Nations Unies A/CN.9/WG.IV/WP.104/Add.3

Assemblée générale

Distr.: Limitée
15 septembre 2003

Français
Original: Anglais

Commission des Nations Unies
pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Quarante-deuxième session
Vienne, 17-21 novembre 2003

Aspects juridiques du commerce électronique

Contrats électroniques: informations de base

Note du secrétariat*

Additif

Table des matières

* Note soumise avec quelques jours de retard par le secrétariat de la Commission des Nations Unies pour le droit commercial international pour cause de sous-effectif.

V.03-87973 (F) 201003 211003

III. Questions liées à l'utilisation de messages de données dans les contrats internationaux

1. Les sections suivantes traitent de questions qui sont propres à la conclusion de contrats par des moyens électroniques ou qui peuvent être mises particulièrement en évidence par l'utilisation de moyens modernes de communication. La section C examine les questions liées au caractère approprié des méthodes d'authentification et des critères d'attribution des messages de données. La section D traite des questions juridiques que pose l'utilisation de systèmes entièrement automatisés dans le commerce électronique, notamment le problème des erreurs. La mise à disposition des clauses contractuelles et les obligations de renseignement pouvant être imposées aux parties utilisant des systèmes d'information électroniques sont abordées dans la section E. Les sections D et E sont publiées dans un autre additif (A/CN.9/WG.IV/WP.104/Add.4).

C. Conditions de forme

2. L'avant-projet de convention sur les contrats électroniques reprend le principe général de la liberté de forme consacré dans la Convention des Nations Unies sur les contrats de vente internationale de marchandises ("la Convention des Nations Unies sur les ventes")[1] et l'étend à tous les contrats entrant dans son champ d'application. Il est toutefois reconnu que des conditions de forme, telles que l'exigence d'un écrit ou d'une signature, peuvent être imposées par la loi applicable, par exemple lorsqu'un État partie à la Convention des Nations Unies sur les ventes a formulé une réserve conformément à l'article 96 de ladite Convention[2]. Même lorsque aucune condition de forme n'est exigée, certains obstacles à l'utilisation de messages de données peuvent découler de règles de preuve qui limitent expressément ou tacitement la possibilité des parties de recourir à de tels messages pour prouver l'existence et le contenu des contrats.

1. Exigence d'un écrit et valeur probante des enregistrements électroniques

3. Bien que la Loi type de la CNUDCI sur le commerce électronique ("la Loi type") ait été largement acceptée et qu'un nombre croissant d'États s'en inspirent pour élaborer leur législation sur le commerce électronique, un instrument international sur les contrats électroniques ne saurait partir de l'hypothèse que les principes énoncés dans la Loi type sont déjà appliqués universellement. Il semble donc utile que le nouvel instrument fixe les conditions dans lesquelles les exigences en matière de forme peuvent être remplies par des moyens électroniques équivalents.

4. Les décisions judiciaires sur la valeur juridique des enregistrements électroniques sont peu nombreuses. Les quelques jugements dont on a connaissance montrent une évolution vers la reconnaissance juridique des enregistrements électroniques et des messages de données mais également une incertitude quant à leur admissibilité comme moyen de formation des contrats et comme mode de preuve du contenu de ces contrats.

5. Aux États-Unis d'Amérique, les juridictions semblent faire preuve de souplesse en ce qui concerne l'admissibilité en preuve des enregistrements

électroniques, y compris des messages électroniques dans les procédures civiles[3]. Certaines ont rejeté des arguments selon lesquels les messages électroniques n'étaient pas admissibles du fait qu'ils n'étaient pas authentifiés et constituaient une preuve testimoniale[4]. Elles ont estimé au contraire que les messages électroniques obtenus du demandeur pendant la procédure de communication des pièces (discovery) s'authentifiaient eux-mêmes, car "la production pendant la procédure de discovery de documents détenus par les parties est un motif suffisant pour considérer ces documents comme s'auto-authentifiant"[5]. Les juridictions prennent généralement en considération tous les éléments de preuve disponibles et ne rejettent pas les enregistrements électroniques comme étant des preuves à première vue insuffisantes.

6. À l'opposé, dans certains pays qui n'ont pas adopté la Loi type, les enregistrements électroniques, en particulier ceux issus d'opérations effectuées par l'intermédiaire d'Internet, sont considérés comme "dépourvus de valeur juridique"[6]. De plus, l'inquiétude face au risque de manipulation de ces enregistrements a conduit les juridictions à nier toute valeur probante, par exemple, aux messages électroniques dans le cadre de procédures judiciaires au motif que ce type de messages n'offre pas de garanties suffisantes d'intégrité[7].

