الشهادة أو إلغائها، يتعين على سلطة التصديق عموماً أن تنشر إشعاراً بالإلغاء أو التعليق أو تبلغ الأمر الى المستفسرين من الأشخاص أو الى الأشخاص الذين يعرف أنهم تلقوا توقيعا رقمياً يمكن التثبت من صحته بالرجوع الى الشهادة التي فقدت عولها.

٤١ - ويمكن أن نتصور سلطات تصديق تشغّلها جهات حكومية وأخرى يشغّلها مقدمو خدمات بالقطاع الخاص. ومن المزمع في عدد من البلدان، لأسباب تتعلق بالسياسة العامة، قصر الترخيص بتشغيل سلطات التصديق على كيانات حكومية. ويرى في بلدان أخرى أن خدمات التصديق ينبغي أن تكون مفتوحة للمنافسة من جانب القطاع الخاص. وبصرف النظر عما إذا كانت سلطات التصديق تشغّلها كيانات حكومية أو يشغّلها مقدمو خدمات بالقطاع الخاص، وعما إذا كانت سلطات التصديق ستحتاج أو لن تحتاج الى الحصول على ترخيص تشغيل، يوجد نموذجيا أكثر من سلطة تصديق واحدة في البنية الأساسية لـ ب م ع. ومن دواعي الاهتمام ما يقام من علاقات بين سلطات التصديق. فسلطات التصديق داخل الـ ب م ع يمكن إنشاؤها في بنية تدرّجية حيث تقتصر وظيفة بعض سلطات التصديق على اعتماد سلطات تصديق أخرى تقدم الخدمات مباشرة الى المستعملين. وفي بنية كهذه، تخضع سلطات التصديق لسلطات تصديق أخرى. وفي بنى أخرى يمكن تصورها، يمكن تشغيل بعض سلطات التصديق على قدم المساواة مع سلطات تصديق أخرى. وفي أي بنية أساسية كبيرة لـ ب م ع، يرجح أن توجد معا سلطات تصديق دنيا وسلطات تصديق عليا. وأياً كان الأمر، ففي غياب ب م ع دولية، قد ينشأ عدد من دواعي الاهتمام فيما يتعلق بالاعتراف بالشهادات التي تصدرها سلطات تصديق في بلدان أجنبية. وكثيراً ما يشار الى الاعتراف بالشهادات الأجنبية بعبارة "التصديق المتبادل عبر الحدود" cross certification. ومن الضروري في مثل هذه الحالة أن يكون تبادل الاعتراف بالخدمات التي تؤديها سلطات التصديق بين سلطات تصديق متعادلة الى حد كبير (أو بين سلطات تصديق لديها الاستعداد لتحمل مخاطر معينة فيما يتعلق بالشهادات الصادرة عن سلطات تصديق أخرى)، وذلك لكي يستطيع المنتفعون بخدمات كل منها أن يتخاطبوا فيما بينهم بمزيد من الكفاءة ومن الإيمان بجدارة الشهادات التي تصدرها بالثقة.

٤٢ - وقد تنشأ مسائل قانونية فيما يتعلق بالتصديق المتبادل عبر الحدود أو بالاعتراف بالشهادات الأجنبية (chaining of certificates) عندما تنتهج سياسات أمان متعددة. ومن أمثلة هذه المسائل، البت فيمن كان سوء تصرفه أو سلوكه هو السبب في وقوع الخسارة، وتحديد شهادات التصديق التي اعتمد عليها المنتفع بالخدمات. ومن الجدير بالذكر أن القواعد القانونية التي يجري النظر في اعتمادها في بلدان معينة تنص على أنه حيث يبلّغ المنتفعون بمستويات الأمان وبالسياسات المنتهجة، وحيث لا يقع إهمال من جانب سلطات التصديق، لا ينبغي أن تتحمل تلك السلطات أي مسؤولية.

٤٣ - وقد يتعين على سلطة التصديق أو السلطة الرئيسية أن تتحقق من أن الشروط التي تنص عليها سياستها العامة يجري الوفاء بها على أساس مستمر. فلئن كان اختيار سلطات التصديق يتوقف على عدد من العوامل يذكر منها قوة المفتاح العام الذي يجري استعماله وهوية مستعمله، فإن الجدارة بالثقة التي تتمتع بها أي سلطة تصديق قد تتوقف أيضا على إنفاذها معايير إصدار الشهادات ومدى عول تقييمها للبيانات التي تتلقاها من المستعملين الراغبين في الحصول على شهادات. ومما يتسم بأهمية بالغة نظام المسؤولية الذي ينطبق على أي سلطة تصديق فيما يتعلق بامتثالها لشروط السياسة العامة والأمان الصادرة عن السلطة الرئيسية أو عن سلطة التصديق العليا، أو بامتثالها لأي شروط أخرى منطبقة، وذلك على أساس مستمر.

٤٤ - وقد يرغب الفريق العامل في أن ينظر في العوامل التالية لوضعها في الاعتبار عند تقدير جدارة سلطة التصديق بالثقة: (١) استقلالها (أي عدم وجود أي مصالح مالية أو غيرها في المعاملات الأساسية)؛ (٢) مصادرها المالية وقدرتها المالية على تحمل المخاطر الناجمة عن مسؤوليتها عن الخسارة؛ (٣) خبرتها المتخصصة في تكنولوجيا المفتاح العام وألفتها إجراءات الأمان السليمة؛ (٤) طول مدة بقائها (ذلك أن سلطات التصديق يمكن أن تطالَب بتقديم شواهد تصديق أو مفاتيح ترميز بعد مضي كثير من السنوات على إتمام المعاملة الأساسية، وذلك في سياق دعوى قضائية أو مطالبة بملكية)؛ (٥) الموافقة على المعدات والبرامجيات؛ (٦) متابعة حسابات المعاملات وإجراء مراجعات بمعرفة كيان مستقل؛ (٧) وجود خطة طوارئ (مثال ذلك التعويض عن الخسائر الناجمة عن الكوارث أو تعليق أيلولة البرامج الحاسوبية أو المفتاح)؛ (٨) اختيار الموظفين والتنظيم والإدارة؛ (٩) ترتيبات الحماية اللازمة للمفتاح الخاص العائد الى سلطة التصديق ذاتها؛ (١٠) الأمن الداخلي؛ (١١) ترتيبات إنهاء العمليات، بما في ذلك إشعار المستعملين؛ (١٢) الضمانات والتصديقات (الممنوحة والممنوعة)؛ (١٣) إقرار حدود المسؤولية؛ (١٤) التأمين؛ (١٥) تبادل التشغيل مع سلطات تصديق أخرى؛ (١٦) إجراءات الإلغاء (في حالة ضياع مفاتيح الترميز أو إلحاق عيوب بها).

(ج) ملخص عملية التوقيع الرقمي

٤٥ - ينطوي استخدام التوقيعات الرقمية عادة على العمليات التالية التي يؤديها إما الموقّع نفسه أو الشخص الذي يتلقى الرسالة الموقعة رقميا:

(١) ينتج المستعمل أو يعطي زوجاً فريداً من مفاتيح الترميز؛

(٢) يعد المرسل رسالته على جهاز حاسوب (في شكل رسالة بريد إلكتروني مثلا)؛

(٣) يعد المرسل "موجز رسالة" باستخدام خوارزمية تشويش مأمونة. وتستخدم في إنشاء التوقيع الرقمي نتيجة تشويش مشتقة من الرسالة الموقعة ومفتاح خاص معين وتكون قاصرة عليهما دون سواهما. ولكفالة أمن نتيجة التشويش يجب أن لا تكون هناك سوى إمكانية ضئيلة لإنشاء نفس التوقيع الرقمي بالجمع بين أي رسالة أخرى وأي مفتاح خاص آخر؛

(٤) يرمّز المرسل موجز الرسالة باستخدام المفتاح الخاص. ويطبق المفتاح الخاص على نص موجز الرسالة باستخدام خوارزمية رياضية. ويتألف التوقيع الرقمي من موجز رسالة مُرمّز؛

