**NATIONS UNIES** **A**

# Assemblée générale

A/CN.9/465
Distr. GÉNÉRALE
23 septembre 1999
FRANÇAIS

Original: ANGLAIS

COMMISSION DES NATIONS UNIES
POUR LE DROIT COMMERCIAL INTERNATIONAL
Trente-troisième session
New York, 12 juin-7 juillet 2000

RAPPORT DU GROUPE DE TRAVAIL SUR LE COMMERCE ÉLECTRONIQUE
SUR LES TRAVAUX DE SA TRENTE-CINQUIÈME SESSION
(Vienne, 6-17 septembre 1999)

TABLE DES MATIÈRES

## INTRODUCTION

1. À sa vingt-neuvième session (1996), la Commission a décidé d'inscrire à son ordre du jour les questions relatives aux signatures numériques et aux autorités de certification. Le Groupe de travail sur le commerce électronique a été prié de réfléchir à l'opportunité et à la possibilité de définir des règles uniformes concernant ces questions. Il a été convenu que les règles uniformes à élaborer devraient être consacrées notamment aux questions ci-après: fondement juridique des opérations de certification, y compris les nouvelles techniques d'authentification et de certification numériques; applicabilité de la certification; répartition des risques et des responsabilités entre utilisateurs, fournisseurs et tiers dans le contexte de l'utilisation de techniques de certification; questions spécifiques à la certification sous l'angle de l'utilisation des registres; et incorporation par référence[1].

2. 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. Le Groupe de travail 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 fournisseurs de services et contrats électroniques (A/CN.9/437, par. 156 et 157).

3. 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 (dénommées ci-après "les Règles uniformes").

4. S'agissant du champ d'application et de la forme exacts de ces Règles uniformes, la Commission est généralement convenue qu'aucune décision ne pouvait être prise à ce stade précoce. On 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 que les Règles uniformes devraient être compatibles avec l'approche techniquement neutre adoptée dans la Loi type de la CNUDCI sur le commerce électronique (dénommée ci-après "la Loi type"). Ainsi, les Règles uniformes ne devraient pas décourager l'utilisation d'autres techniques d'authentification. En outre, s'agissant de la cryptographie à clef publique, il pourrait être nécessaire que les Règles uniformes prennent en considération divers niveaux de sécurité et reconnaissent 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 généralement considéré que le Groupe de travail pourrait utilement envisager l'établissement d'un ensemble minimum de normes que les autorités de certification devraient respecter, en particulier dans les cas de certification transnationale[2].

5. Le Groupe de travail a commencé à élaborer le projet de Règles uniformes à sa trente-deuxième session en se fondant sur une note établie par le secrétariat (A/CN.9/WG.IV/WP.73).

6. 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). Elle a dit sa satisfaction des efforts faits par le Groupe de travail pour rédiger le projet de règles uniformes sur les signatures électroniques. Elle a noté qu'à ses trente et unième et trente-deuxième sessions, il avait eu des difficultés manifestes 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 également été 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 le projet de règles uniformes sur les signatures électroniques prenait progressivement la forme d'une structure utilisable.

7. La Commission a réaffirmé la décision qu'elle avait prise à sa trente et unième session sur la faisabilité de la rédaction de telles règles uniformes et s'est déclarée certaine que le Groupe de travail pourrait progresser encore dans ses travaux à sa trente-troisième session (New-York, 29 juin-10 juillet 1998) 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 unanimement considéré comme un forum international particulièrement important pour les échanges de vues sur les problèmes juridiques liés au commerce électronique et la recherche de solutions correspondantes[3].

8. À sa trente-deuxième session (1999), la Commission était saisie du rapport du Groupe de travail sur les travaux de ses trente-troisième (juillet 1998) et trente-quatrième (février 1999) sessions (A/CN.9/454 et 457). Elle a dit sa satisfaction quant aux efforts faits par le Groupe de travail pour rédiger le projet de Règles uniformes sur les signatures électroniques. 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 senti 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.

9. Selon une opinion, l'approche qu'avait adoptée jusqu'ici le Groupe de travail ne tenait pas suffisamment compte de la nécessité, pour le monde des affaires, de souplesse dans l'utilisation des signatures électroniques et autres techniques d'authentification. Telles qu'actuellement envisagées, les Règles uniformes mettaient trop l'accent sur les signatures numériques et sur une application particulière de ces dernières 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. La réglementation de certaines utilisations des signatures électroniques était peut-être nécessaire en dehors du droit commercial, mais le Groupe de travail ne devrait pas s'engager dans une activité de ce type.

10. Selon l'avis qui a largement prévalu, le Groupe de travail devrait poursuivre sa tâche sur la base de son mandat original (voir ci-dessus, par. 3). 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 d'élaborer une législation sur les questions relatives aux signatures électroniques, y compris la mise en place d'une infrastructure fondée sur la clef publique 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 de la cryptographie à clef publique, 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 à la clef) correspondaient à un modèle possible de cryptographie à clef publique, 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 la cryptographie à clef publique 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 titulaire), 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 de cryptographie à clef publique, et qu'il fallait les traiter de la même façon, 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, on a largement estimé qu'en se concentrant sur les fonctions typiques de la cryptographie à clef publique et non sur un modèle particulier, on parviendrait peut-être plus facilement à élaborer, à un stade ultérieur, une règle tout à fait neutre techniquement (ibid., par. 68).

11. À l'issue du débat, la Commission a réaffirmé ses décisions précédentes quant à la faisabilité de la rédaction de règles uniformes (voir ci-dessus, par. 3 et 5) et s'est déclarée certaine que le Groupe de travail pourrait progresser encore à ses prochaines sessions[4].

12. Le Groupe de travail sur le commerce électronique, qui est composé de tous les États membres de la Commission, a tenu sa trente-cinquième session à Vienne du 6 au 17 septembre 1999. Ont assisté à cette session les représentants des États membres du Groupe de travail ci—après: Allemagne, Australie, Autriche, Bulgarie, Cameroun, Chine, Colombie, Égypte, Espagne, États-Unis d'Amérique, Finlande, France, Honduras, Hongrie, Inde, Iran (République islamique d'), Italie, Japon, Mexique, Nigéria, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Singapour, Thaïlande et Uruguay.

13. Y ont également assisté des observateurs des États ci—après: Angola, Arabie saoudite, Bahreïn, Belgique, Belize, Bolivie, Canada, Costa Rica, Danemark, Géorgie, Guatemala, Indonésie, Iraq, Irlande, Koweït, Liban, Malaisie, Maroc, Nouvelle-Zélande, Pays—Bas, Philippines, Pologne, Portugal, République tchèque, République de Corée, **Slovaquie**, Suède, Suisse, Tunisie, Turquie, Ukraine et Yémen.

14. Y ont en outre assisté des observateurs des organisations internationales ci—après: Conférence des Nations Unies sur le commerce et le développement (CNUCED), Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO), Banque africaine de développement, Commission européenne, Organisation de coopération et de développement économiques (OCDE), Association européenne des étudiants en droit, Association internationale des ports (AIP), Association internationale du barreau, Chambre de commerce internationale (CCI), Internet Law and Policy Forum (ILPF), Electronic Frontier Foundation Europe et Union internationale du notariat latin (UINL).

15. Le Groupe de travail a élu les membres du Bureau ci—après:

*Président*: M. Jacques GAUTHIER (Canada, élu à titre personnel)

*Rapporteur*: M. Pinai NANAKORN (Thaïlande)

16. Le Groupe de travail était saisi des documents ci—après: ordre du jour provisoire (A/CN.9/WG.IV/WP.81); une note du secrétariat contenant un projet révisé de règles uniformes sur les signatures électroniques (A/CN.9/WG.IV/WP.82).

17. Le Groupe de travail a adopté l'ordre du jour ci—après:

1. Élection du Bureau.

2. Adoption de l'ordre du jour.

3. Aspects juridiques du commerce électronique: projet de Règles uniformes sur les signatures électroniques.

4. Questions diverses.

5. Adoption du rapport.

## I. DÉLIBÉRATIONS ET DÉCISIONS

18. Le Groupe de travail a examiné la question des signatures électroniques sur la base de la note établie par le secrétariat (A/CN.9/WG.IV/WP.82). Il est rendu compte de ses délibérations et conclusions à ce sujet dans la section II ci‑dessous. Le secrétariat a été prié d'élaborer, à partir de ces délibérations et conclusions, un ensemble de dispositions révisées, avec d'éventuelles variantes, pour examen par le Groupe de travail lors d'une session future.

## II. PROJET DE RÈGLES UNIFORMES SUR LES SIGNATURES ÉLECTRONIQUES

### A. REMARQUES GÉNÉRALES

19. Les membres du Groupe de travail ont tout d'abord échangé des vues sur les faits nouveaux intervenus en matière de réglementation dans le commerce électronique, notamment l'adoption de la Loi type, les signatures électroniques et l'infrastructure à clef publique dans le contexte des signatures numériques. S'est ainsi confirmé, aux niveaux gouvernemental, intergouvernemental et non gouvernemental, que l'on reconnaissait aujourd'hui l'absolue nécessité de traiter les aspects juridiques du commerce électronique pour favoriser ce commerce et éliminer les obstacles aux échanges. Il a été indiqué qu'un certain nombre de pays avaient récemment adopté, ou étaient sur le point d'adopter, des lois incorporant la Loi type ou traitant de questions connexes relatives à la facilitation du commerce électronique. Un certain nombre de ces propositions législatives portaient également sur les signatures électroniques (ou, dans certains cas, plus particulièrement sur les signatures numériques). D'autres pays avaient créé des groupes de travail, dont certains en étroite coopération avec le secteur privé, qui étudiaient les besoins de modification de la législation pour faciliter le commerce électronique, qui envisageaient activement l'adoption de la Loi type et préparaient les textes nécessaires, et qui travaillaient sur les questions relatives aux signatures électroniques, notamment sur la mise en place d'infrastructures à clef publique ou d'autres projets concernant des questions y étant étroitement liées.

### B. EXAMEN DES PROJETS D'ARTICLES

20. Il a été rappelé qu'à la session précédente, le Groupe de travail n'avait pas pu, faute de temps, examiner le principe de la non-discrimination entre les certificats sur la base du lieu de leur émission (A/CN.9/457, par. 120), non plus que les questions relatives à la reconnaissance internationale des certificats. Avant d'entamer l'examen du projet d'article premier, il a donc décidé de procéder à un échange de vues sur les dispositions du projet d'article 13.

#### Article 13. Reconnaissance des signatures et certificats étrangers

21. Le texte du projet d'article 13 examiné par le Groupe de travail était le suivant:

> "1. Pour déterminer si, ou dans quelle mesure, un certificat [une signature] produit légalement ses effets, il n'est pas tenu compte du lieu où le certificat [la signature] a été émis [émise], ni de l'État dans lequel l'émetteur a son établissement.
>
> Variante A
>
> 2. Les certificats émis par un certificateur d'informations étranger sont reconnus comme équivalant juridiquement aux certificats émis par les certificateurs d'information soumis à ... *[la loi de l'État adoptant]* si les pratiques du certificateur d'informations étranger offrent un niveau de fiabilité au moins équivalent à celui qui est requis des certificateurs d'informations en vertu de ... *[la loi de l'État adoptant]*. [Cette reconnaissance peut se faire par une décision publiée de l'État ou par un accord bilatéral ou multilatéral entre les États concernés].

3. Les signatures conformes aux lois d'un autre État relatives aux signatures numériques ou autres signatures électroniques sont reconnues comme équivalant juridiquement aux signatures conformes à ... *[la loi de l'État adoptant]* si les lois de l'autre État exigent un niveau de fiabilité au moins équivalent à celui qui est exigé pour les signatures en vertu de ... *[la loi de l'État adoptant]*. [Cette reconnaissance peut se faire par une décision publiée de l'État ou par un accord bilatéral ou multilatéral avec d'autres États.]

4. Nonobstant le paragraphe précédent, les parties à des transactions commerciales et autres peuvent spécifier qu'il est nécessaire de recourir à un certificateur d'informations, une catégorie de certificateurs d'informations ou une catégorie de certificats particuliers pour les messages ou signatures qui leurs sont soumis.

Variante B

2. Les certificats émis par un certificateur d'informations étranger sont reconnus comme équivalant juridiquement aux certificats émis par les certificateurs d'informations soumis à ... *[la loi de l'État adoptant]* si les pratiques du certificateur d'informations étranger offrent un niveau de fiabilité au moins équivalent à celui qui est requis des certificateurs d'informations en vertu de ... *[la loi de l'État adoptant]*.

[3. L'équivalence visée au paragraphe 2 peut être déterminée par une décision publiée de l'État ou par un accord bilatéral ou multilatéral avec d'autres États.]

4. Pour la détermination de l'équivalence, il est tenu compte des critères suivants:

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

b) fiabilité du matériel et des logiciels;

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

d) possibilités d'accès à l'information pour les [signataires] [sujets] 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'habilitation ou de l'autorité de certification concernant le respect ou l'existence des critères énumérés ci-dessus;

g) possibilités d'exercice de la compétence des tribunaux de l'État adoptant; et

h) importance des divergences entre la loi applicable au comportement de l'autorité de certification et la loi de l'État adoptant."

Remarques générales

22. On s'est inquiété de savoir si le projet d'article 13 devait s'appliquer à la reconnaissance tant des certificats que des signatures. Selon une opinion, il devait s'appliquer en fait aux certificats et il valait mieux placer toute disposition traitant des effets juridiques des signatures dans les articles de fond relatifs aux signatures figurant au début des Règles uniformes. À l'appui de cet argument, on a déclaré qu'il pourrait être difficile de formuler une règle unique pour la reconnaissance des signatures étant donné les nombreuses fonctions de ces dernières et les différences de niveaux de fiabilité pouvant exister. On a aussi fait observer que l'on pouvait certes tenir compte à juste titre des facteurs énoncés au paragraphe 4 de la variante B pour les

certificats, mais que pour évaluer la fiabilité des signatures au sens de la variante A, il faudrait tenir compte de facteurs différents. Selon un avis contraire, le projet d'article devrait traiter de la reconnaissance tant des signatures que des certificats, puisque les deux étaient importants pour la question de l'identification dans le contexte d'un usage commercial et les Règles uniformes avaient pour objet d'élaborer des règles sur l'utilisation des signatures électroniques, y compris dans le commerce international. Après un débat, le Groupe de travail a décidé que la question devait demeurer ouverte jusqu'à l'examen des articles de fond.