7. La jurisprudence sur cette question est encore balbutiante et, étant donné le faible nombre de décisions judiciaires à ce jour, elle ne constitue pas une base suffisante pour tirer des conclusions définitives. On pourrait toutefois arguer que le commerce international tirerait sans doute profit de la plus grande sécurité juridique qui résulterait de dispositions uniformes prévoyant des critères pour la reconnaissance des enregistrements électroniques et des messages de données dans les échanges internationaux. Le paragraphe 2 de l'article 9 de l'avant-projet de convention reproduit, à cette fin, les critères énoncés à l'article 6 de la Loi type pour que les messages de données soient juridiquement reconnus comme des "écrits".

2. Attribution des messages et exigence d'une signature

8. L'utilisation de méthodes électroniques d'identification soulève deux questions qui méritent probablement d'être examinées par le Groupe de travail: premièrement celle, générale, de l'attribution d'un message à son expéditeur supposé et deuxièmement celle de savoir si la méthode d'identification utilisée par les parties est propre à satisfaire aux conditions légales de forme, en particulier à l'exigence d'une signature. Une attention particulière doit également être accordée aux notions juridiques qui impliquent l'existence d'une signature manuscrite, par exemple la notion de "document" dans certains systèmes juridiques. Même si ces deux questions sont souvent imbriquées voire, selon les circonstances, impossibles à dissocier complètement, il peut être utile de tenter de les analyser séparément, car les juridictions parviennent apparemment à des conclusions différentes suivant la fonction attribuée à la méthode d'identification.

a) Attribution des messages de données

9. La Loi type traite de l'attribution des messages de données dans son article 13, lequel tire son origine de l'article 5 de la Loi type de la CNUDCI sur les virements internationaux, qui définit les obligations de l'expéditeur d'un ordre de paiement. L'article 13 est censé s'appliquer lorsque se pose la question de savoir si un message de données a réellement était envoyé par la personne qui est désignée

comme l'expéditeur. Dans le cas d'une communication sur papier, le problème se poserait lorsque la signature de l'expéditeur présumé semble avoir été contrefaite. Dans un environnement électronique, il se peut qu'une personne non autorisée ait envoyé le message, l'authentification par codage, cryptage ou toute autre méthode étant néanmoins correcte. L'article 13 n'a pas pour objet d'attribuer une responsabilité mais plutôt de traiter la question de l'attribution des messages de données en établissant une présomption selon laquelle, dans certains cas, un message de données serait considéré comme émanant de l'expéditeur.

10. Le paragraphe 1 de l'article 13 de la Loi type rappelle le principe selon lequel l'expéditeur est lié par un message de données s'il l'a effectivement envoyé. Le paragraphe 2 se réfère au cas où le message n'a pas été envoyé par l'expéditeur mais par une personne autorisée à agir en son nom. Le paragraphe 3 traite de deux types de situations dans lesquelles le destinataire pourrait considérer qu'un message de données émane de l'expéditeur: d'une part, lorsqu'il a correctement appliqué une procédure d'authentification que l'expéditeur avait précédemment acceptée; et, d'autre part, lorsque le message de données résulte des actes d'une personne qui, de par ses relations avec l'expéditeur, a eu accès aux procédures d'authentification utilisées par ce dernier.

11. Un certain nombre de pays ont adopté la règle énoncée à l'article 13 de la Loi type, y compris la présomption d'attribution établie au paragraphe 3 de cet article[8]. La loi de certains pays considère expressément l'utilisation de codes, de mots de passe ou d'autres moyens d'identification comme des facteurs créant une présomption d'attribution du message[9]. Il existe également des versions plus générales de l'article 13, dans lesquelles la vérification correcte à l'aide d'une procédure précédemment convenue ne crée pas une présomption mais indique les éléments pouvant être utilisés à des fins d'attribution du message[10].

12. D'autres pays, en revanche, n'ont adopté que les règles générales de l'article 13 selon lesquelles un message de données émane de l'expéditeur s'il a été envoyé par l'expéditeur lui-même ou par une personne agissant en son nom ou encore par un système programmé par l'expéditeur ou en son nom pour fonctionner automatiquement[11]. Enfin, quelques pays qui ont incorporé la Loi type dans leur droit interne n'ont pas prévu de dispositions particulières fondées sur l'article 13[12]. Ces pays sont partis du principe qu'aucune règle particulière n'était nécessaire et qu'il valait mieux utiliser les mêmes moyens de preuve ordinaires pour l'attribution des messages que pour l'attribution des documents sur papier: "Celui qui désire invoquer une signature s'expose toujours à ce que celle-ci soit invalide. La règle demeure la même dans le cas des signatures électroniques[13].

13. Dans les pays qui n'ont pas adopté la Loi type, la législation ne contient apparemment pas de dispositions particulières traitant de l'attribution des messages d'une manière similaire. Dans ces pays, l'attribution dépend généralement de la reconnaissance juridique des signatures électroniques et des présomptions associées aux enregistrements authentifiés par des types particuliers de signature électronique.