(٥) نموذجيا، يرفق المرسل توقيعه الرقمي بالرسالة أو يلحقه بها؛

(٦) يرسل المرسل توقيعه الرقمي ورسالته (غير المرمّزة أو المرمّزة) إلكترونيا الى المتلقي؛

(٧) يستخدم المتلقي المفتاح العام العائد الى المرسل للتثبت من صحة التوقيع الرقمي المرسل. والتثبت من الصحة باستخدام المفتاح العام العائد الى المرسل يثبت أن الرسالة جاءت من المرسل دون سواه؛

(٨) ينشئ المتلقي أيضا "موجز رسالة" باستخدام نفس خوارزمية التشويش المأمونة؛

(٩) يضاهي المتلقي موجزَي الرسالة، فإذا كانا متطابقين فمؤدى ذلك أن المتلقي يعرف أن الرسالة لم تغيَّر بعد توقيعها. فحتى إذا لم يتغير سوى جزء ضئيل جداً من الرسالة بعد أن وقعت رقمياً، فسيكون موجز الرسالة الذي أنشأه المتلقي مختلفاً عن موجز الرسالة الذي أنشأه المرسل؛

(١٠) يحصل المتلقي من سلطة التصديق (أو عن طريق منشئ الرسالة) على شهادة تؤكد صحة التوقيع الرقمي الوارد على رسالة المرسل. وتكون سلطة التصديق، نموذجياً، طرفاً ثالثاً يحظى بالثقة ويدير عمليات التصديق في نظام للتوقيعات الرقمية. وتورد الشهادة ذكر المفتاح العام واسم المرسل (وربما أيضا معلومات إضافية) موقعا عليهما رقميا من جانب سلطة التصديق.

ثانيا - مسائل قانونية وأحكام ممكنة ينظر فيها عند إعداد قواعد موحدة بشأن التوقيعات الرقمية

ألف - نطاق العمل

٤٦ - عندما قررت اللجنة في دورتها التاسعة والعشرين أن تدرج في جدول أعمالها مسألة التوقيعات الرقمية وسلطات التصديق، وافقت أيضا على أنه ينبغي اغتنام هذه الفرصة لتناول مواضيع أخرى اقترحها الفريق العامل للعمل المقبل (انظر الفقرة ٨ أعلاه). وقد يرغب الفريق العامل، قبل الشروع في مناقشة المسائل المتعلقة بالتوقيعات الرقمية، في أن يناقش استصواب وجدوى حصر عمله في نطاق التوقيعات الرقمية أو توسيعه ليشمل أيضا آليات إثبات أخرى قد تكون متوافرة في الوقت الراهن أو لن تلبث أن تطور للاستخدام في التجارة الإلكترونية (انظر الفقرات ١٥-١٧ أعلاه). ومن الجدير بالذكر أنه أثناء إعداد القانون النموذجي كان الفريق العامل مدركا للحاجة الى إقرار قواعد قانونية لا تكون مقيدة بمرحلة معينة من مراحل التطور التقني والتجاري بل توفر بالأحرى مبادئ عامة يمكن توقع بقائها قابلة للتطبيق على امتداد عدد من السنوات بصرف النظر عما قد يطرأ على التكنولوجيا من تغيرات.

٤٧ - وقد يوحي الاستخدام الواسع النطاق للتوقيعات الرقمية، واحتمال اتباع مختلف البلدان نهوجا تشريعية متباينة إزاء التوقيعات الرقمية، بضرورة إقرار أحكام تشريعية موحدة تكون بمثابة إطار قانوني محدد لتقنية التوثيق هذه. غير أن الفريق العامل قد يرغب، مراعاة لنهج "حياد الوسائل" الذي اعتمد في إعداد القانون النموذجي، في أن يناقش ما إذا كان من المناسب الشروع في إعداد قواعد موحدة تنطبق على التوقيعات الرقمية وحدها أو أن تعد تلك القواعد الموحدة فيما يتعلق بتقنيات توثيق أخرى. فإذا توصل الفريق العامل الى استنتاج مؤداه أن الاحتمال الآنف الذكر بأن قوانين متباينة يمكن أن تشترع في مختلف البلدان يوحي بأن ضرورة إعداد قواعد موحدة تنطبق على التوقيعات الرقمية إنما هي ضرورة بالغة الإلحاح، فقد يرغب الفريق العامل في أن يناقش السبل التي يمكن بها إعداد القواعد الموحدة بشأن التوقيعات الرقمية على نحو يتفادى معه احتمال سوء تفسير تلك القواعد الموحدة على أنها تشجع استخدام التوقيعات الرقمية على حساب التقنيات المنافسة التي يمكن اعتبارها هي أيضا أمثلة مقبولة لمفهوم "الطريقة الجديرة بالتعويل عليها" المذكور في المادة ٧ من القانون النموذجي.

٤٨ - وفيما يتعلق بسلطات التصديق، قد يرغب الفريق العامل أيضا أن يضع في اعتباره أن الأنشطة التي يضطلع بها الكيان التجاري بوصفه سلطة تصديق ليست في كثير من المواقف العملية سوى جانب واحد من تشكيلة أوسع من أنشطة ذلك الكيان التجاري باعتباره مقدم خدمات. وعلى ذلك قد يرغب الفريق العامل في مناقشة ما إذا كانت القواعد الموحدة بشأن سلطات التصديق ينبغي قصر نطاقها على إقرار قواعد للسلوك لا تنطبق إلا في سياق أنشطة لمقدم الخدمات الذي يعمل بمثابة سلطة تصديق، أو كان من المستصوب والمجدي إعداد قواعد تنطبق على تشكيلة أوسع من أنشطة مقدمي الخدمات أو أنشطة "أطراف ثالثة موثوقة" في التجارة الإلكترونية.

باء - مجال تطبيق القواعد الموحدة بشأن التوقيعات الرقمية، وأحكام عامة

٤٩ - أعدت هذه المذكرة على افتراض أن القواعد الممكنة بشأن التوقيعات الرقمية ينبغي أن تشتق مباشرة من المادة ٧ من القانون النموذجي، وأن تعتبر طريقة لتوفير معلومات مفصلة عن مفهوم "طريقة" يعول عليها "لتعيين هوية شخص" و"التدليل على موافقة ذلك الشخص" على المعلومات الواردة في رسالة البيانات. وعند النظر في الأحكام العامة التي يمكن إدراجها في مجموعة من القواعد الموحدة بشأن التوقيعات الرقمية، قد يرغب الفريق العامل في أن ينظر بصورة أعم في العلاقة بين هذه القواعد الموحدة وقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية. وقد يرغب الفريق العامل على الأخص في أن يقدم الى اللجنة اقتراحات بشأن ما إذا كانت القواعد الموحدة ينبغي أن تشكل صكا قانونيا منفصلا أو أن تدرج في صيغة موسعة من القانون النموذجي، كأن يكون مثلا فصلا مستقلا في إطار الجزء الثاني من القانون النموذجي.

٥٠ - وبصرف النظر عما إذا كانت القواعد الموحدة بشأن التوقيعات الرقمية تعد بوصفها صكا منفصلا أو باعتبارها إضافة الى القانون النموذجي، فإنه يُرى أن القواعد الموحدة سوف تحتاج الى أن تنهض على أساس أحكام على غرار أحكام المادة ١ (نطاق التطبيق)، والمادة ٢ (أ) و (ج) و (د) (تعاريف المصطلحات، "رسالة البيانات" و"المنشئ" و"المرسل إليه")، والمادة ٣ (التفسير)، والمادة ٤ (التغيير بالاتفاق)، والمادة ٦ (الكتابة)، والمادة ٧ (التوقيع) - من القانون النموذجي. ولئن كانت هذه الأحكام لم تدرج صراحة في هذه المذكرة، فمن الجدير بالذكر أن الأمانة قد أعدت القواعد الموحدة بشأن التوقيعات الرقمية على أساس افتراض بأن هذه الأحكام تشكل جزءا من القواعد الموحدة. وجدير بالملاحظة أيضا في هذا الصدد أن أحكاما على غرار المواد ٢ و ٤ و ٦ و ٧ من القانون النموذجي قد أدرجت في تشريعات التوقيعات الرقمية التي يجري إعدادها في عدد من البلدان، كما أن القانون النموذجي نفسه يرد ذكره أيضا في نصوص يذكر منها **الخطوط التوجيهية للتوقيعات الرقمية** الصادر عن رابطة المحامين الأمريكيين.

