Nations Unies A/CN.9/WG.IV/WP.88

Assemblée générale

Distr.: Limitée
30 janvier 2001

Français
Original: Anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail sur le commerce électronique
Trente-huitième session
New York, 12-23 mars 2001

Signatures électroniques

Projet de guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur les signatures électroniques

Note du Secrétariat

1. En application des décisions prises par la Commission à ses vingt-neuvième (1996)[1] et trentième (1997)[2] sessions, le Groupe de travail sur le commerce électronique a consacré ses trente et unième à trente-septième sessions à l'élaboration du projet de Loi type de la CNUDCI sur les signatures électroniques (appelé ci-après "la Loi type" "le projet de Loi type" ou "la nouvelle Loi type"). Les rapports sur les travaux de ces sessions ont été publiés sous les cotes A/CN.9/437, 446, 454, 457, 465, 467 et 483. Lors de l'élaboration de la Loi type, le Groupe de travail a noté qu'il serait utile de fournir, dans un commentaire, des informations complémentaires sur le texte. Une proposition tendant à ajouter à la Loi type un guide qui aiderait les États à incorporer cet instrument dans le droit interne et à l'appliquer, suivant ainsi la démarche adoptée pour la Loi type de la CNUDCI sur le commerce électronique, a été généralement appuyée. Le guide, qui pourrait être établi en grande partie à partir des travaux préparatoires de la Loi type, pourrait aussi être utile à d'autres utilisateurs du texte.

2. À sa trente-septième session, le Groupe de travail a achevé l'élaboration des projets d'articles de la Loi type et a examiné le texte du projet de guide pour son incorporation dans le droit interne en se fondant sur une note du secrétariat (A/CN.9/WG.IV/WP.86 et Add. 1). Le secrétariat a été prié d'établir une version révisée du projet de guide tenant compte des décisions prises par le Groupe de

travail et fondée sur les divers points de vue, suggestions et préoccupations exprimés à la trente-septième session. Faute de temps, le Groupe de travail n'a pu terminer ses délibérations sur ce texte (A/CN.9/483, par. 23 et 145 à 152). Il a été convenu de réserver un certain temps lors de sa trente-huitième session à la finalisation de ce travail. Il a été noté que le projet de Loi type ainsi que le projet de guide seraient présentés à la Commission pour examen et adoption à sa trente-quatrième session, qui se tiendra à Vienne du 25 juin au 13 juillet 2001.

3. L'annexe de la présente note contient une version révisée du projet de guide établi par le secrétariat.

Annexe

LOI TYPE
DE LA CNUDCI
SUR LES SIGNATURES ÉLECTRONIQUES

ET

GUIDE POUR SON INCORPORATION

2001

TABLE DES MATIÈRES

Première partie

LOI TYPE DE LA CNUDCI SUR LES SIGNATURES ÉLECTRONIQUES (2001)

(Texte approuvé par le Groupe de travail de la CNUDCI sur le commerce électronique à sa trente-septième session, tenue à Vienne du 18 au 29 septembre 2000)

Article premier. Champ d'application

La présente Loi s'applique lorsque des signatures électroniques sont utilisées dans le contexte* d'activités commerciales**. Elle ne se substitue à aucune règle de droit visant à protéger le consommateur.

* La Commission propose le texte suivant aux États qui souhaiteraient étendre l'applicabilité de la présente Loi:

"La présente Loi s'applique lorsque des signatures électroniques sont utilisées, sauf dans les situations suivantes: [...]."

** Le terme "commerciales" devrait être interprété au sens large, comme désignant toute relation d'ordre commercial qu'elle soit contractuelle ou non contractuelle. Les relations d'ordre commercial comprennent, sans s'y limiter, les transactions suivantes: fourniture ou échange de marchandises ou de services; accord de distribution; représentation commerciale; affacturage; crédit-bail; construction d'usines; services consultatifs; ingénierie; licence; investissement; financement; opération bancaire; assurance; accord d'exploitation ou concession; coentreprise et autres formes de coopération industrielle ou commerciale; transport de marchandises ou de voyageurs par voie aérienne ou maritime, par chemin de fer ou par route.

Article 2. Définitions

Aux fins de la présente Loi:

a) Le terme "signature électronique" désigne des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue;

b) Le terme "certificat" désigne un message de données ou un autre enregistrement confirmant le lien entre un signataire et des données afférentes à la création de signature;

c) Le terme "message de données" désigne l'information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie;

d) le terme "signataire" désigne une personne qui détient des données afférentes à la création de signature et qui agit soit pour son propre compte, soit pour celui de la personne qu'elle représente;

e) Le terme “prestataire de services de certification” désigne une personne qui émet des certificats et peut fournir d’autres services liés aux signatures électroniques;

f) Le terme “partie se fiant à la signature ou au certificat” désigne une personne qui peut agir sur la base d’un certificat ou d’une signature électronique.

Article 3. Égalité de traitement des techniques de signature

Aucune disposition de la présente Loi, à l’exception de l’article 5, n’est appliquée de manière à exclure, restreindre ou priver d’effets juridiques une quelconque méthode de création de signature électronique satisfaisant aux exigences mentionnées au paragraphe 1 de l’article 6 ou autrement satisfaisant aux exigences de la loi applicable.

Article 4. Interprétation

1. Pour l’interprétation de la présente Loi, il est tenu compte de son origine internationale et de la nécessité de promouvoir l’uniformité de son application et le respect de la bonne foi.

2. Les questions concernant les matières régies par la présente Loi qui ne sont pas expressément réglées par elle sont tranchées selon les principes généraux dont elle s’inspire.

Article 5. Dérogation conventionnelle

Il est possible de déroger aux dispositions de la présente Loi ou d’en modifier les effets par convention, à moins que cette convention soit invalide ou sans effets en vertu de la loi applicable.

Article 6. Satisfaction de l’exigence de signature

1. Lorsque la loi exige la signature d’une certaine personne, cette exigence est satisfaite dans le cas d’un message de données, s’il est fait usage d’une signature électronique dont la fiabilité est suffisante au regard de l’objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris toute convention en la matière.

2. Le paragraphe 1 s’applique, que l’exigence qui y est visée ait la forme d’une obligation ou que la loi prévoie simplement certaines conséquences en l’absence de signature.

3. Une signature électronique est considérée fiable en ce qu’elle satisfait à l’exigence indiquée au paragraphe 1 si:

a) les données afférentes à la création de signature sont, dans le contexte dans lequel elles sont utilisées, liées exclusivement au signataire;

b) les données afférentes à la création de signature étaient, au moment de la signature, sous le contrôle exclusif du signataire;

c) toute modification apportée à la signature électronique après le moment de la signature est décelable; et

d) dans le cas où l’exigence légale de signature a pour but de garantir l’intégrité de l’information à laquelle elle se rapporte, toute modification apportée à cette information après le moment de la signature est décelable.

4. Le paragraphe 3 ne restreint pas la possibilité pour toute personne:

a) d'établir de toute autre manière, aux fins de satisfaire l'exigence visée au paragraphe 1, la fiabilité de la signature électronique; ni

b) d'apporter des preuves de la non-fiabilité de la signature électronique.

5. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...]

Article 7. Satisfaction des dispositions de l'article 6

1. *[Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué par l'État adoptant comme compétent en la matière]* peut déterminer quelles signatures électroniques satisfont aux exigences de l'article 6.

2. Toute détermination arrêtée en vertu du paragraphe 1 doit être conforme aux normes internationales reconnues.

3. Aucune disposition du présent article n'a d'incidence sur le fonctionnement des règles du droit international privé.

Article 8. Normes de conduite du signataire

1. Lorsque des données afférentes à la création de signature peuvent être utilisées pour créer une signature ayant des effets juridiques, chaque signataire:

a) prend des dispositions raisonnables pour éviter toute utilisation non autorisée de ses données afférentes à la création de signature;

b) avise, sans retard injustifié, toute personne dont il peut raisonnablement penser qu'elle se fie à la signature électronique ou qu'elle fournit des services visant à étayer la signature électronique si:

i) il sait que les données afférentes à la création de signature ont été compromises; ou

ii) il estime, au regard des circonstances connues de lui, qu'il y a un risque important que les données afférentes à la création de signature aient été compromises;

c) prend, lorsqu'un certificat est utilisé pour étayer la signature électronique, des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou devant figurer dans le certificat sont exactes et complètes.

2. Un signataire est responsable de tout manquement aux exigences visées au paragraphe 1.

Article 9. Normes de conduite du prestataire de services de certification

1. Lorsqu'un prestataire de services de certification fournit des services visant à étayer une signature électronique qui peut être utilisée pour produire des effets juridiques en tant que signature, ce prestataire:

a) agit en conformité avec les déclarations qu'il fait concernant ses politiques et pratiques;

b) prend des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou figurant dans le certificat sont exactes et complètes;

c) fournit à toute partie se fiant au certificat des moyens raisonnablement accessibles de déterminer à partir de ce certificat:

i) l'identité du prestataire de services de certification;

ii) si le signataire identifié dans le certificat avait, au moment de l'émission de ce dernier, le contrôle des données afférentes à la création de signature;

iii) si les données afférentes à la création de signature étaient valides au moment ou avant le moment de l'émission du certificat;

d) fournit à toute partie se fiant au certificat des moyens raisonnablement accessibles de déterminer, s'il y a lieu, à partir de ce certificat ou de toute autre manière:

i) la méthode utilisée pour identifier le signataire;

ii) toute restriction quant aux fins ou à la valeur pour lesquelles les données afférentes à la création de signature ou le certificat peuvent être utilisés;

iii) si les données afférentes à la création de signature sont valides et n'ont pas été compromises;

iv) toute restriction quant à l'étendue de la responsabilité stipulée par le prestataire de services de certification;

v) s'il existe des moyens pour le signataire d'adresser une notification conformément à l'alinéa b) du paragraphe 1 de l'article 8;

vi) la disponibilité d'un service de révocation en temps utile;

e) lorsque des services sont fournis au titre du sous-alinéa v) de l'alinéa d), donne au signataire le moyen d'adresser une notification conformément à l'alinéa b) du paragraphe 1 de l'article 8 et, lorsque des services sont fournis au titre du sous-alinéa vi) de l'alinéa b), offre un service de révocation en temps utile;

f) utilise des systèmes, des procédures et des ressources humaines fiables pour la prestation de ses services.

2. Un prestataire de services de certification est responsable de tout manquement aux exigences visées au paragraphe 1.

Article 10. Fiabilité

Aux fins de l'alinéa f) du paragraphe 1 de l'article 9, pour déterminer si, ou dans quelle mesure, tous systèmes, procédures et ressources humaines utilisés par le prestataire de services de certification sont fiables, il peut être tenu compte des facteurs suivants:

a) ressources humaines et financières, y compris l'existence d'avoirs;

b) qualité du matériel et des logiciels;

c) procédures utilisées pour le traitement des certificats et des demandes de certificats et la conservation des enregistrements;

d) possibilité d'accès à l'information pour les signataires identifiés dans les certificats et les éventuelles parties se fiant aux certificats;

e) régularité et étendue des audits effectués par un organisme indépendant;

f) existence d'une déclaration de l'État, d'un organisme d'accréditation ou du prestataire de services de certification concernant le respect ou l'existence des critères énumérés ci-dessus; ou

g) tout autre facteur pertinent.

Article 11. Normes de conduite de la partie se fiant à la signature ou au certificat

Une partie se fiant à une signature ou à un certificat assume les conséquences juridiques découlant du fait qu'elle s'est abstenue de:

a) prendre des mesures raisonnables pour vérifier la fiabilité d'une signature électronique; ou,

b) si une signature électronique est étayée par un certificat, de prendre des mesures raisonnables pour:

i) vérifier que le certificat est valide ou qu'il n'a pas été suspendu ou révoqué; et

ii) tenir compte de toute restriction dont le certificat ferait l'objet.

Article 12. Reconnaissance des certificats et signatures électroniques étrangers

1. Pour déterminer si, ou dans quelle mesure, un certificat ou une signature électronique produit légalement ses effets, il n'est pas tenu compte:

a) du lieu dans lequel le certificat est émis ou la signature électronique créée ou utilisée; ou

b) du lieu dans lequel l'émetteur ou le signataire a son établissement.

2. Un certificat émis en dehors de [*l'État adoptant*] a les mêmes effets juridiques dans [*l'État adoptant*] qu'un certificat émis dans [*l'État adoptant*] à condition qu'il offre un niveau de fiabilité substantiellement équivalent.

3. Une signature électronique créée ou utilisée en dehors de [*l'État adoptant*] a les mêmes effets juridiques dans [*l'État adoptant*] qu'une signature électronique créée ou utilisée dans [*l'État adoptant*] à condition qu'elle offre un niveau de fiabilité substantiellement équivalent.

4. Pour déterminer si des certificats ou des signatures électroniques offrent un niveau de fiabilité substantiellement équivalent aux fins des paragraphes 2 ou 3, il est tenu compte des normes internationales reconnues et de tous autres facteurs pertinents.

5. Lorsque, nonobstant les paragraphes 2, 3 et 4, les parties conviennent, s'agissant de leurs relations, d'utiliser certains types de signatures électroniques ou certificats, cette convention est jugée suffisante aux fins de la reconnaissance internationale, à moins qu'elle soit invalide ou sans effets en vertu de la loi applicable.

Deuxième partie

GUIDE POUR L'INCORPORATION DE LA LOI TYPE DE LA CNUDCI SUR LES SIGNATURES ÉLECTRONIQUES (2001)

Objet du présent Guide

1. Lorsqu'elle a élaboré et adopté la Loi type de la CNUDCI sur les signatures électroniques (également dénommée dans la présente publication "la Loi type" ou "la nouvelle Loi type"), la Commission des Nations Unies pour le droit commercial international (CNUDCI) était consciente du fait que, pour les États qui modernisent leur législation, cette loi serait un outil plus efficace si l'on donnait aux gouvernements et aux parlements des informations générales et des explications pour les aider à l'utiliser. Elle a aussi tenu compte du fait que la Loi type serait probablement utilisée par des pays peu familiarisés avec le type de techniques de communication qui y sont traitées. Le présent Guide, qui a été établi en grande partie sur la base des travaux préparatoires, se veut par ailleurs un instrument utile pour d'autres utilisateurs du texte, tels que juges, arbitres, praticiens et universitaires. Ces informations pourraient aussi aider les États à examiner les dispositions qu'il conviendrait, le cas échéant, de modifier pour tenir compte de conditions qui leur sont propres. Durant l'élaboration de la Loi type, il a été présumé que l'instrument serait accompagné d'un tel guide. Il a été décidé, par exemple, de ne pas régler un certain nombre de points dans le texte de la Loi type, mais de s'y référer dans le Guide afin d'aider les États à appliquer la Loi type le moment venu. Les informations présentées dans le présent Guide visent à expliquer pourquoi les dispositions de la Loi type ont été retenues à titre d'éléments minimaux essentiels d'une législation destinée à atteindre les objectifs de la Loi type.

2. Le présent Guide a été élaboré par le secrétariat conformément à la demande faite par la CNUDCI à la clôture de sa trente-quatrième session, en 2001. Il est fondé sur les délibérations et décisions de la Commission à cette session[8], à laquelle la Loi type a été adoptée, ainsi que sur les considérations du Groupe de travail sur le commerce électronique, qui a mené les travaux préparatoires.

Chapitre premier. Présentation générale de la Loi type

I. OBJET ET ORIGINE DE LA LOI TYPE

A. Objet

3. Le recours accru à des techniques d'authentification électroniques au lieu de signatures manuscrites et d'autres méthodes traditionnelles d'authentification a conduit à penser qu'il serait utile d'avoir un cadre juridique spécifique afin de réduire l'incertitude quant à l'effet juridique pouvant résulter de l'utilisation de telles techniques modernes (qui peuvent être désignées d'une façon générale par le terme "signatures électroniques"). Le risque que divers pays adoptent des approches

législatives divergentes à l'égard des signatures électroniques demande des dispositions législatives uniformes afin d'établir les règles de base de ce qui est intrinsèquement un phénomène international dans lequel l'interopérabilité juridique (ainsi que technique) est essentielle.

4. Partant des principes fondamentaux sur lesquels repose l'article 7 de la Loi type de la CNUDCI sur le commerce électronique (dont le titre est toujours cité en entier dans la présente publication pour éviter toute confusion) pour ce qui est de la réalisation de la fonction de signature dans un environnement électronique, la nouvelle Loi type vise à aider les États à mettre en place un cadre législatif moderne, harmonisé et équitable permettant de traiter de façon plus efficace les questions des signatures électroniques. Supplément modeste mais important de la Loi type de la CNUDCI sur le commerce électronique, la nouvelle Loi type propose des normes concrètes par rapport auxquelles la fiabilité technique des signatures électroniques peut être mesurée. Elle établit en outre un lien entre cette fiabilité technique et l'efficacité juridique que l'on peut attendre d'une signature électronique particulière. Elle ajoute un élément important à la Loi type de la CNUDCI sur le commerce électronique en adoptant une approche qui permet de déterminer à l'avance (ou d'évaluer avant utilisation effective) l'efficacité juridique d'une technique de signature électronique donnée. Elle vise donc à faire mieux comprendre les signatures électroniques et à donner confiance dans l'utilisation de certaines techniques de signature électronique dans des opérations ayant une valeur juridique. En outre, en définissant avec la souplesse requise un ensemble de règles de conduite fondamentale pour les diverses parties pouvant être amenées à utiliser ou avoir affaire à des signatures électroniques (à savoir signataires, parties se fiant à la signature et tiers prestataires de services), la Loi type peut aider au développement de pratiques commerciales plus harmonieuses dans le cyberespace.

5. Les objectifs de la Loi type, qui consistent notamment à permettre ou à faciliter le recours aux signatures électroniques et à accorder le même traitement aux utilisateurs de documents sur papier et aux utilisateurs d'informations sous forme électronique, contribuent de manière décisive à favoriser l'économie et l'efficacité du commerce international. En incorporant dans sa législation nationale les procédures prescrites dans la Loi type (ainsi que les dispositions de la Loi type de la CNUDCI sur le commerce électronique) pour les cas où les parties décident d'utiliser des moyens de communication électroniques, un État adopterait une approche techniquement neutre.

B. Origine

6. La Loi type constitue une nouvelle étape dans une série d'instruments internationaux adoptés par la CNUDCI, qui ou bien portent spécifiquement sur les besoins du commerce électronique ou bien ont été élaborés compte tenu des besoins des moyens modernes de communication. Dans la première catégorie figurent le Guide juridique de la CNUDCI sur les transferts électroniques de fonds (1987), la Loi type de la CNUDCI sur les virements internationaux (1992) et la Loi type de la CNUDCI sur le commerce électronique (1996 et 1998). La deuxième catégorie comprend toutes les conventions internationales et autres instruments législatifs adoptés par la CNUDCI depuis 1978, qui promeuvent tous un formalisme réduit et

contiennent des définitions de “l’écrit” destinées à englober les communications dématérialisées.

7. L’instrument le mieux connu de la CNUDCI dans le domaine du commerce électronique est sa Loi type sur le commerce électronique. Son élaboration, au début des années 90, a pour origine le recours accru à des moyens modernes de communication tels que le courrier électronique et l’échange de données informatisées (EDI) pour la conduite des opérations commerciales internationales. On s’est rendu compte que de nouvelles techniques s’étaient répandues rapidement et continueraient de se développer à mesure que des supports techniques tels que les autoroutes de l’information et l’Internet devenaient plus largement accessibles. Toutefois, la communication d’informations ayant une valeur juridique sous forme de messages sans support papier était entravée par des obstacles juridiques à l’utilisation de tels messages ou par l’incertitude quant à leur effet ou leur validité juridique. Afin de faciliter le recours accru aux moyens modernes de communication, la CNUDCI a élaboré la Loi type sur le commerce électronique, dont l’objectif est d’offrir aux législateurs nationaux un ensemble de règles internationalement acceptables sur la manière de surmonter un certain nombre de ces obstacles et de créer un environnement juridique plus sûr pour ce que l’on appelle aujourd’hui le “commerce électronique”.