Paragraphe 1

23. Le principe de non-discrimination énoncé au paragraphe 1 a bénéficié d'un appui général, mais des doutes ont été exprimés quant au fait de savoir si la disposition, telle qu'actuellement rédigée, reflétait correctement ce principe et s'il était approprié de se référer au pays d'origine. Selon un avis, la référence au pays d'origine se traduisait par une disposition de non-discrimination qui était trop étroite et qui laissait ouverte la possibilité qu'une discrimination se produise pour plusieurs autres motifs, ce qui ne serait pas souhaitable. Selon un autre avis, il pourrait en fait exister des cas où le pays d'origine de la signature ou du certificat était essentiel à la question de la reconnaissance. Il a été estimé, dans l'ensemble, que les avis et préoccupations susmentionnés devraient être pris en compte lors de la reformulation du paragraphe 1 afin de permettre une poursuite de la discussion lors d'une session future.

24. Il a été proposé de formuler plus clairement le principe de non-discrimination en employant le libellé suivant:

> "Pour déterminer si, ou dans quelle mesure, un certificat [une signature] produit légalement ses effets, il n'est pas tenu uniquement compte du lieu où le certificat [la signature] a été émis [émise], ni uniquement de l'État dans lequel l'émetteur a son établissement".

Cette proposition n'a pas été appuyée.

25. S'agissant de la relation entre le paragraphe 1 et les Variantes A et B, l'avis selon lequel seul le paragraphe 1 était nécessaire pour traiter la question de la reconnaissance de signatures et de certificats étrangers a bénéficié d'un appui. Il a été déclaré que les principes reflétés dans les Variantes A et B ne pouvaient être appuyés car ils étaient trop restrictifs, trop difficiles à vérifier et formulés en termes trop généraux pour donner des indications quant à la façon dont l'équivalence pourrait être établie. Il a été mis en avant qu'une règle de non-discrimination telle que celle énoncée au paragraphe 1 aurait pour effet d'inciter les parties à étudier les exigences d'autres juridictions où les transactions nécessitent des signatures et certificats étrangers afin de vérifier les preuves susceptibles d'être exigées pour que les signatures et certificats produisent légalement leurs effets et de déterminer quelle loi applicable serait souhaitable. Selon un avis contraire, une règle sur la non-discrimination n'était pas suffisante pour pouvoir comparer différents certificats et signatures, comparaison qui serait inévitablement requise pour faciliter l'utilisation internationale du commerce électronique. A cette fin, il fallait disposer d'une règle précisant comment la reconnaissance internationale pourrait s'effectuer. Un appui a été exprimé en faveur de l'avis selon lequel ce dont on avait besoin, au plan international, c'étaient d'indications quant aux critères, telle la fiabilité des certificats et signatures évoquée dans les Variantes A et B, sur lesquels la reconnaissance puisse se fonder. Après un débat, il a été généralement estimé que le paragraphe 1 n'était pas suffisant pour faciliter la reconnaissance internationale des certificats et signatures.

Variante A

26. L'avis selon lequel la Variante A, en se référant à la fiabilité, énonçait le critère essentiel d'équivalence sur lequel la reconnaissance pourrait se fonder, a bénéficié d'un appui. Selon un autre avis, la fiabilité devrait se limiter à la fiabilité technique, et des exigences telles que l'enregistrement d'un certificateur d'informations ne devraient pas être envisagées. On a exprimé, cependant, quelques inquiétudes quant à ce qu'une telle règle

pourrait signifier dans la pratique. On a craint que la Variante A ne donne lieu à une discrimination inverse si elle devait avoir pour effet, par exemple, qu'un certificateur d'informations étranger n'ait pas à se conformer à la loi de l'État qui reconnaît les signatures et certificats si ses pratiques sont jugées équivalentes, sur la base de certains critères, aux pratiques d'un certificateur d'informations national. On a craint en particulier, à cet égard, que le certificateur d'informations étranger puisse prendre l'avantage sur le certificateur national, surtout si les critères d'établissement de l'équivalence ne tenaient pas compte de contraintes administratives telles que l'enregistrement du certificateur d'informations. Le Groupe de travail a pris note de ces inquiétudes, compte tenu en particulier de l'accord qui s'était dégagé sur l'importance du principe de non-discrimination, mais il a généralement estimé que ces craintes pourraient être levées en définissant les critères à prendre en compte pour déterminer l'équivalence. Une autre crainte exprimée en rapport avec l'introduction éventuelle d'un critère de fiabilité technique (en particulier en rapport avec les certificats) avait trait à la mesure dans laquelle la fiabilité du certificat dépendait de la fiabilité du certificateur d'informations et, partant, de critères n'ayant pas de rapport direct avec des questions techniques.

27. S'agissant du critère éventuel à appliquer pour établir l'équivalence, on a estimé que l'accent placé, dans la Variante A, sur la fiabilité était trop étroit et que d'autres critères tels que l'environnement contractuel créé par les parties devaient être pris en compte pour déterminer l'équivalence. Il a également été mis en avant que les dispositions de la Variante A présupposaient un niveau de réglementation des certificateurs d'informations et des certificats qui pourrait, dans la pratique, ne pas être universel, et que leur application pourrait être difficile. Selon l'avis qui a prévalu au sein du Groupe de travail, la fiabilité était un critère approprié sur lequel on pouvait fonder la détermination de l'équivalence aux fins de la reconnaissance de certificateurs d'informations étrangers, sous réserve que soient établis certains critères à prendre en compte pour procéder à cette détermination.

28. L'admission de la nécessité d'accords bilatéraux et multilatéraux fixant les modalités de reconnaissance conformément aux paragraphes 2 et 3 de la Variante A a bénéficié d'un large appui.

29. Les membres du Groupe de travail se sont généralement déclarés favorables à l'introduction, dans le projet d'article 13, d'une disposition admettant largement l'autonomie des parties comme fondement de la reconnaissance internationale. Il a également été convenu que la liberté dont jouissaient les parties de s'entendre sur l'utilisation de certificats ou de signatures particuliers conformément au paragraphe 4 de la Variante A devrait être reconnue.

Variante B

30. Différentes vues ont été exprimées quant à la nécessité de conserver les critères énoncés au paragraphe 4 de la Variante B. Des membres de la Commission, qui étaient d'avis qu'il fallait conserver ces critères, ont répété qu'une base était nécessaire pour pouvoir établir la reconnaissance et que ce paragraphe, combiné au paragraphe 1 et à la Variante A, fournissait cette base. Selon un avis contraire, il était inapproprié d'introduire, dans un article traitant de la reconnaissance internationale des certificats et signatures, des exigences en rapport avec des certificateurs d'informations qui n'apparaissaient nulle part ailleurs dans le projet de Règles uniformes. Si les Règles uniformes devaient traiter des opérations des certificateurs d'informations et établir des critères auxquels on pourrait se référer pour évaluer la fiabilité de certificats émis par ces certificateurs d'informations, il faudrait inclure ces dispositions dans des articles de fond tels que le projet d'article 12. En outre, il a été indiqué que le fait de faire figurer ces critères uniquement dans des dispositions traitant de la reconnaissance de certificats et signatures étrangers risquait d'entraîner une discrimination et, partant, d'aller à l'encontre du principe énoncé au paragraphe 1. De surcroît, certaines craintes ont été exprimées quant à la pertinence de tous ces critères dans chaque cas, et quant à la nécessité de veiller à ce que cette disposition ne soit pas formulée comme étant obligatoire, ni comme se limitant aux critères énoncés.

31. Pour tenir compte de certains des avis et craintes exprimés pendant la discussion, il a été proposé une disposition relative à la reconnaissance qui serait libellée comme suit :

> "1. Pour déterminer si, ou dans quelle mesure, un certificat produit légalement ses effets, il n'est pas tenu compte du lieu où le certificat a été émis, ni de l'État dans lequel l'émetteur a son établissement.
>
> 2. Pour déterminer si, ou dans quelle mesure, un certificat produit légalement ses effets, il est fait référence aux lois de l'État qui le reconnaît ou de toute autre loi applicable dont peuvent convenir les parties.
>
> 3. Un certificat n'est pas considéré comme ne produisant pas légalement ses effets en vertu des lois de l'État qui le reconnaît ou de toute autre loi applicable dont conviennent les parties au seul motif qu'une exigence d'enregistrement en vertu de la loi applicable n'a pas été satisfaite.
>
> 4. Si un État reconnaissant le certificat a conclu un accord bilatéral ou multilatéral avec un autre État, un certificat émis conformément à cet accord est reconnu.
>
> 5. Si les parties conviennent d'être liées par un certificat émis par un certificateur d'informations spécifié, ce certificat est reconnu."

32. Des doutes ayant été exprimés quant à la façon dont cette proposition pourrait être interprétée, notamment en cas de problème de conflit de lois, elle a peu été appuyée.

33. Dans le contexte de la discussion sur ceux des critères énoncés au paragraphe 4 de la Variante B qu'il faudrait conserver, il a été mis en avant que ces critères n'étaient peut-être pas tous aussi utiles pour déterminer la fiabilité ou ce qui pourrait être requis pour prouver un certificat. En outre, selon un avis, il fallait bien s'assurer que le coût et la facilité d'établissement des preuves ne fassent pas obstacle à l'utilisation de certificats et de signatures électroniques. Le Groupe de travail a pris note de ces avis en vue de l'examen du paragraphe 4 à un stade ultérieur.

34. Après un débat, le Groupe de travail a conclu qu'en vue d'un réexamen futur: le paragraphe 1 devrait énoncer le principe de non-discrimination, son libellé étant quelque peu modifié pour tenir compte des avis exprimés pendant le débat; les paragraphes 2, 3 et 4 de la Variante A devraient être conservés car ils énonçaient une règle appropriée concernant la reconnaissance des certificats et signatures étrangers; le paragraphe 4 de la Variante B devrait énoncer les critères à prendre en compte pour déterminer l'équivalence de fiabilité en rapport avec les paragraphes 2 et 3 de la Variante A, mais que cette disposition ne devrait ni être obligatoire, ni se limiter aux critères particuliers énumérés; le projet d'article 13 devrait prévoir que la reconnaissance d'une convention entre les parties intéressées concernant l'utilisation de certains types de signatures électroniques ou de certificats est un motif suffisant pour la reconnaissance internationale (entre ces parties) des signatures ou certificats convenus; et la question de savoir si le projet d'article 13 devrait traiter à la fois des certificats et des signatures devrait être réexaminée lorsque des décisions concernant les articles de fond du projet de Règles uniformes auraient été prises.

35. Le Groupe de travail a convenu que, pour poursuivre le débat lors d'une session ultérieure, il faudrait que soit établie une autre version de l'article 13 tenant compte de l'avis selon lequel les critères énoncés en ce qui concerne les signatures ou certificats devraient s'appliquer de la même façon aux signatures ou certificats étrangers et nationaux. À cet effet, la substance de ces critères devrait être énoncée dans le projet d'article 12, le projet d'article 13 faisant quant à lui référence à l'obligation faite aux certificateurs d'informations étrangers de respecter les critères énoncés dans le projet d'article 12 pour obtenir la reconnaissance.

Article premier. Champ d'application

36. Le texte du projet d'article premier examiné par le Groupe de travail était le suivant:

"Les présentes règles s'appliquent aux signatures électroniques utilisées dans le contexte de relations commerciales* et ne se substituent à aucune loi visant à protéger les consommateurs.

*Le terme "relations 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."

37. On a noté tout d'abord que le projet d'article premier, qui reprenait un certain nombre de dispositions figurant dans l'article premier de la Loi type, était fondé sur l'hypothèse de travail selon laquelle les Règles uniformes devraient constituer un instrument juridique séparé et non pas seulement un chapitre séparé de la Loi type (voir A/CN.9/WG.IV/WP.82, par. 16). Selon une opinion, il serait peut-être nécessaire de réexaminer ultérieurement la question de l'adoption éventuelle des Règles uniformes comme supplément à la Loi type, mais le Groupe de travail a approuvé l'hypothèse de travail. Il a aussi été convenu qu'il faudrait s'employer, dans l'élaboration des Règles uniformes, à assurer une cohérence aussi bien avec le fond qu'avec la terminologie de la Loi type. Dans la note explicative, ou dans le guide pour l'incorporation des Règles uniformes, qui serait éventuellement établi à un stade ultérieur, il conviendrait de donner des explications sur la relation entre les règles et la Loi type. Il faudrait indiquer, à cet égard, que les Règles uniformes pourraient être adoptées séparément ou en tant que supplément de la Loi type.

38. Le projet d'article premier a été généralement approuvé quant au fond. S'agissant de la forme, il a été convenu qu'à des fins de cohérence avec la terminologie employée à l'article premier de la Loi type il conviendrait de remplacer les mots "relations commerciales" par les mots "activités commerciales". Il a été convenu par ailleurs que les mots "Les présentes Règles s'appliquent aux signatures électroniques utilisées..." ne traduisaient pas suffisamment bien l'étendue du champ d'application des Règles uniformes et devraient être remplacés par les mots "Les présentes règles s'appliquent lorsque des signatures électroniques sont utilisées...".

39. S'agissant des termes "activités commerciales", on s'est demandé s'il était vraiment nécessaire de limiter le champ d'application des Règles uniformes au domaine commercial. On a fait remarquer que ces règles devraient aussi s'appliquer, par exemple, lorsque des signatures électroniques étaient utilisées dans la soumission de déclarations ou d'autres documents à des administrations. On a fait observer que la question avait déjà été abordée lors de l'élaboration de la Loi type. Comme il était indiqué dans le Guide pour son incorporation, il avait été décidé que "rien dans la Loi type ne devrait empêcher un État d'élargir le champ d'application de la Loi type pour couvrir les utilisations du commerce électronique en dehors du domaine commercial" (Guide pour l'incorporation de la Loi type, par. 26). Il a été généralement convenu que l'on devrait adopter la même politique pour les signatures électroniques. En conséquence, il a été décidé d'insérer un libellé inspiré de la note*** relative à l'article premier de la Loi type dans la version révisée du projet d'article premier devant être élaborée afin de poursuivre la discussion à une session ultérieure.