٥١ - وبالإضافة الى الأحكام آنفة الذكر، قد يرغب الفريق العامل في أن ينظر فيما إذا كان ينبغي أن توضح ديباجة القواعد الموحدة الغرض من تلك القواعد، ألا وهو التشجيع على الاستخدام الكفء للاتصالات الرقمية بإقرار إطار أمان لها وبإضفاء مكانة متساوية للرسائل المكتوبة والرسائل الرقمية من حيث الأثر القانوني لكل منهما.

جيم - مسائل قانونية محددة ومشاريع أحكام بشأن التوقيعات الرقمية

١ - التعاريف

٥٢ - تختلف فيما بينها اختلافا كبيرا القوانين واللوائح والخطوط التوجيهية التي يجري تنفيذها بالفعل أو إعدادها في مجال التوقيعات الرقمية وسلطات التصديق، وذلك من حيث عدد التعاريف التي تستند إليها. وتبعاً للتقليد القانوني الذي تسير عليه الدولة المشترعة، يمكن أن تعالج معظم المسائل المتعلقة بالتوقيعات الرقمية إما بالاستناد الى تعاريف أو بدون إدراج أي تعاريف على الإطلاق.

٥٣ - وعملا بالنهج الذي اتبع في إعداد القانون النموذجي، قد يرغب الفريق العامل في النظر في تعاريف عدد من المفاهيم الجوهرية مثل "التوقيع الرقمي" و"سلطات التصديق" و"الشهادات".

٥٤ - وقد يرغب الفريق العامل في استخدام التعاريف الممكنة التالية كأساس لمداولاته.

(أ) التوقيع الرقمي

٥٥ - "مشروع المادة ألف

(١) التوقيع الرقمي هو قيمة عددية تبصم بها رسالة بيانات وتجعل من الممكن، باستخدام إجراء رياضي معروف يقترن بمفتاح الترميز الخاص لمنشئ الرسالة، القطع بأن هذه القيمة العددية قد تم الحصول عليها باستخدام مفتاح الترميز الخاص لمنشئ الرسالة دون سواه.

(٢) والإجراءات الرياضية المستخدمة في إنتاج توقيعات رقمية معتمدة بموجب [هذا القانون] [هذه القواعد] تستند الى ترميز مفتاح عام. وعندما تطبق تلك الإجراءات الرياضية على رسالة بيانات تحدث في الرسالة تحولا يمكن الشخص الذي يمتلك الرسالة المبدئية ومفتاح الترميز العام لمنشئ الرسالة من أن يبت بدقة

(أ) فيما إذا كان التحول قد أحدث باستخدام مفتاح الترميز الخاص الذي يناظر مفتاح الترميز الخاص للمنشئ؛ و

(ب) فيما إذا كانت الرسالة المبدئية قد غُيّرت بعد أن أحدث فيها التحول.

(٣) يعتبر التوقيع الرقمي الذي تبصم به رسالة بيانات توقيعاً معتمداً إذا أمكن التثبت من صحته باستخدام إجراءات أقرتها سلطة تصديق معتمدة بموجب [هذا القانون] [هذه القواعد].

(٤) تقر الـ ... [السلطة ذات الصلة في الدولة المشترعة] قواعد محددة للشروط التقنية التي يتعين أن تفي بها التوقيعات الرقمية والتثبت من صحة تلك التوقيعات".

ملاحظات

٥٦ - عملا بالنهج الوظيفي الذي اتبع في إعداد القانون النموذجي، تركز الفقرتان (١) و (٢) من الحكم المقترح على وصف موجز الوظائف التقنية التي يؤديها ترميز المفتاح العام. وتعبر الفقرتان (٣) و (٤) عن المبدأ القاضي بأن لا تكون التوقيعات الرقمية صحيحة إلا إذا استخدمت في سياق بنية أساسية لمفتاح عام ((public-key infrastructure (PKI) تنفذها سلطات عامة.

(ب) سلطات التصديق المعتمدة

٥٧ - "مشروع المادة باء

(١) يجوز لـ ... [تحدد الدولة المشترعة الجهاز المختص أو السلطة المختصة باعتماد سلطات التصديق] أن تمنح اعتماداً لسلطات التصديق بأن تتصرف عملا [بهذا القانون] [بهذه القواعد]. ويجوز إلغاء هذا الاعتماد.

(٢) يجوز لـ ... [تحدد الدولة المشترعة الجهاز المختص أو السلطة المختصة بإصدار لوائح بشأن سلطات التصديق المعتمدة] أن تقر قواعد تنظم الشروط التي يمكن بموجبها منح هذا الاعتماد وأن تصدر لوائح بسير عمل سلطات التصديق.

(٣) يجوز لسلطات التصديق المعتمدة أن تصدر شهادات فيما يتعلق بمفاتيح الترميز العائدة الى أشخاص طبيعيين أو أشخاص قانونيين.

(٤) يجوز لسلطات التصديق المعتمدة أن تقدم أو تيسر خدمات التسجيل وختم وقت إرسال واستقبال رسائل البيانات وغير ذلك من المهام المتعلقة بالاتصالات التي تتم بواسطة التوقيعات الرقمية.

(٥) يجوز لـ ... [تحدد الدولة المشترعة الجهاز المختص أو السلطة المختصة بإقرار قواعد محددة فيما يتعلق بالوظائف التي يتعين أن تؤديها سلطات التصديق المعتمدة فيما يتصل بإصدار الشهادات لمختلف الأشخاص الطبيعيين أو القانونيين".

ملاحظات

٥٨ - قد يرغب الفريق العامل في مناقشة ما إذا كان ينبغي القواعد الموحدة المزمع إعدادها أن تذكر صراحةً المعايير التي ينبغي وضعها في الاعتبار عند الترخيص لسلطات التصديق بممارسة مهامها. ومن الجدير بالذكر أنه عند إعداد القانون النموذجي تقرر إدراج هذه المعايير في دليل الاشتراع.

(ج) الشهادات

٥٩ - "مشروع المادة جيم

يُذكر في الشهادة التي تصدرها سلطة التصديق المعتمدة، سواء في شكل رسالة بيانات أو في شكل آخر، على الأقل ما يلي:

(أ) اسم مستعمل التوقيعات الرقمية [وعنوانه أو عنوان محل عمله]؛

(ب) [تاريخ وسنة الميلاد] [قدر كاف من التعريف بالهوية] في حالة ما إذا كان المستعمل شخصاً طبيعياً؛

(ج) وإذا كان المستعمل شخصاً قانونياً، ذكر اسم الشركة وأي معلومات أخرى التعريف بهويتها؛

(هـ) اسم سلطة التصديق وعنوانها أو عنوان محل عملها؛

(و) مفتاح الترميز العام العائد الى المستعمل؛

(ز) أي معلومات ضرورية لبيان الكيفية التي تتاح بها إمكانية التثبت من صحة المفتاح العام العائد الى المستعمل لمتلقي التوقيع الرقمي المعطى وفقاً للشهادة؛

(ح) الرقم المسلسل للشهادة؛

(ط) [تاريخ إصدار وتاريخ انتهاء] [فترة صلاحية] الشهادة."

ملاحظات

٦٠ - تتضمن مشاريع القوانين التي يجري إعدادها في بعض البلدان بشأن التوقيعات الرقمية قوائم بجميع العناصر التي ينص عليها مشروع المادة جيم باعتبارها الحد الأدنى من المعلومات المطلوبة لتلقي أي شهادة تصدرها سلطة تصديق. غير أنه عملا بقرار الفريق العامل وهو بصدد إعداد القانون النموذجي بأن لا يتدخل في المسائل المتعلقة بحماية البيانات الشخصية، قد يرغب الفريق العامل في أن يضع في اعتباره أنه في بلدان كثيرة تكفل الحماية للمعلومات التي تتعلق، مثلا، بتاريخ ميلاد الشخص باعتباره من البيانات الشخصية، وقد توجد قواعد محددة لتنظيم إذاعتها بالوسائل الإلكترونية.