8. La décision de la CNUDCI d’élaborer une législation type sur le commerce électronique découle du fait que, dans un certain nombre de pays, la législation régissant la communication et l’archivage d’informations était inadaptée ou dépassée car elle n’envisageait pas le recours au commerce électronique. Dans certains cas, la législation impose encore directement ou indirectement des restrictions à l’utilisation des moyens modernes de communication, par exemple en prescrivant l’emploi de documents “écrits”, “signés” ou “originaux”. Pour les notions de documents “écrits”, “signés” et “originaux”, la Loi type de la CNUDCI sur le commerce électronique a adopté une approche fondée sur l’équivalence multifonctionnelle.

9. Lorsque la Loi type sur le commerce électronique était en cours d’élaboration, quelques pays avaient adopté des dispositions particulières pour traiter certains aspects du commerce électronique, mais il n’y avait pas de législation traitant ce commerce dans son ensemble. Cela pouvait être source d’incertitude quant à la nature juridique et à la validité d’informations présentées sous une forme autre que celle de documents traditionnels sur papier. En outre, des lois et des pratiques saines étaient nécessaires dans tous les pays où l’utilisation de l’EDI et de la messagerie électronique se généralisait, mais ce besoin se faisait aussi sentir dans de nombreux pays pour des techniques de communication telles que la télécopie et le télex.

10. La Loi type de la CNUDCI sur le commerce électronique aidait aussi à pallier les inconvénients tenant au fait qu’une législation nationale inappropriée entravait le commerce international, dont une proportion importante est liée à l’utilisation des techniques modernes de communication. Les disparités entre les régimes juridiques nationaux régissant l’utilisation de ces techniques de communication et les incertitudes qu’elles entraînent peuvent encore contribuer dans une large mesure à limiter les possibilités qu’ont les entreprises d’accéder aux marchés internationaux.

11. En outre, au niveau international, la Loi type de la CNUDCI sur le commerce électronique peut servir, dans certains cas, d’outil pour interpréter les conventions

internationales et autres instruments internationaux existants qui créent des obstacles juridiques au recours au commerce électronique, par exemple en prescrivant la forme écrite pour certains documents ou certaines clauses contractuelles. Entre les États Parties à de tels instruments internationaux, l'adoption de la Loi type de la CNUDCI sur le commerce électronique comme règle d'interprétation pourrait être le moyen de reconnaître le commerce électronique et d'éviter de devoir négocier un protocole à l'instrument international concerné.

C. Historique

12. Après avoir adopté la Loi type de la CNUDCI sur le commerce électronique, la Commission a, à sa vingt-neuvième session (1996), décidé d'inscrire à son ordre du jour la question des signatures numériques et des autorités de certification. Le Groupe de travail sur le commerce électronique a été prié d'examiner l'opportunité et la faisabilité de l'élaboration de règles uniformes sur ces sujets. Il a été convenu que ces règles devraient être consacrées à des questions telles que le fondement juridique des opérations de certification, y compris les nouvelles techniques d'authentification et de certification numériques; l'applicabilité de la certification; la répartition des risques et des responsabilités entre utilisateurs, fournisseurs et tiers dans le contexte de l'utilisation de techniques de certification; les questions spécifiques à la certification sous l'angle de l'utilisation de registres; et l'incorporation par référence[3].

13. À sa trentième session (1997), la Commission était saisie du rapport du Groupe de travail sur les travaux de sa trente et unième session (A/CN.9/437). Le Groupe de travail a indiqué à la Commission qu'il était parvenu à un consensus quant à l'importance et à la nécessité de travailler à l'harmonisation du droit dans ce domaine. Bien que n'ayant pas pris de décision ferme sur la forme et la teneur de ces travaux, il était arrivé à la conclusion préliminaire qu'il était possible d'entreprendre l'élaboration d'un projet de règles uniformes, du moins sur les questions concernant les signatures numériques et les autorités de certification, et peut-être sur des questions connexes. Il a rappelé que, dans le cadre des travaux futurs dans le domaine du commerce électronique, il pourrait être nécessaire de traiter, outre les questions relatives aux signatures numériques et aux autorités de certification, les sujets suivants: techniques autres que la cryptographie à clef publique; questions générales concernant les fonctions exercées par les tiers prestataires de services et contrats électroniques (A/CN.9/437, par. 156 et 157). La Commission a approuvé les conclusions du Groupe de travail et lui a confié l'élaboration de règles uniformes sur les questions juridiques relatives aux signatures numériques et aux autorités de certification.

14. S'agissant du champ d'application et de la forme exacts des règles uniformes, la Commission a généralement convenu qu'aucune décision ne pouvait être prise à un stade aussi précoce. Elle a estimé qu'il était justifié que le Groupe de travail axe son attention sur les questions relatives aux signatures numériques, étant donné le rôle apparemment prédominant joué par la cryptographie à clef publique dans la nouvelle pratique du commerce électronique, mais les règles uniformes à élaborer devraient être compatibles avec l'approche techniquement neutre adoptée dans la Loi type de la CNUDCI sur le commerce électronique. Ainsi, les règles uniformes ne devraient pas décourager l'utilisation d'autres techniques d'authentification. En

outre, lorsqu'il s'agirait de la cryptographie à clef publique, il pourrait être nécessaire de prendre en considération, dans ces règles uniformes, divers niveaux de sécurité et de reconnaître les divers effets juridiques et niveaux de responsabilité correspondant aux différents types de services fournis dans le contexte des signatures numériques. S'agissant des autorités de certification, la Commission a certes reconnu la valeur des normes issues du marché, mais il a été largement considéré que le Groupe de travail pourrait utilement envisager l'établissement d'un ensemble minimum de normes que les autorités de certification devraient strictement respecter, en particulier dans les cas de certification internationale[4].

15. Le Groupe de travail a commencé à élaborer les règles uniformes (qui sont devenues plus tard la Loi type) à sa trente-deuxième session en se fondant sur une note établie par le secrétariat (A/CN.9/WG.IV/WP.73).

16. À sa trente et unième session (1998), la Commission était saisie du rapport du Groupe de travail sur les travaux de sa trente-deuxième session (A/CN.9/446). Il a été noté que le Groupe de travail avait eu des difficultés manifestes, à ses trente et unième et trente-deuxième sessions, à parvenir à une position commune sur les nouvelles questions juridiques découlant de l'utilisation accrue des signatures numériques et autres signatures électroniques. Il a été également noté qu'il n'y avait toujours pas de consensus sur la manière dont ces questions pourraient être abordées dans un cadre juridique internationalement acceptable. Toutefois, la Commission a estimé, dans l'ensemble, que les progrès accomplis jusqu'ici étaient le signe que les règles uniformes prenaient progressivement la forme d'une structure utilisable.

17. La Commission a réaffirmé la décision qu'elle avait prise à sa trentième session sur la faisabilité de la rédaction de telles règles uniformes et s'est déclarée certaine que le Groupe de travail progresserait encore dans ses travaux à sa trente-troisième session sur la base du projet révisé établi par le secrétariat (A/CN.9/WG.IV/WP.76). Au cours du débat, la Commission a noté avec satisfaction que le Groupe de travail était désormais considéré comme un forum international particulièrement important pour les échanges de vues sur les problèmes juridiques du commerce électronique et la recherche des solutions correspondantes[5].

18. Le Groupe de travail a poursuivi la révision des règles uniformes à ses trente-troisième (1998) et trente-quatrième (1999) sessions sur la base des notes établies par le secrétariat (A/CN.9/WG.IV/WP.76 et A/CN.9/WG.IV/WP.79 et 80). Les rapports des sessions sont publiés sous les cotes A/CN.9/454 et 457.

19. À sa trente-deuxième session (1999), la Commission était saisie du rapport du Groupe de travail sur les travaux de ces deux sessions (A/CN.9/454 et 457). Elle a dit sa satisfaction devant les efforts faits par le Groupe de travail pour rédiger les règles uniformes. On s'est généralement accordé à penser que des progrès sensibles avaient été faits lors de ces sessions concernant la compréhension des aspects juridiques des signatures électroniques, mais on a également estimé que le Groupe de travail avait eu du mal à parvenir à un consensus sur les principes législatifs sur lesquels les règles uniformes devraient être fondées.

20. Selon une opinion, l'approche qu'avait adoptée jusque-là le Groupe de travail ne tenait pas suffisamment compte de la nécessité, dans le monde des affaires, d'une souplesse dans l'utilisation des signatures électroniques ou autres techniques d'authentification. Les règles uniformes, telles qu'alors envisagées, mettaient trop l'accent sur les signatures numériques et, dans cette optique même, sur une

application particulière impliquant la certification d'un tiers. On a donc proposé de limiter les travaux sur les signatures électroniques aux aspects juridiques de la certification transnationale ou de les reporter purement et simplement jusqu'à ce que la pratique commerciale soit mieux établie. Selon une opinion allant dans le même sens, aux fins du commerce international la plupart des questions juridiques liées à l'utilisation des signatures électroniques avaient déjà été résolues dans la Loi type de la CNUDCI sur le commerce électronique (voir ci-après par. 28). Une réglementation de certaines utilisations des signatures électroniques était peut-être nécessaire en dehors du droit commercial, mais le Groupe de travail ne devrait participer à aucune activité de ce type.

21. Selon l'avis qui a largement prévalu, le Groupe de travail devait poursuivre sa tâche sur la base de son mandat original. S'agissant du besoin de règles uniformes sur les signatures électroniques, on a expliqué que, dans de nombreux pays, les gouvernements et les organes législatifs qui avaient entrepris l'élaboration d'une législation sur les questions relatives aux signatures électroniques, y compris la mise en place d'une infrastructure fondée sur la clef publique (ICP) ou d'autres projets sur des questions étroitement liées (voir A/CN.9/457, par. 16), attendaient des orientations de la CNUDCI. Quant à la décision prise par le Groupe de travail de se concentrer sur les questions et la terminologie ICP, on a rappelé que le jeu des relations entre trois types distincts de parties (les détenteurs des clefs, les autorités de certification et les parties se fiant aux clefs) correspondait à un modèle possible d'ICP, mais que d'autres étaient aussi concevables (sans intervention d'une autorité de certification indépendante, par exemple). L'un des principaux avantages qu'il y avait à se concentrer sur les questions relatives à l'ICP était que l'on pouvait ainsi structurer plus facilement les règles uniformes par référence à trois fonctions (ou rôles) associées aux paires de clefs, à savoir la fonction d'émetteur de la clef (ou abonné), la fonction de certification et la fonction de confiance. On s'est généralement accordé à penser que ces trois fonctions étaient communes à tous les modèles d'ICP, et qu'il fallait les traiter, qu'elles soient exercées par trois entités séparées ou que deux d'entre elles soient assurées par la même personne (par exemple lorsque l'autorité de certification était également une partie se fiant à la clef). En outre, il a été largement estimé qu'en se concentrant sur les fonctions typiques de l'ICP et non sur un modèle particulier on parviendrait peut-être plus facilement à élaborer, à un stade ultérieur, une règle tout à fait neutre sur le plan technique (ibid., par. 68).

22. À l'issue du débat, la Commission a réaffirmé ses décisions précédentes quant à la faisabilité de la rédaction de règles uniformes et s'est déclarée certaine que le Groupe de travail pourrait progresser encore à ses prochaines sessions[6].

23. Le Groupe de travail a poursuivi ses travaux à ses trente-cinquième (septembre 1999) et trente-sixième (février 2000) sessions en se fondant sur des notes établies par le secrétariat (A/CN.9/WG.IV/WP.82 et 84). À sa trente-troisième session (2000), la Commission était saisie du rapport du Groupe de travail sur les travaux de ces deux sessions (A/CN.9/465 et 467). Il a été noté que le Groupe de travail, à sa trente-sixième session, avait adopté le texte des projets d'articles 1 et 3 à 12 des règles uniformes. Il restait à clarifier certains points suite à sa décision de supprimer dans les règles uniformes la notion de "signature électronique renforcée". On a exprimé la crainte qu'il soit nécessaire, en fonction des décisions qu'il prendrait concernant les projets d'articles 2 et 13, de réexaminer les autres projets de

dispositions pour éviter que la norme établie dans les règles uniformes ne s'applique de la même façon aux signatures électroniques garantissant un niveau de sécurité élevé et aux certificats de moindre valeur susceptibles d'être utilisés dans les communications électroniques n'étant pas destinées à produire d'effet juridique important.

24. A l'issue du débat, la Commission a félicité le Groupe de travail pour les efforts qu'il avait fournis et les progrès qu'il avait accomplis dans l'élaboration des règles uniformes. Elle l'a instamment prié de terminer ses travaux sur ce texte à sa trente-septième session et d'examiner le projet de guide que devait établir le Secrétariat[7].

25. Le Groupe de travail a terminé l'élaboration des règles uniformes à sa trente-septième session (septembre 2000). Le rapport sur les travaux de cette session a été publié sous la cote A/CN.9/483. Le Groupe de travail a également examiné le projet de guide pour l'incorporation dans le droit interne des règles uniformes. le secrétariat a été prié d'établir une version révisée de ce projet de guide reflétant les décisions prises par le Groupe de travail en fonction des points de vue, suggestions et préoccupations exprimés au cours de la session. Faute de temps, le Groupe de travail n'a pu clore ses délibérations sur ce point. Il a été convenu qu'il devrait se ménager, à sa trente-huitième session, un peu de temps pour en achever l'examen. Il a été noté que les règles uniformes (sous forme de projet de Loi type de la CNUDCI sur les signatures électroniques), ainsi que le projet de guide, seraient soumis à la Commission pour examen et adoption à sa trente-quatrième session (2001). [*Note du secrétariat: cette section relative à l'historique de la Loi types doit être complétée, et éventuellement rédigée de façon légèrement plus concise, après examen final et adoption de la Loi type par la Commission.*]

II. LA LOI TYPE COMME OUTIL D'HARMONISATION DES LOIS

26. Comme la Loi type de la CNUDCI sur le commerce électronique, la nouvelle Loi type se présente sous la forme d'un texte législatif qu'il est recommandé aux États d'incorporer dans leur droit national. Contrairement à ce qui se passe dans le cas d'une convention internationale, l'État qui adopte une loi type n'est pas tenu d'en aviser l'Organisation des Nations Unies ou les autres États qui ont pu eux aussi l'adopter. Les États sont toutefois vivement encouragés à informer le secrétariat de la CNUDCI de l'adoption de ce nouveau texte (ou de toute autre loi type résultant des travaux de la CNUDCI).

27. En incorporant le texte d'une loi type dans son système juridique, un État peut modifier ou exclure certaines de ses dispositions. Dans le cas d'une convention, la possibilité pour les États Parties d'apporter des changements (habituellement appelés "réserves") au texte uniforme est beaucoup plus limitée; en particulier, les conventions de droit commercial, le plus souvent, ou bien interdisent toute réserve, ou bien n'en autorisent que quelques-unes, qui sont spécifiées. La souplesse inhérente à une loi type est particulièrement souhaitable dans les cas où il est probable que l'État voudra apporter diverses modifications au texte uniforme avant d'être prêt à l'adopter dans son droit national. On peut s'attendre à certaines modifications, en particulier lorsque le texte uniforme a un lien étroit avec le système judiciaire et procédural national. Mais cela signifie aussi que le degré d'harmonisation, et de certitude quant à l'harmonisation, atteint par une loi type sera

probablement moins élevé que dans le cas d'une convention. Cet inconvénient relatif peut néanmoins être compensé par le fait qu'il y a probablement plus d'États adoptant une loi type que d'États adhérant à une convention. Pour atteindre un degré satisfaisant d'harmonisation et de sécurité, il est recommandé que les États apportent aussi peu de modifications que possible lors de l'incorporation de la nouvelle Loi type dans leur système juridique. D'une façon générale, lors de l'adoption de cette nouvelle Loi type (ou de la Loi type de la CNUDCI sur le commerce électronique), il est souhaitable d'adhérer autant que possible au texte uniforme de manière à rendre le droit national aussi transparent et familier que possible pour les étrangers qui l'utiliseront.

28. Il faut noter que certains pays considèrent que les questions juridiques liées à l'utilisation de signatures électroniques ont déjà été réglées par la Loi type de la CNUDCI sur le commerce électronique et qu'ils ne prévoient pas d'adopter d'autres règles sur les signatures électroniques tant que les pratiques du marché dans ce nouveau domaine ne seront pas mieux établies. Toutefois, les États qui adopteront la nouvelle Loi type en plus de la Loi type de la CNUDCI sur le commerce électronique peuvent en attendre des avantages supplémentaires. Pour ceux dont les organes exécutifs et législatifs préparent actuellement une loi sur les questions relatives aux signatures électroniques, y compris l'établissement d'une infrastructure à clef publique (ICP), la Loi type offre des lignes directrices d'un instrument international qui a été élaboré en tenant compte des questions et de la terminologie de l'ICP. Pour tous les pays, la Loi type offre un ensemble de règles pouvant avoir des applications allant au-delà du modèle ICP, puisqu'elle envisage le jeu des relations entre trois fonctions distinctes intervenant dans tout type de signature électronique (à savoir la création, la certification et la confiance). Ces trois fonctions doivent être traitées, qu'elles soient exercées par trois entités séparées ou que deux d'entre elles soient exercées par la même personne (par exemple lorsque l'autorité de certification est également une partie se fiant à la signature). La Loi type offre donc des bases communes pour les systèmes d'ICP fondés sur des autorités de certification indépendantes et les systèmes de signature électronique où aucun tiers indépendant de ce type n'intervient dans le processus de signature. Dans tous les cas, la nouvelle Loi type offre une sécurité supplémentaire concernant l'efficacité juridique des signatures électroniques, sans limiter l'application du critère souple énoncé à l'article 7 de la Loi de la CNUDCI sur le commerce électronique (voir ci-après par. 67 et 70 à 75).

III. OBSERVATIONS GÉNÉRALES SUR LES SIGNATURES ÉLECTRONIQUES[8]

A. Fonctions de la signature

29. L'article 7 de la Loi type de la CNUDCI sur le commerce électronique se fonde sur la reconnaissance des fonctions remplies par la signature dans un environnement papier. Lors des travaux préparatoires sur cette loi, le Groupe de travail a examiné les fonctions suivantes traditionnellement remplies par les signatures manuscrites: identification d'une personne; certitude quant à la participation en personne de l'intéressé dans l'acte de signature; association de cette

personne avec la teneur d'un document. Il a été noté qu'en outre la signature pouvait remplir diverses fonctions, selon la nature du document signé. Par exemple, une signature peut témoigner de l'intention d'une partie d'être liée par la teneur d'un contrat signé; de l'intention d'une personne de revendiquer la paternité d'un texte (montrant ainsi qu'elle a conscience du fait que l'acte de signature peut avoir éventuellement des conséquences juridiques); de l'intention d'une personne de s'associer à la teneur d'un document rédigé par quelqu'un d'autre; du fait que et du moment où une personne se trouvait en un lieu donné. La relation entre la nouvelle Loi type et l'article 7 de la Loi type de la CNUDCI sur le commerce électronique est examinée plus avant aux paragraphes 67 et 70 à 75 du présent Guide.

30. Dans un environnement électronique, l'original d'un message ne se distingue pas d'une copie, ne comporte aucune signature manuscrite et ne figure pas sur papier. Les possibilités de fraude sont énormes, du fait de la facilité qu'il y a à intercepter et modifier l'information sous forme électronique sans risque d'être détecté, ainsi que de la rapidité avec laquelle on peut traiter de multiples transactions. La finalité des diverses techniques actuellement disponibles sur le marché ou en cours d'élaboration est de créer les moyens techniques grâce auxquels un certain nombre ou la totalité des fonctions perçues comme caractéristiques d'une signature manuscrite peuvent être remplies dans un contexte électronique. On peut regrouper ces techniques sous le terme générique de "signatures numériques".