14. L'avant-projet de convention ne contient pas pour l'instant de règles particulières d'attribution fondées sur l'article 13 de la Loi type. Le Groupe de travail souhaitera peut-être examiner, toutefois, s'il serait utile d'énoncer des dispositions sur ce point séparément des dispositions sur les signatures électroniques. En effet, les signatures ne sont pas le seul mode d'identification

reconnu par la loi pour attribuer des documents et des enregistrements à une personne déterminée, comme l'expliquent les commentaires officiels concernant l'article 9 de la loi uniforme des États-Unis sur les opérations électroniques[14]:

"1. Conformément à l'alinéa a) [de l'article 9 de la loi uniforme], si l'enregistrement électronique ou la signature électronique résulte de l'action d'une personne, il ou elle sera attribué(e) à cette personne – l'effet juridique de cette attribution est traité à l'alinéa b). Cet article ne modifie pas les règles de droit existant en matière d'attribution. Son objet est d'assurer l'application de ces règles dans l'environnement électronique. Par action d'une personne, on entend également les actions des agents humains mais aussi celles d'un agent électronique – à savoir l'outil – de la personne. Bien que cette règle semble énoncer une évidence, elle garantit que l'enregistrement ou la signature sera attribué, non pas à une machine, mais à la personne exploitant ou programmant la machine.

L'enregistrement électronique comme la signature électronique seraient attribuables à une personne conformément à l'alinéa a) dans chacun des cas suivants:

A. Lorsque la personne tape son nom dans une commande par courrier électronique;

B. Lorsque l'employé de la personne, conformément au pouvoir qui lui a été donné, tape le nom de la personne dans une commande par courrier électronique;

C. Lorsque l'ordinateur de la personne, programmé pour commander des biens sur réception d'informations concernant les stocks suivant des paramètres particuliers, émet une commande dans laquelle figure le nom de la personne, ou d'autres informations identifiantes.

Dans chacun des cas susmentionnés, une loi autre que la loi uniforme sur les opérations électroniques attribuerait la signature et l'action à la personne si un support papier a été utilisé. L'alinéa a) prévoit expressément que le même résultat sera obtenu en cas d'utilisation d'un support électronique.

2. Aucune disposition [de l'article 9 de la loi uniforme] n'a d'incidence sur l'utilisation d'une signature pour attribuer un enregistrement à une personne. En effet, une signature est souvent le principal moyen d'attribuer un enregistrement. Dans les exemples qui précèdent, une fois que la signature électronique a été attribuée à la personne, l'enregistrement électronique lui serait également attribué, à moins que celle-ci n'établisse l'existence d'une fraude, d'une falsification ou d'un autre motif d'invalidation. Toutefois, une signature n'est pas le seul mode d'attribution.

3. L'utilisation de la transmission par télécopie fournit plusieurs exemples d'attribution à partir d'informations autres qu'une signature. Un fax peut être attribué à une personne en raison des informations imprimées en haut de la page qui indiquent la machine à partir de laquelle il a été envoyé. De même, le document transmis peut contenir un en-tête qui identifie l'expéditeur. Dans certaines décisions, cet en-tête a été considéré comme constituant effectivement une signature parce qu'il s'agissait d'un symbole adopté par

l'expéditeur dans l'intention d'authentifier le fax. Toutefois, la détermination de la signature découlait de la nécessité d'établir l'intention en l'espèce. Dans d'autres décisions, les en-têtes de fax n'ont PAS été considérés comme des signatures car l'intention requise était absente. L'important est qu'avec ou sans signature, l'information contenue dans l'enregistrement électronique sera très probablement suffisante pour fournir les éléments conduisant à l'attribution d'un enregistrement électronique à une partie déterminée.

En principe, le contenu de l'enregistrement fournira les informations nécessaires aux fins d'attribution. Il se peut également qu'une relation d'affaires durable entre les parties conduise à l'attribution de l'enregistrement. Tout comme pour un document papier, la preuve d'une falsification ou d'une contrefaçon peut être rapportée pour réfuter la preuve de l'attribution de l'enregistrement.

4. Un environnement électronique peut contenir certaines informations qui ne semblent pas attribuer un enregistrement particulier à une personne mais qui lient clairement les deux. Les codes numériques, les numéros d'identification personnels et les paires de clefs publique et privée servent à établir la partie à laquelle un enregistrement électronique devrait être attribué. Bien évidemment, les procédures de sécurité seront un autre élément de preuve dont on dispose pour établir l'attribution.