٢ - توقيع أشخاص طبيعيين وأشخاص قانونيين

٦١ - "مشروع المادة دال

(١) يجوز للأشخاص الطبيعيين وللأشخاص القانونيين على السواء أن يحصلوا على تصديق لمفاتيح ترميز عامة يقتصر استخدامها على أغراض تحديد الهوية.

(٢) يجوز للشخص القانوني أن يحدد هوية رسالة بيانات بأن يبصم على تلك الرسالة بمفتاح الترميز الخاص المعتمد لذلك الشخص القانوني. ولا ينظر الى الشخص القانوني إلا على أنه [منشئ] [وافق على إرسال] الرسالة، إذا كانت الرسالة موقعة رقميا أيضا من جانب شخص طبيعي مرخص له بالتصرف نيابة عن ذلك الشخص القانوني."

ملاحظات

٦٢ - يقصد بالحكم الوارد أعلاه توضيح الظروف التي يجوز فيها استخدام التوقيعات الرقمية لإلزام أشخاص قانونيين. وهو يعتمد على تمييز بين وظيفتين يؤديهما التوقيع بموجب المادة ٧ (١) (أ) من القانون النموذجي، ألا وهما تعيين هوية مؤلف رسالة بيانات والتدليل على موافقة الشخص على المعلومات الواردة في رسالة البيانات. ولئن كانت الوظيفتان يمكن عادة تأديتهما باستخدام مفتاح وحيد معتمد لشخص طبيعي، فإن المفاتيح العامة المعتمدة لأشخاص قانونيين ستستخدم لمجرد توفير تأمين فيما يتعلق بهوية الشخص القانونية بوصفه مرسل الرسالة. وعلى ذلك فإن "التوقيع الرقمي" للشخص القانوني لن يكون له إلا تأثير محدود. وأي موافقة على الرسالة سوف تتطلب فضلا عن "التوقيع الرقمي" (أي تعيين الهوية) للشخص القانوني، التوقيع الرقمي لشخص طبيعي، الذي سيعين هوية ذلك الشخص ويدلل في الوقت نفسه، بالنيابة عن الشخص القانوني، على نية الموافقة على محتوى الرسالة.

٦٣ - وفي حين أن مشروع الحكم يتضمن إشارة الى "شخص طبيعي مرخص له بالتصرف نيابة عن" شخص قانوني، فليس المقصود هو الحلول محل قانون الوكالة المحلي. وعلى ذلك فإن السؤال عما إذا كان الشخص الطبيعي يمتلك في الواقع وفي القانون سلطة التصرف نيابة عن الشخص القانوني متروك أمر الإجابة عنه للقواعد القانونية الملائمة خارج القواعد الموحدة.

٣ - إسناد الرسائل التي تحمل توقيعا رقميا

٦٤ - "مشروع المادة هاء

(١) إن منشئ رسالة بيانات بصمت بالتوقيع الرقمي للمنشئ ملزم بمحتوى الرسالة بنفس طريقة التزامه لو أن الرسالة كانت موجودة في شكل موقع [يدويا] وفقا للقانون المنطبق على محتوى الرسالة.

(٢) يخول الشخص المرسل إليه رسالة بيانات بصمت بتوقيع رقمي حق اعتبار أن رسالة البيانات هي رسالة المنشئ، والتصرف على أساس هذا الافتراض إذا:

(أ) طبّق المرسل إليه، بهدف التحقق مما إذا كانت رسالة البيانات هي رسالة المنشئ، تطبيقا سليما، المفتاح العام العائد الى المنشئ على رسالة البيانات كما تلقاها، وأسفر تطبيق المفتاح العام العائد الى المنشئ: عن أن رسالة البيانات المتلقاة كانت قد رمّزت، بواسطة مفتاح الترميز الخاص العائد الى المنشئ؛ وأن الرسالة الأولية لم تُغيَّر بعد ترميزها باستخدام مفتاح الترميز العام العائد الى المنشئ؛

أو

(ب) كانت رسالة البيانات كما تلقاها المرسل إليه قد جاءت نتيجة لأفعال شخص مكنته علاقته بالمنشئ أو بأي وكيل المنشئ من الوصول الى مفتاح الترميز الخاص العائد الى المنشئ.

(٣) لا تنطبق الفقرة (٢):

(أ) منذ الوقت الذي عرف فيه المرسل إليه أو كان عليه أن يعرف إذا التمس المعلومات من سلطة التصديق المعتمدة أو بذل العناية المعقولة على نحو آخر، أن صلاحية مفتاح الترميز العام العائد الى المنشئ قد انتهت، أو أن الشهادة الصادرة عن سلطة التصديق قد ألغيت أو علقت؛

أو

(ب) في حالة تندرج في إطار الفقرة (٢) (ب)، في أي وقت عرف فيه المرسل إليه أو كان عليه أن يعرف إذا بذل العناية المعقولة أو استخدم أي إجراء متفق عليه، أن رسالة البيانات ليست رسالة المنشئ".

ملاحظات

٦٥ - قد يرغب الفريق العامل في مناقشة ما إذا كان إسناد الرسائل الموقعة رقميا يمكن تناوله بمجرد الإحالة الى المادة ١٣ من القانون النموذجي. والمقصود من مشروع المادة هاء، الذي صيغ على غرار المادة ١٣ من القانون النموذجي، تقديم مثال للمبادئ المنصوص عليها في المادة ١٣ في سياق التوقيعات الرقمية. وهو مبني على ضرورة توفير اليقين فيما يتعلق بالأثر القانوني للتوقيعات الرقمية التي تعتبر في الوقت الراهن إجراء للتوثيق يتسم بدرجة عالية من الأمان. ويلقي مشروع الحكم عبئا ثقيلا على عاتق منشئ الرسالة التي تحمل التوقيع الرقمي لذلك المنشئ. وجدير بالذكر أنه بموجب المادة ٢ (ج) من القانون النموذجي، تعني كلمة "منشئ" أي شخص يُعتبر أن إرسال رسالة البيانات قد تم على يديه أو نيابة عنه. ويوضح مشروع الحكم ضرورة أن يتولى أي مستعمل لتوقيع رقمي حماية مفتاحها الخاص الذي إذا استخدم لترميز رسالة فسينشئ قرينة قاطعة بأن الرسالة هي رسالة المنشئ المعني.

٤ – إلغاء الشهادات

٦٦ – "مشروع المادة واو

(١) يجوز لحامل زوج من المفاتيح المعتمدة أن يلغي الشهادة المناظرة لهما. ويصبح الإلغاء نافذاً منذ الوقت الذي [يسجل فيه لدى] [تتسلمه فيه] سلطة التصديق.

(٢) يكون حامل زوج من المفاتيح المعتمدة ملزماً بإلغاء الشهادة المناظرة لهما حين يعلم أن مفتاح الترميز الخاص قد فقد أو لحق به عيب أو تجري إساءة استخدامه من نواح أخرى. وإذا قصر حامل زوج المفاتيح في إلغاء الشهادة في موقف كهذا، كان مسؤولا عن أي خسارة تلحق بأطراف ثالثة اعتمدت على محتوى رسائل معينة نتيجة لتقصيره في الاضطلاع بهذا الإلغاء."

ملاحظات

٦٧ – قد يرغب الفريق العامل في أن يحيط علما بأنه إذا نُصَّ في القواعد الموحدة بشأن التوقيعات الرقمية على أن إلغاء الشهادة يصبح نافذا في الوقت الذي تتسلمه فيه سلطة التصديق، فمن الممكن حذف الفقرة (٤) من مشروع المادة حاء (المسؤولية) نظرا لأنه لن يكون هناك أساس لمسؤولية سلطة التصديق عن خطأ أو إهمال في تسجيل الإلغاء.

٥ – سجل الشهادات

٦٨ – "مشروع المادة زاي

(١) تحتفظ سلطة التصديق المعتمدة بسجل إلكتروني بما صدر من شهادات تتاح للجمهور إمكانية الوصول إليه، ويبين الوقت الذي تصدر فيه كل شهادة ووقت انتهائها أو تعليقها أو إلغائها.

