Nations Unies A/CN.9/630/Add.2

Assemblée générale

Distr.: Générale
26 avril 2007

Français
Original: Anglais

Commission des Nations Unies pour le droit commercial international
Quarantième session
Vienne, 25 juin-12 juillet 2007

Travaux futurs possibles dans le domaine du commerce électronique

Document de référence général sur les éléments nécessaires à l'élaboration d'un cadre juridique favorable au commerce électronique: exemple de chapitre sur l'utilisation internationale des méthodes d'authentification et de signature électroniques.

Note du Secrétariat*

Additif

L'on trouvera en annexe à la présente note une partie d'un exemple de chapitre (première partie, chapitre II, sections A et B) d'un document de référence général consacré aux aspects juridiques de l'utilisation internationale des méthodes d'authentification et de signature électroniques.

* La présentation de cette note par le Secrétariat de la Commission des Nations Unies pour le droit commercial international a été retardée pour cause de sous-effectif.

V.07-82828 (F) 040607 050607

Annexe

Table des matières

Première partie.
Méthodes d'authentification et de signature électroniques

[…]

II. Régime juridique applicable à l'authentification et aux signatures électroniques

1. Le commerce électronique ne peut se développer que dans un climat de confiance et des règles spéciales peuvent être nécessaires pour que son utilisation soit plus certaine et plus sûre. Ces règles peuvent revêtir la forme de textes législatifs très divers: instruments juridiques internationaux (traités et conventions), lois-types transnationales, législations nationales (fréquemment fondées sur les lois types), instruments d'autorégulation[1] ou accords contractuels.[2]

2. Pour une large part, les opérations relevant du commerce électronique se font par des circuits fermés, c'est-à-dire par l'intermédiaire de groupes qui ne comportent qu'un nombre limité de participants et auxquels n'ont accès que les personnes ou entreprises préalablement autorisées. Les réseaux fermés sont utilisés dans le cadre des opérations d'une seule et même entité ou bien d'un groupe restreint d'usagers préexistants, comme une institution financière participant à un système de compensation interbancaire, les bourses des valeurs et des produits ou une association de compagnies aériennes et d'agences de voyage. En pareils cas, la participation au réseau est habituellement restreinte aux institutions et sociétés préalablement admises à l'intérieur du groupe. La plupart de ces systèmes existent depuis plusieurs décennies, ont recours à des technologies perfectionnées et fonctionnement avec beaucoup de compétence. Le développement rapide du commerce électronique enregistré au cours des dix dernières années a débouché sur la mise au point d'autres modèles de réseaux, comme les chaînes d'approvisionnement ou les plateformes commerciales.

3. Bien que, dans un premier temps, ces nouveaux groupes aient été articulés autour de connexions directes d'ordinateur à ordinateur, comme la plupart des réseaux fermés qui existaient déjà, l'on constate une tendance croissante à l'utilisation de moyens de raccordement communs accessibles à tous, comme l'Internet. Même dans le cas de ces modèles les plus récents, un réseau fermé conserve son caractère exclusif. Habituellement, ils opèrent sur la base de normes contractuelles, d'accords, de procédures et de règles

---

[1] Voir par exemple Commission économique pour l'Europe, Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques, recommandation No 32 – "Instruments d'autorégulation du commerce électronique (codes de conduite)", (ECE/TRADE/277) disponible à l'adresse: http://www.unece.org/cefact/recommendations/rec_index.htm, consulté le mars 2007.

[2] Beaucoup d'initiatives, aux échelons aussi bien national qu'international, visent à élaborer des contrats-types. Voir par exemple Commission économique pour l'Europe, Groupe de travail sur la facilitation des procédures du commerce international, recommandation No 26 – "Utilisation commerciale d'accords d'échange aux fins de l'échange de données informatisé" (TRADE/WP.4/R.1133/Rev.1), et recommandation No 31 – "Accords de commerce électronique" (ECE/TRADE/257), disponibles à l'adresse : http://www.unece.org/cefact/recommendations/rec_index.htm, consulté le 28 mars 2007.

préétablies qualifiés d'appellations diverses comme "règles du système", "règles de fonctionnement" ou "accords entre partenaires commerciaux", conçus de manière à fournir et garantir la fonctionnalité, la fiabilité et la sécurité opérationnelles nécessaires aux membres du groupe. Ces règles et accords traitent fréquemment de question comme la reconnaissance de la valeur juridique des communications électroniques, la date et le lieu d'expédition et de réception des messages de données, les procédures de sécurité à suivre pour avoir accès au réseau ou les méthodes d'authentification devant être employées par les parties.[3] Dans les limites de la liberté contractuelle reconnues par le droit applicable, ces règles et accords sont habituellement d'application directe.