La mention expresse des procédures de sécurité en tant que moyen de prouver l'attribution d'un enregistrement est salutaire en raison de l'importance capitale de ce type de procédure dans l'environnement électronique. Dans certains cas, une procédure technique et technologique de sécurité peut être le meilleur moyen de convaincre un juge que tel ou tel enregistrement ou signature électronique est le fait d'une personne déterminée. Dans certaines circonstances, l'utilisation d'une procédure de sécurité pour établir qu'un enregistrement et la signature s'y rattachant proviennent de l'entreprise de la personne sera peut-être nécessaire pour réfuter une allégation de piratage informatique. Le fait que l'article mentionne les procédures de sécurité ne veut pas dire que d'autres formes de preuve devraient se voir attribuer un effet persuasif moindre. Il importe aussi de rappeler que la valeur particulière d'une procédure donnée n'a pas d'incidence sur son caractère même de procédure de sécurité mais influe seulement sur le poids à lui accorder en tant que preuve tendant à établir l'attribution."

15. Il semble également important de ne pas perdre de vue qu'une présomption d'attribution ne se substituerait pas à l'application des règles de droit sur les signatures, lorsqu'une signature est nécessaire pour valider ou prouver un acte. Lorsqu'il est établi qu'un enregistrement ou une signature est attribuable à une partie, "l'effet d'un enregistrement ou d'une signature doit être déterminé à la lumière du contexte et des circonstances, y compris toute convention éventuelle des parties" ainsi qu'en fonction "d'autres conditions légales envisagées à la lumière de ce contexte"[15].

16. il existe aussi une approche plus restrictive comme le montrent plusieurs récentes affaires de ventes aux enchères sur Internet, dans lesquelles les juridictions ont appliqué une règle stricte pour l'attribution de messages de données. Les actions avaient été le plus souvent intentées pour violation de contrat en raison du non-

paiement de biens prétendument achetés aux enchères sur Internet, le demandeur soutenant chaque fois que le défendeur était l'acheteur, attendu que l'offre la plus élevée avait été authentifiée par le mot de passe du défendeur et avait été envoyée depuis l'adresse électronique de ce dernier. Les juridictions ont estimé que ces éléments n'étaient pas suffisants pour conclure avec certitude que le défendeur avait bien participé à la vente aux enchères et soumis l'offre retenue. Elles ont invoqué divers arguments pour justifier cette position. Par exemple, les mots de passe n'étaient pas fiables car toute personne connaissant le mot de passe du défendeur aurait pu utiliser l'adresse électronique de ce dernier depuis n'importe où et participer à la vente aux enchères en se servant de son nom[16]. Ce risque a été jugé "très élevé" par certaines juridictions, au vu des avis d'experts concernant les menaces d'atteinte à la sécurité des réseaux de communications par Internet, en particulier par l'utilisation de "chevaux de Troie" permettant de "voler" le mot de passe d'une personne[17]. Le risque d'une utilisation non autorisée d'un mode d'identification (mot de passe) devait être supporté par la partie qui offrait les biens ou services par un moyen particulier, faute de présomption légale selon laquelle les messages envoyés par l'intermédiaire d'un site Web sur Internet à l'aide du mot de passe d'une personne permettant d'accéder à ce site étaient attribuables à cette personne[18]. Une telle présomption pouvait éventuellement être attachée à une "signature électronique avancée", telle que définie dans la loi, mais le détenteur d'un simple "mot de passe" ne devait pas assumer le risque que celui-ci soit détourné par des personnes non autorisées[19].

17. Des règles uniformes d'attribution des messages de données seraient probablement utiles pour permettre à une partie de savoir avec plus de certitude à quels éléments elle peut se fier pour attribuer la responsabilité d'un message de données. Ces règles pourraient être formulées sous la forme d'une présomption, à partir d'éléments de l'article 13 de la Loi type. Elles peuvent avoir pour autre avantage de limiter la portée des questions devant être résolues par des règles communes sur les signatures électroniques, lesquelles ont souvent un objectif différent.

b) Exigence d'une signature

18. En ce qui concerne l'exigence d'une signature, une question que le Groupe de travail aura à examiner est de savoir si l'avant-projet de convention devrait se limiter à énoncer une disposition générale sur la reconnaissance des signatures électroniques ou s'il devrait fixer plus en détail les conditions de leur reconnaissance juridique. Dans le premier cas, le Groupe de travail souhaitera peut-être insérer dans le nouvel instrument une disposition du paragraphe 1 de l'article 7 de la Loi type. Cette solution est présentée dans la variante A du paragraphe 3 du projet d'article 9. Dans le second cas, le Groupe de travail aurait recours à un texte plus détaillé semblable au paragraphe 3 de l'article 6 de la Loi type de la CNUDCI sur les signatures électroniques. Cette solution est présentée dans la variante B du paragraphe 3 du projet d'article 9. Il est à noter que ces deux solutions ne s'excluent pas mutuellement, puisque le paragraphe 1 de l'article 7 de la Loi type sur le commerce électronique a servi de base à l'élaboration des règles plus détaillées du paragraphe 3 de l'article 6 de la Loi type sur les signatures électroniques.