(٢) تحتفظ سلطة التصديق بالسجل لفترة لا تقل عن [عشر] سنوات اعتباراً من تاريخ إلغاء أي شهادة أصدرتها سلطة التصديق هذه أو من تاريخ انتهاء مدتها التشغيلية".

ملاحظات

٦٩ – قد يرغب الفريق العامل في أن يناقش ما إذا كان سجل الشهادات ينبغي أن تتاح للجمهور إمكانية الوصول إليه أو كان من الممكن قصر إمكانية الوصول الى السجل على الأطراف المعنية. وفيما يتعلق بالوقت الذي ينبغي طواله الاحتفاظ بهذا السجل، قد يرغب الفريق العامل في أن يناقش ما إذا كان ينبغي النص في القواعد الموحدة على أي فترة محددة من الزمن أو ترك أمر البت في طول الفترة لتقدير الدولة المشترعة، أو كان ينبغي محاولة النص على معيار أشد مرونة، كأن يُذكر مثلا أن السجل ينبغي أن تظل إمكانية الوصول إليه متاحة التثبت من صحة الشهادات أثناء الفترة التشغيلية لكل شهادة والى أن تنتهي الفترة الزمنية التي تستخدم أثناءها الرسائل الموقعة رقمياً بموجب شهادات سلطة التصديق أو تنشأ أثناءها الحاجة الى التثبت من صحة تلك الرسائل، الأمر الذي قد يقتضي النص على عدة فترات زمنية تبعا للقوانين السارية بشأن فترة التقادم والحق المكتسب بالتقادم.

٦ – المسؤولية

٧٠ – "مشروع المادة حاء

(١) تكون سلطة التصديق المعتمدة مسؤولة أمام أي شخص تصرف بحسن نية معتمداً على شهادة أصدرتها سلطة التصديق، عن أي خسارة ناجمة عن أي عيوب في التسجيل الذي أجرته سلطة التصديق أو عن تعطل تقني

أو عن ظروف مماثلة [حتى إذا لم تكن الخسارة ناجمة عن] [إذا كانت الخسارة ناجمة عن] إهمال من جانب سلطة التصديق.

(٢) البديل ر لا تتجاوز المسؤولية عن أي خسارة فردية [المبلغ]. ويجوز لـ ... [تحدد الدولة المشترعة الجهاز المختص أو السلطة المختصة بمراجعة المبلغ الأقصى] أن تحدد هذا المبلغ كل سنتين بحيث يعكس تطورات الأسعار.

البديل ص يجوز لـ ... [تحدد الدولة المشترعة الجهاز المختص أو السلطة المختصة بإصدار لوائح بشأن المسؤولية] أن تصدر لوائح بشأن مسؤولية سلطات التصديق.

(٣) عندما يكون الطرف الذي تكبد الخسارة قد أسهم في ذلك عن عمد أو عن إهمال يجوز تخفيض التعويض أو الامتناع عن منحه.

[(٤) حيث تكون سلطة تصديق معتمدة قد تلقت إشعاراً بإلغاء شهادة، تسجل السلطة هذا الإلغاء على الفور. وإذا قصرت السلطة في القيام بذلك، فإنها تكون مسؤولة عن أي خسارة يتكبدها المستعمل نتيجة لذلك.]

ملاحظات

٧١ - قد يرغب الفريق العامل في أن يناقش ما إذا كان ينبغي توسيع نطاق حكم بشأن المسؤولية لكي يشمل حالات غير حالات الإهمال من جانب سلطة التصديق. كما قد يرغب الفريق العامل في مناقشة ما إذا كان ينبغي - والى أي مدى - تطبيق مبدأ استقلال الأطراف لكي تتاح لسلطات التصديق إمكانية التحكم - بموجب اتفاق خاص مع المستعملين - في المدى الذي ينبغي أن تذهب إليه مسؤولياتها.

٧٢ - وقد يرغب الفريق العامل في أن ينظر في إدراج حكم وقائي على النحو التالي:

"لا تكون سلطة التصديق التي تمتثل [لهذا القانون] [لهذه القواعد] ولأي قانون أو عقد منطبق آخر، مسؤولة عن أي خسارة

(١) يتكبدها حامل شهادة صادرة عن سلطة التصديق هذه نتيجة لاعتماد حامل الشهادة على تلك الشهادة، أو

(٢) تنجم عن اعتماد على شهادة صادرة عن سلطة التصديق هذه، أو على توقيع رقمي يمكن التثبت من صحته بالرجوع الى مفتاح عام مدرج بشهادة صادرة عن سلطة التصديق هذه، أو على معلومات واردة في مثل هذه الشهادة".

٧ - المسائل المتعلقة بالتصديق المتبادل عبر الحدود

٧٣ - "مشروع المادة طاء

(١) الشهادات التي تصدرها سلطات تصديق أجنبية يجوز استخدامها في توقيعات رقمية بنفس الشروط المنطبقة على التوقيعات الرقمية الخاضعة لـ [هذا القانون] [هذه القواعد] إذا كانت معترفا بها من جانب سلطة تصديق معتمدة وضمنت سلطة التصديق المعتمدة - الى نفس المدى الذي تضمن إليه شهاداتها - صواب التفاصيل الواردة في الشهادة وكذلك صحة الشهادة وسريانها.

(٢) يرخص لـ ... [تحدد الدولة المشترعة الجهاز المختص أو السلطة المختصة بإقرار قواعد بشأن الموافقة على الشهادات الأجنبية] بالموافقة على الشهادات الأجنبية وبإقرار قواعد محددة بشأن تلك الموافقة".

ملاحظات

٧٤ - ينبغي مشروع المادة طاء على مفهوم مؤداه أن الاعتراف بالشهادات الأجنبية ينبغي أن يُنص عليه تحت مسؤولية سلطة تصديق محلية على أساس المعاملة بالمثل. وقد يرغب الفريق العامل، عند مناقشة المسائل المتعلقة بالتصديق المتبادل عبر الحدود، أن ينظر فيما إذا كان ينبغي اشتراط تطبيق كامل لمبدأ المعاملة بالمثل، أم أن ضمانات صواب وصحة الشهادات الأجنبية يمكن أن لا تقدم بالضرورة على نفس المستوى من جانب جميع السلطات التي ستشكل جزءاً من مخطط تصديق متبادل عبر الحدود. وقد يرغب الفريق العامل أيضا في النظر فيما إذا كان التدخل الحكومي ينبغي بالضرورة أن يكون مطلوبا للاعتراف بالشهادات الأجنبية.

٧٥ - وقد يرغب الفريق العامل في أن ينظر، على سبيل إيجاد بديل لمشروع المادة طاء، في نهج اتبع في إعداد مشاريع القوانين في بلدان معينة ويقضي بأن الاعتراف بالشهادات الأجنبية لا ينبغي توفيره إلا على أساس اتفاقات دولية، ثنائية أو متعددة الأطراف.

٨ - العلاقات بين مستعملي التوقيعات الرقمية وسلطات التصديق

٧٦ - "مشروع المادة ياء

(١) لا يسمح لسلطة التصديق أن تطالب من المعلومات إلا ما يكون ضروريا لتحديد هوية المستعمل.

(٢) تقدم سلطة التصديق معلومات عما يلي عندما يطالب تلك المعلومات أشخاص قانونيون أو طبيعيون:

(أ) الشروط التي يمكن بها استخدام الشهادة؛

(ب) الشروط المقترنة باستخدام التوقيعات الرقمية؛

(ج) تكاليف الاستعانة بخدمات سلطة التصديق؛

(د) سياسة أو ممارسات سلطة التصديق فيما يتعلق باستخدام المعلومات الشخصية وخزنها وإبلاغها؛

(هـ) المتطلبات التقنية لسلطة التصديق فيما يتعلق بأجهزة الاتصال التي يستخدمها المستعمل؛

(و) الظروف التي توجه فيها سلطة التصديق تحذيرات الى المستعملين في حالة نشوء عيوب أو أخطاء في تشغيل أجهزة الاتصال؛

(ز) أي حدود لمسؤولية سلطة التصديق؛

(ح) أي قيود تفرضها سلطة التصديق على استخدام الشهادة؛

(ط) الظروف التي يكون للمستعمل فيها حق فرض قيود على استخدام الشهادة.