40. S'agissant de la définition du terme "commercial", une question a été posée concernant la pertinence des mots "relation d'ordre commercial, qu'elle soit contractuelle ou non contractuelle". Toutefois, de l'avis général, les relations d'ordre commercial pouvaient certes être considérées comme intrinsèquement contractuelles dans certains pays, mais elles pouvaient également être considérées comme non contractuelles dans la législation

d'autres pays. En outre, il a été noté que la même définition du terme "commercial" avait été utilisée avec succès dans d'autres textes de la CNUDCI.

41. Il a été proposé d'exclure du champ d'application des Règles uniformes les utilisations des signatures électroniques dans lesquelles intervenaient des consommateurs. Il a été rappelé que le Groupe de travail avait examiné la question des consommateurs à sa précédente session (voir A/CN.9/457, par. 20, 56 et 70). Après un débat, le Groupe de travail a réaffirmé la décision adoptée à cette session, à savoir de n'affecter aucune loi visant à protéger les consommateurs. Toutefois, selon cette même décision, les consommateurs ne devraient pas être exclus du champ d'application des Règles uniformes puisque dans certains cas ces règles pourraient se révéler utiles pour eux.

42. Après avoir examiné le projet d'article premier, le Groupe de travail a décidé de reporter l'examen des définitions figurant au projet d'article 2 jusqu'à ce qu'il ait achevé d'examiner les dispositions de fond des Règles uniformes.

## Article 3. [Non-discrimination] [Neutralité technique]

43. Le texte du projet d'article 3 examiné par le Groupe de travail était le suivant:

> "[Aucune des dispositions des présentes Règles n'est appliquée] [Les dispositions des présentes Règles ne sont pas appliquées] de manière à exclure, restreindre ou priver d'effet juridique toute méthode [de signature] satisfaisant aux exigences de [*l'article 7 de la Loi type sur le commerce électronique*].

44. Les membres du Groupe de travail se sont généralement déclarés favorables à un principe s'inspirant du projet d'article 3, qui énonçait clairement que les Règles uniformes n'avaient pas pour objet de privilégier ou d'avantager certaines techniques, ce qui risquerait d'entraîner une discrimination à l'encontre d'autres techniques. Le Groupe de travail a réaffirmé l'importance du principe de neutralité technique sur lequel se fondait la Loi type et qui était aussi un élément essentiel du mandat confié au Groupe de travail pour la préparation des Règles uniformes.

45. Certaines craintes ont été exprimées quant à la façon dont la règle de non-discrimination devrait être formulée dans les Règles uniformes et quant au rapport entre ce principe et l'article 7 de la Loi type. L'un des problèmes avait trait au rôle de l'autonomie des parties au projet d'article 3. Selon un avis, toute référence à l'article 7 de la Loi type, puisqu'il s'agissait d'une disposition obligatoire non sujette à dérogation conventionnelle, limiterait l'aptitude des parties à s'entendre sur la façon de mener leurs transactions entre elles et, en particulier, sur ce qui pourrait constituer une signature. Il a été proposé de résoudre ce problème en supprimant la référence à l'article 7 et en terminant le projet d'article après le mot "méthode" ou en soumettant le projet d'article 3 aux dispositions relatives à l'autonomie des parties contenues dans le projet d'article 5. En vertu de la première proposition, le projet d'article 3 serait une déclaration générale de non-discrimination. En vertu de la seconde, le projet d'article 3 pourrait faire l'objet d'une dérogation conventionnelle en application du projet d'article 5. On a objecté que le projet d'article 3 mettait l'accent sur les mesures qu'un État pourrait prendre en matière législative en ce qui concerne la reconnaissance (ou l'effet juridique) de différentes techniques. Dans ce contexte, la question de l'autonomie des parties était sans objet. Il a par ailleurs été observé que, si l'article 7 de la Loi type offrait le moyen d'établir un équivalent fonctionnel pour les exigences légales applicables à une signature, il n'excluait pas des méthodes de signature qui pourraient quand même produire des effets juridiques même si elles ne satisfaisaient pas à ces exigences de forme. C'est pourquoi la question de l'autonomie des parties n'avait pas davantage d'objet dans le cadre d'un examen du projet d'article 3.

46. Une autre crainte exprimée quant à la relation entre le projet d'article 3 et l'article 7 de la Loi type avait trait au fait que, puisque les Règles uniformes pourraient être un texte indépendant ou autonome, le projet d'article 3 n'aurait que peu de sens pour les États qui n'adoptaient pas la Loi type ou, du moins, l'article 7 de

la Loi type. Pour résoudre cette difficulté, il a été proposé que le projet d'article 3 se réfère aux dispositions de la loi de l'État (adoptant les Règles uniformes) qui avaient trait aux signatures ou signatures électroniques. Il a été mis en avant que l'objet de la référence à l'article 7 était d'aller plus loin que la simple reconnaissance de signatures produisant des effets juridiques dans la loi nationale et de proposer le critère énoncé à l'article 7 aux États qui cherchent à adopter une nouvelle loi sur les signatures. À cet effet, la référence figurant dans le projet d'article 3 pourrait être soit une référence spécifique à l'article 7, soit une référence aux critères énoncés à l'article 7, soit encore une référence au projet d'article 6-2 des Règles uniformes, qui reprenait les critères de l'article 7. Il a été mis en avant qu'une référence aux critères de l'article 7 présenterait l'avantage de préserver ces critères dans les Règles uniformes puisque les pays qui adoptaient la Loi type pourraient modifier l'article 7 ou y déroger pour atténuer l'effet de ces critères. Si la proposition visant à adopter une référence à la loi nationale était retenue, cette référence serait alors une référence à quelque chose d'autre que les critères de l'article 7 de la Loi type. L'inclusion d'une référence aux critères de l'article 7, que ce soit en les reproduisant directement dans le projet d'article ou par une référence à l'article 6-2, et l'inclusion d'une référence à la loi applicable, ont toutes deux bénéficié d'un certain appui.

47. Plusieurs propositions de nature rédactionnelle ont été faites. Le premier ensemble de mots d'ouverture "Aucune des dispositions des présentes Règles..." a bénéficié d'un certain appui. Les propositions visant soit à conserver, soit à supprimer les mots "[de signature]" et à ajouter le qualificatif "électronique" avant "signature" ont également bénéficié d'un certain appui. Le Groupe de travail a convenu qu'il s'agissait là d'une question de rédaction qui dépendait, le cas échéant, des mots utilisés pour achever la phrase. Il a en outre été proposé de remplacer "priver d'effet juridique" par les mots "exercer une discrimination à l'encontre de", mais cette proposition n'a pas reçu d'appui. Les deux alternatives figurant entre crochets en titre du projet d'article 3 ont toutes deux bénéficié d'un appui. Il a également été proposé le titre "Égalité de traitement des signatures électroniques". Une certaine préférence a été accordée à l'inclusion, dans le titre du projet d'article 3, d'une référence au principe de neutralité technique.

48. Après un débat, le Groupe de travail a convenu qu'un article s'inspirant du projet d'article 3 était très important pour s'assurer que le principe de non-discrimination s'applique à différents types de technique de signature, que cette technique soit actuellement utilisée ou qu'elle soit éventuellement mise au point à l'avenir; qu'il n'existait aucun rapport entre les projets d'articles 3 et 5 des Règles uniformes et que, par conséquent, aucune disposition de dérogation conventionnelle n'était nécessaire dans le projet d'article 3; que les mots d'ouverture du projet d'article 3 devraient être "Aucune des dispositions des présentes Règles..."; que s'il existait une certaine préférence, s'agissant du titre du projet d'article 3, pour "Neutralité technique", le secrétariat pourrait souhaiter envisager d'autres titres possibles pour tenir compte des avis exprimés par le Groupe de travail; que la référence à l'article 7 de la Loi type, bien qu'elle eût exclusivement pour objet d'être une référence à l'article 7 tel que promulgué par les États adoptants, devrait être remplacée par une référence au projet d'article 6-2 des Règles uniformes y compris aux critères énoncés à l'article 7 de la Loi type (tels que proposés initialement et énoncés au par. 55 du document A/CN.9/457); qu'on pourrait ajouter, pour compléter la référence au projet d'article 6-2, les mots "[ou satisfaisant autrement aux exigences de la loi applicable]" en vue de leur examen ultérieur par le Groupe de travail.

### Article 4. Interprétation

49. Le texte du projet d'article 4 examiné par le Groupe de travail était le suivant:

> "1. Pour l'interprétation des présentes Règles uniformes, il est tenu compte de leur origine internationale et de la nécessité de promouvoir l'uniformité de leur application et le respect de la bonne foi dans le commerce électronique.
>
> 2. Les questions concernant les matières régies par les présentes Règles uniformes qui ne sont pas expressément réglées par elles sont tranchées selon les principes généraux dont elles s'inspirent."

50. Le projet d'article 4 tel qu'il était rédigé a reçu dans l'ensemble un accueil favorable, bien que certains doutes aient été émis quant au sens des mots "dans le commerce électronique" au paragraphe 1. Il a été noté que le commerce électronique n'était pas défini. Bien que le sens de ce terme soit examiné dans le Guide pour l'incorporation de la Loi type, il a été jugé que cela ne suffisait pas et que, si l'on conservait la référence à la bonne foi "dans le commerce électronique", le texte des Règles uniformes devrait indiquer clairement quelle serait la portée exacte de ces mots. Selon un autre avis, ces mots pourraient contribuer à définir le domaine dans lequel l'exigence de la bonne foi devait opérer, comme c'était le cas dans d'autres textes de la CNUDCI, par exemple l'article 7 de la Convention des Nations Unies sur les contrats de vente internationale de marchandises ("Convention sur les ventes"), qui faisait référence à la bonne foi "dans le commerce international", ou l'article 5 de la Convention des Nations Unies sur les garanties indépendantes et les lettres de crédit stand-by, qui faisait référence à la bonne foi "dans la pratique internationale en matière de garantie indépendante et de lettre de crédit stand-by". Toutefois, après un débat, il a été décidé de supprimer les mots "dans le commerce électronique".

Article 5. Dérogation conventionnelle

51. Le texte du projet d'article 5 examiné par le Groupe de travail était le suivant:

Variante A

"[Les parties sont libres, par convention expresse ou tacite, de déroger à tout aspect des présentes Règles ou de s'en écarter,] [Il est possible de déroger à tout aspect des présentes Règles ou de s'en écarter, par convention expresse ou tacite,] à moins que cette dérogation ou cet écart ne porte atteinte aux droits des tiers.

Variante B

1. Les présentes Règles sont sans effet sur tout droit qui pourrait exister de modifier par convention l'une des règles de droit visées aux articles 6 et 7.

2. Il est possible de déroger à tout aspect des articles 9 à 12 des présentes Règles ou de s'en écarter par convention expresse ou tacite, à moins que cette dérogation ou cet écart ne porte atteinte aux droits des tiers."

Remarques générales

52. Pour ce qui est du principe général de l'autonomie des parties, il a été déclaré que les seules restrictions que les Règles uniformes devraient imposer aux parties commerciales, pour ce qui est de la réglementation des questions commerciales entre elles et avec des tiers, devraient être les restrictions imposées par les lois des États adoptant les Règles uniformes.

53. Pour ce qui est des variantes A et B, on s'est déclaré favorable à la suppression des membres de phrase faisant référence aux droits des tiers. Il a été déclaré que ce principe, de même que le principe selon lequel les parties ne pouvaient modifier par convention les règles de droit impératif, était un principe reconnu internationalement comme fondamental, qui n'avait donc pas à être énoncé dans les Règles uniformes. Selon un autre avis, la référence aux droits et obligations des tiers entrerait dans la catégorie plus générale des exceptions à l'autonomie des parties fondées sur des raisons d'ordre public, exceptions qu'il pourrait être utile d'énoncer dans cet article. Selon un avis contraire, les questions d'ordre public devraient être laissées au droit interne et non être traitées dans les Règles uniformes.

54. Le Groupe de travail a procédé a un échange de vues sur le titre du projet d'article 5 et diverses propositions de changement ont été faites, telles que "Autonomie des parties "et "Liberté contractuelle". Après

un débat, le Groupe de travail a prié le secrétariat de prendre ces avis en considération lorsqu'il réviserait le projet d'article 5.

Variante A

55. Divers avis ont été exprimés à l'appui de la variante A. Selon un avis, comme la règle énoncée dans la variante B spécifiait quels articles des Règles uniformes devaient être considérés comme impératifs, elle exprimait le principe de l'autonomie des parties de manière plus restrictive que la variante A. La variante B risquerait donc d'avoir pour effet d'inhiber, plutôt que de faciliter, le développement du commerce électronique. Il a été noté que l'absence de réglementation avait grandement facilité le développement de l'échange de données informatisées et avait permis aux parties de trouver des solutions contractuelles aux questions juridiques qui se posaient. Pour ces raisons, les Règles uniformes ne devraient pas tenter d'énoncer des dispositions impératives telles que celles qui figuraient dans la variante B. Selon un autre avis, dans un contexte commercial, les parties devraient être entièrement libres de convenir de la manière dont elles conduiraient leurs relations et leurs transactions, y compris de ce qu'elles considéreraient comme une signature. Il a été reconnu que les parties commerciales pouvaient effectivement conclure de telles conventions "entre elles", mais on a exprimé quelques doutes quant à la valeur juridique que pourraient avoir de telles conventions lorsque des conditions de forme s'appliquaient au contexte commercial.

56. On a toutefois fait valoir qu'il serait possible de décider à un stade ultérieur des délibérations du Groupe de travail si certains articles des Règles uniformes devraient être impératifs et, si nécessaire, d'indiquer cette décision dans les articles pertinents, plutôt que de diluer l'article sur l'autonomie des parties. À cette fin il a été proposé de modifier comme suit les premiers mots de la variante A: "Sauf disposition contraire des présentes Règles...".

57. Pour ce qui est de la forme, il a été proposé de supprimer la référence à une convention "expresse ou tacite" et de remplacer le verbe "déroger" par le verbe "modifier". Vu les décisions prises ultérieurement par le Groupe de travail, ces suggestions n'ont pas été retenues.

Variante B

58. La variante B a reçu un accueil favorable. Il a été noté que les projets de paragraphes 1 et 2 s'inspiraient fortement de l'article 4 de la Loi type. Ainsi, les projets d'articles 6 et 7 des Règles uniformes, comme les articles 7 et 8 de la Loi type sur lesquels ils se fondaient, seraient des dispositions impératives. De même, conformément au paragraphe 2 de l'article 4 de la Loi type, le projet de paragraphe 1 de la variante B préservait le droit des parties de modifier des dispositions impératives lorsque la loi nationale le leur permettrait. Les projets d'articles 9 à 12 des Règles uniformes, par comparaison, étaient des dispositions auxquelles les parties pouvaient librement déroger, de même que les dispositions du chapitre III de la Loi type.