B. Signatures numériques et autres signatures électroniques

31. Lorsqu'elle a examiné s'il était opportun et possible d'élaborer la nouvelle Loi type, et défini son champ d'application, la CNUDCI a examiné les diverses techniques de signature électronique qui étaient utilisées ou en cours d'élaboration. L'objectif commun à ces techniques est de fournir des équivalents fonctionnels à 1) la signature manuscrite et 2) aux autres types de mécanismes d'authentification utilisés dans un environnement papier (par exemple, sceaux ou cachets). Les mêmes techniques peuvent remplir des fonctions supplémentaires dans le domaine du commerce électronique, qui découlent des fonctions d'une signature mais où elles n'ont aucun équivalent strict dans un environnement papier.

32. Ainsi qu'il a été indiqué plus haut (voir par. 21 et 28), les gouvernements et parlements de nombreux pays qui sont en train d'élaborer une législation sur les questions relatives aux signatures électroniques, y compris la mise en place d'une infrastructure à clef publique (ICP) ou autres projets sur des questions étroitement liées (voir A/CN.9/457, par. 16) attendent des orientations de la CNUDCI. Quant à la décision prise par cette dernière de se concentrer sur les questions et sur la terminologie de l'ICP, il convient de noter que le jeu des relations entre trois types distincts de parties (les signataires, les prestataires de services de certification et les parties se fiant aux signatures) correspond à un modèle possible d'ICP, mais que d'autres modèles sont déjà couramment utilisés sur le marché (sans intervention d'une autorité de certification indépendante, par exemple). L'un des principaux avantages qu'il y a à se concentrer sur les questions relatives à l'ICP est que l'on peut ainsi structurer plus facilement la Loi type par référence à trois fonctions (ou rôles) associées aux signatures électroniques, à savoir, la fonction de signataire (émetteur de la clef ou abonné) la fonction de certification, et la fonction de confiance. Ces trois fonctions sont communes à tous les modèles d'ICP et il faudrait les traiter, qu'elles soient exercées par trois entités séparées ou que deux d'entre

elles soient assurées par la même personne (par exemple, lorsque le prestataire de services de certification est également une partie se fiant à la signature). En outre, en se concentrant sur les fonctions typiques de l'ICP et non sur un modèle particulier, on parvient plus facilement à élaborer une règle tout à fait neutre sur le plan technique dans la mesure où des fonctions similaires sont remplies dans le cas d'une technique de signature électronique autre qu'une infrastructure à clef publique.

1. Signatures électroniques faisant appel à des techniques autres que la cryptographie à clef publique

33. Parallèlement aux "signatures numériques" s'appuyant sur la cryptographie à clef publique, il existe divers autres mécanismes, englobés eux aussi dans la notion plus large de "signature électronique", qui peuvent être en usage ou dont on envisage l'utilisation dans l'avenir, en vue de remplir une ou plusieurs des fonctions susmentionnées des signatures manuscrites. Par exemple, certaines techniques s'appuient sur l'authentification par dispositif biométrique fondé sur la signature manuscrite. Avec un tel dispositif, le signataire apposerait sa signature manuscrite à l'aide d'un stylo spécial, soit sur un écran d'ordinateur, soit sur un bloc numérique. La signature manuscrite serait alors analysée par ordinateur et mise en mémoire sous forme d'un ensemble de valeurs numériques, qui pourrait être ajouté à un message de données et affiché par le destinataire aux fins d'authentification. Ce système d'authentification présupposerait que des échantillons de la signature manuscrite ont été préalablement analysés et mis en mémoire par le dispositif biométrique. D'autres techniques reposent sur l'utilisation de numéros d'identification personnels (codes PIN) de signatures numérisées et d'autres méthodes, comme celles qui consistent à cliquer sur la case "valider".

34. La CNUDCI a souhaité élaborer une législation uniforme de nature à faciliter l'utilisation aussi bien des signatures numériques que d'autres formes de signature électronique. À cet effet, elle a essayé de traiter les questions juridiques liées aux signatures électroniques à un niveau intermédiaire entre le caractère très général de sa Loi type sur le commerce électronique et le degré de détail qui peut être nécessaire dans le cas d'une signature particulière. En tout état de cause, conformément au principe de neutralité technique énoncé dans la Loi type sur le commerce électronique, la nouvelle Loi type ne doit pas être interprétée comme décourageant l'utilisation d'une quelconque méthode de signature électronique, que celle-ci existe déjà ou doive être mise en œuvre dans l'avenir.

2. Signatures numériques fondées sur la cryptographie à clef publique[9]

35. Étant donné l'usage croissant des techniques de signature numérique dans un certain nombre de pays, l'introduction ci-après pourra être utile à ceux qui élaborent des lois sur les signatures électroniques.

a) Notions et terminologie techniques

i) Cryptographie

36. Les signatures numériques sont créées et vérifiées grâce à la cryptographie, branche des mathématiques appliquées qui s'occupe de la transformation de messages en des formes apparemment inintelligibles et de leur restitution dans leur

forme initiale. Les signatures numériques utilisent ce que l'on appelle la "cryptographie à clef publique", qui est souvent basée sur l'utilisation de fonctions algorithmiques pour créer deux "clefs" (c'est-à-dire des nombres de plusieurs chiffres générés à l'aide d'une série de formules mathématiques appliquées aux nombres premiers) différentes mais mathématiquement liées entre elles. L'une de ces clefs est utilisée pour créer une signature numérique ou pour transformer des données en une forme apparemment inintelligible, et l'autre pour vérifier une signature numérique ou restituer le message dans sa forme initiale. Le matériel et le logiciel informatiques utilisant deux clefs de ce type sont souvent appelés collectivement "cryptosystèmes" ou, plus précisément "cryptosystèmes asymétriques" lorsqu'ils utilisent des algorithmes asymétriques.

37. Bien que le recours à la cryptographie soit l'une des principales caractéristiques des signatures numériques, le simple fait qu'une signature numérique soit utilisée pour authentifier un message contenant des données sous forme numérique ne doit pas être assimilé à l'utilisation plus générale de la cryptographie à des fins de confidentialité. Le codage pour raison de confidentialité est une méthode utilisée pour coder une communication électronique de manière que seuls l'initiateur et le destinataire du message seront en mesure de le lire. Dans un certain nombre de pays, la loi restreint l'utilisation de la cryptographie à cette fin pour des raisons d'ordre public qui peuvent comporter des considérations de défense nationale. Cependant, l'utilisation de la cryptographie aux fins d'authentification par la création d'une signature numérique n'implique pas nécessairement le recours au codage pour garantir le caractère confidentiel d'une communication, étant donné que la signature numérique codée peut être tout simplement jointe à un message non codé.

ii) Clefs publiques et privées

38. Les clefs complémentaires utilisées pour les signatures numériques sont appelées la "clef privée", qui n'est utilisée que par le signataire pour créer la signature numérique, et la "clef publique", qui est d'ordinaire plus largement connue et est utilisée par une partie se fiant à la signature pour vérifier la signature numérique. Il appartient à l'utilisateur d'une clef privée de garder la clef privée secrète. On notera que l'utilisateur individuel n'a pas besoin de connaître la clef privée. Celle-ci est normalement conservée sur une carte à mémoire, ou est normalement accessible grâce à un numéro d'identification personnel ou, dans l'idéal, grâce à un dispositif d'identification biométrique, par exemple un dispositif de reconnaissance d'empreinte de pouce. Si de nombreuses personnes ont besoin de vérifier les signatures numériques du signataire, la clef publique doit être rendue accessible ou distribuée à l'ensemble de ces personnes, par exemple en la publiant dans un répertoire en ligne ou dans toute autre forme de répertoire public où elle est facilement accessible. Bien que les clefs de la paire soient mathématiquement liées, si un système de cryptographie asymétrique a été conçu et mis en œuvre de façon sécurisée, il est pratiquement impossible, connaissant la clef publique, de déduire la clef privée. Les algorithmes les plus courants de chiffrement par utilisation de clefs publiques et privées reposent sur une caractéristique importante des grands nombres premiers: une fois multipliés ensemble pour produire un nouveau nombre, il est particulièrement difficile et long de déterminer les deux nombres premiers qui ont créé ce nouveau nombre plus élevé[10]. Ainsi, bien que de nombreuses personnes

connaissent la clef publique d'un signataire donné et l'utilisent pour vérifier ses signatures, elles ne peuvent découvrir sa clef privée et l'utiliser pour falsifier des signatures numériques.

39. On notera cependant que le concept de cryptographie à clef publique ne nécessite pas forcément l'utilisation des algorithmes susmentionnés, fondés sur des nombres premiers. On utilise ou on met au point actuellement d'autres techniques mathématiques telles que des systèmes de cryptographie fondés sur des courbes elliptiques, souvent décrits comme offrant un niveau élevé de sécurité malgré l'utilisation de longueurs de clefs considérablement réduites.

iii) Fonction de hachage

40. Outre la production de paires de clefs, un autre processus fondamental, généralement appelé "fonction de hachage", est utilisé à la fois pour créer et pour vérifier une signature numérique. Une fonction de hachage est un processus mathématique fondé sur un algorithme, qui crée une représentation numérique, ou forme comprimée du message, souvent appelée "abrégé" ou "empreinte digitale", et qui prend la forme d'une "valeur de hachage" ou d'un "résultat de hachage" d'une longueur normalisée généralement bien plus courte que le message lui-même mais qui lui est néanmoins unique. Toute modification apportée au message produit inévitablement un résultat de hachage différent lorsqu'on utilise la même fonction de hachage. Dans le cas d'une fonction de hachage sécurisée, parfois appelée "fonction de hachage unidirectionnelle", il est pratiquement impossible, connaissant la valeur de hachage, de déduire le message initial. Les fonctions de hachage permettent donc au programme de création de signatures numériques d'opérer sur des volumes de données plus limités et prévisibles tout en établissant une solide corrélation avec la teneur du message initial, ce qui lui permet d'assurer qu'aucune modification n'a été apportée au message depuis que ce dernier a été signé sous forme numérique.

iv) Signature numérique

41. Pour signer un document ou toute autre information, le signataire commence par définir précisément les limites de ce qu'il doit signer. Ensuite, une fonction de hachage opérant dans le programme du signataire calcule un résultat de hachage propre (à toutes fins pratiques) à l'information qui doit être signée. Le programme du signataire transforme ensuite le résultat de hachage en une signature numérique à l'aide de la clef privée du signataire. La signature numérique résultante est par conséquent propre à la fois à l'information signée et à la clef privée utilisée pour créer la signature numérique.

42. Généralement, une signature numérique (un résultat de hachage signé numériquement) est attachée au message et stockée ou transmise avec ce message. Cependant, elle peut également être envoyée ou stockée comme élément de données distinct, aussi longtemps qu'elle maintient une association fiable avec le message correspondant. Étant donné qu'une signature numérique est propre à son message, elle est inutile si on la dissocie de façon permanente de ce dernier.

v) Vérification de la signature numérique

43. La vérification de la signature numérique consiste à vérifier cette dernière par rapport au message initial et à une clef publique donnée, et à déterminer de cette façon si elle a été créée pour ce même message à l'aide de la clef privée correspondant à la clef publique référencée. Une telle vérification s'effectue en calculant un nouveau résultat de hachage du message initial au moyen de la fonction de hachage utilisée pour créer la signature numérique. Ensuite, à l'aide de la clef publique et du nouveau résultat de hachage, le vérificateur vérifie si la signature numérique a été créée à l'aide de la clef privée correspondante, et si le résultat de hachage nouvellement calculé correspond au résultat de hachage initial qui a été transformé en signature numérique au cours du processus de signature.

44. Le programme de vérification confirmera la signature numérique comme étant "vérifiée": 1) si la clef privée du signataire a été utilisée pour signer numériquement le message, ce qui est avéré si sa clef publique a été utilisée pour vérifier la signature étant donné que cette clef publique permettra de vérifier uniquement une signature numérique créée à l'aide de la clef privée du signataire; et 2) si le message ne subit aucune modification, ce qui est avéré si le résultat de hachage calculé par la personne chargée de la vérification est identique au résultat de hachage extrait de la signature numérique lors du processus de vérification.

b) Infrastructure à clef publique (ICP) et prestataires de services de certification

45. Pour vérifier une signature numérique, le vérificateur doit avoir accès à la clef publique du signataire et s'assurer que celle-ci correspond bien à la clef privée de ce dernier. Cependant, une paire de clefs publique et privée n'a aucune association intrinsèque avec une personne quelconque; il s'agit simplement d'une paire de nombres. Un mécanisme supplémentaire est nécessaire pour associer de manière fiable une personne ou une entité particulière à la paire de clefs. Si l'on veut que le chiffrement à clef publique remplisse sa fonction, il faut trouver un moyen d'envoyer les clefs à un grand nombre de personnes, dont beaucoup sont inconnues de l'expéditeur, et alors même qu'aucune relation de confiance ne s'est forgée entre les parties. Pour ce faire, les parties concernées doivent avoir une très grande confiance dans les clefs publiques et privées émises.

46. Le degré requis de confiance peut exister entre des parties qui se font confiance, qui ont traité l'une avec l'autre sur une certaine durée, qui communiquent sur des systèmes fermés, qui fonctionnent à l'intérieur d'un groupe fermé, ou dont les relations peuvent être régies par contrat – par exemple dans le cadre d'un accord de partenariat commercial. Si une transaction ne fait intervenir que deux parties, chacune peut simplement communiquer (par un moyen relativement sûr tel qu'un coursier ou un téléphone, qui permet la reconnaissance de voix) la clef publique de la paire de clefs que chaque partie va utiliser. Cependant, il se peut que le même degré de confiance soit absent lorsque les parties ont peu affaire l'une à l'autre, communiquent sur des systèmes ouverts (par exemple Internet), ne font pas partie d'un groupe fermé ou ne sont pas liées juridiquement, par exemple par un accord de partenariat commercial.

47. En outre, étant donné que le chiffrement à clef publique est une technique hautement mathématique, tous les utilisateurs doivent avoir confiance dans les compétences, les connaissances et les dispositifs de sécurité des parties émettant les clefs publiques et privées[11].

48. Un signataire éventuel pourrait faire une déclaration publique indiquant que les signatures vérifiables au moyen d'une clef publique donnée devraient être considérées comme provenant de lui. Cependant, d'autres parties pourraient refuser d'accepter cette déclaration, en particulier lorsqu'il n'existe aucun contrat préalable établissant avec certitude l'effet juridique de ladite déclaration. Une partie se fiant à une telle déclaration non étayée publiée dans un système ouvert risquerait beaucoup de faire confiance, à son insu, à un imposteur ou d'avoir à établir qu'il n'y a pas eu dénégation injustifiée de signature numérique (question souvent évoquée à propos de la "non-répudiation" des signatures numériques) dans le cas où une transaction s'avérerait défavorable au signataire supposé.

49. L'une des solutions à ce problème consiste à recourir à un ou plusieurs tiers de confiance pour associer un signataire identifié ou le nom de ce signataire à une clef publique spécifique. Ce tiers de confiance est généralement appelé, dans la plupart des normes et directives techniques, "autorité de certification" ou "prestataire de services de certification" (dans la Loi type, c'est l'expression "prestataire de services de certification" qui a été retenue). Dans plusieurs pays, ces autorités de certification s'organisent de façon hiérarchique en ce que l'on appelle souvent une infrastructure à clef publique.

i) Infrastructure à clef publique (ICP)

50. La création d'une infrastructure à clef publique est un moyen d'inspirer confiance dans le fait que: 1) la clef publique de l'utilisateur n'a pas été falsifiée et correspond effectivement à sa clef privée; 2) les techniques de chiffrement utilisées sont bonnes; 3) les entités délivrant les clefs cryptographiques préserveront ou recréeront les clefs publiques et privées susceptibles d'être utilisées pour le chiffrement afin d'assurer la confidentialité lorsque le recours à cette technique est autorisé; 4) il y a interopérabilité des différents systèmes de chiffrement. Pour inspirer cette confiance, une ICP peut offrir un certain nombre de services, dont les suivants: 1) gérer les clefs cryptographiques utilisées pour les signatures numériques; 2) certifier qu'une clef publique correspond bien à une clef privée; 3) fournir des clefs aux utilisateurs finaux; 4) décider quels utilisateurs se verront conférer tel ou tel privilège dans le système; 5) publier un répertoire sécurisé des clefs publiques ou des certificats; 6) gérer des objets personnalisés (par exemple cartes à mémoire) capables d'identifier l'utilisateur au moyen d'éléments d'identification qui lui sont spécifiques ou capables de créer et de garder en mémoire les clefs privées d'un individu; 7) vérifier l'identité des utilisateurs finaux et leur offrir des services; 8) offrir des services de non-répudiation; 9) offrir des services d'horodatage; 10) gérer les clefs de chiffrement utilisées pour le chiffrement de confidentialité lorsque le recours à cette technique est autorisé.

51. Une infrastructure à clef publique s'appuie souvent sur divers niveaux d'autorité. Par exemple, les modèles envisagés dans certains pays pour établir ce type d'infrastructure se réfèrent notamment aux niveaux suivants: 1) une autorité principale ("autorité racine") unique, qui certifierait la technologie et les pratiques

de toutes les parties autorisées à produire les paires de clefs cryptographiques ou les certificats concernant l'utilisation de ces paires de clefs, et qui enregistrerait les autorités de certification inférieures[12]; 2) diverses autorités de certification, situées en dessous de "l'autorité racine", qui certifieraient que la clef publique d'un utilisateur correspond effectivement à sa clef privée (autrement dit, que la clef n'a pas été manipulée); et 3) diverses autorités locales d'enregistrement, placées en dessous des autorités de certification et chargées, d'une part, de recevoir les demandes de paires de clefs cryptographiques ou de certificats relatifs à l'utilisation de ces paires de clefs adressées par des utilisateurs et, d'autre part, d'exiger une preuve d'identification et de vérifier l'identité des utilisateurs éventuels. Dans certains pays, il est envisagé de confier à des officiers publics la fonction d'autorité locale d'enregistrement, ou tout au moins d'apporter leur concours à cette fonction.

52. Il se peut que les questions relatives à l'IPC ne se prêtent pas aisément à une harmonisation internationale. En effet, l'organisation d'une IPC peut faire intervenir diverses questions techniques ainsi que des questions d'ordre public que les États sont peut-être mieux à même de régler individuellement en l'état actuel des choses[13]. À cet égard, chacun d'entre eux devra peut-être prendre des décisions concernant l'établissement d'une ICP, notamment pour ce qui est de: 1) déterminer la forme et le nombre de niveaux d'autorité devant constituer l'IPC; 2) déterminer si seules certaines autorités appartenant à l'infrastructure devraient être autorisées à délivrer les paires de clefs cryptographiques ou si ces dernières peuvent être créées par les utilisateurs eux-mêmes; 3) savoir si les autorités de certification garantissant la validité des paires de clefs cryptographiques devraient être des entités publiques ou si des entités privées pourraient agir en cette qualité; 4) déterminer si l'autorisation donnée à une entité d'agir en qualité d'autorité de certification devrait prendre la forme d'une autorisation expresse ou de l'octroi d'une "licence" par l'État, ou si d'autres méthodes devraient être utilisées pour contrôler la qualité de ces autorités si on les dispense d'une autorisation spécifique; 5) déterminer dans quelle mesure la cryptographie devrait être autorisée à des fins de confidentialité; et 6) savoir si l'État devrait conserver l'accès à l'information chiffrée, au moyen d'un mécanisme de séquestre de la clef ("key escrow") ou autrement. La Loi type ne traite pas de ces questions.

ii) Prestataires de services de certification

53. Pour associer une paire de clefs à un signataire éventuel, un prestataire de services de certification (ou autorité de certification) délivre un certificat, enregistrement électronique qui indique la clef publique ainsi que le nom du titulaire du certificat identifié comme "sujet" de ce certificat et qui peut confirmer que le signataire éventuel identifié dans le certificat détient la clef privée correspondante. La fonction essentielle d'un certificat est d'associer une clef publique à un détenteur précis. Un "destinataire" du certificat souhaitant se fier à une signature numérique créée par le titulaire indiqué dans le certificat peut utiliser la clef publique figurant dans le certificat pour vérifier que la signature numérique a bien été créée avec la clef privée correspondante. Si cette vérification est positive, le destinataire est assuré que la signature numérique a effectivement été créée par le détenteur de la clef publique indiqué dans le certificat, et que le message correspondant n'a pas été modifié depuis qu'on y a apposé une signature numérique.