(٣) تقدم المعلومات المدرجة بالفقرة (١) أعلاه الى المستعمل قبل إبرام اتفاق نهائي بشأن التصديق [يجوز لسلطة التصديق أن تقدم تلك المعلومات في شكل بيان بشأن ممارسة التصديق].

(٣) يجوز للمستعمل، رهنا بإعطاء مهلة [شهر واحد] أن ينهي اتفاق الوصل بسلطة التصديق. وتبدأ مهلة الإنهاء هذه عندما تتلقى سلطة التصديق إشعاراً بها.

(٤) يجوز لسلطة التصديق، رهنا بإعطاء مهلة [ثلاثة أشهر] أن تنهي اتفاق الوصل بسلطة التصديق. وتبدأ مهلة الإنهاء هذه عند تلقي الإشعار بها.

ثالثا – الإدراج بالإشارة

ألف – المناقشات السابقة

٧٧ – أثناء الدورة الثامنة والعشرين للفريق العامل، قدم اقترلح بأن يدرج في مشروع القانون النموذجي بشأن الجوانب القانونية للتبادل الإلكتروني للبيانات وما يتصل به من وسائل الإبلاغ حكم يقضي بالاعتراف لإدرلج أحكام وشروط معينة في سجل بيانات بمجرد الإشارة إليها في ذلك السجل بنفس درجة الفعالية القانونية التي تكون لها لو أنها اقتبست بالكامل في نص سجل البيانات. وذكر أن مسألة إدراج أحكام معينة في رسائل التبادل الإلكتروني للبيانات يتسم بأهمية حاسمة بالنسبة للمنتفعين بهذا التبادل وأن ثمة حاجة ملحة الى اليقين عند اللجوء الى هذا الأسلوب. وقيل إن ثمة من الحجج ما يثبت أن التبادل الإلكتروني للبيانات إنما هو في ذاته نظام للإدراج بالإشارة بالنظر الى أن رسائله لا يكون لها معنى ولا قيمة تعاقدية تذكر دون أن تدرج بالإشارة معايير الإبلاغ ذات الصلة. وتقرر أن يتناول الفريق العامل، في إحدى دوراته المقبلة مسألة إدراج الأحكام والشروط في رسالة بيانات بمجرد الإشارة الى تلك الأحكام والشروط (A/CN.9/406، الفقرتان ٩٠ و ١٧٨).

٧٨ – وكان معروضا على الفريق العامل في دورته التاسعة والعشرين اقتراحان بمشروع حكم بشأن الإدراج بالإشارة، قدم أحدهما المراقب عن الغرفة التجارية الدولية (A/CN.9/WG.IV/WP.65)، وقدمت الآخر المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية (A/CN.9/WG.IV/WP.66). وتمثل الرأي السائد في أن المسألة لم تكن بالنضج الكافي لإدراجها في القانون النموذجي وأنها بحاجة الى المزيد من الدراسة. وذكر أن كلا الاقتراحين المقدمين الى الفريق العامل بحاجة الى التوضيح بصدد عدد من المسائل التي يذكر منها أي الأحكام تدرج وفي أي ظروف. وذكر فضلا عن ذلك أن الاقتراحين قد يؤخذا على أنهما تدخل في الأحكام العامة لقانون العقود. كما ذكر أن الإدراج بالإشارة في بيئة إلكترونية ليس بحاجة الى أن يعالج في القانون النموذجي نظرا لأنه، في جوهره، يثير نفس المسائل التي يثيرها الإدراج بالإشارة في بيئة ورقية، وهي مسائل يتناولها قانون العقود العام. وقيل أخيراً إن حكما يفرّق بين الإدراج بالإشارة في بيئة ورقية والإدراج بالإشارة في بيئة التبادل الإلكتروني للبيانات سوف يتعارض مع النهج الذي اتبعه الفريق العامل حتى الآن والذي يستهدف كفالة "حياد الوسائل". وذكر رداً على ذلك أن الممارسين لديهم إدراك بأن مسألة الإدراج بالإشارة أشد تعقيداً في بيئة إلكترونية منه في بيئة ورقية بالنظر مثلاً الى أن عدد البلاغات المرسلة في الأولى أكبر وأن الأحكام التي تدرج فيها بالإشارة ربما كان التثبت من صحتها أشد صعوبة عندما تكون في شكل رسالة بيانات. كما أن لدى الممارسين حاجة مدركة الى أحكام محددة بشأن الإدراج بالإشارة في سياق الاتصالات الإلكترونية. وأثيرت نقطة أخرى مؤداها أنه بالنظر الى عدد رسائل البيانات المتبادلة إلكترونيا في إطار علاقة تعاقدية معينة، يرجح كثيراً أن تنشأ في سياق الاتصالات الإلكترونية المشكلة المعروفة باسم "معركة الاستمارات". واتفق الفريق العامل على أن مسألة الإدراج بالإشارة ربما احتاجت الى مزيد من الدراسة في سياق الأعمال المقبلة (A/CN.9/407، الفقرات ١٠٠ – ١٠٥ و ١١٧).

٧٩ – وفي دورته الثلاثين، اتفق الفريق العامل عموماً، على أن ثمة حاجة الى العمل في مجال الإدراج بالإشارة. وأعرب عن رأي مؤداه أنه في أي محاولة لإقرار معايير قانونية لأحكام تتعلق بالإدراج بالإشارة في رسائل البيانات، ينبغي الوفاء بالشروط الثلاثة التالية: (١) ينبغي إيراد بند الإشارة في رسالة البيانات؛ (٢) يتعين أن يكون المستند المشار إليه، كالأحكام والشروط العامة مثلا، معروفا بالفعل لدى الطرف الذي قد يرتكز عليه ضده؛ (٣) يتعين أن يكون المستند المشار إليه، فضلا عن كونه معروفاً، مقبولا من ذلك الطرف. واتفق عموماً على أن من المناسب تناول موضوع الإدراج بالإشارة في سياق العمل الأعم المتعلق بمسائل هيئات التسجيل ومقدمي الخدمات (A/CN.9/421، الفقرة ١١٤). وكان الفريق العامل قد اتفق عموماً في دورته التاسعة والعشرين على أنه يمكن تناول المسألة في سياق العمل بشأن سلطات التصديق (A/51/17، الفقرة ٢٢٢).

باء – الحاجة المحتملة الى قواعد موحدة بشأن الإدراج بالإشارة

٨٠ – الإدراج بالإشارة وسيلة مختصرة للإشارة عموماً في وثيقة ما الى أحكام ترد تفصيلا في وثيقة أخرى بدلا من إيراد النص الكامل لهذه الأحكام. من ذلك مثلا أنها تجعل من غير الضروري إيراد نصوص مطولة لشروط موحدة عند التفاوض

بشأن عقود أو عند إبرامها. وهكذا يمكن أن تدرج الشروط في الوثيقة أو رسالة البيانات التي تشير إليها باللجوء الى وسيلة لتحديد هوية هذه الشروط تحديداً كافياً وبيان نية شمولها. وفي بيئة إلكترونية يمكن تعريف الإدراج بالإشارة بأنه طريقة لجعل رسالة بيانات واحدة أو سجل بيانات واحد (أو جزء من المعلومات الواردة فيها) يصبح جزءاً من رسالة بيانات أخرى منفصلة أو سجل بيانات آخر منفصل بالإشارة الى الأولى في الثانية، والإعلان بأن الأولى ستؤخذ وتعتبر جزءاً من الثانية كما لو كانت مقتبسة فيها بالكامل.