59. Afin de tenir compte de certains des avis et préoccupations exprimés à propos des deux variantes, la proposition suivante relative à l'autonomie des parties a été faite:

"Il est possible de déroger aux présentes Règles ou de s'en écarter par convention, à moins que:

a) les présentes Règles n'en disposent autrement;

b) la loi de l'État adoptant n'en dispose autrement."

60. Cette proposition a reçu dans l'ensemble un accueil favorable. Des préoccupations ont toutefois été exprimées à propos du paragraphe b), au motif qu'il s'agissait là d'une disposition très large, qui laissait les États libres d'imposer une réglementation restrictive quant à l'utilisation des signatures électroniques et n'encourageait pas l'adoption d'une norme telle que l'article 7 de la Loi type. Le Groupe de travail a noté qu'il

serait certes impossible d'empêcher un État d'adopter une telle position, mais qu'on pourrait mentionner dans un guide ou dans un rapport explicatif relatif aux Règles uniformes que ces dispositions restrictives devraient être l'exception plutôt que la règle. Il a aussi été proposé que le paragraphe b) soit placé entre crochets, dans l'attente d'un examen plus approfondi par le Groupe de travail. Après un débat, le Groupe de travail a adopté la proposition.

61. Il a été proposé, quant à la forme, que la référence à la "dérogation" ou à l'"écart" porte sur les "effets" des Règles, plutôt que sur les Règles elles-mêmes. Il a été convenu, comme ce type de disposition figurait dans un grand nombre d'instruments internationaux (par exemple, la Convention sur les ventes), que l'on se conformerait à la formulation habituelle.

Article 6. [Respect des exigences concernant la signature] [Présomption de signature]

62. Le texte du projet d'article 6 examiné par le Groupe de travail était le suivant:

"Variante A

1. Lorsque, dans le cas d'un message de données, il est fait usage d'une signature électronique renforcée, le message de données est présumé signé.

2. 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 tout accord en la matière.

[3. 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 renforcée.]

4. Les paragraphes 2 et 3 s'appliquent, 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.

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

Variante B

1. Lorsque, dans le cas d'un message de données, il est fait usage d'une [méthode] [signature électronique] qui:

a) est particulière au détenteur de la signature [aux fins pour lesquelles] [dans le contexte où] elle est utilisée;

[b) peut être utilisée pour identifier objectivement le détenteur de la signature dans le cadre du message de données; et]

c) a été créée et apposée au message de données par le détenteur de la signature ou à l'aide d'un moyen dont seul ce détenteur a le contrôle [et par nulle autre personne];

le message de données est présumé signé.

2. 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.

3. Le paragraphe 2 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.

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

Objet de l'article 6

63. De l'avis général, le projet d'article 6 devrait avoir principalement pour objet d'établir un degré de certitude quant aux effets juridiques qui découleraient de l'utilisation de signatures électroniques. Quant à ce que ces effets juridiques pourraient être, le débat s'est développé dans différentes directions, une référence constante étant faite à la question de la satisfaction des exigences de signature évoquées à l'article 7 de la Loi type.

Types de signature électronique

64. Selon un avis, 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 méthodes de signature électronique reconnues comme fiables; et 2) inversement, qu'aucun effet juridique de ce type ne découlerait de l'utilisation de méthodes 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, les Règles uniformes 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 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*, éventuellement longtemps après que la signature électronique eût été utilisée, pouvait déterminer ce qui constituait une technique fiable de signature compte tenu des circonstances en vertu de l'article 7 de la Loi type. En revanche, l'avantage escompté des Règles uniformes pour certaines techniques reconnues comme étant particulièrement fiables indépendamment des circonstances dans lesquelles elles étaient utilisées était de 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.

65. La question a été posée de savoir si un effet juridique devrait découler de l'utilisation de techniques de signature électronique qui ne satisferaient pas à toutes les fonctions décrites à l'article 7-1 a) de la Loi type, à savoir de signatures électroniques qui ne seraient pas faites dans l'intention d'indiquer une approbation de l'information contenue dans le message de données. On a généralement estimé qu'en apposant une signature (qu'elle soit manuscrite ou électronique) à une information, le signataire présumé 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 des Règles uniformes. Dans ce contexte, le Groupe de travail a convenu que les Règles uniformes ne devraient pas porter atteinte au droit général des contrats ou des obligations.

66. Il a été noté que les variantes A et B, bien que visant le même résultat dans la pratique, différaient quant au fait de savoir si elles se fondaient ou non sur la notion de "signature électronique renforcée". Le maintien de la notion de signature électronique renforcée, décrite comme particulièrement apte à fournir une certitude quant à l'utilisation d'un certain type de signature électronique, à savoir les signatures numériques appliquées au moyen d'infrastructures à clef publique, a bénéficié d'un appui. On a fait valoir, à l'opposé, que la notion de "signature électronique renforcée" compliquait inutilement la structure des Règles uniformes. En outre, cette

notion se prêterait à des malentendus en suggérant que différents niveaux de fiabilité pourraient correspondre à un nombre également diversifié d'effets juridiques. De nombreuses délégations ont exprimé la crainte que l'on considère une signature électronique renforcée comme une notion juridique distincte plutôt que comme l'expression d'un ensemble de critères techniques dont l'utilisation rendait une méthode de signature particulièrement fiable. Tout en reportant sa décision finale sur la question de savoir si les Règles uniformes se fonderaient sur la notion de "signature électronique renforcée", le Groupe de travail a généralement convenu que, lors de l'établissement d'une version révisée des Règles uniformes en vue de la poursuite du débat à une session ultérieure, il serait utile de présenter une version des projets d'articles qui ne se fondait pas sur cette notion.

Relations avec l'article 7 de la Loi type

67. Selon un avis, la référence à l'article 7 de la Loi type au paragraphe 2 du projet d'article 6 (qui était également utile comme rappel de l'origine conceptuelle des Règles uniformes) devait être interprétée comme limitant le champ d'application des Règles aux situations dans lesquelles 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 loi contenait très peu de prescriptions de ce type applicables aux documents utilisés dans les transactions commerciales, le champ d'application des Règles uniformes 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) était incompatible avec l'interprétation du terme "loi" adoptée par la Commission au paragraphe 68 du Guide pour l'incorporation de la Loi type, 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". Le paragraphe 1 tant de la variante A que de la variante B ne contenait aucune référence à une "exigence légale" et le paragraphe 2 reprenait le libellé de l'article 7 de la Loi type mais, selon l'interprétation de la plupart des délégations, il n'existait aucune différence de champ d'application entre les deux paragraphes, ce champ étant 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.

Effet juridique: présomption ou règle de fond

68. Divers avis ont été exprimés quant à savoir précisément quel effet juridique devrait découler de l'utilisation d'une signature électronique fiable. Selon un avis, la question de savoir si le document devrait être considéré comme "signé" devrait être distinguée de la question de savoir s'il devrait être considéré comme signé par une personne donnée. Selon un autre avis, il serait inapproprié d'établir une présomption selon laquelle l'information était "signée" car, en vertu des lois de plusieurs pays, le mot "signature" indiquait l'intention émise par le signataire d'être lié, par exemple dans un contexte contractuel. Le fait de présumer l'intention risquerait de faire porter un poids excessif sur le signataire présumé, et risquerait de porter atteinte à la loi existante relative à la formation de contrats ou d'obligations. En conséquence, il a été proposé qu'au lieu d'établir une présomption selon laquelle le message de données était "signé", les Règles uniformes devraient se contenter d'établir la présomption d'un lien entre la signature électronique et le signataire présumé, ainsi qu'une présomption quant à la fiabilité de la méthode de signature utilisée. Toute conclusion supplémentaire concernant l'effet de la signature électronique à l'égard de la substance du message de données devrait, a-t-on déclaré, relever de la loi applicable par ailleurs. Ces avis ont bénéficié d'un certain appui.

69. À ce sujet, il a aussi été indiqué que l'approche adoptée dans le projet d'article 6 de pair avec la définition de la "signature électronique" au projet d'article 2 était acceptable. Selon cette approche, l'utilisation d'une signature électronique fiable devrait entraîner la "signature" du message de données par le détenteur du dispositif de signature, en partant de l'hypothèse que les conséquences de cette "signature", en particulier quant à l'intention du signataire présumé concernant l'information contenue dans le message de données, seraient traitées par la loi applicable en dehors des Règles uniformes.

70. Le Groupe de travail a généralement convenu que l'article 6 devrait être axé sur la réplication, dans un environnement électronique, des conséquences juridiques de l'utilisation d'une signature manuscrite. Puisqu'il avait été déclaré que l'emploi du verbe "signer" était, dans certains pays, inapproprié dans le contexte des messages électroniques, il a été proposé de partir du principe que l'on faisait référence, dans les discussions, à l'équivalent fonctionnel de ce terme, sauf lorsque le contexte montrait qu'il s'agissait d'une signature manuscrite. Le Groupe de travail a ensuite examiné le fait de savoir si les effets juridiques de l'utilisation d'un dispositif de signature électronique fiable devraient être exprimés au moyen d'une présomption ou d'une règle de fond.

71. Il a été estimé qu'une disposition de fond était nécessaire, au lieu d'une présomption qui pourrait être considérée dans certains systèmes juridiques comme limitée au domaine de la procédure civile, pour reconnaître les effets juridiques de l'utilisation de signatures électroniques. Il a été proposé d'adopter, sur le modèle du paragraphe 1 de la variante A, une règle libellée comme suit: "Lorsque, dans le cas d'un message de données, il est fait usage d'une signature électronique, il est attribué à cette signature électronique un effet juridique analogue [à celui qui serait produit si l'information contenue dans le message de données avait été manuscrite et signée] [à celui attribué à une signature manuscrite en vertu de la loi applicable]". Il a été mis en avant qu'un libellé analogue pourrait être établi sur la base du paragraphe 1 de la variante B. Cette proposition a bénéficié d'un certain appui. Selon un avis, le principe figurant dans le texte proposé devrait s'appliquer à toutes les signatures électroniques, mais un certain nombre de délégations ont fait observer que la disposition de fond devrait être de portée limitée, de manière à ne viser que les signatures électroniques "renforcées" selon le projet d'article 2.

72. Selon un avis largement partagé, cependant, le projet d'article 6 était rédigé de façon appropriée sous la forme d'une présomption réfragable. L'avis selon lequel une présomption réfragable de "signature" par un signataire présumé était l'effet le plus approprié qui pouvait résulter de l'utilisation d'une méthode de signature fiable a bénéficié d'un appui. L'effet d'une telle présomption consisterait à placer sur le signataire présumé la charge de prouver que la signature électronique ne devrait pas être attribuée à cette personne ou qu'elle ne devrait pas être considérée comme contraignante. Dans ce contexte, bien que des craintes aient été exprimées quant à la façon dont le signataire présumé réfuterait la présomption, par exemple dans le contexte de la formation d'un contrat, il a été rappelé que les Règles uniformes ne faisaient qu'établir l'équivalence entre certaines signatures électroniques et manuscrites, et n'avaient pas pour objet de porter atteinte au droit général des contrats ou des obligations.

73. Selon un avis, que le projet d'article 6 établisse une présomption selon laquelle les données étaient "signées" ou une simple présomption selon laquelle la signature électronique était techniquement fiable et liée à un message donné, la charge de réfuter ces présomptions pourrait être trop onéreuse dans le contexte de transactions de consommateurs, qu'il pourrait donc être nécessaire d'exclure du champ d'application du projet d'article 6.

74. En ce qui concerne la nature de la présomption à établir, on a déclaré qu'il fallait certes intégrer la substance de la proposition de création d'une règle de fond (voir ci-dessus le paragraphe 71) dans le projet d'article 6, mais qu'il était nécessaire de créer une présomption qui tienne davantage compte du contexte, en matière de règles de la preuve, dans lequel elle serait appliquée. On a fait remarquer qu'il pourrait être moins ambitieux mais plus réaliste d'établir une présomption uniquement à des fins de preuve que d'établir des critères généraux de fiabilité sur lesquels on se fonderait pour présumer que des messages de données étaient "signés". D'une part, la fiabilité technique était une réalité qui évoluait rapidement. Il pourrait donc être extrêmement difficile d'exprimer des critères techniques en des termes suffisamment neutres pour qu'ils ne deviennent pas rapidement obsolètes. D'autre part, étant donné l'évolution des pratiques d'utilisation des signatures électroniques, il fallait un critère souple, comme celui qui était énoncé au paragraphe 1 b) de l'article 7 de la

Loi type, plutôt qu'un critère général de fiabilité inspiré du paragraphe 1 du projet d'article 6. Pour illustrer l'approche suggérée, le texte ci-après a été proposé:

"Article 6. Présomptions ayant des incidences sur les signatures électroniques

1. Les conséquences juridiques de l'utilisation d'une signature s'appliquent également à l'utilisation des signatures électroniques.

2. 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.

3. Si les exigences du paragraphe 4 sont satisfaites, un tribunal judiciaire ou administratif est fondé à présumer qu'une signature électronique prouve un ou plusieurs des points suivants:

a) conformité de la signature électronique à la norme de fiabilité énoncée au paragraphe 2;

b) identité du signataire présumé;

c) approbation par le signataire présumé du message de données auquel se rapporte la signature électronique.

4. Les présomptions établies au paragraphe 3 s'appliquent uniquement si:

a) la personne se fiant à la signature électronique adresse* au signataire présumé une notification affirmant qu'une signature électronique donnée prouve un ou plusieurs des points énoncés aux alinéas a) à c) du paragraphe 3; et

b) le signataire présumé n'adresse* pas de notification réfutant un ou plusieurs des points énoncés dans la notification mentionnée à l'alinéa a) et fournit les motifs de cette réfutation.

*Les exigences en matière de notification (y compris les délais) sont régies par la loi applicable. Certains États pourraient souhaiter ajouter des dispositions pour traiter ces questions."