54. Pour assurer l'authenticité du certificat (soit tant de son contenu que de sa source), l'autorité de certification y appose une signature numérique. Celle-ci peut être vérifiée au moyen de la clef publique de cette autorité de certification figurant sur un autre certificat délivré par une autre autorité de certification (qui peut, mais ne doit pas nécessairement, être une autorité hiérarchiquement supérieure), et cet autre certificat peut à son tour être authentifié par la clef publique figurant sur un autre certificat encore, et ainsi de suite, jusqu'à ce que la personne devant se fier à la signature numérique soit convaincue de son authenticité. Dans chaque cas, l'autorité de certification délivrant le certificat doit apposer une signature numérique sur son propre certificat pendant la période de validité de l'autre certificat utilisé pour vérifier sa signature numérique.

55. Une signature numérique correspondant à un message, qu'elle soit créée par le détenteur de la paire de clefs pour authentifier un message ou par l'autorité de certification pour authentifier son certificat, devrait généralement être horodatée de manière à permettre au vérificateur de déterminer de manière fiable si elle a bien été créée pendant la "période de validité" indiquée dans le certificat, ce qui est l'une des conditions de la vérifiabilité d'une signature numérique.

56. Pour qu'une clef publique et son association à un détenteur spécifique soient aisément vérifiables, le certificat peut être publié dans un répertoire ("repository") ou mis à disposition par d'autres moyens. Généralement, les répertoires sont des bases de données en ligne regroupant des certificats et d'autres informations pouvant être appelés et utilisés pour vérifier les signatures numériques.

57. Une fois délivré, un certificat peut se révéler sujet à caution, par exemple si le détenteur a donné une fausse identité à l'autorité de certification. Dans d'autres cas, un certificat peut être fiable au moment où il est délivré, mais devenir sujet à caution par la suite. Si la clef privée est "compromise", par exemple parce que son détenteur en a perdu le contrôle, le certificat peut perdre sa fiabilité. L'autorité de certification (à la demande du détenteur ou même sans son consentement, selon les circonstances) peut alors suspendre (interrompre provisoirement la période de validité) ou révoquer (annuler définitivement) le certificat. Dès cette suspension ou cette révocation, elle doit généralement publier une notification ou en aviser les personnes qui l'interrogent ou dont elle sait qu'elles ont reçu une signature numérique vérifiable par référence à un certificat qui n'est pas fiable.

58. Les autorités de certification pourraient être des organismes relevant de l'État ou des prestataires de services privés. Dans certains pays, on envisage, pour des raisons d'ordre public, que seuls des organismes publics soient autorisés à assurer la fonction de certification. Dans d'autres, on considère que les services de certification doivent être ouverts à la concurrence sur le marché privé. Quelle que soit l'option retenue et que les autorités de certification aient ou non besoin d'une licence pour fonctionner, une infrastructure à clef publique comprend généralement plusieurs autorités. Ce qui est particulièrement important est la relation entre les différentes autorités de certification. Elle peuvent, au sein de l'infrastructure, être organisées hiérarchiquement, certaines ne faisant que certifier celles qui fournissent directement les services aux usagers. Dans ce type de structure, il y a donc subordination de certaines autorités de certification à d'autres. Mais on peut aussi envisager qu'elles fonctionnent toutes sur un pied d'égalité. Dans toute infrastructure importante il y aura vraisemblablement des autorités de certification subordonnées et supérieures. En tout état de cause, en l'absence d'une ICP

internationale, un certain nombre de questions peuvent se poser s'agissant de la reconnaissance de certificats par les autorités de certification d'autres pays. La reconnaissance des certificats étrangers s'effectue souvent au moyen de ce que l'on appelle une "certification croisée". En pareil cas, il est indispensable que des autorités de certification essentiellement équivalentes (ou acceptant tout au moins d'assumer certains risques pour les certificats délivrés par d'autres autorités de certification) reconnaissent mutuellement les services qu'elles fournissent, afin que leurs usagers respectifs puissent communiquer entre eux de manière plus efficace et en accordant une plus grande confiance dans la fiabilité des certificats émis.

59. Des questions juridiques peuvent se poser en cas certification croisée ou de chaînes de certificats, lorsque des politiques de sécurité multiples entrent en jeu. Il peut être nécessaire par exemple de déterminer quelle faute a causé une perte, ou aux garanties de qui s'est fié l'utilisateur. On notera que les règles juridiques envisagées dans certains pays prévoient que, lorsque les politiques en vigueur et les niveaux de sécurité sont connus des utilisateurs, et lorsqu'il n'y a pas négligence de la part des autorités de certification, il n'y a pas responsabilité.

60. Il peut incomber à l'autorité de certification ou à l'autorité racine de veiller à ce que ses prescriptions soient systématiquement respectées. Si la sélection des autorités de certification peut se faire sur la base d'un certain nombre de facteurs, dont la solidité de la clef publique utilisée et l'identité de l'utilisateur, la fiabilité de chacune d'entre elles peut également dépendre de la façon dont elle applique les normes de délivrance de certificats et de la fiabilité de son évaluation des données communiquées par les utilisateurs qui demandent des certificats. D'une importance toute particulière est le régime de responsabilité qui s'applique concernant le respect des prescriptions en matière de politique générale et de sécurité édictées par l'autorité racine ou par l'autorité de certification supérieure, ou de toute autre prescription applicable, et ce de manière permanente.

61. Lors de l'élaboration de la Loi type, les éléments énumérés ci-après ont été considérés comme des facteurs qui pourraient être pris en considération pour évaluer la fiabilité d'une autorité de certification: 1) indépendance (c'est-à-dire absence d'intérêts financiers ou autres dans les transactions sous-jacentes; 2) solidité et ressources financières permettant d'assumer le risque de devoir répondre d'un préjudice; 3) maîtrise de la technologie des clefs publiques et bonne connaissance des procédures de sécurité adéquates; 4) longévité (il peut en effet être demandé aux autorités de certification d'apporter le preuve de la fourniture de certificats ou de clefs de déchiffrement de nombreuses années après la fin de la transaction sous-jacente, par exemple dans le cadre d'une action en justice ou d'un litige relatif à la propriété); 5) approbation du matériel et du logiciel; 6) mise en place d'une piste d'audit et d'un audit par une entité indépendante; 7) existence d'un plan d'urgence (par exemple logiciel de "récupération après sinistre " ou mécanisme de "séquestre" de la clef); 8) sélection et gestion du personnel; 9) dispositif de protection pour la clef privée de l'autorité de certification; 10) sécurité interne; 11) dispositions pour la cessation d'activité, y compris notification aux utilisateurs; 12) garanties (données ou exclues); 13) limites de responsabilité; 14) assurance; 15) interopérabilité entre autorités de certification; 16) procédures de révocation (dans les cas où les clefs cryptographiques viendraient à être perdues ou compromises).

c) Résumé du processus de signature numérique

62. L'utilisation d'une signature numérique implique habituellement les opérations suivantes, effectuées soit par le signataire, soit par le destinataire du message signé numériquement:

1) L'utilisateur crée ou se voit attribuer une paire de clefs cryptographiques qui lui est propre;

2) L'expéditeur rédige un message (par exemple sous forme d'un courrier électronique) sur un ordinateur;

3) L'expéditeur établit un "abrégé" de son message à l'aide d'un algorithme de hachage sûr. La création de la signature numérique utilise un résultat de hachage découlant à la fois du message signé et d'une clef privée donnée et qui leur est unique. Pour que le résultat du hachage soit sécurisé, il est impératif qu'il n'y ait qu'une possibilité infime que la même signature numérique soit créée par la combinaison de tout autre message ou de toute autre clef;

4) L'expéditeur chiffre l'abrégé à l'aide de la clef privée. Celle-ci est appliquée au texte de l'abrégé à l'aide d'un algorithme mathématique. La signature numérique est constituée par l'abrégé ainsi chiffré;

5) L'expéditeur appose ou annexe généralement sa signature numérique au message;

6) L'expéditeur envoie sa signature numérique et le message (chiffré ou non) au destinataire par voie électronique;

7) Le destinataire utilise la clef publique de l'expéditeur pour vérifier la signature numérique de ce dernier. Cette vérification prouve que le message provient exclusivement dudit expéditeur;

8) Le destinataire crée lui aussi un "abrégé" du message à l'aide du même algorithme de hachage sûr;

9) Le destinataire compare les deux abrégés. S'ils sont identiques, il sait que le message n'a pas été modifié après avoir été signé. Même si le message a subi une très légère modification après avoir été signé numériquement, l'abrégé créé par le destinataire sera différent de celui créé par l'expéditeur;

10) Le destinataire reçoit de l'autorité de certification (ou par l'intermédiaire de l'auteur du message) un certificat qui confirme la signature numérique apposée au message de l'expéditeur. L'autorité de certification est généralement un tiers de confiance qui administre la certification dans le système de signature numérique. Le certificat contient la clef publique et le nom de l'expéditeur (éventuellement accompagnés de renseignements complémentaires) et est signé numériquement par l'autorité de certification.

IV. PRINCIPALES CARACTÉRISTIQUES DE LA LOI TYPE

A. Nature législative de la Loi type

63. La Loi type a été rédigée en partant du principe qu'elle devrait découler directement de l'article 7 de la Loi type de la CNUDCI sur le commerce électronique et être considérée comme un moyen de donner des renseignements détaillés sur la notion de "méthode fiable" utilisée pour identifier "une personne" et pour indiquer "qu'elle approuve l'information" contenue dans le message de données (voir A/CN.9/WG.IV/WP.71, par. 49).

64. La question de la forme que pourrait prendre l'instrument a été soulevée, et l'on a noté la nécessité d'étudier la relation entre la forme et le contenu. Différentes méthodes ont été proposées quant à ce que pourrait être cette forme, y compris des règles contractuelles, des dispositions législatives ou des principes directeurs destinés aux États envisageant d'adopter une législation sur les signatures électroniques. Il a été convenu, comme hypothèse de travail, que le texte devrait prendre la forme de règles législatives assorties d'un commentaire, et non simplement de principes directeurs (voir A/CN.9/437, par. 27; A/CN.9/446, par. 25; et A/CN.9/457, par. 51 et 72). Le texte a été finalement adopté sous forme de loi type (A/CN.9/483, par. 137 et 138).

B. Relations avec la Loi type de la CNUDCI sur le commerce électronique

1. La nouvelle Loi type comme instrument juridique distinct

65. Les nouvelles dispositions auraient pu être incorporées dans une version augmentée de la Loi type de la CNUDCI sur le commerce électronique, par exemple pour former une nouvelle troisième partie. Afin d'indiquer clairement que la nouvelle Loi type pourrait être adoptée soit de façon indépendante, soit en combinaison avec la Loi type sur le commerce électronique, il a été finalement décidé qu'elle serait établie en tant qu'instrument juridique distinct (voir A/CN.9/465, par. 37). Cette décision découle essentiellement du fait qu'au moment où elle était finalisée, la Loi type sur le commerce électronique avait déjà été appliquée avec succès dans plusieurs pays et que de nombreux autres envisageaient de l'adopter. L'élaboration d'une version augmentée de cet instrument aurait pu compromettre le succès de la version originale en donnant à penser qu'il était nécessaire d'améliorer ce texte au moyen d'une mise à jour. En outre, l'élaboration d'une nouvelle version de la Loi type sur le commerce électronique aurait pu introduire une confusion dans les pays qui l'avaient récemment adoptée.

2. Pleine conformité de la nouvelle Loi type avec la Loi type de la CNUDCI sur le commerce électronique

66. Lors de l'élaboration de la nouvelle Loi type, tout a été mis en œuvre pour assurer une cohérence aussi bien avec le fond qu'avec la terminologie de la Loi type sur le commerce électronique (voir A/CN.9/465, par. 37). Les dispositions générales de cette dernière ont été reproduites dans le nouvel instrument, à savoir l'article premier (Champ d'application); les alinéas a), c) et e) de l'article 2 (Définitions de

"message de données", "expéditeur" et "destinataire"), et les articles 3 (Interprétation), 4 (Dérogation conventionnelle) et 7 (Signature).

67. S'inspirant de la Loi type de la CNUDCI sur le commerce électronique, le nouvel instrument traduit en particulier le principe de la neutralité quant aux techniques employées; une approche ne désavantageant pas les équivalents fonctionnels des concepts et pratiques traditionnels fondés sur le papier et une large place donnée à l'autonomie des parties (A/CN.9/WG.IV/WP.84, par. 16). Il devrait servir à la fois de normes minimales dans un environnement "ouvert" (c'est-à-dire où les parties communiquent par des moyens électroniques sans convention préalable) et de dispositions contractuelles types dans un environnement "fermé" (c'est-à-dire où les parties sont liées par des règles et procédures contractuelles préexistantes qu'elles doivent suivre lorsqu'elles communiquent par des moyens électroniques).

3. Relations avec l'article 7 de la Loi type de la CNUDCI sur le commerce électronique

68. Lors de l'élaboration de la nouvelle Loi type, il a été déclaré que la référence à l'article 7 de la Loi type de la CNUDCI sur le commerce électronique dans l'article 6 du nouvel instrument devait être interprétée comme limitant le champ d'application de cet instrument aux cas dans lesquels une signature électronique était utilisée pour satisfaire à une prescription légale impérative selon laquelle certains documents devaient être signés pour être valides. Dans la mesure où la plupart des pays avaient dans leur législation très peu de prescriptions de ce type applicables aux documents utilisés dans les transactions commerciales, le champ d'application de la nouvelle Loi type était très étroit. On a généralement convenu, en réponse à cet argument, que cette interprétation de l'article 6 (et de l'article 7 de la Loi type sur le commerce électronique) était incompatible avec l'interprétation du terme "loi" adoptée par la Commission au paragraphe 68 du Guide pour l'incorporation de la Loi type sur le commerce électronique, selon laquelle "le terme 'loi' doit être interprété comme renvoyant non seulement aux dispositions législatives et réglementaires mais également aux règles découlant de la jurisprudence et autres règles processuelles". En fait, le champ d'application tant de l'article 7 de la Loi type sur le commerce électronique que de l'article 6 de la nouvelle Loi type est particulièrement vaste dans la mesure où la plupart des documents utilisés dans le contexte de transactions commerciales devraient probablement, dans la pratique, satisfaire aux exigences du droit de la preuve concernant la preuve écrite (A/CN.9/465, par. 67).

C. Règles "cadres" devant être complétées par des règlements techniques et par contrat

69. En tant que supplément à la Loi type de la CNUDCI sur le commerce électronique, la nouvelle Loi type a pour objet d'exposer des principes essentiels devant faciliter l'utilisation des signatures électroniques. Cependant, en tant que "cadre", elle n'énonce pas toutes les règles et tous les règlements qui peuvent être nécessaires (en sus des arrangements contractuels entre utilisateurs) pour appliquer ces techniques dans un État adoptant. Qui plus est, comme l'indique le présent

Guide, elle n'a pas pour objet de couvrir chaque aspect de l'utilisation des signatures électroniques. En conséquence, un État adoptant pourra souhaiter compléter par un règlement les procédures autorisées par la Loi type et prendre ainsi en compte la situation particulière, et peut-être en évolution, qui y prévaut, sans compromettre les objectifs de la Loi type. Il est recommandé à tout État adoptant qui déciderait d'adopter un tel règlement d'accorder une attention particulière à la nécessité de maintenir une certaine souplesse dans l'utilisation des systèmes de signature électronique par leurs utilisateurs.

70. On notera que les techniques de signature électronique envisagées dans la Loi type, outre qu'elles soulèvent des questions de procédure qu'il pourrait être nécessaire de traiter dans le règlement technique d'application, peuvent poser certains problèmes juridiques dont la réponse ne se trouvera pas nécessairement dans cet instrument, mais plutôt dans d'autres branches du droit, dont, par exemple, les textes applicables de droit administratif, contractuel, pénal et de procédure judiciaire, que la Loi type n'a pas vocation à traiter.

D. Certitude supplémentaire quant aux effets juridiques des signatures électroniques

71. L'une des principales caractéristiques de la nouvelle Loi type est de conférer davantage de certitude à l'application des critères souples énoncés à l'article 7 de la Loi type de la CNUDCI sur le commerce électronique s'agissant de la reconnaissance d'une signature électronique comme équivalent fonctionnel d'une signature manuscrite. L'article 7 de la Loi type de la CNUDCI sur le commerce électronique est rédigé comme suit:

> "1. Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données:
>
> *a)* Si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données; et
>
> *b)* Si la fiabilité de cette méthode est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière.
>
> 2. Le paragraphe 1 s'applique que l'exigence qui y est visée ait la forme d'une obligation ou que la loi prévoie simplement certaines conséquences s'il n'y a pas de signature.
>
> 3. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...]".

72. L'article 7 est fondé sur la reconnaissance des fonctions remplies par une signature dans un environnement papier. Lors de l'élaboration de la Loi type de la CNUDCI sur le commerce électronique, les fonctions ci-après d'une signature ont été envisagées: identifier une personne; apporter la certitude de la participation personnelle de cette personne à l'acte de signer; associer cette personne à la teneur d'un document. On a noté que la signature pouvait en outre remplir diverses autres fonctions, selon la nature du document. Par exemple, elle pouvait attester l'intention

d'une partie d'être liée par le contrat qu'elle avait signé; l'intention d'une personne de revendiquer la paternité d'un texte; l'intention d'une personne de s'associer à la teneur d'un document écrit par quelqu'un d'autre; le fait qu'une personne s'était rendue en un lieu donné, à un moment donné.

73. Afin de garantir qu'un message devant être authentifié ne puisse se voir refuser valeur juridique du simple fait qu'il n'a pas été authentifié de la manière voulue pour les documents sur papier, une formule générale a été retenue pour l'article 7. Cet article définit les conditions générales dans lesquelles les messages de données seraient réputés authentifiés avec suffisamment de crédibilité et seraient opposables au vu des exigences en matière de signature entravant actuellement le commerce électronique. L'article 7 s'attache aux deux fonctions essentielles d'une signature, à savoir l'identification de l'auteur d'un document et la confirmation que l'auteur approuve la teneur dudit document. Le paragraphe 1 a) énonce le principe selon lequel, dans un environnement électronique, les fonctions juridiques essentielles d'une signature sont respectées par une méthode qui permet d'identifier l'expéditeur d'un message de données et de confirmer que l'expéditeur approuve la teneur de ce message de données.

74. Le paragraphe 1 b) institue une approche souple en ce qui concerne le degré de sécurité que doit garantir la méthode d'identification utilisée au paragraphe 1 a). La méthode utilisée en vertu du paragraphe 1 a) devrait être aussi fiable que cela est approprié au vu de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris tout accord entre l'expéditeur et le destinataire du message de données.