١ – القواعد التقليدية التي أعدت بصدد بيئة ورقية

(أ) الإدراج بالإشارة

٨١ – إن المسائل القانونية التي يثيرها الإدراج بالإشارة معروفة في سياق الاتصالات الورقية، وتوجد في كثير من النظم القانونية قواعد قانونية تقر الشروط القانونية التي يمكن بمقتضاها اعتبار معلومات غير واردة بالكامل في وثيقة مكتوبة وكأنها جزء من تلك الوثيقة. من ذلك مثلا أنه في ظروف معينة، يمكن إيراد إشارة الى شرط أو أكثر من شروط التجارة الدولية (إنكوتيرمز) مثل "النقل مدفوع الى" (CPT) أو "النقل والتأمين مدفوعان الى" (CIP) في أمر شراء أو في فاتورة، مما يترتب عليه أن هذا الشرط من شروط التجارة الدولية سيعد واحداً من شروط عقد البيع المناظر دون إيراد تعريف كامل للـ CPT أو الـ CIP في أي من الوثائق التعاقدية. ومن العوامل التي قد تيسر الإدراج بالإشارة أن الغرفة التجارية الدولية هي التي أعدت هذه الشروط بهدف محدد هو إيراد ذكرها في العقود باستخدام مختصراتها، وهي مختصرات معروفة ويوصي باستخدامها كل من الغرفة التجارية الدولية والأونسيترال. ومن الأمثلة الأخرى لنص كثيراً ما يدرج بالإشارة "الأعراف والممارسات الموحدة للاعتمادات المستندية (UCP 500) التي أعدتها غرفة التجارة الدولية. وكثيراً ما يكون المنطق القانوني المتبع للسماح بإدراج نص مثل الـ UCP 500 بالإشارة في عقدٍ ما مبنياً على الاعتراف بأن نصا كهذا يسجل ممارسات معروفة ومقبولة عبر العالم ويفترض أنه معروف لجميع الأطراف المعنية.

٨٢ – وحيث لا ينطبق مثل هذا الافتراض، فإن الشروط التي يحددها القانون الوطني لاعتماد الإدراج بالإشارة قد تنطوي على متطلبات صارمة، كمعرفة جميع الأطراف للمعلومات المدرجة بالإشارة معرفة فعلية، أو حتى الموافقة الصريحة على هذه المعلومات من جانب الطرف المزمع إنفاذ الشرط المدرج بالإشارة ضده. ومن جهة أخرى، فبموجب قوانين وطنية معينة تكون متطلبات اعتماد الإدراج بالإشارة أكثر تساهلا. من ذلك مثلا أن اختبارات قانونية تقليدية معينة للإدراج بالإشارة قد تركز على وضوح البند الذي يتم به الإدراج بالإشارة وعلى إمكانية الوصول الى المعلومات المدرجة بالإشارة.

(ب) "معركة الاستمارات"

٨٣ – ينبغي أن لا يكون هناك خلط بين مسألة الإدراج بالإشارة والمسألة التي تعرف عموماً بـ "معركة الاستمارات". وقد تنشأ "معركة الاستمارات" مثلا حيث تذكر الأحكام والشروط العامة للتعاقد التي يقترحها المشتري بحروف طباعة صغيرة على ظهر أمر الشراء، في حين تذكر مجموعة مختلفة من الأحكام والشروط العامة للتعاقد على ظهر الفاتورة التي يصدرها البائع. وحيث لا يكون قد أبرم بين المشتري والبائع اتفاق محدد على أي الأحكام والشروط ستنطبق على عقد معين، وتكون مجموعتان متعارضتان من الأحكام والشروط قد أبلغهما الطرفان كل على ظهر مستنداته التعاقدية، قد تنشأ حاجة الى البت فيما هناك من شك في أي الأحكام والشروط ستنظم المعاملة. وفي كثير من البلدان ضُمِّن قانون التعاقد قواعد قانونية يقصد بها توضيح هذا اللبس.

٢ - المسائل التي تثار بصدد بيئة التجارة الإلكترونية

(أ) الاستخدام الواسع النطاق الإدراج بالإشارة

٨٤ - يعد الإدراج بالإشارة أحد العناصر الأساسية في الاستخدام الواسع النطاق للتبادل الإلكتروني للبيانات، والبريد الإلكتروني، والشهادات الرقمية وغير ذلك من أشكال التجارة الإلكترونية. من ذلك مثلا أن التخاطب عن طريق الرسائل الموحدة للتبادل الإلكتروني البيانات، والاتصالات الإلكترونية عموما، تبنى على نحو يتسنى معه تبادل أعداد كبيرة من الرسائل التي تحتوي كل منها على معلومات مختصرة وتعتمد أكثر كثيراً من اعتماد الوثائق الورقية على الإشارة الى معلومات متاحة في وثائق أخرى. فرسائل البيانات المتبادلة إلكترونيا وغيرها من أشكال البيانات الموحدة ومحكمة التصميم تلجأ كلها الى الاستخدام الواسع النطاق للإدراج بالإشارة بغية تعزيز كفاءة تجهيز البيانات. وقد ذكر في دورة سابقة من دورات الفريق العامل أن التبادل الإلكتروني للبيانات وأشكالاً شتى من التجارة الإلكترونية إنما هي في الأساس نظم الإدراج بالإشارة. ومن الاعتبارات العملية أن رسائل التبادل الإلكتروني للبيانات تكون احتمالا أقل وثوقا من الناحية القانونية إذا لم يكفل الوضوح لصحة وفعالية الإدراج بالإشارة لما قد ينطبق على تلك الرسائل من أحكام وشروط وبنود واتفاقات ومعايير وقواعد وخطوط توجيهية، قانونية وتقنية وإدارية.

٨٥ - وفيما يتعلق بالمواقف التي قد تنشأ فيها "معارك استمارات" في بيئة ورقية، ينبغي أن لا يعزب عن البال أن التبادل الإلكتروني للرسائل لا يقصد به - بل ولا هو مجهّز - لأن ينقل مع كل رسالة نصوصا مثل الأحكام والشروط العامة التي تطبع - نموذجيا - على ظهر المستندات الورقية. وتضمين جميع الأحكام والشروط من شأنه أن يكون مكلفا ومعدوم الكفاءة. فهو يبطئ الاتصال الإلكتروني وربما يوقفه بل وقد ينال من فعالية الإشعار إذ قد يجبر الأطراف المعتمدة عليه على طباعة أو استخراج نصوص بهذا الطول. ومن ثم ضرورة وضع قواعد بشأن الكيفية التي يمكن بها اعتبار نصوص كهذه وكأنها مدرجة برسالة. وينبغي أن يكون القصد من هذه القواعد، إن أمكن، الحد في بيئة إلكترونية من الصعوبات التي تنجم - في بيئة ورقية - عن معركة استمارات، أو على الأقل ضمان أن تكون الحلول المعدة في إطار كثير من القوانين الوطنية لتذليل هذه الصعاب في بيئة ورقية، متاحة أيضا في بيئة إلكترونية. ومن الجدير بالملاحظة أن وضع مثل هذه القواعد لن يترتب عليه بالضرورة تغيير الحلول التي يمكن أن تستمد من القانون الوطني فيما يتعلق بكيفية حسم المواقف المنطوية على "معارك استمارات".

٨٦ - وربما كانت معايير إدراج رسائل بيانات بالإشارة في رسائل بيانات أخرى أمراً جوهريا أيضا بالنسبة لاستخدام شهادات المفاتيح العامة نظراً لأن هذه الشهادات تكون عموماً سجلات مختصرة تضم محتويات مصممة بدقة شديدة ومتناهية الحجم. ومن جهة أخرى فإن الطرف الثالث المؤتمن، الذي يصدر الشهادة، يرجح أن يطالب بإدراج الشروط اللازمة لتحديد مسؤوليته. وعلى ذلك فإن نطاق الشهادة والغرض منها وتأثيرها في الممارسات التجارية ستكون غامضة وغير مؤكدة إذا لم تدرج بالإشارة شروط خارجة عنها. وتلك هي الحال، بنوع خاص في سياق الاتصالات الدولية التي تشترك فيها أطراف شتى تتبع ممارسات وأعرافا تجارية متباينة.