19. En définitive, le choix entre les deux variantes implique de déterminer le niveau de détail souhaitable pour fournir des orientations utiles et assurer un degré

d'uniformité acceptable. En tout état de cause, il semble important que les règles laissent une marge de manœuvre appropriée pour que les parties et les juges puissent évaluer l'adéquation et la fiabilité des méthodes d'authentification utilisées à la lumière de toutes les circonstances de l'espèce.

20. Dans certains pays, les juridictions ont eu tendance à interpréter l'exigence de signature de manière extensive. Les juges américains ont été réceptifs à la reconnaissance législative des signatures électroniques, admettant leur utilisation également dans des situations qui ne sont pas expressément prévues dans la loi habilitante, par exemple dans le cas des mandats judiciaires[20]. Fait plus important, dans le domaine contractuel, ils ont également déterminé si l'identification était adéquate en tenant compte des transactions entre les parties plutôt qu'en recourant à une règle stricte pour toutes les situations. Ainsi, lorsque les parties avaient régulièrement utilisé des messages électroniques dans leurs négociations, ils ont estimé que le nom dactylographié de l'expéditeur figurant dans un message électronique satisfaisait à l'exigence légale de signature[21]. Le "choix délibéré" d'une personne "de dactylographier son nom à la fin de tous ses messages électroniques" a été considéré comme une authentification valable[22]. Une interprétation aussi extensive est adoptée par les juridictions colombiennes, qui ont confirmé l'admissibilité des procédures judiciaires menées entièrement au moyen de communications électroniques. Les conclusions échangées pendant ces procédures étaient valables, même si elles ne comportaient pas de signature numérique[23], attendu que les communications électroniques utilisaient des méthodes permettant d'identifier les parties[24].

21. À l'opposé, dans d'autres pays comme la France, les juridictions ont hésité à accepter les moyens électroniques d'identification comme équivalant à une signature manuscrite avant l'adoption d'une législation reconnaissant expressément la validité des signatures électroniques[25]. Parallèlement, toutefois, certaines décisions acceptent le dépôt par voie électronique de plaintes administratives pour respecter un délai fixé par la loi, du moins à condition que ces plaintes soient ensuite confirmées par courrier ordinaire[26].

22. Alors qu'elles ont adopté une approche restrictive pour l'attribution des messages de données dans la formation des contrats, les juridictions allemandes ont fait preuve de souplesse dans la reconnaissance des méthodes d'identification comme équivalant aux signatures manuscrites dans le cadre de procédures judiciaires. Le débat en Allemagne a porté sur l'utilisation de plus en plus fréquente d'images numérisées de la signature d'avocats pour authentifier des fax contenant des déclarations d'appel transmis directement par modem depuis un ordinateur à un télécopieur d'un tribunal. Dans les premières affaires jugées, les cours d'appel[27] et la cour fédérale (*Bundesgerichtshof*)[28] avaient estimé qu'une image numérisée d'une signature manuscrite ne satisfaisait pas aux exigences existant en matière de signature et ne prouvait pas l'identité d'une personne. Une fonction d'identification pouvait éventuellement être attribuée à une "signature électronique avancée", telle que définie dans la loi allemande. Toutefois, il incombait généralement au législateur et non aux juges d'établir les conditions d'équivalence entre les écrits et les communications dématérialisées par transferts de données[29]. Cette interprétation a finalement été infirmée en raison de l'opinion unanime des autres cours fédérales supérieures qui ont accepté la remise de certaines pièces de procédure par

communication électronique d'un message de données contenant l'image numérisée d'une signature[30].

23. Il n'est pas dit que les considérations justifiant une approche souple dans le cadre de procédures d'appel judiciaire ou administratif puissent être directement transposées dans le contexte des contrats internationaux. En effet, si dans un contexte contractuel une partie s'expose au risque de voir l'accord rejeté par l'autre partie, dans une procédure civile, c'est généralement la partie utilisant une signature ou un enregistrement électronique qui souhaite confirmer qu'elle approuve l'enregistrement et son contenu. Néanmoins, la discussion ci-dessus montre comment les juridictions tendent dans la pratique à évaluer la fiabilité des méthodes d'authentification en fonction de la finalité de leur utilisation.

24. Le Groupe de travail souhaitera peut-être également tenir compte, dans ses débats, du fait que, conformément au paragraphe 3 de l'article 7 de la Loi type sur le commerce électronique et au paragraphe 5 de l'article 6 de la Loi type sur les signatures électroniques, un État adoptant a la possibilité d'exclure la reconnaissance des signatures électroniques dans certains cas devant être indiqués dans la législation interne. Pour favoriser au mieux l'harmonisation du droit au niveau international, l'idéal serait une liste d'exclusions arrêtée d'un commun accord. Il est admis, toutefois, que ce résultat ne sera probablement pas facile à obtenir. Une solution possible, que le Groupe de travail voudra peut-être examiner, serait d'exclure seulement les cas dans lesquels la législation interne soit rejette catégoriquement les signatures électroniques, soit prescrit l'utilisation d'un type particulier de signature électronique ("signature avancée" ou "signature sécurisée").