75. Pour déterminer si la méthode utilisée en vertu du paragraphe 1 est appropriée, les facteurs juridiques, techniques et commerciaux à prendre en considération sont les suivants: 1) le degré de perfectionnement du matériel utilisé par chacune des parties; 2) la nature de leur activité commerciale; 3) la fréquence avec laquelle elles effectuent entre elles des opérations commerciales; 4) la nature et l'ampleur de l'opération; 5) le statut et la fonction de la signature dans un régime législatif et réglementaire donné; 6) la capacité des systèmes de communication; 7) le respect des procédures d'authentification établies par les intermédiaires; 8) la série de procédures d'authentification communiquée par tout intermédiaire; 9) l'observation des habitudes et pratiques commerciales; 10) l'existence de mécanismes d'assurance contre les messages non autorisés; 11) l'importance et la valeur de l'information contenue dans le message de données; 12) la disponibilité d'autres méthodes d'identification et le coût de leur mise en œuvre; 13) le degré d'acceptation ou de non-acceptation de la méthode d'identification dans le secteur ou domaine pertinent, tant au moment où la méthode a été convenue qu'à celui où le message de données a été communiqué; et 14) tout autre facteur pertinent (Guide pour l'incorporation de la Loi type de la CNUDCI sur le commerce électronique, par. 53 et 56 à 58).

76. S'appuyant sur le critère souple énoncé à l'article 7-1 b) de la Loi type de la CNUDCI sur le commerce électronique, les articles 6 et 7 de la nouvelle Loi type établissent un mécanisme par lequel les signatures électroniques qui satisfont à des critères objectifs de fiabilité technique peuvent bénéficier d'une détermination rapide quant à leur efficacité juridique. La Loi type a pour effet de reconnaître deux catégories de signatures électroniques. La première, et la plus large, est celle décrite à l'article 7 de la Loi type de la CNUDCI sur le commerce électronique. Elle comprend toute "méthode" pouvant être utilisée pour satisfaire à une exigence

légale de signature manuscrite. L'efficacité juridique d'une telle "méthode" comme équivalent d'une signature manuscrite dépend de la démonstration de sa "fiabilité" à un juge des faits. La seconde catégorie, plus étroite, est celle créée par la Loi type. Elle comprend des méthodes de signature électronique qui peuvent être reconnues par une autorité publique, une entité privée accréditée, ou les parties elles-mêmes comme satisfaisant aux exigences de fiabilité technique énoncées dans la Loi type. L'avantage d'une telle reconnaissance est la sécurité qu'elle apporte aux utilisateurs de ces techniques de signature électronique (parfois appelées "renforcées", "sécurisées" ou "qualifiées") avant que ceux-ci ne les utilisent effectivement.

E. Règles fondamentales de conduite applicables aux parties concernées

77. La Loi type ne traite pas en détail des questions de responsabilité qui peuvent intéresser les différentes parties prenant part au fonctionnement de systèmes de signature électronique. Ces questions relèvent de la loi applicable en dehors de la Loi type. Cependant, cette dernière fixe des critères permettant d'évaluer la conduite desdites parties, c'est-à-dire le signataire, la partie se fiant à la signature et le prestataire de services de certification.

78. En ce qui concerne le signataire, la Loi type part du principe de base qu'il doit prendre des dispositions raisonnables à l'égard de son dispositif de signature électronique. Il doit normalement prendre des dispositions raisonnables pour éviter toute utilisation non autorisée de ce dispositif. Lorsqu'il sait ou aurait dû savoir que le dispositif a été compromis, il doit en informer sans tarder toute personne dont on peut raisonnablement penser qu'elle se fiera à la signature électronique ou offrira des services étayant cette signature. Lorsqu'un certificat est utilisé pour étayer la signature électronique, le signataire doit prendre des dispositions raisonnables pour garantir l'exactitude et l'exhaustivité de toutes les déclarations essentielles faites par lui en rapport avec le certificat.

79. Une partie se fiant à une signature électronique doit prendre des mesures raisonnables pour vérifier la fiabilité de cette signature. Lorsque cette signature est étayée par un certificat, la partie se fiant à la signature doit prendre des mesures raisonnables pour vérifier la validité, la suspension ou la révocation du certificat, et tenir compte de toute restriction dont il peut être assorti.

80. Il incombe, en règle générale, à un prestataire de services de certification d'utiliser des systèmes, des procédures et des ressources humaines fiables, et d'agir en conformité avec les déclarations qu'il fait s'agissant de sa politique et de ses pratiques. En outre, le prestataire de services de certification doit prendre des dispositions raisonnables pour garantir l'exactitude et l'exhaustivité de toutes les déclarations essentielles faites par lui en rapport avec le certificat. Dans ce document, il doit fournir des renseignements essentiels permettant à la partie se fiant à la signature de l'identifier. Il doit également déclarer: 1) que la personne qui est identifiée dans le certificat contrôlait le dispositif de signature au moment de la signature; et 2) que le dispositif de signature était opérationnel à la date ou avant la date à laquelle le certificat a été émis. Lorsqu'il traite avec la partie se fiant à la signature, il doit fournir des renseignements supplémentaires concernant: 1) la méthode utilisée pour identifier le signataire; 2) toute restriction apportée à l'objet ou à la valeur pour lequel ou laquelle le dispositif de signature ou le certificat peut

être utilisé; 3) l'état opérationnel du dispositif de signature; 4) toute restriction apportée au champ d'application ou à la portée de la responsabilité du prestataire de services de certification; 5) le fait de savoir si le signataire a ou non les moyens de notifier qu'un dispositif de signature a été compromis; et 6) le fait de savoir si un service de révocation rapide est offert ou non.

81. Pour faciliter l'évaluation de la fiabilité des systèmes, des procédures et des ressources humaines utilisés par le prestataire de services de certification, la Loi type fournit une liste non exhaustive de facteurs indicatifs.

F. Un cadre neutre quant aux techniques employées

82. Compte tenu de la rapidité des progrès techniques, la Loi type prévoit la reconnaissance juridique des signatures électroniques quelle que soit la technologie employée (signatures numériques fondées sur la cryptographie asymétrique; biométrie; utilisation de numéros d'identification personnels (codes PIN); versions numérisées des signatures manuscrites et autres méthodes comme celle consistant à cliquer sur la case "valider".

V. ASSISTANCE DU SECRÉTARIAT DE LA CNUDCI

A. Aide à l'élaboration d'une législation

83. Dans le cadre de ses activités de formation et d'assistance, le secrétariat de la CNUDCI peut aider les États, par des consultations techniques, à élaborer une législation sur la base de la Loi type de la CNUDCI sur les signatures électroniques. La même assistance est offerte aux États qui envisagent d'adopter une législation fondée sur d'autres lois types de la CNUDCI (à savoir la Loi type sur l'arbitrage commercial international, la Loi type sur les virements internationaux, la Loi type sur la passation des marchés de biens, de travaux et de services, la Loi type sur le commerce électronique et la Loi type sur l'insolvabilité internationale), ou qui envisagent d'adhérer à l'une des conventions de droit commercial international élaborées par la CNUDCI.

84. Pour tout renseignement complémentaire concernant la Loi type et les autres lois types et conventions élaborées par la CNUDCI, on peut s'adresser au secrétariat à l'adresse suivante:

Service du droit commercial international, Bureau des affaires juridiques
Organisation des Nations Unies
Centre international de Vienne
B.P. 500
A-1400 Vienne (Autriche)

Téléphone:	(+43-1) 26060-4060 ou 4061
Télécopie:	(+43-1) 26060-5813
Adresse électronique:	uncitral@uncitral.org
Site Internet:	http://www.uncitral.org

B. Renseignements sur l'interprétation des textes législatifs fondés sur la Loi type

85. Le secrétariat apprécie toute observation concernant la Loi type et le Guide, ainsi que tous renseignements concernant l'adoption de textes législatifs fondés sur la Loi type. Une fois incorporé, cet instrument sera inclus dans le système d'information sur la jurisprudence relative aux instruments de la CNUDCI, qui rassemble et diffuse des informations sur la jurisprudence relative aux conventions et lois types émanant de la CNUDCI. Ce système a pour but de faire connaître au niveau international les textes législatifs élaborés par la CNUDCI et de faciliter leur interprétation et leur application uniformes. Le secrétariat publie, dans les six langues officielles de l'Organisation des Nations Unies, des résumés de décisions et met à disposition, contre remboursement des frais de reproduction, les décisions à partir desquelles les résumés ont été établis. Le système est expliqué dans un guide de l'utilisateur disponible auprès du secrétariat sous forme imprimée (A/CN.9/SER.C/GUIDE/1) ainsi que sur le site Internet susmentionné.

Chapitre II. Observations article par article

Titre

“Loi type”

86. Pendant toute son élaboration, l’instrument a été conçu comme un complément de la Loi type de la CNUDCI sur le commerce électronique devant être traité sur un pied d’égalité et avoir la même nature juridique que celui qui l’a précédé.

Article premier. Champ d’application

La présente Loi s’applique lorsque des signatures électroniques sont utilisées dans le contexte* d’activités commerciales**. Elle ne se substitue à aucune règle de droit visant à protéger le consommateur.

*La Commission propose le texte suivant aux États qui souhaiteraient étendre l’applicabilité de la présente Loi:

“La présente Loi s’applique lorsque des signatures électroniques sont utilisées, sauf dans les situations suivantes: [...].”

**Le terme “commerciales” devrait être interprété au sens large, comme désignant toute relation d’ordre commercial, quelle soit contractuelle ou non contractuelle. Les relations d’ordre commercial comprennent, sans s’y limiter, les transactions suivantes: fourniture ou échange de marchandises ou de services; accord de distribution; représentation commerciale; affacturage; crédit-bail; construction d’usines; services consultatifs; ingénierie; licence; investissement; financement; opération bancaire; assurance; accord d’exploitation ou concession; coentreprise et autres formes de coopération industrielle ou commerciale; transport de marchandises ou de voyageurs par voie aérienne ou maritime, par chemin de fer ou par route.

Observations générales

87. L’article premier a pour objet de délimiter le champ d’application de la Loi type. L’approche retenue dans cette dernière consiste à couvrir en principe toutes les situations de fait dans lesquelles des signatures électroniques sont utilisées, indépendamment du type de signature électronique ou de la technique d’authentification appliquée. Il a été estimé au cours de l’élaboration de la Loi type que l’exclusion d’une forme ou d’un support quelconque par la limitation du champ d’application de l’instrument pourrait soulever des difficultés pratiques et serait contraire à l’intention d’élaborer des règles véritablement neutres quant à la technique utilisée. Toutefois, une attention spéciale a été accordée aux “signatures numériques”, c’est-à-dire aux signatures électroniques obtenues par l’application d’une cryptographie à double clef, que le Groupe de travail de la CNUDCI sur le commerce électronique a considéré comme une technologie particulièrement répandue. La Loi type est axée sur l’utilisation des technologies modernes et, sauf si elle l’indique expressément, elle n’est pas censée modifier les règles traditionnelles concernant les signatures manuscrites.

*Note de bas de page***

88. Il a été estimé que la Loi type devait indiquer qu'elle était axée sur les situations rencontrées dans le domaine commercial et qu'elle avait été élaborée en fonction des relations commerciales et financières. C'est pour cette raison que l'article premier fait référence aux "activités commerciales" et donne à la note de bas de page** des indications sur ce que cela signifie. Ces précisions, qui peuvent être particulièrement utiles pour les pays qui ne disposent pas d'un corpus distinct de droit commercial, reprennent, pour des raisons de cohérence, la note de bas de page qui correspond à l'article premier de la Loi type de la CNUDCI sur l'arbitrage commercial international (également reproduite en tant que note de bas de page**** correspondant à l'article premier de la Loi type de la CNUDCI sur le commerce électronique). Dans certains pays, l'emploi de notes de bas de page dans un texte réglementaire ne serait pas considéré comme une pratique législative acceptable. Les autorités nationales qui mettent en œuvre la Loi type pourront donc envisager d'inclure éventuellement le texte de ces notes dans le corps même du texte.

*Note de bas de page**

89. La Loi type s'applique à tous les types de messages de données auxquels est attachée une signature électronique légalement significative, et rien dans cette Loi ne devrait empêcher à un État d'élargir son champ d'application pour couvrir les utilisations des signatures électroniques en dehors du domaine commercial. Par exemple, bien que la Loi type ne porte pas principalement sur les relations entre utilisateurs de signatures électroniques et pouvoirs publics, elle ne devrait pas leur être inapplicable. La note de bas de page* propose une variante qui pourrait être utilisée par les États qui jugeraient approprié d'élargir le champ d'application de la Loi type au-delà du domaine commercial.

Protection du consommateur

90. Certains pays ont adopté des lois particulières sur la protection du consommateur qui peuvent régir certains aspects de l'utilisation des systèmes d'information. S'agissant de cette législation sur les consommateurs, il a été estimé, comme pour les instruments précédents de la CNUDCI (par exemple la Loi type de la CNUDCI sur les virements internationaux et la Loi type de la CNUDCI sur le commerce électronique), qu'il conviendrait d'indiquer dans la Loi type que celle-ci avait été rédigée sans que soit accordée une attention particulière aux questions qui pourraient se poser dans le contexte de la protection des consommateurs. En même temps, on a estimé qu'il n'y avait aucune raison d'exclure du champ d'application, au moyen d'une disposition générale, les situations faisant intervenir des consommateurs, d'autant que les dispositions de la Loi type pourraient être jugées très bénéfiques pour la protection des consommateurs, en fonction de la législation adoptée dans chaque État. L'article premier reconnaît donc que cette législation relative à la protection du consommateur peut prévaloir sur les dispositions de la Loi type. Si les législateurs parviennent à des conclusions différentes quant à l'effet bénéfique de la Loi type sur les opérations impliquant des consommateurs dans un pays donné, ils pourront envisager d'exclure les consommateurs du champ d'application du texte législatif incorporant la Loi type. La détermination des personnes physiques ou morales qui devraient être considérées comme des "consommateurs" relève de la législation applicable en dehors de la Loi type.

Utilisation des signatures électroniques dans les transactions internationales et nationales

91. Il est recommandé que l'application de la Loi type soit aussi large que possible. Il faudrait faire preuve d'une prudence particulière avant d'exclure cette application en limitant la portée du texte aux utilisations internationales des signatures électroniques, car on pourrait considérer qu'une telle limitation ne permet pas d'atteindre pleinement les objectifs de la Loi type. En outre, la diversité des procédures applicables en vertu de cette loi pour limiter au besoin l'utilisation des signatures électroniques (par exemple, pour des raisons d'ordre public), rend moins indispensable une limitation de son champ d'application. La sécurité juridique qu'offrira la Loi type est nécessaire pour les échanges commerciaux tant nationaux qu'internationaux, et l'existence de deux régimes régissant l'utilisation des signatures électroniques pourrait sérieusement entraver le recours à de telles techniques.

Références aux documents de la CNUDCI

A/CN.9/467, par. 22 à 24;
A/CN.9/WG.IV/WP.84, par. 22;
A/CN.9/465, par. 36 à 42;
A/CN.9/WG.IV/WP.82, par. 21;
A/CN.9/457, par. 53 à 64.

Article 2. Définitions

Aux fins de la présente Loi:

a) Le terme "signature électronique" désigne des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue;

b) Le terme "certificat" désigne un message de données ou un autre enregistrement confirmant le lien entre un signataire et des données afférentes à la création de signatures;

c) Le terme "message de données" désigne l'information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie;

d) Le terme "signataire" désigne une personne qui détient des données afférentes à la création de signatures et qui agit soit pour son propre compte, soit pour celui de la personne qu'elle représente;

e) Le terme "prestataire de services de certification" désigne une personne qui émet des certificats et peut fournir d'autres services liés aux signatures électroniques;

f) Le terme "partie se fiant à la signature ou au certificat" désigne une personne qui peut agir sur la base d'un certificat ou d'une signature électronique.

Définition du terme "Signature électronique"

La signature électronique comme équivalent fonctionnel de la signature manuscrite

92. La notion de "signature électronique" est censée englober toutes les utilisations classiques d'une signature manuscrite destinée à produire des effets juridiques, l'identification du signataire et l'intention de signer en tant que le plus petit commun dénominateur des différentes conceptions de la "signature" que l'on trouve dans les divers systèmes juridiques. Ces fonctions d'une signature manuscrite ont déjà été examinées dans le contexte de l'élaboration de l'article 7 de la Loi type sur le commerce électronique. Par conséquent, définir une signature électronique comme capable d'indiquer l'approbation d'informations revient essentiellement à établir une condition préalable d'ordre technique pour la reconnaissance d'une technologie donnée comme capable de créer un équivalent d'une signature manuscrite. La définition ne fait pas abstraction du fait que des technologies couramment appelées "signatures électroniques" peuvent servir à d'autres fins que la création d'une signature ayant une valeur juridique; elle illustre simplement l'accent mis dans la Loi type sur l'utilisation de signatures électroniques comme équivalents fonctionnels des signatures manuscrites (voir A/CN.9/483, par. 62).

Autres utilisations possibles d'une signature électronique

93. Une distinction devrait être établie entre la notion juridique de "signature" et la notion technique de "signature électronique", terme technique visant des pratiques qui ne supposent pas nécessairement la production de signatures ayant une valeur juridique. Lors de l'élaboration de la Loi type, il a été estimé qu'il fallait appeler l'attention des utilisateurs sur le risque de confusion qui pourrait résulter de l'utilisation du même outil technique pour la production d'une signature ayant une valeur juridique et pour d'autres fonctions d'authentification et d'identification (ibid.).

Définition du terme "Certificat"

Nécessité d'une définition

94. Le sens du terme "certificat" tel qu'employé dans le contexte de certains types de signatures électroniques et tel que défini dans la Loi type diffère peu de son sens général de document par lequel une personne confirme certains faits. Toutefois, étant donné que la notion générale de "certificat" n'existe pas dans tous les systèmes juridiques, voire dans toutes les langues, il a été jugé utile d'inclure une définition dans le contexte de la Loi type (ibid., par. 65).

Objet d'un certificat

95. Le certificat a pour objet de reconnaître, montrer ou confirmer un lien entre les données afférentes à la création de signature et le signataire. Ce lien est créé lorsque ces données sont générées (ibid., par. 67).

"Données afférentes à la création de signatures"

96. Le terme "données afférentes à la création de signature" désigne les clefs secrètes, codes ou autres éléments qui, dans le processus de création d'une signature électronique, sont utilisées pour établir un lien sûr entre la signature électronique

résultante et la personne du signataire. Par exemple, dans le contexte des signatures numériques s'appuyant sur la cryptographie asymétrique, l'élément principal qui peut être décrit comme "lié exclusivement au signataire" est la paire de clefs cryptographiques. Dans le contexte des signatures électroniques s'appuyant sur des dispositifs biométriques, l'élément essentiel serait l'indicateur biométrique, tel qu'une empreinte digitale ou des données de balayage de la rétine. La définition porte uniquement sur les éléments essentiels devant demeurer confidentiels pour garantir la qualité du processus de signature, à l'exclusion de tout autre élément qui, quoique pouvant contribuer au processus de signature, pourrait être révélé sans compromettre pour autant la fiabilité de la signature électronique en résultant. Ainsi, dans le cas des signatures numériques, si la clef publique comme la clef privée sont liées à la personne du signataire, seule la clef privée doit être visée par la définition puisqu'elle seule doit demeurer confidentielle et que la clef publique doit par nature être mise à la disposition du public (A/CN.9/483, par. 71). Parmi les éléments à ne pas inclure dans la définition, le texte signé électroniquement, quoique jouant également un rôle important dans le processus de création de signature (par une fonction de hachage ou autrement) ne doit manifestement pas être soumis à la même confidentialité que l'information qui identifie le signataire (ibid., par. 72 et 76). L'article 6 exprime l'idée que les données afférentes à la création de signature devraient être liées exclusivement au signataire (ibid., par. 75).

Définitions du terme "Message de données"

97. La définition du terme "message de données" est tirée de l'article 2 de la Loi type de la CNUDCI sur le commerce électronique en tant que notion large englobant tous les messages créés dans le contexte du commerce électronique, y compris le commerce par le Web (ibid., par. 69). La notion de "message de données" ne se limite pas aux données communiquées mais englobe aussi les données enregistrées sur ordinateur qui ne sont pas destinées à être communiquées. La notion de "message" inclut donc celle d'"enregistrement".