٨٧ - وذكر مراراً في دورات سابقة للفريق العامل أن وضع معايير لإدراج رسائل بيانات بالإشارة في رسائل بيانات أخرى يعد أمراً حاسماً بالنسبة لنمو هياكل أساسية تجارية قائمة على الحواسيب. وما لم يتوافر اليقين القانوني الذي تدعمه مثل هذه المعايير، ستصبح المعاملات التجارية الحاسوبية مثقلة بتضمين مقادير كبيرة من المواد تجعلها عصية المأخذ بالنسبة للأطراف المعنية والنظام الذي ييسر تنفيذ المعاملة. وبدون هذه المعايير الموحدة قد تكون هناك مخاطرة هامة بأن تطبيق المقاييس للبت في إنفاذية الشروط التي يُسعى الى إدراجها بالإشارة ربما تكون غير مجدية عندما تطبق على الشروط المناظرة في التجارة الدولية بسبب الفروق بين آليات التجارة التقليدية وآليات التجارة الإلكترونية. من ذلك مثلاً أن بعض الاختبارات القانونية التقليدية للإدراج بالإشارة تسأل عما إذا كانت الأحكام المدرجة "واضحة جلية"، أو عما إذا كانت تحتوي على "عبارات إشارة مناسبة تثبت نية صريحة على الإدراج"، أو عما إذا كان الإدراج المقصود "واضحاً ومقنعاً". وقد تقيم اختبارات كهذه حواجز في وجه تيسير التجارة الإلكترونية. وقد تدعو الحاجة الى وضع قواعد محددة نظراً لأن الأساليب

المتبعة في الإشعار وفي التحقق من إمكانية الوصول الى المعلومات قد تختلف في البيئة الإلكترونية عنها في البيئة الورقية، مما قد يترتب عليه في بعض الولايات القضائية، أن تفضي القواعد التقليدية للإدراج بالإشارة الى تمييز لا مبرر له ضد التجارة الإلكترونية.

(ب) إمكانية الوصول الى النص المدرج بالإشارة

٨٨ - تعتمد التجارة الإلكترونية اعتماداً كبيراً على آلية الإدراج بالإشارة. غير أنه يمكن في الوقت نفسه، بفضل استخدام الاتصالات الإلكترونية، إدخال تحسينات كبيرة على إمكانية الوصول الى النص الكامل المعلومات المدرجة بالإشارة. فإذا أخذنا مثلا رسالة أدمجت بها محدّدات موحدة لمواضع الموارد (URL) لتوجيه القارئ الى الوثيقة المشار إليها، فإن هذه المحددات يمكن أن توفر وصلات فائقة بالنصوص تتيح للقارئ توجيه أداة باحثة (كقارئ الحاسوب مثلا) نحو كلمة مرشدة ذات صلة بتلك المحددات مما يؤدي الى ظهور النص.

٨٩ - ويمكن استخدام نفس الطرق في بيئة إلكترونية لضمان وصول جميع المستعملين الى طائفة متنوعة من النصوص مثل: (١) نصوص تضم الممارسات التجارية الراسخة (الممارسات والأعراف الموحدة الاعتمادات المستندية UCP 500 مثلا)؛ (٢) المعايير التقنية التي تنظم الاتصال؛ (٣) بيانات تصدرها سلطات التصديق بشأن ممارسات التصديق؛ (٤) معلومات أكثر تحديداً يذكر منها مثلا الأحكام والشروط التعاقدية العامة التي تطبقها شركة معينة. غير أن الأثر القانوني لهذه الطرق لا يمكن التعويل عليه بثقة بدون وجود معايير إدراج رسائل بيانات بالإشارة إليها في رسائل بيانات أخرى.

٩٠ - وتنشأ الحاجة الى وضع قواعد بشأن الإدراج بالإشارة في بيئة إلكترونية من أمرين أولهما كثرة إشارة رسائل البيانات الى معلومات مدونة في مواضع أخرى، والثاني توافر الوسائل التقنية التي تجعل التثبت من صحة تلك المعلومات أيسر وأسرع منه في بيئة ورقية.

جيم - أحكام ممكنة

٩١ - عند القيام بصياغة أحكام ممكنة بشأن الإدراج بالإشارة في التجارة الإلكترونية، قد يرغب الفريق العامل في أن يضع في اعتباره أنه في بعض الولايات القضائية، صيغت القواعد الحالية التي وضعت للاستخدام في بيئة ورقية، بدافع الحرص على أن يسترعى انتباه المرسل إليه أو طرف ثالث حسبما يكون الحال، الى الأحكام وغيرها من المعلومات المدرجة بالإشارة. وحيثما وجدت قواعد قانونية من هذا القبيل، فربما كان من المناسب تطبيقها بصرف النظر عما إذا كان الإدراج بالإشارة يتم بوسائل التبادل الإلكتروني البيانات أو بوسائل اتصال أخرى.

٩٢ - ومع ذلك قد يبدو من الممكن صوغ مبدأ عام يوضّح أن الإدراج بالإشارة يكون مجديا في التجارة الإلكترونية شريطة أن يوضّح في الوقت نفسه أن هذا المبدأ لا ينال، من أي قواعد قد تكون سارية فيما يتعلق: (١) بضرورة استرعاء انتباه أي طرف يراد أن تنطبق عليه أحكام أو معلومات أخرى، الى محتوى أو موضع تلك الأحكام أو المعلومات أو ضرورة توفيرها لذلك الطرف؛ أو (٢) بأي شرط قانوني ينص على أن الأحكام ينبغي أن تقبَل قبل أن تشكل جزءاً من عقد. والمبدأ الأساسي هو أن استخدام الإدراج بالإشارة ينبغي أن يكون معترفاً به لكي لا يكون عدم وجود معلومات معينة إلا في موضع آخر في حد ذاته سبباً لمنع إدراج تلك المعلومات في رسالة بيانات بالإشارة إليها في تلك الرسالة.

٩٣ - وقد يرغب الفريق العامل في استئناف نظره في المسائل المتعلقة بالإدراج بالإشارة انطلاقاً من البديلين التاليين:

البديل ألف

ما لم يتفق على غير ذلك، عندما تكون أحكام أو شروط أو بنود أو اتفاقات أو معايير أو قواعد أو خطوط توجيهية - يسيرة المنال [بما يكفي] [بدرجة معقولة]، مشاراً إليها بالكامل أو جزئياً في رسالة بيانات بنيّة [بادية] لإدراجها كجزء من محتوى الرسالة أو على سبيل جعلها ملزمة قانونياً على نحو آخر، يفترض أن هذه الأحكام قد أدرجت بالإشارة في

رسالة البيانات تلك. وفيما بين الأطراف، تكون لتلك الأحكام نفس التأثير القانوني والإلزام القانوني اللذين يكونان لها لو أنها اقتبست بالكامل في رسالة البيانات، وذلك الى المدى الذي يسمح به القانون.

البديل باء

(١) تنطبق هذه المادة عندما تشير معلومات مدوّنة أو مبلّغة في رسالة بيانات الى معلومات، مدونة في موضع آخر ("المعلومات الإضافية")، أو عندما لا يمكن التحقق من الأولى بالكامل إلا بالإشارة الى الثانية.

(٢) رهنا بالفقرة (٤)، يكون لرسالة البيانات نفس التأثير الذي يكون لها لو أن المعلومات الإضافية اقتبست بالكامل في رسالة البيانات، ولا يمكن التحقق من رسالة البيانات إلا بالإشارة إلى المعلومات الإضافية، إذا كانت رسالة البيانات:

(أ) تعرّف المعلومات الإضافية:

'١' باسم جامع أو بوصف؛ و

'٢' بتعيين هوية السجل وأجزاء ذلك السجل المحتوية على المعلومات الإضافية؛ والمكان الذي يمكن العثور فيه على السجل إذا لم يكن متاحاً للجمهور؛ و

(ب) تبيّن صراحة أو تحمل متضمنات واضحة على أن رسالة البيانات ينبغي أن يكون لها نفس التأثير الذي يكون لها لو أن المعلومات الإضافية قد اقتبست بالكامل في رسالة البيانات.

(٣) لا ينال أي شيء في هذه المادة من:

(أ) أي قاعدة قانونية تقضي بإعطاء إشعار كاف بمحتوى المعلومات المدونة في موضع آخر، أو بالسجل أو المكان الذي يمكن العثور فيه على تلك المعلومات، أو تقضي بأن يكون هذا السجل أو المكان بحيث يتمكن شخص آخر من الوصول إليه؛ أو

(ب) أي قاعدة قانونية تتعلق بقبول عرض لأغراض تكوين العقد.