75. Cette proposition a bénéficié d'un appui, en particulier parce qu'elle serait applicable aux transactions dans lesquelles interviennent des consommateurs, puisque la présomption pourrait être réfragable par simple notification de réfutation. Toutefois, il a été généralement estimé, en particulier pour ce qui était des nouveaux paragraphes 3 et 4, que le libellé suggéré pourrait être par trop axé sur les pratiques suivies en matière de preuve dans les procédures judiciaires de certains systèmes juridiques et pourrait être difficile à reformuler en des termes suffisamment neutres pour l'adapter à tous les systèmes juridiques. De manière générale, on a estimé que le paragraphe 4 proposé cherchait trop à harmoniser les règles de la procédure civile, domaine qui ne se prêtait pas aisément à un traitement dans des instruments internationaux. S'agissant des paragraphes 1 et 2, on a déclaré qu'il faudrait peut-être revoir les rapports entre les deux dispositions afin d'éviter que l'on puisse penser à tort que les signatures électroniques sans réserves seraient traitées plus favorablement que les signatures électroniques devant satisfaire à des critères de fiabilité.

76. En réponse à l'objection soulevée concernant le texte des nouveaux paragraphes 3 et 4, il a été proposé de remplacer ces derniers par un seul paragraphe 3 qui se lirait comme suit:

"[3. En l'absence de preuve contraire, il est présumé que la confiance dans une signature électronique prouve:

a) la conformité de la signature électronique à la norme de fiabilité énoncée au paragraphe 2;

b) l'identité du signataire présumé; et

c) l'approbation par le signataire présumé du message de données auquel se rapporte la signature électronique.]"

77. On a estimé que le Groupe de travail devrait continuer, à une future session, de chercher à déterminer s'il était possible d'élaborer une règle de procédure acceptable selon laquelle, lorsque le signataire présumé entendait réfuter sa signature, il devait en aviser promptement la partie s'y fiant et donner les motifs raisonnables de cette réfutation. À cet égard, il a été proposé de s'inspirer de l'article 16 de la Loi type de la CNUDCI sur l'insolvabilité internationale. Mais on a fait remarquer, à l'encontre de cette proposition, que si l'on pouvait concevoir une harmonisation limitée de la procédure civile dans le contexte restreint de l'insolvabilité internationale, cela pourrait être plus difficile pour les questions plus larges relatives aux signatures électroniques.

Critères de fiabilité d'une signature électronique

78. Dans le cadre du débat sur la manière de formuler le projet d'article 6 comme présomption réfragable, les membres du Groupe de travail ont accordé une attention particulière aux critères sur lesquels se fonder pour mesurer la fiabilité de la technique de signature. Pour exprimer de façon plus objective les critères énoncés au paragraphe 1 de la variante B, il a été proposé de rédiger comme suit le projet d'article 6:

"Article 6. Respect des exigences juridiques concernant la 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 méthode 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 tout accord en la matière.

2. Une méthode est présumée fiable, en ce qu'elle satisfait à l'exigence énoncée au paragraphe 1, lorsqu'elle garantit:

a) que les données utilisées pour la création d'une signature électronique sont particulières au détenteur du dispositif de création de signature dans le contexte dans lequel ce dispositif est utilisé;

b) que le détenteur du dispositif de création de signature a seul le contrôle de ce dispositif;

c) que la signature électronique est liée au message de données auquel elle se rapporte [d'une manière qui garantit l'intégrité du message];

d) que le détenteur du dispositif de création de signature est objectivement identifié dans le contexte [dans lequel le dispositif est utilisé] [du message de données]."

79. La formulation du projet d'article 6 en tant que présomption de la fiabilité technique a bénéficié d'un appui considérable. On s'est toutefois demandé s'il était nécessaire d'établir des critères techniques détaillés pour mesurer cette fiabilité. Selon un avis, dans la plupart des situations pratiques, la fiabilité serait prédéterminée, soit par convention entre les parties, soit du fait de la confiance dans une infrastructure à clef publique de caractère public ou privé. Cette opinion a été largement partagée mais on a aussi estimé qu'il serait souhaitable de prévoir des critères par défaut pour l'évaluation de la fiabilité des techniques de signature électronique, principalement à l'intention des pays ne disposant pas encore d'une infrastructure à clef publique bien établie.

80. S'agissant des différents critères proposés, on a fait observer que les Règles uniformes, ou tout guide pour leur incorporation ou toute note explicative qui pourraient être établis ultérieurement, devraient préciser les points suivants: 1) les dispositions selon lesquelles le détenteur du dispositif de création de signature devait être le seul à en avoir le contrôle ne devraient pas avoir d'incidences sur le droit de la représentation ou sur la représentation du détenteur du dispositif au moyen d'un objet servant d'intermédiaire de communication; et 2) "l'identification objective" du détenteur du dispositif ne devrait pas impliquer qu'une personne soit nécessairement identifiée par son nom, puisque la notion "d'identité" devrait être interprétée comme englobant éventuellement des caractéristiques significatives du détenteur du dispositif, telles que la position ou l'autorité, soit en association avec un nom, soit sans référence à un nom (voir A/CN.9/WG.IV/WP.82, par. 29). En outre, on a demandé s'il était approprié de faire référence à l'intégrité du message lorsqu'il s'agissait d'établir si un message de données était "signé", puisque la vérification de "l'intégrité" ne faisait pas intrinsèquement partie du processus de signature (qu'il s'agisse d'une signature électronique ou manuscrite) et pourrait sembler plus pertinente lorsqu'il fallait déterminer si le message devait être considéré comme "original".

81. De manière plus générale, s'agissant des critères à utiliser pour déterminer la fiabilité d'une méthode de signature, il a été déclaré que tout critère de ce type devrait être libellé de manière à appuyer la présomption et ne devrait pas revenir à prouver de façon indépendante la conclusion devant être présumée. Les critères de reconnaissance des certificats étrangers au projet d'article 13 et, éventuellement, les responsabilités d'un certificateur d'informations au projet d'article 12, pourraient constituer, a-t-on avancé, des critères supplémentaires utiles pour déterminer la fiabilité. Par ailleurs, les critères figurant dans la variante B n'aidaient que peu ou pas du tout à déterminer si une méthode de signature était fiable. La plupart, sinon la totalité, s'appliqueraient à n'importe quelle méthode. On a déclaré que le principal objectif devait être de déterminer le degré de confiance pouvant résulter de l'application des critères établis. Même les signatures numériques étayées par des certificats offraient différents niveaux de garantie. On a fait observer que les membres du Groupe de travail ne s'étaient pas encore accordés sur le niveau de garantie nécessaire pour la présomption proposée.

82. Après un débat, le Groupe de travail est convenu de reprendre l'examen du projet d'article 6 à une session ultérieure. Il a été demandé au secrétariat d'établir une version révisée du projet tenant compte des vues et préoccupations susmentionnées qui pourraient constituer des variantes. En établissant ces variantes, le secrétariat devrait envisager une version du projet d'article 6 qui combinerait les approches proposées aux paragraphes 74, 76 et 78 ainsi que les paragraphes 3 et 4 de la variante B.

## Article 7. [Présomption d'original]

83. Le texte du projet d'article 7 examiné par le Groupe de travail était le suivant:

> "1. Lorsque, dans le cas d'un message de données, [il est fait usage d'une signature électronique renforcée] [il est fait usage d'une signature électronique [méthode] qui offre une garantie fiable quant à l'intégrité de l'information à compter du moment où elle a été créée pour la première fois sous sa forme définitive, en tant que message de données ou autre], le message de données est présumé original.
>
> 2. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...]."

84. L'objet du projet d'article 7 a suscité un certain nombre de questions et on s'est demandé s'il était nécessaire d'inclure un tel article dans les Règles uniformes. Il a été noté que ce projet d'article avait pour objet d'établir que les critères offrant une garantie fiable quant à l'intégrité de l'information figurant dans un message de données (dans le contexte d'un original au sens de l'article 8 de la Loi type) seraient satisfaits ou seraient présumés être satisfaits par l'utilisation d'une méthode de signature électronique. Selon un avis, l'utilisation d'une signature en tant que moyen de satisfaire de tels critères, énoncés à l'article 8 de la Loi type, ne serait peut-être pas appropriée à la notion d'"original" et pourrait avoir pour effet d'imposer l'utilisation d'une

signature en tant que condition de l'original, même quand une signature ne serait pas nécessaire par ailleurs. En outre, on a estimé qu'il n'apparaissait pas clairement de quelle manière fonctionnerait l'article 7 lorsque ce qui était requis était un original unique. Il a également été jugé que l'utilisation d'une méthode particulière de signature afin d'établir la présomption d'un original pourrait être interprétée comme s'écartant du critère souple énoncé au paragraphe 3 de l'article 8 de la Loi type et ne serait sans doute pas neutre du point de vue technique.

85. Selon un autre avis encore, si le projet d'article 7 avait pour objet de donner un moyen de satisfaire aux critères énoncés à l'article 8, non seulement l'alinéa a), mais aussi l'alinéa b) du paragraphe 1 de l'article 8 devraient être mentionnés dans le projet d'article 7. De même, il a été noté que l'établissement de la présomption d'un original au projet d'article 7 n'était pas entièrement conforme à l'article 8 de la Loi type, qui faisait référence à une information "sous sa forme originale". Comme la notion d'"original" était difficile à comprendre dans le contexte du commerce électronique, la présomption énoncée au projet d'article 7 devrait faire référence au fait que le message de données avait la valeur d'un original ou était l'équivalent d'un original. Selon un autre avis, le projet d'article 7 devrait avoir pour objet, pour ce qui est de l'intégrité du message de données, d'établir que, par l'utilisation d'une méthode de signature, ce message pouvait être présumé non altéré; la question ne devrait pas être de savoir si le message de données satisfaisait à l'exigence d'un original, car cela faisait l'objet de l'article 8 de la Loi type.

86. Pour ce qui est de la manière dont le projet d'article 7 fonctionnerait dans la pratique, il a été noté que, dans son libellé actuel, le projet était dans une certaine mesure circulaire. Il a été jugé qu'au fond, le projet d'article 7 disposait que, lorsqu'une méthode permettait de démontrer l'intégrité par référence à certains critères techniques et que cette méthode était utilisée, on pouvait présumer l'intégrité. Dans ce cas, toutefois, l'intégrité serait prouvée par l'utilisation d'une méthode; il s'agissait donc là d'un fait et non de quelque chose que l'on pouvait présumer. De même, si le projet d'article 7 faisait référence à l'utilisation d'une signature électronique renforcée, l'utilisation d'une telle signature conduirait à la présomption d'intégrité. Toutefois, si on l'examinait à la lumière de la définition de la signature électronique renforcée figurant dans le projet d'article 2, le projet d'article 7 n'aurait pas grande utilité car l'intégrité était potentiellement une caractéristique de la signature électronique renforcée.

87. À l'appui du maintien du projet d'article 7, il a été noté que, si les Règles uniformes devaient constituer un texte indépendant de la Loi type, le projet d'article 7 pourrait jouer un rôle utile, notamment dans les cas où la Loi type, ou du moins son article 8, ne serait pas adoptée. Afin de préciser cette notion et de répondre aux préoccupations relatives à la répétition d'une partie seulement et non de la totalité de l'article 8 de la Loi type dans le projet d'article 7, il a été proposé que le texte soit modifié comme suit et soit accompagné d'une note dans un guide expliquant que, dans les cas où il n'avait pas déjà été adopté, les États pouvaient adopter l'article 8 de la Loi type dans son intégralité:

> "Un message de données est présumé être une information originale aux fins de [*la loi de l'État adoptant*] s'il est conforme aux exigences de [*l'article 8 de la Loi type tel qu'adoptée dans l'État adoptant*]."

Cette proposition n'a pas reçu un large appui, mais selon une opinion, il ne fallait pas faire abstraction des quatre paragraphes de l'article 8 de la Loi type.

88. Selon un autre avis, le projet d'article 7 était utile, car il offrait un moyen de garantir l'intégrité du message de données, notamment lorsqu'une signature électronique renforcée était utilisée. Selon un avis connexe, si la question de l'intégrité n'était pas traitée dans le contexte du projet d'article 7, il faudrait peut-être envisager de l'inclure dans le projet d'article 6 parmi les critères de la signature, conformément à ce qui était proposé dans la définition de la signature électronique renforcée dans le projet d'article 2.

89. Après un débat, le Groupe de travail est convenu, qu'en vue d'un examen ultérieur, les Règles uniformes devraient comporter, entre crochets, un projet d'article 7 en vertu duquel, lorsqu'une méthode entrant dans le

cadre du projet d'article 6 était utilisée et que cette méthode satisfaisait aux exigences des alinéas a) et b) du paragraphe 1 de l'article 8 de la Loi type (ces paragraphes devant être repris intégralement dans le projet d'article), il serait présumé que le message de données était sous sa forme originale. Une telle disposition constituerait un ajout par rapport à la Loi type, car elle offrirait une méthode permettant de créer une signature qui pourrait établir la présomption d'un original. À propos de cette décision, il a également été convenu que la version révisée du projet d'article qu'établirait le secrétariat ne ferait plus mention d'une "signature électronique renforcée", mais que cela ne devrait pas être interprété comme préjugeant de la décision définitive que prendrait ultérieurement le Groupe de travail sur le point de savoir si le projet de Règles uniformes ferait ou non référence à cette notion.

Article 8. Détermination de la signature électronique [renforcée]

90. Le texte du projet d'article 8 examiné par le Groupe de travail était le suivant:

> 1. [*L'organe ou l'autorité indiqué par l'État adoptant comme compétent en la matière*] peut déterminer [qu'une signature électronique est une signature électronique renforcée] [quelles [méthodes] [signatures électroniques] satisfont aux exigences énoncées aux articles 6 et 7].
>
> 2. Toute détermination en vertu du paragraphe 1 doit être conforme aux normes internationales reconnues.

91. Le maintien du projet d'article 8 a été jugé dans l'ensemble utile. Selon une opinion, même s'il ne constituait pas une disposition d'habilitation qui pourrait ou serait nécessairement adoptée par les États sous sa forme actuelle, il n'en indiquait pas moins clairement qu'il était possible d'assurer certitude et prévisibilité en déterminant quelles étaient les techniques de signature qui satisfaisaient aux critères de fiabilité énoncés dans les projets d'article 6 et 7, à condition que cette détermination soit conforme aux normes internationales. On a par ailleurs insisté sur le fait que, pour faciliter le développement du commerce électronique, il fallait qu'il y ait certitude et prévisibilité au moment de l'utilisation éventuelle d'une technique de signature par les parties commerciales et non pas au moment où un différent était porté devant les tribunaux. Lorsqu'une technique de signature donnée pouvait satisfaire aux exigences visant à assurer un degré de fiabilité et de sécurité plus élevé, 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 forme ou une autre de reconnaissance, comme le prévoyait le mécanisme du projet d'article 8.