98. La référence à des "moyens analogues" vise à tenir compte du fait que la Loi type n'a pas été conçue uniquement pour être applicable dans le contexte des techniques de communication existantes, mais aussi pour tenir compte des progrès techniques prévisibles. La définition du terme "message de données" a pour but d'englober tous les types de message créés, stockés, ou envoyés essentiellement sans support papier. À cette fin, tous les moyens de communication et de stockage d'informations qui peuvent être utilisés pour des fonctions parallèles à celles qui sont assurées grâce aux moyens énumérés dans la définition sont censés être englobés dans les termes "moyens analogues", même si des moyens de communication "électroniques" et "optiques", par exemple, peuvent ne pas être à proprement parler analogues. Aux fins de la Loi type, le terme "analogue" signifie "fonctionnellement équivalent".

99. La définition du terme "message de données" doit aussi s'appliquer en cas de révocation ou de modification. Un message de données est présumé contenir des informations fixes, mais il peut être révoqué ou modifié par un autre message de données (Guide pour l'incorporation de la Loi type de la CNUDCI sur le commerce électronique, par. 30 à 32).

Définition du terme "Signataire"

"une personne"

100. Conformément à l'approche adoptée pour la Loi type de la CNUDCI sur le commerce électronique, toute référence, dans la nouvelle loi, à une "personne" devrait être interprétée comme visant tous les types de personnes ou d'entités, qu'il s'agisse de personnes physiques, de personnes morales ou d'autres entités juridiques (A/CN.9/483, par. 86).

"au nom de la personne qu'elle représente"

101. L'analogie avec des signatures manuscrites n'est peut-être pas toujours appropriée pour tirer parti des possibilités qu'offrent les techniques modernes. Dans un environnement papier, par exemple, des personnes morales ne peuvent être, à proprement parler, signataires de documents établis en leur nom, parce que seules des personnes physiques peuvent apposer des signatures manuscrites authentiques. Par contre, on peut concevoir que des signatures électroniques soient attribuables à des sociétés ou à d'autres personnes morales (y compris des administrations ou d'autres organismes publics), et il se peut, dans certains cas, que l'identité de la personne qui crée effectivement la signature, lorsqu'une intervention humaine est nécessaire, soit sans intérêt aux fins pour lesquelles la signature est créée (ibid., par. 85).

102. Néanmoins, en vertu de la Loi type, la notion de "signataire" ne peut être dissociée de la personne ou de l'entité qui crée effectivement la signature électronique, puisque plusieurs obligations propres aux signataires en vertu de cette loi sont logiquement liées au contrôle effectif des données afférentes à la création de signature. Toutefois, afin de tenir compte des cas où le signataire agirait en tant que représentant d'une autre personne, l'expression "soit pour celui de la personne qu'elle représente" a été retenue dans la définition du "signataire". La mesure dans laquelle une personne serait liée par une signature électronique créée "pour son compte" doit être réglée conformément à la loi régissant, selon qu'il convient, les relations juridiques entre le signataire et la personne pour le compte de qui la signature électronique est créée, d'une part, et la partie qui se fie à cette signature, d'autre part. Cette question, ainsi que d'autres relatives à la transaction sous-jacente, y compris les questions de représentation et celle de savoir à qui (du signataire ou de la personne représentée par lui) incombe en dernier ressort la responsabilité d'un manquement par le signataire aux obligations résultant de l'article 8, n'entrent pas dans le champ d'application de la Loi type (ibid., par. 86 et 87).

Définition du terme "Prestataire de services de certification"

103. Le prestataire de service de certification tel que défini aux fins de la Loi type devra fournir au minimum des services de certification, et éventuellement d'autres services (ibid., par. 100).

104. Aucune distinction n'a été faite dans la Loi type entre les cas où un prestataire de services de certification fournit lesdits services dans le cadre de son activité principale ou en fait une activité auxiliaire, habituelle ou occasionnelle, directement ou par l'intermédiaire d'un sous-traitant. La définition vise toutes les entités qui fournissent des services de certification dans le cadre de la Loi type, c'est-à-dire "dans le contexte d'activités commerciales". Toutefois, étant donné la limitation du

champ d'application de la Loi type, les entités qui émettent des certificats à des fins internes et non à des fins commerciales n'entreraient pas dans la catégorie des "prestataires de services de certification" tels que définis à l'article 2 (ibid., par. 94 à 99).

Définition du terme "Partie se fiant à la signature ou au certificat"

105. La définition du terme "partie se fiant à la signataire ou au certificat" vise à assurer une symétrie dans la définition des diverses parties impliquées dans le fonctionnement des mécanismes de signature électronique régis par la Loi type (ibid., par. 107). Aux fins de cette définition, le mot "agir" devrait être interprété au sens large comme renvoyant non seulement à un acte mais également à une omission (ibid., par. 108).

Références aux documents de la CNUDCI

A/CN.9/483, par. 59 à 109;
A/CN.9/WG.IV/WP.84, par. 23 à 36;
A/CN.9/465, par. 42;
A/CN.9/WG.IV/WP.82, par. 22 à 33;
A/CN.9/457, par. 22 à 47; 66 et 67; 89; 109;
A/CN.9/WG.IV/WP.80, par. 7 à 10;
A/CN.9/WG.IV/WP.79, par. 21;
A/CN.9/454, par. 20;
A/CN.9/WG.IV/WP.76, par. 16 à 20;
A/CN.9/446, par. 27 à 46 (projet d'article premier), 62 à 70 (projet d'article 4), 113 à 131 (projet d'article 8), 132 et 133 (projet d'article 9);
A/CN.9/WG.IV/WP.73, par. 16 à 27, 37 et 38, 50 à 57, et 58 à 60;
A/CN.9/437, par. 29 à 50, et 90 à 113 (projets d'articles A, B et C); et
A/CN.9/WG.IV/WP.71, par. 52 à 60.

Article 3. Égalité de traitement des techniques de signature

Aucune disposition de la présente Loi, à l'exception de l'article 5, n'est appliquée de manière à exclure, restreindre ou priver d'effets juridiques une quelconque méthode de création de signature électronique satisfaisant aux exigences mentionnées au paragraphe 1 de l'article 6 ou autrement satisfaisant aux exigences de la loi applicable.

Neutralité technique

106. L'article 3 consacre le principe fondamental selon lequel aucune méthode de signature électronique ne devrait faire l'objet d'une discrimination, c'est-à-dire qu'il faudrait donner à toutes les techniques la même possibilité de satisfaire aux exigences de l'article 6. En conséquence, il ne devrait pas y avoir de différence de traitement entre les messages signés électroniquement et les documents sur papier portant des signatures manuscrites, ni entre divers types de messages signés électroniquement, à condition qu'ils satisfassent aux exigences fondamentales énoncées au paragraphe 1 de l'article 6 de la Loi type ou à toute autre exigence énoncée dans la loi applicable. Ces exigences peuvent, par exemple, prescrire l'utilisation d'une technique de signature spécifiquement désignée dans des situations particulières, ou bien fixer autrement une norme qui pourrait être supérieure ou

inférieure à celle qui est énoncée à l'article 7 de la Loi type de la CNUDCI sur le commerce électronique (et à l'article 6 de la Loi type). Le principe fondamental de non-discrimination est destiné à trouver une application générale. Il convient toutefois de noter qu'un tel principe n'est pas censé porter atteinte à la liberté contractuelle reconnue à l'article 5. Les parties devraient donc rester libres entre elles et dans la mesure permise par la loi, d'exclure par convention l'utilisation de certaines techniques de signature électronique. En énonçant qu'"aucune disposition de la présente Loi n'est appliquée de manière à exclure, restreindre ou priver d'effets juridiques une quelconque méthode de création de signature électronique", l'article 3 indique simplement que la forme sous laquelle est appliquée une signature électronique donnée ne peut être invoquée comme seul motif de lui refuser l'efficacité juridique. Il ne faudrait toutefois pas interpréter de façon erronée l'article 3 comme établissant la validité juridique de n'importe quelle technique de signature ou information signée électroniquement.

Références aux documents de la CNUDCI

A/CN.9/476, par. 25 à 32;
A/CN.9/WG.IV/WP.84, par. 37;
A/CN.9/465, par. 43 à 48;
A/CN.9/WG.IV/WP.82, par. 34;
A/CN.9/457, par. 53 à 64.

Article 4. Interprétation

1. Pour l'interprétation de la présente Loi, il est tenu compte de son origine internationale et de la nécessité de promouvoir l'uniformité de son application et le respect de la bonne foi.

2. Les questions concernant les matières régies par la présente Loi qui ne sont pas expressément réglées par elle sont tranchées selon les principes généraux dont elle s'inspire.

Source

107. L'article 4 s'inspire de l'article 7 de la Convention des Nations Unies sur les contrats de vente internationale de marchandises et est repris de l'article 3 de la Loi type de la CNUDCI sur le commerce électronique. Il fournit des lignes directrices pour l'interprétation de la Loi type par les tribunaux d'arbitrage, les juridictions d'État et les autorités administratives nationales ou locales. Il devrait avoir pour effet de limiter la mesure dans laquelle un texte uniforme, une fois incorporé dans la législation locale, pourrait être interprété uniquement par référence aux concepts du droit local.

Paragraphe 1

108. Le paragraphe 1 a pour objet d'attirer l'attention de toute personne qui pourrait être appelée à appliquer la Loi type sur le fait que, même si, une fois adoptées, les dispositions de la Loi type (ou les dispositions de l'instrument d'application) faisaient partie intégrante de la législation interne et avaient donc un caractère national, elles devraient être interprétées compte tenu de leur origine internationale,

de façon à assurer l'uniformité de leur interprétation dans les différents pays adoptants.

Paragraphe 2

109. Parmi les principes généraux sur lesquels la Loi type est fondée, la liste non exhaustive ci-après pourrait être jugée applicable: 1) faciliter le commerce électronique entre les États et dans chaque État; 2) valider les opérations conclues au moyen des nouvelles technologies de l'information; 3) promouvoir et encourager de manière techniquement neutre l'application des nouvelles technologies de l'information en général et des signatures électroniques en particulier; 4) promouvoir l'uniformité du droit; et 5) appuyer les pratiques commerciales. Bien qu'ayant pour objectif général de faciliter l'utilisation des signatures électroniques, la Loi type ne doit en aucune façon être interprétée comme imposant cette utilisation.

Références aux documents de la CNUDCI

A/CN.9/467, par. 33 à 35;
A/CN.9/WG.IV/WP.84, par. 38;
A/CN.9/465, par. 49 et 50;
A/CN.9/WG.IV/WP.82, par. 35.

Article 5. Dérogation conventionnelle

Il est possible de déroger aux dispositions de la présente Loi ou d'en modifier les effets par convention, à moins que cette convention soit invalide ou sans effets en vertu de la loi applicable.

Respect de la loi applicable

110. La décision d'entreprendre l'élaboration de la Loi type s'est appuyée sur la reconnaissance du fait que, dans la pratique, c'est essentiellement dans des contrats que l'on recherche des solutions aux difficultés juridiques soulevées par l'utilisation des moyens modernes de communication. La Loi type a ainsi pour objet de soutenir le principe de l'autonomie des parties. La loi applicable, cependant, fixe parfois des limites à l'application de ce principe. L'article 5 ne devrait pas être interprété à tort comme autorisant les parties à déroger à des règles obligatoires, par exemple à des règles adoptées pour des raisons d'ordre public, comme encourageant les États à adopter des lois contraignantes qui limiteraient l'effet de l'autonomie des parties en matière de signatures électroniques, ou comme invitant de quelque autre façon les États à restreindre la liberté qu'ont les parties de s'entendre entre elles sur les critères de forme qui régissent leurs communications.

111. Le principe de l'autonomie des parties s'applique de façon large en ce qui concerne les dispositions de la Loi type, puisque cette dernière ne contient aucune disposition impérative. Ce principe s'applique également dans le contexte du paragraphe 1 de l'article 13. Dès lors, bien que les tribunaux de l'État adoptant ou les autorités chargées de l'application de la Loi type ne doivent pas nier ou annuler les effets juridiques d'un certificat étranger en raison uniquement du lieu où il a été émis, le paragraphe 1 de l'article 13 ne limite pas la liberté des parties à une transaction commerciale de convenir de l'utilisation de certificats émis en un lieu particulier (A/CN.9/483, par. 112).

Convention expresse ou implicite

112. Quant à la façon d'exprimer le principe de l'autonomie des parties dans l'article 5, il a généralement été admis, lors de l'élaboration de la Loi type, que la convention pourrait être expresse ou implicite. Le libellé de l'article 5 a été maintenu aligné sur celui de l'article 6 de la Convention des Nations Unies sur les contrats de vente internationale de marchandises (A/CN.9/467, par. 38).

Convention bilatérale ou multilatérale

113. L'article 5 a pour vocation de s'appliquer non seulement dans le contexte de relations entre des expéditeurs et des destinataires de messages de données, mais aussi dans le contexte de relations faisant intervenir des intermédiaires. Ainsi, il pourrait être dérogé aux dispositions de la Loi type soit par convention bilatérale ou multilatérale entre les parties, soit par des règles systémiques convenues par les parties. Normalement, la loi applicable limiterait l'autonomie des parties aux droits et obligations naissant entre les parties de façon à éviter toute incidence sur les droits et obligations des tiers.

Références aux documents de la CNUDCI

A/CN.9/467, par. 36 à 43;
A/CN.9/WG.IV/WP.84, par. 39 et 40;
A/CN.9/465, par. 51 à 61;
A/CN.9/WG.IV/WP.82, par. 36 à 40;
A/CN.9/457, par. 53 à 64.

Article 6. Satisfaction de l'exigence de signature

1. Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données, s'il est fait usage d'une signature électronique dont la fiabilité est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris toute convention en la matière.

2. Le paragraphe 1 s'applique, que l'exigence qui y est visée ait la forme d'une obligation ou que la loi prévoie simplement certaines conséquences en l'absence de signature.

3. Une signature électronique est considérée fiable en ce qu'elle satisfait à l'exigence indiquée au paragraphe 1 si:

a) les données afférentes à la création de signature sont, dans le contexte dans lequel elles sont utilisées, liées exclusivement au signataire;

b) les données afférentes à la création de signature étaient, au moment de la signature, sous le contrôle exclusif du signataire;

c) toute modification apportée à la signature électronique après le moment de la signature est décelable; et,

d) dans le cas où l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte, toute

modification apportée à cette information après le moment de la signature est décelable.

4. Le paragraphe 3 ne restreint pas la possibilité pour toute personne:

a) d'établir de toute autre manière, aux fins de satisfaire l'exigence visée au paragraphe 1, la fiabilité de la signature électronique; ni

b) d'apporter des preuves de la non-fiabilité de la signature électronique.

5. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...]

Importance de l'article 6

114. L'article 6 est l'une des dispositions essentielles de la Loi type. Il a pour objet de développer l'article 7 de la Loi type de la CNUDCI sur le commerce électronique et d'indiquer comment satisfaire au critère de fiabilité de l'article 7-1 b). Lorsqu'on interprète l'article 6, il faut avoir à l'esprit que cette disposition a pour objet de garantir que toute conséquence juridique qui aurait découlé de l'utilisation d'une signature manuscrite doit aussi découler de l'utilisation d'une signature électronique fiable.

Paragraphes 1, 2 et 5

115. Les paragraphes 1, 2 et 5 de l'article 6 introduisent des dispositions tirées, respectivement, des paragraphes 1 b), 2 et 3 de l'article 7 de la Loi type de la CNUDCI sur le commerce électronique. Un libellé inspiré de l'article 7-1 a) de cette Loi type est déjà inclus dans la définition du terme "signature électronique" figurant à l'alinéa a) de l'article 2.

Notions d'"identité" et d'"identification"

116. Le Groupe de travail est convenu qu'aux fins de la définition du terme "signature électronique" dans la Loi type, le terme "identification" pouvait être plus large que la simple identification du signataire par un nom. La notion d'identité ou d'identification consiste notamment à distinguer le signataire, par son nom ou autrement, de toute autre personne, et peut renvoyer à d'autres caractéristiques importantes telles que la position ou l'autorité, que ce soit en association avec un nom ou sans référence à ce nom. Partant, il n'est pas nécessaire d'opérer une distinction entre l'identité et d'autres caractéristiques importantes, ni de limiter la Loi type aux cas dans lesquels ne sont utilisés que des certificats qui désignent nommément le détenteur du dispositif de signature (A/CN.9/467, par. 56 à 58).

Effets de la Loi type variant avec le niveau de fiabilité technique

117. Lors de l'élaboration de la Loi type, on a fait observer qu'il faudrait établir, pour le projet d'article 6 (soit par une référence à la notion de "signature électronique renforcée", soit par une mention directe des critères d'établissement de la fiabilité technique d'une méthode de signature donnée), un double objectif: 1) que les effets juridiques découlent de l'application des techniques de signature électronique reconnues comme fiables; et 2) inversement, qu'aucun effet juridique de ce type ne découle de l'utilisation de techniques moins fiables. On a généralement estimé,

cependant, qu'il pourrait être nécessaire d'établir une distinction plus subtile entre les différentes techniques possibles de signature électronique, la Loi type devant éviter de désavantager quelque forme de signature électronique que ce soit, aussi simple et non sécurisée puisse-t-elle apparaître dans des circonstances données. Toute technique de signature électronique utilisée pour signer un message de données conformément à l'article 7-1 a) de la Loi type de la CNUDCI sur le commerce électronique produirait donc probablement des effets juridiques, à condition qu'elle soit suffisamment fiable compte tenu de toutes les circonstances, y compris de toute convention entre les parties. Cependant, seul un tribunal ou un autre juge des faits intervenant *ex post*, peut-être longtemps après que la signature électronique a été utilisée, peut déterminer ce qui constitue une technique fiable de signature compte tenu des circonstances en vertu de l'article 7 de la Loi type de la CNUDCI sur le commerce électronique. En revanche, la nouvelle Loi type est censée avantager certaines techniques reconnues comme étant particulièrement fiables indépendamment des circonstances dans lesquelles elles sont utilisées. C'est là l'objet du paragraphe 3, qui est censé garantir (soit par une présomption, soit par une règle de fond), qu'au moment de l'utilisation de cette technique de signature électronique ou avant (*ex ante*), elle entraînerait des effets juridiques équivalents à ceux d'une signature manuscrite. Le paragraphe 3 est donc indispensable si l'on veut que la Loi type atteigne son objectif, qui est d'offrir davantage de sécurité que n'en offre actuellement la Loi type de la CNUDCI sur le commerce électronique quant aux effets juridiques qu'on peut escompter de l'utilisation de types particulièrement fiables de signatures électroniques (voir A/CN.9/465, par. 64).

Présomption ou règle de fond

118. Pour établir la certitude quant aux effets juridiques résultant de l'usage de ce qui pourrait éventuellement être appelé une "signature électronique améliorée" selon l'article 2, le paragraphe 3 établit expressément les effets juridiques qui résulteraient de la réunion de certaines caractéristiques techniques d'une signature électronique. Quant à la manière d'établir ces effets juridiques, il a été convenu que les États adoptants devaient, selon leurs règles de procédure civile et commerciale, être libres de créer une présomption ou d'affirmer directement l'existence d'un lien entre certaines caractéristiques techniques et l'effet juridique d'une signature (voir A/CN.9/467, par. 61 et 62).