Notes

[1] Nations Unies, *Recueil des Traités*, vol. 1489, n° 25567, p.3 (également accessible à l'adresse www.uncitral.org/french/texts/sales/CISG-f.htm).

[2] Aux termes de l'article 96:

> "Tout État contractant dont la législation exige que les contrats de vente soient conclus ou constatés par écrit peut à tout moment déclarer, conformément à l'article 12, que toute disposition de l'article 11, de l'article 29 ou de la deuxième partie de la présente Convention autorisant une forme autre que la forme écrite pour la conclusion, la modification ou la résiliation amiable d'un contrat de vente, ou pour toute offre, acceptation ou autre manifestation d'intention, ne s'applique pas dès lors qu'une des parties a son établissement dans cet État."

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

[4] Dans l'affaire *Sea-Land Service, Inc. v. Lozen International, Llc.,* par exemple, une cour d'appel a infirmé une décision d'un tribunal de district qui avait rejeté un message électronique interne à la société dont l'un des employés du demandeur était l'auteur. Le tribunal avait écarté cet élément de preuve au motif que le défendeur "n'avait pas d'argument et n'avait pas présenté de preuve indiquant l'identité ou la fonction de cet employé". La cour d'appel a noté que l'original du message électronique, une note interne, se terminait par une "signature" électronique indiquant le nom et la fonction de l'auteur. Le tribunal de district avait donc abusé de son pouvoir discrétionnaire en refusant d'admettre le message électronique en preuve (United States

Court of Appeals for the Ninth Circuit, 3 avril 2002, Federal Reporter, 3rd series, vol. 285, p. 808).

[5] *Superhighway Consulting, Inc. v. Techwave, Inc.,* United States District Court for the Northern District of Illinois, Eastern Division, 16 novembre 1999, U.S. Dist. LEXIS 17910.

[6] Déclaration (non datée) de Ruy Rosado de Aguiar Jr., juge du Tribunal supérieur de justice du Brésil ("*Comércio eletrônico não tem valor jurídico*", à l'adresse www.trabalhodeeconomia.hpg.ig.com.br/juri.html, page consultée le 12 septembre 2003).

[7] Amtsgericht Bonn, Décision n° 3 C 193/01, 25 octobre 2001, *JurPC – Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 332/2002 (www.jurpc.de/rechtspr/20020332.htm, page consultée le 11 septembre 2003). Dans cette affaire, le demandeur a assigné le défendeur en paiement d'une commission pour ses services d'intermédiaire dans une vente de cigarettes en gros. Le tribunal a rejeté la demande faute de preuve de l'existence d'un accord en vue du versement d'une commission. Il a considéré que les tirages papier d'un message électronique produits par le demandeur et rejetés par le défendeur n'avaient pas de valeur probante, car "tout le monde sait" que les messages électroniques ordinaires peuvent être facilement altérés ou falsifiés.

[8] Voir Colombie (*Ley Número 527 de 1999: Ley de comercio electrónico*, art. 17); Équateur (*Ley de comercio electrónico, firmas electrónicas y mensajes de datos, 2002,* art. 10); Jordanie (Electronic Transactions Law (n° 85) of 2001, art. 15); Maurice (Electronic Transactions Act, 2000, art. 12-2); Philippines (Electronic Commerce Act, 2000, art. 18, par. 3); République de Corée (loi cadre sur le commerce électronique de 1999, art. 7, par. 2); Singapour (Electronic Transactions Act, 1998, art. 13-3); Thaïlande (loi sur les opérations électroniques de 2002, art. 16); et Venezuela (*Decreto n° 1024 de 10 de febrero de 2001 – Ley sobre mensajes de datos y firmas electrónicas,* art. 9). Les mêmes règles ont également été adoptées dans la législation de Jersey (dépendance de la Couronne britannique) (Electronic Communications (Jersey) Law 2000, art. 8), des Bermudes (territoire d'outre-mer britannique) (Electronic Transactions Act, 1999, art. 16, par. 2) et des Îles Turques et Caïques (également territoire d'outre-mer britannique) (Electronic Transactions Ordinance, 2000, art. 14).