92. S'agissant du respect des critères de fiabilité énoncés au projet d'article 6, il a été proposé d'examiner non pas le respect de ces critères en termes absolus, mais la mesure dans laquelle telle ou telle technique pouvait garantir ce respect. Cette proposition a été appuyée.

93. On a déclaré toutefois qu'il ne faudrait pas voir dans le projet d'article une disposition donnant à l'utilisation de certains types de techniques de signature des effets juridiques obligatoires ou imposant l'utilisation des techniques dont on avait déterminé qu'elles satisfaisaient aux exigences de fiabilité des projets d'articles 6 et 7. Les parties devraient être libres, par exemple, d'utiliser des techniques autres que ces dernières si elles en avaient convenu ainsi. Elles devraient également être libres de démontrer, devant un tribunal judiciaire ou arbitral, que la méthode de signature qu'elles avaient choisie satisfaisait effectivement aux exigences des projets d'articles 6 et 7, même si elle n'avait pas fait l'objet d'une détermination préalable à cet effet. Il ne faudrait pas non plus voir dans le projet d'article une recommandation aux États sur le seul moyen d'assurer la reconnaissance des techniques de signature, mais plutôt une indication des limites à appliquer si les États souhaitaient adopter une telle approche. Ces points, a-t-on déclaré, devraient être clairement expliqués, éventuellement dans un guide accompagnant les Règles uniformes.

94. Des doutes ont été émis quant au rôle de l'État dans la détermination mentionnée au paragraphe 1. Selon un avis, tout organe ou toute autorité chargé de déterminer la fiabilité technique des méthodes de signature devrait émaner de l'industrie. Selon un autre avis, le projet d'article ne devrait pas être axé sur la question de savoir qui devrait être habilité à procéder à cette détermination mais plutôt sur les questions à examiner en cas de détermination. On a également exprimé des craintes quant à la signification des mots "normes internationales reconnues". On pourrait être amené à se demander par exemple ce qu'était une norme "reconnue" et par qui elle devrait être reconnue. Par ailleurs, le mot "normes" devait être interprété au sens large, englobant les pratiques industrielles et les usages commerciaux, les textes émanant d'organisations telles que la Chambre de commerce internationale, ainsi que les travaux de la CNUDCI elle-même (y compris les présentes Règles et la Loi type); il ne devait pas être limité aux normes officielles élaborées, par exemple, par l'Organisation internationale de normalisation (ISO) et l'Internet Engineering Task Force (IETF). Pour régler ce problème, il a été proposé de remplacer les termes "normes reconnues" par "normes pertinentes" et d'inclure une explication sur ces questions dans un guide accompagnant les Règles uniformes.

95. Afin de tenir compte de certains des doutes et préoccupations susmentionnés, les propositions ci-après ont été formulées pour remplacer le texte de projet d'article 8:

> "a) Toute détermination par [*l'État*] quant aux signatures électroniques qui satisfont aux exigences de l'article 6 est conforme aux normes internationales reconnues.
>
> b) L'État adoptant peut désigner un organe ou une autorité chargé de déterminer, conformément aux normes internationales, quelles techniques ou quelles signatures électroniques satisferaient aux articles 6 et 7.
>
> c) Pour déterminer si les présomptions énoncées aux articles 6 et 7 sont applicables aux signatures électroniques, il est tenu dûment compte des normes internationales reconnues.
>
> d) Il peut être déterminé qu'une ou plusieurs méthodes de signature électronique satisfont à priori aux exigences des articles 6 et 7 [à condition que ces méthodes soient conformes aux normes internationales reconnues]."

96. Les principes énoncés dans ces diverses options ont bénéficié d'un appui considérable. On a fait observer que les deux premiers paragraphes proposés contenaient une référence à l'organe qui pourrait procéder à la détermination, alors que les deux autres étaient axés sur la détermination elle-même.

97. S'agissant de la forme, les membres du Groupe de travail se sont déclarés favorables à l'emploi des termes "quelles méthodes satisfont aux exigences énoncées aux articles 6 et 7" au paragraphe 1 et au remplacement des termes "doit être conforme" par les termes "est conforme" au paragraphe 2.

98. Après un débat, le Groupe de travail s'est accordé sur les points suivants: 1) le texte révisé du projet d'article 8 devrait tenir compte, éventuellement sous la forme de deux variantes, des propositions énoncées ci-dessus; 2) il faudrait préciser, dans un guide ou une note explicative accompagnant les Règles uniformes, que le mécanisme exposé dans le projet d'article 8 pour déterminer le respect des exigences énoncées aux projets d'articles 6 et 7 n'était pas le seul moyen d'assurer la certitude et la prévisibilité concernant les techniques de signature; 3) il conviendrait de bien préciser par ailleurs qu'il fallait moins insister sur le rôle de l'État dans cette détermination et davantage sur la création d'un organe ou d'une autorité; 4) le projet d'article devrait faire référence uniquement à l'utilisation des signatures électroniques et non plus aux signatures électroniques renforcées, mais sans préjuger de la décision définitive du Groupe de travail, qui sera prise ultérieurement, sur la question de savoir si les Règles uniformes feraient ou non référence à cette notion; 5) toute détermination au sens de ce projet d'article devrait être conforme aux normes internationales; et 6) toute détermination devrait

porter non seulement sur la question de savoir si certaines méthodes satisfaisaient aux exigences énoncées aux projets d'articles 6 et 7, mais également sur la mesure dans laquelle ces exigences étaient satisfaites.

Article 9. [Responsabilités] [devoirs] du détenteur de la signature

99. Le texte du projet d'article 9 examiné par le Groupe de travail était le suivant:

"1. Le détenteur d'une signature [a le devoir]:

a) De faire preuve [Fait preuve] de la diligence voulue pour veiller à ce que les déclarations faites par lui concernant l'émission, la suspension ou l'annulation d'un certificat, ou figurant dans ce certificat soient exactes et complètes;

b) D'avertir [Avertit] les personnes voulues sans retard excessif [s'il sait que sa signature a été compromise] [si sa signature a été ou risque d'être compromise];

c) De faire preuve [Fait preuve] de la diligence voulue pour garder le contrôle de sa signature et éviter qu'elle ne soit utilisée sans autorisation, à partir du moment où il détient seul le contrôle du dispositif de signature.

2. Dans le cas [de codétenteurs] [où plus d'une personne a le contrôle] [de la clef] [du dispositif de signature], les [obligations] [devoirs] [prévues] [prévus] au paragraphe 1 sont [conjointes] [conjoints] et solidaires.

3. Le détenteur d'une signature est responsable de [l'inexécution des obligations [devoirs] énoncées [énoncés] [la non-satisfaction des exigences énoncées] au paragraphe 1.

4. [La responsabilité du détenteur de la signature ne peut être supérieure au préjudice qu'il avait prévu ou aurait dû prévoir au moment de l'inexécution de ses obligations en considérant les faits dont il savait ou aurait dû savoir qu'ils pouvaient découler de [l'inexécution de ses obligations [devoirs]] [la non-satisfaction des exigences] énoncées [énoncés] au paragraphe 1.]"

Titre

100. Il a été convenu dans l'ensemble qu'afin de ne pas être source de confusion du fait de l'utilisation des mots "obligations" ou "devoirs", qui pourraient supposer différents types de responsabilités et de sanctions dans les différents systèmes juridiques, le titre du projet d'article 9 devrait simplement faire référence à la "conduite" ou aux "responsabilités" du détenteur de la signature. Pour ce qui est de la notion de "détenteur de la signature", on a jugé qu'il serait plus approprié d'utiliser le terme "détenteur du dispositif de signature" car on préciserait ainsi la distinction qu'il faut établir entre la notion juridique de "signature" d'une part et la notion technique de "dispositif de signature" d'autre part. Aucune décision n'a été prise par le Groupe de travail à ce propos, mais il a été jugé dans l'ensemble que la question devrait sans doute être réexaminée dans le contexte du projet d'article 2.

Paragraphe 1

101. Pour les mêmes raisons que pour le titre du projet d'article 9 (voir par. 100), il a été décidé que le paragraphe 1 s'ouvrirait sur les mots suivants "Le détenteur d'une signature:" (suivis du présent) (pour la suite du débat, voir ci-après par. 105).

102. L'alinéa a) a reçu un accueil favorable quant au fond. Toutefois, à propos des mots "l'émission, la suspension ou l'annulation d'un certificat", il a été jugé dans l'ensemble qu'il faudrait utiliser un libellé plus

large, afin d'englober l'intégralité du cycle de vie du certificat. Ce cycle pouvait commencer avant que le certificat ne soit effectivement émis, par exemple, lorsque le certificateur d'informations recevait une demande d'émission du certificat. De même, il pouvait aller au-delà du moment de l'expiration initialement prévue, par exemple, en cas de renouvellement ou de prorogation du certificat. Vu le large éventail de situations à prendre en compte, il a été convenu d'utiliser une formule souple, afin d'éviter d'avoir à spécifier chaque fait pouvant se produire durant le cycle de vie du certificat. Il a également été convenu que le libellé utilisé à l'alinéa a) n'était pas suffisamment neutre, car il pourrait être interprété comme signifiant que le dispositif de signature supposait nécessairement l'utilisation d'un certificat. Afin qu'il soit bien clair que tous les dispositifs de signature ne se fondaient pas sur des certificats, il a été décidé d'ajouter les mots suivants au début de l'alinéa a): "Lorsque le dispositif de signature suppose l'utilisation d'un certificat...". Pour la même raison, il a été décidé que l'alinéa a) serait placé après les alinéas b) et c). Pour ce qui est de la forme, il a été convenu que les mots "ou figurant dans ce certificat" seraient remplacés par les mots "ou devant être inclus dans le certificat".

103. Pour ce qui est de l'alinéa b), le maintien d'une formule telle que "il savait que sa signature avait ou pouvait avoir été compromise" a suscité un large appui. On a toutefois craint que cette règle ne mette excessivement l'accent sur une détermination suggestive de ce que "savait" le détenteur de la signature. Il a été proposé d'ajouter dans le texte une référence plus objective à ce que le détenteur de la signature "aurait dû savoir". Il a été rappelé, en réponse à la suggestion, que les mots "ou aurait dû savoir" n'avaient pas été inclus dans le projet d'article 9, car il serait difficile au détenteur de la signature de remplir une obligation de notification fondée sur quelque chose qu'il aurait dû savoir, mais qu'il ne savait en fait pas. Afin de répondre à la préoccupation qui avait été exprimée, il a été proposé de modifier comme suit l'alinéa b):

> "Avise les personnes voulues sans retard excessif si:
>
> i) il sait que le dispositif de signature a été compromis; ou si
>
> ii) au vu des circonstances connues de lui, il y a un risque important que le dispositif de signature ait été compromis."

Le Groupe de travail a accepté cette proposition.

104. L'alinéa c) a été jugé dans l'ensemble acceptable quant au fond, mais il a été décidé qu'il n'était pas nécessaire de faire référence au moment où le détenteur de la signature détenait seul le contrôle du dispositif de signature. Pour ce qui est de la forme, il a été décidé, afin d'éviter toute ambiguïté quant au sens de la notion de "contrôle" du dispositif de signature, de modifier comme suit la disposition: "fait preuve de la diligence voulue pour éviter une utilisation non autorisée de sa signature". Afin que la terminologie utilisée soit cohérente, le secrétariat a été invité à étudier si un terme unique pourrait être utilisé dans la version anglaise à la place des deux notions de "due diligence" à l'alinéa a) et "due care" à l'alinéa c). Il a été proposé de remplacer, par exemple, ces deux notions par les mots "reasonable care" (soin raisonnable).

Paragraphe 2

105. Le débat a porté sur la question de savoir si, lorsque le dispositif de signature était détenu conjointement par plus d'un détenteur, la responsabilité en cas de non-satisfaction des exigences énoncées au paragraphe 1 serait conjointe et solidaire. Il a été jugé dans l'ensemble que le paragraphe 2 risquerait de constituer une ingérence inappropriée dans la loi régissant la responsabilité en dehors des Règles uniformes. Pour ce qui est du fond, il a été déclaré qu'il existait des cas où il ne serait pas équitable de disposer que chaque détenteur du dispositif serait responsable de la totalité du préjudice pouvant avoir résulté d'une utilisation non autorisée du dispositif, par exemple si le dispositif de signature d'une société avait été utilisé sans autorisation par un certain nombre d'employés. Il a été décidé que chaque détenteur ne devrait être tenu responsable que dans la mesure où il avait personnellement manqué aux obligations énoncées au paragraphe 1. À cette fin, il a été décidé de

supprimer le paragraphe 2 et de modifier comme suit les premiers mots du paragraphe 1: “Chaque détenteur d’un mécanisme de signature:”.

Paragraphe 3

106. Le Groupe de travail a jugé que le paragraphe 3 était dans l’ensemble acceptable quant au fond, en tant que disposition générale sur la responsabilité du détenteur d’une signature ne satisfaisant pas aux exigences énoncées au paragraphe 1. Pour ce qui est de la forme, il a été proposé de modifier comme suit cette disposition: “Le détenteur d’une signature assume les conséquences juridiques du fait qu’il ne s’est pas conformé aux exigences du paragraphe 1”. Après un débat, le Groupe de travail a décidé, afin que l’on ne puisse pas penser que les Règles uniformes traitaient de manière un tant soit peu détaillée des conséquences juridiques du non-respect par le détenteur d’une signature de ses obligations, que le paragraphe 3 serait libellé comme suit: “Le détenteur d’une signature est responsable de la non-satisfaction par lui des exigences énoncées au paragraphe 1”.