Intention du signataire

119. La question reste de savoir si un effet juridique devrait découler de l'utilisation de techniques de signature électronique faite sans intention expresse, de la part du signataire, d'être juridiquement lié par l'approbation de l'information signée électroniquement. En pareille circonstance, la deuxième fonction décrite à l'article 7-1 a) de la Loi type de la CNUDCI sur le commerce électronique n'est pas satisfaite, car il n'existe aucune "intention d'indiquer une approbation de l'information contenue dans le message de données". Le point de vue adopté dans la nouvelle Loi type est que les conséquences juridiques de l'utilisation d'une signature manuscrite devraient avoir leur pendant dans un environnement électronique. Ainsi, en apposant une signature (qu'elle soit manuscrite ou électronique) à une information, le signataire devrait être réputé avoir approuvé l'établissement d'un lien entre son identité et cette information. Le fait que l'établissement de ce lien produise des effets juridiques (contractuels ou non) dépendrait de la nature de l'information

signée, et de toute autre circonstance à évaluer conformément à la loi applicable en dehors de la Loi type. Dans ce contexte, la Loi type ne doit pas porter atteinte au droit général des contrats ou des obligations (voir A/CN.9/465, par. 65).

Critères de fiabilité technique

120. Les alinéas a) à d) du paragraphe 3 ont pour objet d'exprimer des critères objectifs de fiabilité technique des signatures électroniques. L'alinéa a) est centré sur les caractéristiques objectives des données afférentes à la création de signature, qui doivent être "liées exclusivement au signataire". D'un point de vue technique, les données afférentes à la création de signature pourraient être "liées" exclusivement au signataire sans être "uniques" en soi. Le lien existant entre les données utilisées pour créer la signature et le signataire est l'élément essentiel (A/CN.9/467, par. 63). Si certaines données afférentes à la création de signatures électroniques peuvent être partagées par divers utilisateurs, par exemple lorsque plusieurs employés partagent celles d'une société, elles doivent néanmoins permettre d'identifier sans ambiguïté un utilisateur dans le contexte de chaque signature électronique.

Contrôle exclusif des données afférentes à la signature par le signataire

121. L'alinéa b) traite des circonstances dans lesquelles sont utilisées les données afférentes à la création de signature. Lors de leur utilisation, ces données doivent être sous le contrôle exclusif du signataire. S'agissant de la notion de contrôle exclusif du signataire, se pose la question de savoir si le signataire resterait habilité à autoriser une autre personne à utiliser les données en son nom. Une telle situation risquerait de se produire lorsque les données afférentes à la signature sont utilisées dans le cadre d'une société, ladite société étant elle-même le signataire mais ayant besoin que plusieurs personnes puissent signer en son nom (A/CN.9/467, par. 66). On pourrait citer comme autre exemple les applications commerciales où les données afférentes à la signature existent sur un réseau et peuvent être utilisées par plusieurs personnes. Le réseau serait alors vraisemblablement lié à une entité particulière qui serait le signataire et continuerait d'exercer son contrôle sur les données. Si tel n'était pas le cas et que les données étaient largement accessibles, la situation ne devrait pas entrer dans le champ d'application la Loi type (A/CN.9/467, par. 67). Lorsqu'une clef juridique est mise en œuvre par plus d'une personne dans le cadre d'un système de "clef fractionnée" ou d'un autre système de "secret partagé", la notion de "signataire" vise ces personnes envisagées conjointement (A(CN.9/483, par. 152).

Mandat

122. Les alinéas a) et b) convergent pour garantir que les données afférentes à la signature ne pourront être utilisées que par une seule personne à quelque moment que ce soit, principalement lors de la création de la signature. La question du mandat ou de l'utilisation autorisée de ces données est traitée dans la définition du "signataire" (A/CN.9/467, par. 68).

Intégrité

123. Les alinéas c) et d) traitent des questions de l'intégrité de la signature électronique et de l'intégrité de l'information signée électroniquement. Il aurait été possible de combiner les deux dispositions pour souligner que, lorsqu'une signature est apposée à un document, l'intégrité du document et l'intégrité de la signature sont

si étroitement liées qu'il est difficile de concevoir l'une sans l'autre. Lorsqu'une signature est utilisée pour signer un document, l'idée de l'intégrité du document est inhérente à l'utilisation de la signature. Cependant, il a été décidé que la Loi type devrait suivre la distinction établie dans la Loi type de la CNUDCI sur le commerce électronique entre les articles 7 et 8. Bien que certaines technologies garantissent à la fois l'authentification (article 7 de la Loi type de la CNUDCI sur le commerce électronique) et l'intégrité (article 8 de la Loi type de la CNUDCI sur le commerce électronique), ces notions peuvent être considérées comme juridiquement distinctes et traitées comme telles. Puisqu'une signature manuscrite ne garantit ni l'intégrité du document auquel elle est apposée, ni la non-détectabilité d'une modification apportée au document, l'approche de l'équivalence fonctionnelle impose que ces notions ne soient pas traitées dans une disposition unique. Le paragraphe 3 c) a pour objet d'énoncer le critère à remplir pour démontrer qu'une méthode particulière de signature électronique est suffisamment fiable pour satisfaire à une exigence légale de signature. Cette exigence légale pourrait être satisfaite sans avoir à démontrer l'intégrité de l'ensemble du document (A/CN.9/467, par. 72 à 80).

Équivalent fonctionnel du document original

124. L'alinéa d) est essentiellement destiné à être utilisé dans les pays où les règles de droit qui régissent actuellement l'utilisation des signatures manuscrites n'établissent pas de distinction entre l'intégrité de la signature et l'intégrité de l'information signée. Dans d'autres pays, l'alinéa d) pourrait créer une signature qui serait plus fiable qu'une signature manuscrite et irait ainsi au-delà du concept d'équivalent fonctionnel d'une signature. En toute circonstance, l'alinéa d) aurait pour effet de créer un équivalent fonctionnel d'un document original.

Signature électronique d'une partie d'un message

125. À l'alinéa d), le lien nécessaire entre la signature et l'information signée est exprimé de façon à éviter de laisser entendre que la signature électronique ne peut s'appliquer qu'à l'intégralité d'un message de données. Souvent, en fait, l'information signée ne correspond qu'à une partie de l'information contenue dans le message de données. Une signature électronique peut, par exemple, se rapporter uniquement à une information annexée au message à des fins de transmission.

Dérogation conventionnelle

126. Le paragraphe 3 n'a pas pour objet de limiter l'application de l'article 5 ou de toute loi applicable reconnaissant la liberté qu'ont les parties de stipuler dans une convention pertinente qu'une technique de signature donnée serait considérée entre eux comme un équivalent fiable d'une signature manuscrite.

Références aux documents de la CNUDCI

A/CN.9/467, par. 44 à 87;
A/CN.9/WG.IV/WP.84, par. 41 à 47;
A/CN.9/465, par. 62 à 82;
A/CN.9/WG.IV/WP.82, par. 42 à 44;
A/CN.9/457, par. 48 à 52;
A/CN.9/WG.IV/WP.80, par. 11 et 12.

Article 7. Satisfaction des dispositions de l'article 6

1. [*Toute personne, tout organe ou toute autorité, de droit public ou privé, indiqué par l'État adoptant comme compétent en la matière*] peut déterminer quelles signatures électroniques satisfont aux exigences de l'article 6.

2. Toute détermination arrêtée en vertu du paragraphe 1 doit être conforme aux normes internationales reconnues.

3. Aucune disposition du présent article n'a d'incidence sur le fonctionnement des règles du droit international privé.

Prédétermination du statut de la signature électronique

127. L'article 7 décrit le rôle joué par l'État adoptant pour ce qui est d'établir ou de reconnaître toute entité pouvant valider l'utilisation de signatures électroniques ou certifier d'autre manière leur qualité. À l'instar de l'article 6, l'article 7 repose sur l'idée selon laquelle la condition requise, pour faciliter le développement du commerce électronique, est l'existence d'une certitude et d'une prévisibilité au moment où les parties commerciales utilisent des techniques de signature électronique et non au moment où un différend les oppose devant un tribunal. Lorsqu'une technique de signature particulière peut satisfaire à des exigences rigoureuses de fiabilité et de sécurité, il devrait exister un moyen d'évaluer les aspects techniques de la fiabilité et de la sécurité et d'accorder à la technique de signature une certaine forme de reconnaissance.

Objet de l'article 7

128. L'article 7 a pour objet de préciser qu'un État adoptant peut désigner un organe ou une autorité qui sera habilité(e) à déterminer quelles technologies peuvent bénéficier des présomptions ou de la règle de fond créées en vertu de l'article 6. L'article 7 n'est pas une disposition habilitante qui pourrait être ou serait nécessairement adoptée par les États sous sa forme actuelle. Il a cependant pour objet d'indiquer clairement que la certitude et la prévisibilité peuvent être obtenues en déterminant quelles techniques de signature électronique satisfont aux exigences de fiabilité énoncées à l'article 6, à condition que cette détermination s'effectue conformément aux normes internationales. Il ne devrait pas être interprété d'une façon qui, soit prescrirait des effets juridiques obligatoires en cas d'utilisation de certains types de signature électronique, soit limiterait l'utilisation de la technologie aux techniques dont on aurait déterminé qu'elles satisfont aux exigences de fiabilité de l'article 6. Les parties devraient être libres, par exemple, d'utiliser des techniques dont on n'aurait pas déterminé qu'elles satisfont aux exigences de fiabilité de l'article 6, si c'était ce qu'elles étaient convenues de faire. Elles devraient aussi être libres de montrer, devant une juridiction étatique ou arbitrale, que la méthode de signature qu'elles avaient choisi d'utiliser satisfaisait effectivement aux exigences de l'article 6, sans pour autant avoir fait l'objet d'une détermination préalable à cet effet.

Paragraphe 1

129. Le paragraphe 1 indique clairement que toute entité qui pourrait valider l'utilisation de signatures électroniques ou certifier autrement leur qualité ne devrait

pas nécessairement avoir le statut d'autorité d'État. Ce paragraphe ne devrait pas être interprété comme donnant aux États une recommandation quant au seul moyen d'obtenir la reconnaissance de techniques de signature, mais plutôt comme indiquant les restrictions qui devraient s'appliquer s'ils souhaitaient adopter une telle méthode.

Paragraphe 2

130. En ce qui concerne le paragraphe 2, la notion de "norme" ne devrait pas se limiter aux normes officielles établies, par exemple, par l'Organisation internationale de normalisation (ISO) et par l'Internet Engineering Task Force (IETF), ou à d'autres normes techniques. Le mot "normes" devrait être interprété dans un sens large qui inclurait les pratiques des divers secteurs d'activité et les usages commerciaux, les textes émanant d'organisations internationales telles que la Chambre de commerce internationale, ainsi que les textes de la CNUDCI elle-même (y compris la présente Loi type et la Loi type sur le commerce électronique). L'absence éventuelle de normes pertinentes ne devrait pas empêcher les personnes ou autorités compétentes d'opérer la détermination visée au paragraphe 1. Quant à la référence aux "normes reconnues", on pourrait s'interroger sur ce qui constitue la "reconnaissance" et sur l'entité dont on exige cette reconnaissance (voir A/CN.9/465, par. 94). La question est également examinée à propos de l'article 12 (voir ci-après, par. 154).

Paragraphe 3

131. Le paragraphe 3 a pour objet d'indiquer très clairement que l'article 7 n'a pas pour objet d'affecter le fonctionnement normal des règles du droit international privé (voir A/CN.9/467, par. 94). En l'absence d'une telle disposition, le projet d'article 7 pourrait être interprété à tort comme encourageant les États adoptants à défavoriser les signatures électroniques étrangères en raison de leur non-conformité aux règles édictées par la personne ou l'autorité visée au paragraphe 1.

Références aux documents de la CNUDCI

A/CN.9/467, par. 90 à 95;
A/CN.9/WG.IV/WP.84, par. 49 à 51;
A/CN.9/465, par. 90 à 98;
A/CN.9/WG.IV/WP.82, par. 46;
A/CN.9/457, par. 48 à 52;
A/CN.9/WG.IV/WP.80, par. 15.

Article 8. Normes de conduite du signataire

1. Lorsque des données afférentes à la création de signature peuvent être utilisées pour créer une signature ayant des effets juridiques, chaque signataire:

a) prend des dispositions raisonnables pour éviter toute utilisation non autorisée de ses données afférentes à la création de signature;

b) avise, sans retard injustifié, toute personne dont il peut raisonnablement penser qu'elle se fie à la signature électronique ou qu'elle fournit des services visant à étayer la signature électronique si:

i) il sait que les données afférentes à la création de signature ont été compromises; ou

ii) il estime, au regard de circonstances connues de lui, qu'il y a un risque important que les données afférentes à la création de signature aient été compromises;

c) prend, lorsqu'un certificat est utilisé pour étayer la signature électronique, des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou devant figurer dans le certificat sont exactes et complètes.

2. Un signataire est responsable de tout manquement aux exigences visées au paragraphe 1.

Titre

132. L'article 8 (et les articles 9 et 11) devaient initialement contenir des règles concernant les obligations et responsabilités des différentes parties concernées (le signataire, la partie se fiant à la signature et tout prestataire de services de certification). Cependant, en raison des changements rapides touchant les aspects techniques et commerciaux du commerce électronique ainsi que du rôle joué actuellement, dans certains pays, par l'auto-réglementation du commerce électronique, il est devenu difficile de parvenir à un consensus sur la teneur de ces règles. Les articles ont été rédigés de façon à présenter un "code de conduite" minimal applicable aux différentes parties. Les conséquences d'un non-respect de ce code de conduite relèvent de la loi applicable en dehors de la Loi type.

Paragraphe 1

133. Les alinéas a) et b) s'appliquent généralement à toutes les signatures électroniques, tandis que l'alinéa c) ne s'applique qu'aux signatures électroniques étayées par un certificat. L'obligation faite à l'alinéa a), en particulier, de prendre des dispositions raisonnables pour éviter toute utilisation non autorisée de ses données afférentes à la création de signature, constitue une obligation fondamentale généralement présente, par exemple, dans les conventions relatives à l'utilisation de cartes de crédit. En vertu de la politique adoptée au paragraphe 1, une telle obligation devrait également s'appliquer à toutes données afférents à la signature électronique qui pourraient être utilisées pour exprimer une intention juridiquement signifiante. La dérogation conventionnelle prévue à l'article 5, cependant, permet de déroger aux normes fixées à l'article 8 là où celles-ci seraient jugées inappropriées ou susceptibles d'entraîner des conséquences indésirables.

134. L'alinéa b) renvoie à la notion de "personne dont [on] peut raisonnablement penser qu'elle se fie à la signature électronique ou qu'elle fournit des services visant à étayer la signature électronique". En fonction de la technologie utilisée, cette "partie qui se fie à la signature" peut être non seulement une personne qui cherche à se fier à la signature, mais aussi une personne telle qu'un prestataire de services de certification, un prestataire de services de révocation de certificats ou toute autre partie concernée.

135. L'alinéa c) s'applique lorsqu'un certificat est utilisé pour étayer les données afférentes à la signature. La notion de "cycle de vie du certificat" doit être interprétée

dans un sens large comme couvrant la période allant de la demande ou de la création d'un certificat jusqu'à son expiration ou sa révocation.

Paragraphe 2

136. Le paragraphe 2 ne précise ni les conséquences, ni les limites de la responsabilité, qui relèvent toutes deux de la législation nationale. Cependant, tout en renvoyant les conséquences de la responsabilité à la législation nationale, le paragraphe 2 n'en indique pas moins clairement aux États adoptants que tout manquement aux exigences visées au paragraphe 1 devrait entraîner une responsabilité. Le paragraphe 2 s'appuie sur la conclusion à laquelle est parvenu le Groupe de travail à sa trente-cinquième session, selon laquelle il serait sans doute difficile d'arriver à un consensus sur les conséquences pouvant découler de la responsabilité du détenteur des données afférentes à la signature. Selon le contexte dans lequel la signature électronique est utilisée, ces conséquences pourraient aller, d'après la loi existante, d'une responsabilité juridique du détenteur des données afférentes à la signature vis-à-vis de la teneur du message à une responsabilité en dommages-intérêts. En conséquence, le paragraphe 2 se contente d'établir le principe selon lequel le détenteur des données afférentes à la signature devrait être tenu responsable de tout manquement aux exigences visées au paragraphe 1, et renvoie à la loi applicable dans chaque État adoptant, en dehors de la Loi type, les conséquences juridiques qui découleraient d'une telle responsabilité (voir A/CN.9/465, par. 108).

Références aux documents de la CNUDCI

A/CN.9/467, par. 96 à 104;
A/CN.9/WG.IV/WP.84, par. 52 et 53;
A/CN.9/465, par. 99 à 108;
A/CN.9/WG.IV/WP.82, par. 50 à 55;
A/CN.9/457, par. 65 à 98;
A/CN.9/WG.IV/WP.80, par. 18 et 19.

Article 9. Normes de conduite du prestataire de services de certification

1. Lorsqu'un prestataire de services de certification fournit des services visant à étayer une signature électronique qui peut être utilisée pour produire des effets juridiques en tant que signature, ce prestataire:

a) agit en conformité avec les déclarations qu'il fait concernant ses politiques et pratiques;

b) prend des dispositions raisonnables pour assurer que toutes les déclarations qu'il fait concernant le certificat durant tout son cycle de vie ou figurant dans le certificat sont exactes et complètes;

c) fournit à toute partie se fiant au certificat des moyens raisonnablement accessibles de déterminer à partir de ce certificat:

i) l'identité du prestataire de services de certification;

ii) si le signataire identifié dans le certificat avait, au moment de l'émission de ce dernier, le contrôle des données afférentes à la création de signature;

iii) si les données afférentes à la création de signature étaient valides au moment ou avant le moment de l'émission du certificat;

d) fournit à toute partie se fiant au certificat des moyens raisonnablement accessibles de déterminer, s'il y a lieu, à partir de ce certificat ou de toute autre manière:

i) la méthode utilisée pour identifier le signataire;

ii) toute restriction quant aux fins ou à la valeur pour lesquelles les données afférentes à la création de signature ou le certificat peuvent être utilisés;

iii) si les données afférentes à la création de signature sont valides et n'ont pas été compromises;

iv) toute restriction quant à l'étendue de la responsabilité stipulée par le prestataire de services de certification;

v) s'il existe des moyens pour le signataire d'adresser une notification conformément à l'alinéa b) du paragraphe 1 de l'article 8;

vi) la disponibilité d'un service de révocation en temps utile;

e) lorsque des services sont fournis au titre du sous-alinéa v) de l'alinéa d), donne au signataire le moyen d'adresser une notification conformément à l'alinéa b) du paragraphe 1 de l'article 8 et, lorsque des services sont fournis au titre du sous-alinéa vi) de l'alinéa d), offre un service de révocation en temps utile;

f) utilise des systèmes, des procédures et des ressources humaines fiables pour la prestation de ses services.

2. Un prestataire de services de certification est responsable de tout manquement aux exigences visées au paragraphe 1.

Paragraphe 1

137. L'alinéa a) énonce la règle fondamentale selon laquelle un prestataire de services de certification devrait se conformer à ses déclarations et à ses engagements tels qu'exprimés, par exemple, dans une déclaration de pratiques de certification ou dans tout autre type de déclaration de politique générale. L'alinéa b) reproduit, dans le contexte des activités du prestataire de services de certification, le code de conduite énoncé à l'article 8-1 c) applicable au signataire.

138. L'alinéa c) définit la teneur et les effets essentiels de tout certificat en vertu de la Loi type. L'alinéa d) énumère les éléments additionnels qui doivent être inclus dans le certificat ou autrement mis à la disposition de la partie se fiant à la signature dans le cas de certains certificats. L'alinéa e) n'a pas pour objet de s'appliquer à des certificats tels que des certificats de transactions, qui sont des certificats ponctuels,

ou à des certificats à faible coût portant sur des applications à faible risque, qui pourraient ne pas être sujets à révocation.