[9] Mexique (*Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal, 26 avril 2000,* art. 90, par. I*).*

[10] Par exemple, la loi uniforme des États-Unis sur les opérations électroniques (Uniform Electronic Transactions Act (UETA)) prévoit dans son article 9 a) qu'un enregistrement électronique ou une signature électronique "peut être attribué à une personne si cet enregistrement ou cette signature était l'acte de cette personne. L'acte de la personne peut être prouvé par tout moyen, y compris par la démonstration de l'efficacité de toute procédure de sécurité appliquée pour déterminer à qui l'enregistrement électronique ou la signature électronique était attribuable". L'article 9 b) dispose en outre que l'effet d'un enregistrement électronique ou d'une signature électronique attribué à une personne en vertu de l'alinéa a) "est déterminé à partir du contexte et des circonstances entourant sa création, son exécution ou son adoption, y compris toute convention éventuelle des parties, et de toute autre manière prévue par la loi".

[11] Australie (Electronic Transactions Act, 1999, art. 15, par. 1)); des règles essentiellement identiques sont prévues dans la législation des pays suivants: Inde (Information Technology Act, 2000, art. 11); Pakistan (Electronic Transactions Ordinance, 2002, art. 13-2); Slovénie (Electronic Commerce and Electronic Signature Act, 2000, art. 5); Île de Man (dépendance de la Couronne britannique) (Electronic Transactions Act, 2000, art. 2); et Région administrative spéciale de Hong Kong (Chine) (Electronic Commerce Ordinance, 2000, art.18).

[12] Par exemple, le Canada, la France, l'Irlande, la Nouvelle-Zélande et l'Afrique du Sud.

[13] Conférence pour l'harmonisation des lois au Canada, Loi uniforme sur le commerce électronique (annotée), commentaire sur l'article 10-2 (www.ulcc.ca/fr/poam2/index.cfm?sec=1999&sub=1999ia, page consultée le 11 septembre 2003).

[14] National Conference of Commissioners on Uniform State Laws, *Uniform Electronic Transactions Act (1999)*, loi approuvée et recommandée pour adoption dans tous les États à la 108e conférence annuelle (Denver, Colorado, 23-30 juillet 1999), avec préface et commentaires (www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm, page consultée le 11 septembre 2003).

[15] Ibid.

[16] Amtsgericht Erfurt, Décision n° 28 C 2354/01, 14 septembre 2001, *JurPC – Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 71/2002 (www.jurpc.de/rechtspr/20020071.htm, page consultée le 25 août 2003).

[17] Landgericht Konstanz, Décision n° 2 O 141/01 A, 19 avril 2002, *JurPC – Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 291/2002 (www.jurpc.de/rechtspr/20020291.htm, page consultée le 25 août 2003).

[18] Landgericht Bonn, Décision n° 2 O 450/00, 7 août 2001, *JurPC – Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 136/2002 (www.jurpc.de/rechtspr/20020136.htm, page consultée le 25 août 2003).

[19] Oberlandesgericht Köln, Décision n° 19 U 16/02, 19 avril 2002, *JurPC – Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 291/2002 (www.jurpc.de/rechtspr/20020291.htm, page consultée le 25 août 2003).

[20] *Department of Agriculture & Consumer Services v. Haire*, Court of Appeal of Florida, Décisions nos 4D02-2584 et 4D02-3315, 15 janvier 2003 (www.4dca.org/Jan2003/01-15-03/4D02-2584op.pdf, page consultée le 12 septembre 2003).

[21] Dans l'affaire *Cloud Corporation v. Hasbro, Inc*., une action en violation de contrat a été intentée contre le défendeur, qui niait avoir passé un certain nombre de commandes. Les parties avaient communiqué par messagerie électronique. Il s'est avéré que certains des messages échangés n'étaient pas signés. Le tribunal de district a tranché en faveur du défendeur, la preuve des prétendus engagements d'achat n'ayant pas été faite. La cour d'appel a infirmé ce jugement, estimant que le nom de l'expéditeur figurant dans un message électronique satisfaisait à l'exigence de signature imposée par la loi sur les fraudes. Elle a également considéré que ni la *common law* ni le Code de commerce uniforme (Uniform Commercial Code) n'exigeaient de signature manuscrite, "même si une telle signature est une meilleure preuve d'identité qu'une signature dactylographiée". Selon la cour, la loi sur les fraudes a pour but "d'empêcher une partie contractante de soulever, à propos des clauses du contrat – voire de l'existence même d'un contrat – une contestation donnant matière à procès sur le seul fondement de ses propres allégations. Aucune signature manuscrite n'est requise à cette fin, en particulier dans un cas où, hormis l'écrit, il existe des éléments autres que les simples allégations de la partie pour prouver l'existence du contrat" (United States Court of Appeals for the Seventh Circuit, 26 décembre 2002, Federal Reporter, 3rd series, vol. 314, p. 296).