Paragraphe 4

107. Il a été rappelé que le paragraphe 4 se fondait sur l’article 74 de la Convention sur les ventes. Il établissait une règle fondée sur un critère de prévisibilité du préjudice, mais se limitait au non-respect des obligations du détenteur de la signature énoncées au paragraphe 1. Le Groupe de travail a craint que la responsabilité pouvant découler d’un contrat de vente de marchandises ne soit pas la même que celle pouvant découler de l’utilisation d’une signature et ne puisse être quantifiée de la même manière. Il a également été déclaré qu’un critère de prévisibilité ne serait peut-être pas approprié dans le contexte de la relation contractuelle entre le détenteur de la signature et le certificateur des informations, encore qu’il puisse l’être dans le contexte de la relation entre le détenteur de la signature et une partie se fiant à la signature (pour le débat ayant déjà eu lieu sur cette question, voir A/CN.9/457, par. 93 à 98). Il a été répondu que le fait d’énoncer un critère de prévisibilité dans le contexte du projet d’article 9 revenait tout simplement à réénoncer une règle fondamentale qui s’appliquerait en vertu de la loi normalement applicable dans de nombreux pays. Lorsque cette règle fondamentale n’était pas normalement applicable, le paragraphe 4 donnerait des orientations utiles aux tribunaux judiciaires et arbitraux pour évaluer la responsabilité du détenteur de la signature et permettrait d’éviter dans la pratique l’imposition de dommages-intérêts indirects ou punitifs qui pourraient largement dépasser le montant de tout préjudice raisonnablement prévisible par le détenteur de la signature au moment où la signature électronique avait été appliquée.

108. Toutefois, selon l’avis qui a prévalu, il serait sans doute difficile d’arriver à un consensus sur les conséquences pouvant découler de la responsabilité du détenteur de la signature. Selon le contexte dans lequel la signature électronique était utilisée, ces conséquences pouvaient être très diverses en vertu des lois existantes: le détenteur de la signature pouvait, par exemple, être lié par la teneur du message, ou il pouvait être simplement tenu de verser des dommages-intérêts. Il a été déclaré qu’il ne faudrait pas, dans le cadre des Règles uniformes, élaborer une disposition pouvant constituer une ingérence dans le droit général des obligations. De ce fait, la question devait être simplement régie par le paragraphe 3, qui énonçait le principe selon lequel le détenteur de la signature devait être tenu responsable de la non-satisfaction par lui des exigences énoncées au paragraphe 1, et par la loi applicable en dehors des lois uniformes dans chaque État adoptant, pour ce qui est des conséquences juridiques découlant d’une telle responsabilité. Après un débat, le Groupe de travail a décidé de supprimer le paragraphe 4.

Article 10. Foi accordée à une signature électronique renforcée

109. Le texte du projet d’article 10 examiné par le Groupe de travail était le suivant:

> “1. Une personne [est] [n’est pas] fondée à se fier à une signature électronique renforcée dans la mesure où il [est] [n’est pas] raisonnable de le faire.

2. Pour déterminer s'il [est] [n'est pas] raisonnable de se fier à la signature, il est tenu compte, s'il y a lieu, des facteurs suivants:

a) la nature de l'opération sous-jacente que la signature est censée étayer;

b) l'adoption ou non par la partie se fiant à la signature de mesures appropriées pour en déterminer la fiabilité;

c) le fait que la partie se fiant à la signature savait ou aurait dû savoir que celle-ci avait été compromise ou annulée;

d) toute convention ou toute pratique existant entre la partie se fiant à la signature et le titulaire ou tout usage commercial pouvant s'appliquer;

e) tout autre facteur pertinent."

110. Le maintien du projet d'article 10 a eu à la fois des partisans et des détracteurs. En faveur du maintien, on a fait remarquer que cet article était utile dans la mesure où il établissait la conduite à suivre par la partie se fiant à la signature, sur le modèle d'un code de conduite. Selon une autre opinion, puisque les signatures électroniques étaient un phénomène nouveau et soulevaient des problèmes relatifs à la confiance que ne posaient pas les signatures manuscrites, le projet d'article 10 pouvait donner aux tribunaux judiciaires et arbitraux des indications utiles. Par ailleurs, puisque le projet d'article 11 était axé sur les certificats, le projet d'article 10 pouvait traiter des types de signatures qui n'étaient pas étayées par des certificats et aider le Groupe de travail à formuler des règles permettant un degré satisfaisant de neutralité technique.

111. Plusieurs membres du Groupe de travail se sont prononcés par contre en faveur de la suppression du projet d'article. Selon un avis, cette disposition introduisait une notion nouvelle, celle de confiance relative à la fois au message et à la signature et qui pourrait soulever des difficultés au regard du droit des obligations et de la répartition des risques. S'agissant de la répartition des risques, on a déclaré que le projet d'article soulevait des problèmes qu'il ne réglait pas explicitement et risquait donc d'entraîner confusion et incertitude. Si on le maintenait, il faudrait préciser sa relation avec les questions de la répartition des risques.

112. Des inquiétudes ont été exprimées quant au lien entre les projets d'articles 10 et 16. Selon une opinion, prévoir une disposition qui portait sur la question de savoir si l'on pouvait ou non se fier à une signature équivalait à traiter de la fiabilité de la méthode de signature, question déjà traitée dans le projet d'article 6. À l'encontre de cet argument, on a fait valoir que le projet d'article 10 était axé sur la conduite à suivre pour que la confiance soit possible et non sur la fiabilité d'une méthode de signature au sens du projet d'article 6. Selon un autre avis, lorsque les questions de confiance étaient réglées par contrat, il faudrait s'en tenir au projet d'article 6 et à la détermination de la technique de signature qui satisfaisait aux critères de fiabilité. Pour ce qui était des tiers, lorsqu'un contrat n'entrait pas en jeu, la simple confiance ne suffirait pas à établir une obligation de la part du détenteur de la signature. Dans la mesure où le projet d'article 10 traitait uniquement de la simple confiance, il n'ajoutait pas grand-chose aux Règles uniformes et pouvait donc être supprimé. Ce qu'il fallait, a-t-on en outre suggéré, c'était une disposition qui traitait d'autre chose en plus de la fiabilité de la signature et c'est ce que faisait le projet d'article 11, qui traitait de la confiance dans les certificats.

113. S'agissant de la forme, certains membres du Groupe de travail se sont déclarés favorables à une formulation négative du projet d'article 10, ce qui irait dans le sens de l'établissement d'un code de conduite dans les projets d'articles 9 à 12, qui n'indiqueraient pas les conséquences à prévoir si la conduite énoncée n'était pas suivie. Sur le fond, toutefois, il a été noté que les critères énoncés au paragraphe 2 ne constituaient pas véritablement des règles de conduite, à l'exception peut-être de l'alinéa b). Un code de conduite pourrait certes être utile pour régler les questions exposées dans le projet d'article 10, mais ce dernier, sous sa forme

actuelle, ne permettait pas d'atteindre ce but. Il a aussi été proposé, s'agissant du libellé, d'ajouter un autre critère au paragraphe 2, selon lequel il faudrait vérifier si la signature électronique était étayée par un certificat.

114. Après un débat, le Groupe de travail a décidé qu'avant d'émettre une conclusion définitive sur le projet d'article 10, il était nécessaire d'examiner le projet d'article 11, ainsi que les responsabilités qui pouvaient incomber aux certificateurs d'informations au titre du projet d'article 12.

Article 11. Foi accordée à un certificat

115. Le texte du projet d'article 11 examiné par le Groupe de travail était le suivant:

"1. Une personne [est] [n'est pas] fondée à se fier à un certificat dans la mesure où il [est] [n'est pas] raisonnable de le faire.

2. Pour déterminer s'il [est] [n'est pas] raisonnable de se fier au certificat, il est tenu compte, s'il y a lieu, des facteurs suivants:

a) toutes restrictions dont le certificat peut faire l'objet;

b) l'adoption ou non par la partie se fiant au certificat de mesures appropriées pour en déterminer la fiabilité, y compris la consultation d'une liste d'annulations de certificats, le cas échéant;

c) toute convention ou toute pratique existant entre la partie se fiant au certificat et le certificateur d'informations ou le titulaire ou tout usage commercial pouvant s'appliquer;

d) [tout] [Tous les] autre[s] facteur[s] pertinent[s]."

116. Au début du débat sur le projet d'article 11, il a été déclaré que cette disposition devrait mettre l'accent sur la confiance dans les informations contenues dans le certificat, et non sur le certificat en tant que tel. Cette question pourrait certes être traitée au projet d'article 2 dans la définition du terme "certificat", mais il serait préférable de le faire expressément dans le projet d'article 11. On s'est demandé par ailleurs si le projet d'article 11 devrait se concentrer sur la conduite à suivre pour établir que la confiance était raisonnable ou porter sur les critères permettant de déterminer la qualité ou la fiabilité d'un certificat. Des membres du Groupe de travail ont estimé que le projet d'article 11 devrait traiter des questions relatives à la confiance dans le certificat et non à la fiabilité de ce dernier.

117. On s'est inquiété de ce que le projet d'article 11, tout comme le projet d'article 10, introduisaient une nouvelle notion de confiance. Si le projet d'article 11 énonçait les critères sur lesquels se fonder pour déterminer que la confiance était raisonnable, il n'abordait cependant pas la question de savoir ce qui se passerait si certaines de ces questions n'étaient pas correctement examinées ou si une partie se fiait au certificat, alors qu'il pouvait ne pas avoir été raisonnable de le faire. En d'autres termes, il ne traitait pas des conséquences de la non-application des critères énoncés au paragraphe 2. Des membre du Groupe de travail se sont prononcés en faveur du traitement, dans le projet d'article 11, des conséquences qu'auraient ces situations pour la partie se fiant au certificat. S'agissant de la teneur d'une disposition allant dans ce sens, deux approches ont été proposées. Il a été suggéré d'inclure un libellé s'inspirant des projets de dispositions cités après le paragraphe 58 du document A/CN.9/WG.IV/WP.82, aux termes duquel, lorsque la conduite prévue au paragraphe 2 n'était pas suivie, la partie se fiant au certificat assumerait le risque que la signature ne soit pas valable en tant que signature. Selon une autre proposition, si une personne se fiant au certificat n'adoptait pas la conduite prescrite, elle ne pourrait se retourner ni contre le certificateur d'informations ni contre le détenteur de la signature. Les deux approches susmentionnées ont bénéficié d'un appui, mais on s'est demandé si des règles allant dans ce sens seraient appropriées dans tous les cas. Plusieurs exemples ont été cités à cet égard montrant qu'il ne faudrait pas aboutir à une situation dans laquelle les parties se fiant au certificat assumeraient le risque que la signature ne soit pas

valable simplement parce qu'elles n'auraient pas suivi la conduite énoncée au projet d'article 11 (par exemple, lorsque la partie se fiant au certificat n'avait pas consulté une liste de révocations de certificats mais que cette liste n'aurait pas révélé que la signature avait été compromise). À l'appui de cette opinion, il a été déclaré que le projet d'article 11 n'avait pour objet ni de prévaloir sur les clauses contractuelles ni d'ôter aux tribunaux judiciaires ou arbitraux compétents le pouvoir de statuer sur le fond de chaque affaire.

118. Selon un avis, le projet d'article 11 ne devrait pas préciser les conséquences, mais être conçu davantage comme un code de conduite, avis déjà exprimé à propos du projet d'article 10. Selon une opinion allant dans le même sens, il était préférable de formuler de manière négative le projet d'article 11 car il ne créait pas d'effets juridiques, ce qui allait dans le sens d'un code de conduite. À l'appui de cette dernière opinion, on a fait observer que des juridictions différentes adoptaient des règles différentes sur la responsabilité, par exemple sur l'application de la notion de fautes concurrentes, et qu'il serait très difficile de parvenir à un accord sur la façon de traiter les conséquences. Selon une autre opinion encore, le droit du commerce électronique ne constituant pas un domaine du droit à part entière, les règles proposées par le Groupe de travail concernant des notions qui existaient déjà dans le droit national (même si c'était dans des contextes légèrement différents et même si l'application particulière de ces notions au commerce électronique pouvait être incertaine), ne pouvaient pas faire abstraction de la manière dont ces notions étaient traitées. Cela était particulièrement vrai pour les questions de responsabilité et pour les conséquences de cette responsabilité. Il a été proposé que le Groupe de travail se concentre sur l'énonciation des facteurs qui aideraient les tribunaux judiciaires et arbitraux à étendre les notions existantes au commerce électronique.

119. Des doutes ont été émis quant à l'emploi du mot "entitlement" dans la version anglaise et quant à l'opportunité de donner un "droit" à se fier à un certificat dans le projet d'article 11. Le terme "entitlement" pourrait en effet donner à penser que l'on conférait à la partie se fiant au certificat un droit qui s'ajoutait à ce qui était applicable par ailleurs. Pour régler ce problème, il a été proposé de formuler une disposition se lisant comme suit:

> "Pour déterminer s'il était raisonnable qu'une personne se soit fiée aux informations figurant dans un certificat, il est tenu compte des facteurs suivants: [insérer les alinéas a) à d) du paragraphe 2]"

120. Des membres du Groupe de travail ont approuvé la teneur des critères énoncés au paragraphe 2 et il a été proposé d'en ajouter un autre calqué sur le paragraphe 2 c) du projet d'article 10, mais s'appliquant au dispositif de signature. S'agissant de la forme, on a déclaré que, pour être complet, on pourrait ajouter à la liste d'annulations mentionnée au paragraphe 2 b) une liste de suspensions.

121. S'agissant de l'emplacement du projet d'article 11 dans les Règles uniformes, il a été proposé de placer les projets d'articles 9 et 12 avant les projets d'articles 10 et 11, puisque qu'ils établissaient les responsabilités des détenteurs de signatures et des certificateurs d'informations et se rapportaient tous deux à la question de la confiance et à l'étendue des responsabilités de la partie se fiant à la signature. Il a été proposé par ailleurs de fondre les projets d'articles 10 et 11 en un seul article qui traiterait à la fois des signatures et des signatures étayées par des certificats. On a fait observer, toutefois, que cette proposition reprenait un ancien projet de texte qui avait été divisé en deux articles au motif que des considérations différentes s'appliqueraient aux notions de confiance dans une signature et de confiance dans une signature étayée par un certificat (A/CN.9/WG.IV/WP.82, par. 56).

122. Après un débat, le Groupe de travail a, s'agissant des projets d'articles 10 et 11, décidé ce qui suit: 1) bien que le débat sur le projet d'article 10 ne soit pas clos, le secrétariat devrait établir un texte révisé de cet article pour tenir compte des délibérations du Groupe de travail; 2) le secrétariat devrait établir un texte révisé de projet d'article 11 pour tenir compte (éventuellement sous forme de deux variantes ou de deux paragraphes consécutifs), de la proposition formulée au paragraphe 119 ci-dessus et des deux types de conséquences exposées au paragraphe 117; 3) les projets d'articles 10 et 11 devraient être placés après le projet d'article 12;

et 4) les projets d'articles 10 et 11 ne devraient pas être regroupés pour les raisons examinées par le Groupe de travail.