139. On peut considérer qu'il est raisonnable d'attendre de tout prestataire de services de certification, et non pas seulement de ceux qui émettent des certificats de "grande valeur", qu'il s'acquitte des devoirs et obligations prévus à l'article 9. Toutefois, les auteurs de la Loi type ont pris soin de ne pas exiger d'un signataire ou d'un prestataire de services de certification un niveau de diligence ou de fiabilité sans rapport raisonnable avec les fins pour lesquelles la signature électronique ou le certificat sont utilisés. La Loi type privilégie donc une solution qui lie les obligations énoncées dans les articles 8 et 9 à la production de signatures électroniques ayant une valeur juridique (A/CN.9/483, par. 117). En limitant le champ d'application de l'article 9 au large éventail de cas dans lesquels les services de certification servent à étayer une signature électronique qui peut être utilisée pour produire des effets juridiques en tant que signature, la Loi type ne vise pas à créer de nouveaux types d'effets juridiques pour les signatures (ibid., par. 119).

Paragraphe 2

140. Le paragraphe 2 fait pendant à la règle de base relative à la responsabilité énoncée au paragraphe 2 de l'article 8 pour le signataire. Cette disposition a pour effet de laisser à la législation nationale le soin de déterminer les conséquences de la responsabilité. Sous réserve des règles applicables du droit national, le paragraphe 2 n'est pas destiné par ses auteurs à être interprété comme une règle de responsabilité absolue. Il n'a pas été prévu que ce paragraphe ait pour effet d'exclure la possibilité, pour le prestataire de services de certification, de prouver, par exemple, l'absence de faute ou de faute secondaire.

141. Les premières versions de l'article 9 contenaient un paragraphe supplémentaire, qui traitait des conséquences de la responsabilité énoncées au paragraphe 2. Lors de la préparation de la Loi type, il a été observé que les prestataires de services de certification remplissaient des fonctions intermédiaires qui étaient indispensables au commerce électronique et qu'une disposition unique s'inspirant du paragraphe 2 ne suffirait pas à traiter la question de la responsabilité de ces professionnels. Le paragraphe 2 peut énoncer un principe approprié applicable aux signataires, mais il peut n'être pas suffisant pour couvrir les activités professionnelles et commerciales visées par l'article 9. L'une des façons possibles de pallier cette insuffisance aurait été d'énumérer dans le texte de la Loi type les facteurs à prendre en compte pour évaluer tout préjudice résultant d'un manquement du prestataire de services de certification aux exigences du paragraphe 1. Il a finalement été décidé de faire figurer dans le Guide une liste non exhaustive de facteurs indicatifs. Pour évaluer le préjudice, il faudrait notamment prendre en compte les facteurs suivants: a) le coût d'obtention du certificat; b) la nature de l'information certifiée; c) l'existence et l'ampleur de toute restriction aux fins pour lesquelles le certificat peut être utilisé; d) l'existence de toute déclaration limitant le champ d'application ou l'étendue de la responsabilité du prestataire de services de certification; et e) toute conduite fautive de la partie se fiant à la signature.

Références aux documents de la CNUDCI

A/CN.9/483, par. 114 à 127;
A/CN.9/467, par. 105 à 109;
A/CN.9/WG.IV/WP.84, par. 54 à 60;
A/CN.9/465, par. 123 à 142 (projet d'article 12);
A/CN.9/WG.IV/WP.82, par. 59 à 68 (projet d'article 12);
A/CN.9/457, par. 108 à 119;
A/CN.9/WG.IV/WP.80, par. 22 à 24.

Article 10. Fiabilité

Aux fins de l'alinéa f) du paragraphe 1 de l'article 9, pour déterminer si, ou dans quelle mesure, tous systèmes, procédures et ressources humaines utilisés par le prestataire de services de certification sont fiables, il est tenu compte des facteurs suivants:

a) ressources humaines et financières, y compris l'existence d'avoirs;

b) qualité du matériel et des logiciels;

c) procédures utilisées pour le traitement des certificats et des demandes de certificats et la conservation des enregistrements;

d) possibilité d'accès à l'information pour les signataires identifiés dans les certificats et les éventuelles parties se fiant aux certificats;

e) régularité et étendue des audits effectués par un organisme indépendant;

f) existence d'une déclaration de l'État, d'un organisme d'accréditation ou du prestataire de services de certification concernant le respect ou l'existence des critères énumérés ci-dessus; ou

g) tout autre facteur pertinent.

Flexibilité de la notion de "fiabilité"

142. L'article 10 faisait, à l'origine, partie de l'article 9. Bien que cette partie soit par la suite devenue un article distinct, elle a essentiellement pour objet de faciliter l'interprétation de la notion de "systèmes, procédures et ressources humaines fiables" à l'article 9-1 f). L'article 10 se présente sous la forme d'une liste non exhaustive de facteurs à prendre en compte pour déterminer la fiabilité. Cette liste a pour objet de définir une notion souple de la fiabilité, dont les contours pourraient varier en fonction de ce que l'on attend du certificat dans le contexte dans lequel il est créé.

Références aux documents de la CNUDCI

A/CN.9/483, par. 128 à 133;
A/CN.9/467, par. 114 à 119.

Article 11. Normes de conduite de la partie se fiant à la signature ou au certificat

Une partie se fiant à une signature ou à une certificat assume les conséquences juridiques découlant du fait qu'elle s'est abstenue de:

a) prendre des mesures raisonnables pour vérifier la fiabilité d'une signature électronique; ou,

b) si une signature électronique est étayée par un certificat, de prendre des mesures raisonnables pour:

i) vérifier que le certificat est valide ou qu'il n'a pas été suspendu ou révoqué; et

ii) tenir compte de toute restriction dont le certificat ferait l'objet.

Caractère raisonnable de la confiance

143. L'article 11 reflète l'idée selon laquelle une partie qui entend se fier à une signature électronique devrait se poser la question de savoir si et dans quelle mesure cette confiance est raisonnable compte tenu des circonstances. Il n'a pas pour objet de traiter la question de la validité d'une signature électronique, qui l'est à l'article 6 et qui ne devrait pas dépendre de la conduite de la partie se fiant à la signature ou au certificat. La question de la validité d'une signature électronique devrait demeurer distincte de la question de savoir s'il est raisonnable, pour une partie se fiant à la signature ou au certificat, de se fier à une signature qui ne satisfait pas à l'exigence énoncée à l'article 6.

Questions relatives aux consommateurs

144. Si l'article 11 peut faire peser une lourde charge sur les parties qui se fient à une signature, en particulier lorsque ces parties sont des consommateurs, il peut être utile toutefois de rappeler que la Loi type n'a pas pour objet d'annuler toute règle régissant la protection des consommateurs. Elle pourrait, cependant, être utile pour éduquer toutes les parties concernées, y compris les parties qui se fient à la signature, quant à la norme de conduite raisonnable à appliquer en matière de signatures électroniques. En outre, l'établissement d'une norme de conduite en vertu de laquelle la partie qui se fie à la signature devrait vérifier la fiabilité de cette dernière par des moyens facilement accessibles peut être considéré comme essentiel au développement de tout système d'infrastructure à clef publique.

Notion de "partie se fiant à la signature"

145. Conformément à la définition qui en est donnée, la notion de "partie se fiant à la signature" couvre toute partie qui pourrait se fier à une signature électronique. En fonction des circonstances, il peut donc s'agir de toute personne ayant ou non une relation contractuelle avec le signataire ou le prestataire de services de certification. Il est même concevable que le prestataire de services de certification ou le signataire devienne lui-même une "partie se fiant à la signature". Cette notion large ne doit cependant pas entraîner, pour le titulaire d'un certificat, l'obligation de vérifier la validité du certificat qu'il achète au prestataire de services de certification.

Manquement aux exigences de l'article 11

146. Quant aux conséquences éventuelles de l'établissement d'une obligation générale qui serait faite à la partie se fiant à la signature électronique de vérifier la validité de cette signature ou du certificat, un problème se pose lorsque cette partie ne satisfait pas aux exigences de l'article 11. Doit-elle alors être mise dans l'impossibilité de se prévaloir de la signature ou du certificat si une vérification raisonnable n'aurait pas révélé que ces derniers n'étaient pas valides. Il pourrait être nécessaire de traiter une telle situation dans la loi applicable en dehors de la Loi type.

Références aux documents de la CNUDCI

A/CN.9/467, par. 130 à 143;
A/CN.9/WG.IV/WP.84, par. 61 à 63;
A/CN.9/465, par. 109 à 122 (projets d'articles 10 et 11);
A/CN.9/WG.IV/WP.82, par. 56 à 58 (projets d'articles 10 et 11);
A/CN.9/457, par. 99 à 107;
A/CN.9/WG.IV/WP.80, par. 20 et 21.

Article 12. Reconnaissance des certificats et signatures électroniques étrangers

1. Pour déterminer si, ou dans quelle mesure, un certificat ou une signature électronique produit légalement ses effets, il n'est pas tenu compte:

a) du lieu dans lequel le certificat est émis ou la signature électronique créée ou utilisée; ou

b) du lieu dans lequel l'émetteur ou le signataire a son établissement.

2. Un certificat émis en dehors de [*l'État adoptant*] a les mêmes effets juridiques dans [*l'État adoptant*] qu'un certificat émis dans [*l'État adoptant*] à condition qu'il offre un niveau de fiabilité substantiellement équivalent.

3. Une signature électronique créée ou utilisée en dehors de [*l'État adoptant*] a les mêmes effets juridiques dans [*l'État adoptant*] qu'une signature électronique créée ou utilisée dans [*l'État adoptant*] à condition qu'elle offre un niveau de fiabilité substantiellement équivalent.

4. Pour déterminer si des certificats ou des signatures électroniques offrent un niveau de fiabilité substantiellement équivalent aux fins des paragraphes 2 ou 3, il est tenu compte des normes internationales reconnues et de tous autres facteurs pertinents.

5. Lorsque, nonobstant les paragraphes 2, 3 et 4, les parties conviennent, s'agissant de leurs relations, d'utiliser certains types de signatures électroniques ou certificats, cette convention est jugée suffisante aux fins de la reconnaissance internationale, à moins qu'elle soit invalide ou sans effets en vertu de la loi applicable.

Règle générale de non-discrimination

147. Le paragraphe 1 vise à traduire le principe fondamental selon lequel le lieu d'origine ne doit en aucun cas, être par lui-même un facteur permettant de déterminer si et dans quelle mesure des certificats ou des signatures électroniques étrangers produisent légalement leurs effets. Cette détermination ne doit pas dépendre du lieu dans lequel le certificat ou la signature électronique a été émis (voir A/CN.9/483, par. 27) mais de sa fiabilité technique.

"Niveau de fiabilité substantiellement équivalent"

148. Le paragraphe 2 a pour objet de définir le critère général pour la reconnaissance transfrontière des certificats, faute de quoi les prestataires de services de certification seraient astreints à la lourde obligation d'obtenir des licences dans un grand nombre de pays. À cette fin, le paragraphe 2 fixe un seuil d'équivalence technique des certificats étrangers fondé sur une comparaison de leur niveau de fiabilité par rapport à celui qui est exigé dans l'État adoptant conformément à la Loi type (ibid., par. 31). Ce critère doit s'appliquer quelle que soit la nature du régime de certification existant dans le pays d'où émane le certificat ou la signature (ibid., par. 29).

Différences de niveau de fiabilité entre pays

149. En faisant référence à la notion centrale de "niveau de fiabilité substantiellement équivalent", le paragraphe 2 reconnaît qu'il peut exister d'importantes différences entre les exigences des différents pays. L'exigence d'équivalence, telle que visée au paragraphe 2, ne signifie pas que le niveau de fiabilité d'un certificat étranger doit être exactement identique à celui d'un certificat national (ibid., par. 32).

Différences de niveau de fiabilité dans un même pays

150. Il convient de noter par ailleurs que dans la pratique les prestataires de service de certification émettent des certificats ayant différents niveaux de fiabilité, selon l'utilisation que veulent en faire leurs clients. De ce fait, il n'est pas toujours indispensable qu'un certificat produise des effets juridiques, que ce soit dans le pays où il a été émis ou à l'étranger. En appliquant la notion d'équivalence telle qu'employée au paragraphe 2, il convient donc de garder à l'esprit que l'équivalence à établir est entre des certificats du même type. Toutefois, la Loi type ne tente pas d'établir une correspondance entre des certificats de différents types émis par différents prestataires de services de certification dans différents pays. Son but est d'envisager une éventuelle hiérarchie des différents types de certificats. Dans la pratique, une juridiction étatique ou arbitrale appelée à décider de l'effet juridique d'un certificat étranger examinerait normalement chaque certificat en fonction de ses caractéristiques propres et tenterait de l'assimiler aux certificats ayant le niveau le plus proche dans l'État adoptant (ibid., par. 33).

Égalité de traitement des certificats et d'autres types de signatures électroniques

151. Le paragraphe 3 énonce, en ce qui concerne les signatures électroniques, la même règle que celle qui est énoncée au paragraphe 2 concernant les certificats (ibid., par. 41).

Reconnaissance de certains effet juridiques à l'application des lois d'un pays étranger

152. Les paragraphes 2 et 3 traitent exclusivement du critère de fiabilité internationale à appliquer pour l'évaluation de la fiabilité d'un certificat ou d'une signature électronique étranger. Toutefois, lors de l'élaboration de la Loi type, on a gardé à l'esprit le fait que les États adoptants pourraient souhaiter se dispenser de vérifier la fiabilité de certaines signatures ou de certains certificats lorsqu'ils considèrent que la loi du pays d'où provient la signature prévoit une norme satisfaisante de fiabilité. Pour ce qui est des techniques juridiques que pourrait utiliser un État adoptant pour reconnaître a priori la fiabilité de certificats et de signatures conformes à la loi d'un État étranger (par exemple une déclaration unilatérale ou un traité), la Loi type ne contient aucune proposition particulière (ibid., par. 39 et 42).

Facteurs à prendre en considération pour l'évaluation de l'équivalence substantielle des certificats et signatures étrangers

153. Lors de l'élaboration de la Loi type, le paragraphe 4 a d'abord été conçu comme une liste de facteurs à prendre en considération pour déterminer si un certificat ou une signature électronique offrait un niveau de fiabilité substantiellement équivalent aux fins des paragraphes 2 ou 3. Il a été jugé ultérieurement que la plupart de ces facteurs figuraient déjà dans les articles 6, 9 et 10. Les énoncer à nouveau dans le cadre de l'article 12 aurait été superflu. Une autre solution possible, à savoir un renvoi, au paragraphe 4, aux dispositions appropriées de la Loi type où les critères pertinents étaient mentionnés, en ajoutant éventuellement d'autres critères particulièrement importants pour la reconnaissance internationale, a été jugée inadéquate car elle entraînait une formulation par trop complexe (voir en particulier A/CN.9/483, par. 43 à 49). On a finalement opté pour les termes généraux "tous autres facteurs pertinents", ceux énoncés aux articles 6, 9 et 10 pour l'évaluation des certificats et des signatures électroniques nationaux étant particulièrement importants. En outre, le paragraphe 4 tire les conséquences du fait que l'évaluation de l'équivalence des certificats étrangers est quelque peu différente de l'évaluation de la fiabilité d'un prestataire de services de certification au titre des articles 9 et 10. c'est pourquoi on y a ajouté une référence aux "normes internationales reconnues".

Normes internationales reconnues

154. La notion de "norme internationale reconnue" devrait être interprétée de façon large comme englobant à la fois les normes internationales techniques et commerciales (c'est-à-dire les normes du marché) et les normes et règles adoptées par des organismes gouvernementaux ou intergouvernementaux (ibid., par. 49). Des "normes internationales reconnues" peuvent prendre la forme de déclarations sur les pratiques techniques, juridiques ou commerciales acceptées, qu'elles aient été mises au point par le secteur public ou par le secteur privé (ou les deux), de nature normative ou interprétative, généralement acceptées comme internationalement applicables. De telles normes peuvent se présenter sous forme d'exigences, de recommandations, de principes directeurs, de codes de conduite ou de déclarations de bonnes pratiques ou de règles (ibid., par. 101 à 104).

Reconnaissance des conventions entre les parties intéressées

155. Le paragraphe 5 prévoit la reconnaissance des conventions entre les parties intéressées concernant l'utilisation de certains types de signatures électroniques ou de certificats comme motifs suffisants de reconnaissance internationale (entre ces parties) des signatures ou certificats convenus (ibid., par. 54). Il est à noter que, conformément au paragraphe 5 de l'article 5, l'intention n'est pas de passer outre toute loi contraignante, en particulier toute exigence impérative concernant les signatures manuscrites que les États adoptants peuvent souhaiter maintenir dans leur droit applicable (ibid., par. 113). Le paragraphe 5 est nécessaire pour donner effet aux stipulations contractuelles en vertu desquelles les parties peuvent convenir, entre elles, de reconnaître l'utilisation de certaines signatures électroniques ou de certains certificats (qui peuvent être considérés comme étrangers dans certains ou dans la totalité des États où les parties peuvent demander la reconnaissance juridique de ces signatures ou certificats), sans que ces derniers soient soumis au critère de l'équivalence substantielle énoncé aux paragraphes 2, 3 et 4. Le paragraphe 5 n'a pas d'incidences sur la situation juridique des tiers (ibid., par. 56).

Références aux documents de la CNUDCI

A/CN.9/483, par. 25 à 28 (art. 12);
A/CN.9/WG.IV/WP.84, par. 61 à 68 (projet d'article 13);
A/CN.9/465, par. 21 à 35;
A/CN.9/WG.IV/WP.82, par. 69 à 71;
A/CN.9/454, par. 173;
A/CN.9/446, par. 196 à 207 (projet d'article 19);
A/CN.9/WG.IV/WP.73, par. 75;
A/CN.9/437, par. 74 à 89 (projet d'article premier); et
A/CN.9/WG.IV/WP.71, par. 73 à 75.

Notes

[1] *Documents officiels de l'Assemblée générale, cinquante et unième session, Supplément n° 17* (A/51/17), par. 223 et 224.

[2] Ibid., *cinquante-deuxième session, Supplément n°7* (A/52/17), par. 249 à 251.

[3] *Documents officiels de l'Assemblée générale, cinquante et unième session, Supplément n° 17* (A/55/17), par. 223 et 224.

[4] Ibid., *cinquante-deuxième session, Supplément n° 17* (A/52/17), par. 249 à 251.

[5] Ibid., *cinquante-troisième session, Supplément n° 17* (A/53/17), par. 207 à 211.

[6] Ibid., *cinquante-quatrième session, Supplément n° 17* (A/54/17), par. 308 à 314.

[7] Ibid., cinquante-cinquième session, Supplément n° 17 (A/55/17), par. 380 à 383.

[8] C ette section est reprise du document A/CN.9/WG.IV/WP.71, partie I.

[9] De nombreux éléments de la description du fonctionnement d'un système de signature numérique dans la présente section s'appuient sur les directives en matière de signature numérique (Digital Signature Guidelines) élaborées par l'Association du barreau américain, p. 8 à 17.

[10] Certaines normes existantes telles que les directives concernant les signatures électroniques de l'Association du barreau américain contiennent la notion d'"infaisabilité informatique" pour décrire l'irréversibilité escomptée du processus, c'est-à-dire l'espoir qu'il sera impossible de déduire la clef privée secrète d'un utilisateur à partir de sa clef publique. "La notion d'infaisabilité informatique est une notion relative fondée sur la valeur des données protégées, l'infrastructure informatique requise pour les protéger, le temps nécessaire pour les protéger, ainsi que le coût et le temps nécessaires pour attaquer les données, ces facteurs étant évalués tant en fonction de la situation actuelle que des futurs progrès technologiques" (directives concernant les signatures électroniques de l'Association du barreau américain, p. 9, note 23).

[11] Dans les cas où les clefs cryptographiques publiques et privées seraient émises par les utilisateurs eux-mêmes, il pourrait être nécessaire de charger les certificateurs de clefs publiques d'assurer cette confiance.

[12] La question de savoir si un gouvernement devrait avoir la capacité technique de conserver ou de recréer des clefs de confidentialité privées peut être traitée au niveau de l'autorité racine.

[13] Dans le contexte d'une certification croisée, cependant, il faudrait, pour assurer une interopérabilité internationale, que toutes les infrastructures à clef publique établies dans différents pays puissent communiquer entre elles.