[22] *Jonathan P. Shattuck v. David K. Klotzbach*, Superior Court of Massachusetts, 11 décembre 2001, 2001 Mass. Super. LEXIS 642. L'acheteur a assigné les vendeurs en exécution d'un contrat de vente d'un bien immobilier et en réparation d'une prétendue violation de ce contrat. Les vendeurs ont présenté une requête en irrecevabilité alléguant qu'il n'y avait pas de contrat de vente écrit et signé satisfaisant aux conditions de forme fixées par les lois du Massachusetts. Les parties avaient négocié la vente d'un bien immobilier en échangeant des messages électroniques. Tous ces messages se terminaient par une signature dactylographiée. Le tribunal a considéré que les parties s'étaient entendues sur les clauses essentielles du contrat de vente: les parties, le lieu, la nature de l'opération et le prix d'achat, satisfaisant ainsi aux conditions posées par la loi sur les fraudes. Il a en outre estimé que l'intention du vendeur était d'authentifier les messages qu'il avait envoyés à propos des conditions de vente en y apposant son nom dactylographié.

[23] La Colombie a adopté la Loi type de la CNUDCI sur le commerce électronique. Bien que la législation colombienne contienne une disposition générale semblable à l'article 7 de la Loi type, elle n'établit une présomption d'authenticité que pour les signatures numériques (*Ley Número 527 de 1999: Ley de comercio electrónico, article 28*).

[24] *Juan Carlos Samper v. Jaime Tapias*, Juzgado Segundo Promiscuo Municipal Rovira Tolima, 21 juillet 2003, Rad. 73-624-40-89-002-2003-053-00 (www.alfa-redi.org/documento/alexdiaz.pdf, page consultée le 12 septembre 2003).

[25] La Cour de cassation a jugé irrecevable une déclaration d'appel signée électroniquement, attendu qu'il existait des doutes sur l'identité de la personne ayant créé la signature et que la déclaration avait été signée électroniquement avant l'entrée en vigueur de la loi du 13 mars 2000, qui reconnaissait l'effet juridique des signatures électroniques (Cour de cassation, deuxième Chambre civile, 30 avril 2003, *Société Chalets Boisson* c. M. X., www.juriscom.net/jpt/visu.php?ID=239, page consultée le 12 septembre 2003).

[26] Conseil d'État, 28 décembre 2001, n° 235784, *Élections municipales d'Entre-Deux-Monts* (www.rajf.org/article.php3?id_article=467, page consultée le 12 septembre 2003).

[27] Par exemple, Oberlandesgericht Karlsruhe, Décision n° 14 U 202/96, 14 novembre 1997, *JurPC – Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 09/1998 (www.jurpc.de/rechtspr/19980009.htm, page consultée le 12 septembre 2003).

[28] Bundesgerichtshof, Décision n° XI ZR 367/97, 29 septembre 1998, *JurPC – Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 291/2002 (www.jurpc.de/rechtspr/19990005.htm, page consultée le 12 septembre 2003).

[29] Le Bundesgerichtshof a reconnu que la jurisprudence acceptait depuis quelques temps l'utilisation du télécopieur pour la transmission de conclusions. Dans ces cas, toutefois, l'original devait être signé de la main de l'avocat et cette signature figurait généralement sur le fax reçu par les tribunaux. Or, les fax générés et transmis directement par ordinateur ne produisaient pas de document original sous forme matérielle. Le document n'était pas non plus signé de la main de l'avocat. Seule la version papier du fax imprimée par le télécopieur du tribunal constituait un document physique. Accepter les fax transmis par ordinateur reviendrait en définitive à renoncer à l'exigence d'un écrit fixé par la loi. Le législateur a été invité à fixer les conditions d'équivalence entre les écrits et les communications dématérialisées par transferts de données. Selon le Bundesgerichtshof, ce résultat ne pouvait être obtenu que par la loi et non par la jurisprudence (voir note 28).

[30] Dans une décision sur une affaire que lui avait soumise le Bundesgerichtshof (voir note 26 ci-dessus), le Sénat commun des Cours suprêmes de la Fédération (Gemeinsamer Senat der obersten Gerichtshöfe des Bundes) a noté que les conditions de forme dans les procédures judiciaires n'étaient pas une fin en soi. Leur but était d'assurer une détermination suffisamment fiable ("*hinreichend zuverlässig*") du contenu de l'écrit et de l'identité de la personne dont émanait cet écrit. Le Sénat commun a constaté que l'application, dans la pratique, des conditions de forme avait évoluée, de manière à tenir compte des récentes innovations technologiques, telles que le télex ou le fax. Il a estimé que l'acceptation de la remise de certaines pièces de procédure par communication électronique d'un message de données contenant une image numérisée d'une signature serait conforme à l'esprit de la jurisprudence existante (Gemeinsamer Senat der obersten Gerichtshöfe des Bundes, GmS-OGB 1/98, 5 avril 2000, *JurPC – Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 160/2000 (www.jurpc.de/rechtspr/20000160.htm, page consultée le 12 septembre 2003)).