Article 12. [Obligations] [devoirs] d'un certificateur d'informations

123. Le texte du projet d'article 12 examiné par le Groupe de travail était le suivant:

"1. Un certificateur d'informations [a l'obligation] [notamment]:

a) [d'agir] [agit] conformément aux déclarations qu'il fait concernant ses pratiques;

b) [de prendre] [prend] des mesures raisonnables pour s'assurer de l'exactitude de tous les faits ou informations qu'il certifie dans le certificat, [y compris l'identité du détenteur de la signature];

c) [de fournir] [fournit] des moyens raisonnablement accessibles qui permettent à une partie se fiant au certificat de s'assurer:

i) de l'identité du certificateur d'informations;

ii) du fait que la personne qui est [nommée] [identifiée] dans le certificat détient [au moment pertinent] [la clef privée correspondant à la clef publique] [le dispositif de signature] indiqué[e] dans le certificat;

[iii) du fait que les clefs sont une paire de clefs qui fonctionne];

iv) de la méthode employée pour identifier le détenteur de la signature;

v) de toute restriction quant aux fins ou à la valeur pour lesquelles la signature peut être utilisée; et

vi) du fait que le dispositif de signature est valable et n'a pas été compromis;

d) [de fournir] [fournit] un moyen permettant au détenteur de la signature d'avertir qu'une signature électronique renforcée a été compromise et d'assurer [assure] un service prompt d'annulation;

e) [de faire] [fait] preuve de la diligence voulue afin de veiller à l'exactitude et à l'exhaustivité de toutes les déclarations faites par lui qui sont pertinentes pour l'émission, la suspension ou l'annulation d'un certificat ou qui figurent dans le certificat;

f) [d'utiliser] [utilise] des systèmes, des procédures et des ressources humaines fiables pour la fourniture de ses services.

Variante X

2. Un certificateur d'informations est [responsable] [comptable] de l'inexécution des [obligations] [devoirs] [conditions] énoncé[e]s au paragraphe 1.

3. La responsabilité du certificateur d'informations ne peut être supérieure à la perte qu'il prévoyait ou aurait dû prévoir au moment de l'inexécution à la lumière des faits ou problèmes dont il avait connaissance ou aurait dû avoir connaissance comme étant des conséquences possibles de son non-respect des [obligations] [devoirs] [conditions] énoncé[e]s au paragraphe 1.

Variante Y

2. Sous réserve du paragraphe 3, si le préjudice a été causé parce que le certificat était incorrect ou défectueux, un certificateur d'informations est tenu responsable du préjudice subi:

a) soit par une partie qui a passé un contrat avec le certificateur d'informations pour la délivrance d'un certificat;

b) soit par une personne qui se fie raisonnablement à un certificat émis par le certificateur d'informations.

3. Un certificateur d'informations n'est pas tenu responsable en vertu du paragraphe 2:

a) si et dans la mesure où il a inclus dans le certificat une déclaration limitant la portée ou l'étendue de sa responsabilité envers toute personne; ou

b) s'il prouve qu'il [n'a pas été négligent] [a pris toutes les mesures raisonnables pour prévenir le préjudice]."

Remarques générales

124. Il a été noté d'emblée que le champ d'application du projet d'article 12 devrait être compris comme ne couvrant que les activités des certificateurs d'informations ayant un rapport avec les signatures électroniques qui devaient produire des effets juridiques en vertu des projets d'articles 6 et 7. Leurs autres activités, y compris l'éventuelle émission de certificats de moindre fiabilité, n'étaient pas couvertes par les Règles uniformes.

125. S'agissant de la forme, il a été estimé que l'on pourrait gagner à remplacer le terme "certificateur d'informations" par celui, plus descriptif, de "fournisseur de services de certification". Il a été convenu qu'il faudrait peut-être examiner de façon plus approfondie cette question dans le contexte du projet d'article 2.

Titre

126. De l'avis général, le titre du projet d'article 12 devrait se lire parallèlement à celui du projet d'article 9 (voir ci-dessus, par. 100).

Paragraphe 1

127. Pour des raisons de cohérence, il a également été convenu que les mots d'ouverture du paragraphe 1 devrait refléter ceux du paragraphe 1 du projet d'article 9 (voir ci-dessus, par. 101 et 105). Il a été proposé de remplacer les mots "qui permettent à une partie se fiant au certificat de s'assurer" par les mots "qui permettent à une partie se fiant au certificat de s'assurer de l'un quelconque des points suivants que le certificateur d'informations est en mesure de divulguer". Il a été fait objection à cette proposition au motif que les points énumérés à l'alinéa c) ne correspondaient pas à ce que le certificateur d'informations était en mesure ou non de divulguer, mais devaient être considérés comme constituant une liste directive de renseignements cumulatifs auxquels le certificateur d'informations devrait permettre l'accès en toute circonstance.

Alinéa a)

128. Il a été estimé que l'alinéa a) était généralement acceptable quant au fond. S'agissant de la forme, il a été proposé de remplacer la référence aux "pratiques" du certificateur d'informations par une référence à ses "activités". Il a cependant été estimé, compte tenu de l'utilisation généralisée qui est faite de concepts tels que celui de "déclaration relative aux pratiques de certification", que la référence aux "pratiques" devrait être conservée.

Alinéas b) et e)

129. Il a été estimé que les deux alinéas étaient généralement acceptables quant au fond. Compte tenu de la similarité de leur teneur, il a été convenu qu'ils devraient être fusionnés en un alinéa qui serait libellé comme suit: "[de faire] [fait] preuve de la diligence voulue afin de veiller à l'exactitude et à l'exhaustivité de toutes les déclarations faites par lui qui sont pertinentes pour le cycle de vie du certificat ou qui sont certifiées dans le certificat".

Alinéa c)

130. Il a été estimé que les alinéas c) i) et c) iv) à vi) étaient généralement acceptables quant au fond.

131. Il a été noté que l'alinéa c) ii) faisait référence à la fois à une "paire de clefs" et à un "dispositif de signature". Pour tenir compte de la démarche de neutralité technique adoptée dans les Règles uniformes, le Groupe de travail a convenu qu'il faudrait utiliser, au lieu de "paire de clefs", une formulation techniquement neutre telle que "dispositif de signature" ou "dispositif de création de signature", dans la mesure où "paire de clefs" renvoyait spécifiquement aux signatures numériques. L'utilisation de l'expression "paire de clefs" en rapport avec la définition du terme "certificat" pouvait convenir dans des cas où les certificats n'étaient utilisés que dans un contexte de signature numérique.

132. S'agissant de la forme de l'alinéa c) ii), il a été proposé, conformément à la démarche adoptée dans le contexte du projet d'article 6 (voir ci-dessus, par. 80), d'utiliser le mot "identifiée" au lieu du mot "nommée". En vertu de cette démarche, le concept d'identité devrait être interprété plus largement qu'une simple référence au nom du détenteur de signature, car il pourrait se référer à d'autres caractéristiques importantes telles que la position ou l'autorité, soit en association avec un nom, soit sans référence à un nom (voir A/CN.9/WG.IV/WP.82, par. 29). Après un débat, le Groupe de travail a convenu que l'alinéa c) ii) devrait être libellé comme suit: "du fait que la personne qui est identifiée dans le certificat détient, au moment pertinent, le dispositif de signature indiqué dans le certificat".

133. De l'avis général, l'alinéa c) iii) devrait être supprimé. Si la clef publique à laquelle il était fait référence dans le certificat correspondait à la clef privée détenue par le détenteur de signature et s'il existait, par conséquent, une correspondance mathématique entre les deux clefs, on ne voyait pas clairement quelle fonctionnalité supplémentaire serait obtenue si l'on exigeait que la paire de clefs soit "une paire de clefs qui fonctionne". Il n'était pas certain non plus que le certificateur d'informations puisse fournir, outre les informations exigées à l'alinéa c) ii), des informations indiquant cette fonctionnalité supplémentaire.

Alinéas d) et f)

134. Il a été estimé que les alinéas d) et f) étaient généralement acceptables quant au fond.

Dispositions supplémentaires proposées

135. Dans le cadre du débat sur l'alinéa c), il a été avancé que le projet d'article 12 devrait établir une règle additionnelle déterminant le contenu minimum d'un certificat (voir A/CN.9/WG.IV/WP.82, par. 61). Il a été proposé qu'une telle règle se fonde sur certains éléments de l'alinéa c), ainsi que sur l'alinéa a) du paragraphe 3 de la variante Y et soit libellée comme suit:

"Un certificat énonce les éléments suivants:

a) l'identité du certificateur d'informations;

b) le fait que la personne qui est identifiée dans le certificat détient, au moment pertinent, le dispositif de signature indiqué dans le certificat;

c) le fait que le dispositif de signature était valide à la date ou avant la date à laquelle le certificat a été émis;

d) toute restriction quant aux fins ou à la valeur pour lesquelles le certificat peut être utilisé; et

e) toute restriction quant à la portée ou à l'étendue de la responsabilité que le certificateur accepte envers toute personne."

136. Une autre proposition a été faite, liée à une proposition antérieure relative au projet d'article 13, selon laquelle les caractéristiques d'un certificateur d'informations, telles que décrites dans le projet d'article 13, ne devraient pas être retenues seulement pour les entités étrangères, mais aussi pour les certificateurs d'informations nationaux (voir ci-dessus, par. 30 et 35). Il a donc été proposé qu'un alinéa g) soit ajouté à la fin du paragraphe 1 et soit libellé comme suit:

"g) Pour déterminer si, et dans quelle mesure, tous systèmes, procédures et ressources humaines sont fiables aux fins de l'alinéa f), il est tenu compte des facteurs suivants: [alinéas a) à h) du projet d'article 13-4, Variante B]."

137. Ces deux propositions ont suscité un intérêt considérable. Il a été convenu que les questions qu'elles soulevaient devraient sans doute être examinées plus avant lors d'une session ultérieure, sur la base d'un projet de paragraphe 1 révisé qu'établirait le secrétariat, compte tenu du débat résumé ci-dessus.

Paragraphe 2

138. Il a été noté qu'il était souhaitable d'établir des règles fondamentales relatives à la responsabilité des certificateurs d'informations, mais il a été jugé dans l'ensemble qu'il serait sans doute difficile d'arriver à un consensus quant à la teneur de ces règles. Pour les raisons déjà évoquées dans le contexte du projet d'article 9 (voir ci-dessus, par. 107 et 108), nombre de participants ont estimé que, dans le cadre des Règles uniformes, on ne pouvait faire beaucoup plus qu'adopter le paragraphe 2 de la Variante X, énonçant ainsi un principe général selon lequel le certificateur d'informations qui ne satisferait pas aux exigences énoncées au paragraphe 1 engagerait sa responsabilité. Quant à la nature précise de cette responsabilité (par exemple, responsabilité contractuelle ou extracontractuelle, responsabilité quasi délictuelle ou responsabilité sans faute), il ne faudrait pas tenter dans les Règles uniformes d'inclure une disposition risquant d'entrer en conflit avec les théories juridiques actuelles relatives à la responsabilité en vertu de la loi applicable.

139. Selon une opinion tout aussi largement partagée, les auteurs des Règles uniformes ne devraient pas manquer l'occasion qui leur était donnée d'énoncer des principes directeurs et des normes minima quant à la responsabilité et la répartition des risques dans le domaine des signatures électroniques. De telles orientations seraient utiles aux législateurs et aux tribunaux qui devaient faire face aux problèmes pratiques liés à la responsabilité dans le commerce électronique. Des normes de responsabilité internationalement reconnues étaient également nécessaires pour les praticiens des signatures électroniques, y compris les certificateurs d'informations eux-mêmes. On a donné des exemples de lois nationales traitant expressément des signatures électroniques qui, à propos de la responsabilité des certificateurs d'informations, énonçaient simplement que les clauses contractuelles limitant la responsabilité de ces certificateurs devraient être considérées comme nulles et non avenues. Faute d'une harmonisation minimale à l'échelon international, les lois nationales applicables par le biais des règles de conflit risqueraient donc d'imposer des normes extrêmement strictes qui pourraient nuire au développement et à l'offre au niveau mondial des techniques de commerce électronique.

140. Diverses suggestions ont été faites sur la manière dont des dispositions minimales sur la responsabilité pourraient être rédigées. Selon une proposition, il faudrait adopter le paragraphe 3 de la Variante X. Toutefois, s'il a été dans l'ensemble convenu que la responsabilité du certificateur d'informations devrait sans doute être traitée différemment de celle du détenteur de la signature, on a douté que le critère de prévisibilité ait plus de chances de faire l'objet d'un consensus à propos du projet d'article 12 que cela avait été le cas dans le contexte du projet d'article 9 (voir ci-dessus, par. 107). Selon un autre avis, les Règles uniformes, sans s'ingérer dans le fonctionnement des lois nationales, pourraient énoncer une liste de facteurs à prendre en considération pour l'application des lois nationales aux certificateurs d'informations. Le libellé suivant a été proposé:

"Pour l'évaluation du préjudice, il est tenu compte des facteurs suivants:

a) coût de l'obtention du certificat;

b) nature de l'information certifiée;

c) existence et portée de toute restriction quant à l'objet pour lequel le certificat peut être utilisé;

d) existence de toute déclaration limitant la portée ou l'étendue de la responsabilité du certificateur d'informations; et

e) toute faute concurrente de la partie se fiant au certificat."

141. Cette suggestion a suscité un intérêt considérable. Il a été déclaré qu'un tel libellé donnerait des orientations utiles, tout en préservant la souplesse nécessaire pour éviter d'entraver le fonctionnement des lois nationales concernant, par exemple, une évaluation différenciée du préjudice, ou une évaluation différenciée de la faute concurrente, ou encore le point de savoir si la responsabilité était contractuelle ou extracontractuelle.

142. Faute de temps, le Groupe de travail n'a pas achevé ce débat et a décidé de le reprendre à sa session suivante. Le secrétariat a été prié d'établir un projet révisé de paragraphe 2 tenant compte du débat ci-dessus. Il a été noté que, conformément à la décision prise par la Commission à sa trente-deuxième session, la trente-sixième session du Groupe de travail aurait lieu à New York du 14 au 25 février 2000 (A/54/17, par. 434)[5].

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° 17 (A/52/17), par. 249 à 251.

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

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

[5]Ibid., par. 434.