4. En l'absence de règles contractuelles, toutefois, ou dans la mesure où le droit applicable peut limiter leur application, la valeur juridique des méthodes d'authentification de signatures électroniques utilisées par les parties sera déterminée par les règles de droit applicables, sous forme de règles supplétives ou obligatoires. Les différentes formules utilisées par divers pays pour mettre en place un cadre juridique de réglementation des méthodes d'authentification de signatures électroniques sont examinées dans le présent chapitre.

A. Approche technologique des textes législatifs

5. Les lois et règlements relatifs aux méthodes d'authentification électroniques élaborés aux plans national et international ont revêtu de nombreuses formes différentes. L'on peut distinguer essentiellement trois approches des méthodes d'authentification et de signature: a) l'*approche minimaliste*; b) l'*approche technospécifique;* et c) l'*approche dualiste*.[4]

1. Approche minimaliste

6. Quelques pays,[5] suivant une politique de neutralité technologique, reconnaissent toutes les méthodes de signature électronique. Cette approche est également appelée minimaliste car elle ne confère qu'un statut juridique minimum aux différentes formes de signature électronique. Selon cette approche minimaliste, les signatures électroniques sont considérées comme l'équivalent fonctionnel de signatures manuscrites à condition que la technologie employée soit conçue de manière à aboutir à certains résultats spécifiés et, par ailleurs, réponde à certaines exigences de fiabilité sans rapport avec la méthode employée.

7. La Loi type de la CNUDCI sur le commerce électronique[6] contient la série de critères législatifs la plus largement utilisée aux fins de l'établissement d'une équivalence fonctionnelle générique entre les signatures électroniques et manuscrites. Le paragraphe 1 de son article 7 dispose ce qui suit:

---

[3] Pour un examen des questions qui font habituellement l'objet des accords entre partenaires commerciaux, voir Amelia H. Boss, “Electronic data interchange agreements: private contracting toward a global environment”, *Northwestern Journal of International Law and Business*, vol. 13, No.1 (1992), p. 45.

[4] Susanna F. Fischer, “Saving Rosencrantz and Guildenstern in a virtual world? A comparative look at recent global electronic signature legislation,” *Journal of Science and Technology Law*, vol. 7, No.2 (2001), pp. 234 et suivantes.

[5] Par exemple, l'Australie et la Nouvelle-Zélande.

[6] Voir note […] Publication des Nations Unies, numéro de vente: F. 99.V.4.

"1. Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données:

a) si une méthode est utilisée pour identifier la personne en question pour indiquer qu'elle approuve l'information contenue dans le message de données; et

b) si la fiabilité de cette méthode est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière."

8. Cette disposition reflète les deux principales fonctions des signatures manuscrites: identifier le signataire et indiquer l'intention de celui-ci en ce qui concerne l'information signée. Aux termes de la Loi type sur le commerce électronique, toute technologie pouvant jouer ce double rôle sous forme électronique peut être considérée comme satisfaisant aux conditions que doit réunir une signature pour avoir valeur juridique. La Loi type est donc neutre du point de vue technologique: autrement dit, elle ne dépend pas de l'utilisation d'un type de technologie déterminé ni ne présuppose l'emploi d'une méthode spécifique et elle peut être appliquée à la communication et au stockage de tous types d'informations. Cette neutralité technologique est particulièrement importante étant donné la rapidité de l'innovation technique et aide à garantir que la législation puisse s'accommoder des progrès futurs sans devenir obsolète trop rapidement. Aussi la Loi type évite-t-elle soigneusement toute mention d'une méthode technique spécifique de transmission ou de stockage de l'information.

9. Ce principe général a été reflété dans la législation de beaucoup de pays. Le principe de neutralité technologique permet également d'accommoder l'évolution future de la technologie. En outre, cette approche privilégie la liberté des parties de choisir la technologie la mieux adaptée à leurs besoins. Il appartient alors aux parties de déterminer le degré de sécurité qu'elles jugent suffisant pour leurs communications. Cela permet d'éviter une complexité technologique excessive et les surcroîts de coûts que cela entraîne.[7]

10. Sauf en Europe, où la législation a été influencée surtout par les directives de l'Union européenne,[8] la plupart des pays qui ont promulgué des textes concernant le commerce électronique ont utilisé la Loi type sur le commerce électronique comme un modèle.[9] La Loi type a également servi de base à l'harmonisation au plan national des lois

---

[7] Mason, "Electronic signatures in practice", *Journal of High Technology Law,* vol. VI, No.2 (2006), p.153.

[8] En particulier la Directive CE/1999/93 du Parlement européen et du Conseil relative à l'établissement d'un cadre communautaire pour les signatures électroniques, (voir note […]) [*Journal officiel des Communautés européennes*, L 13]. La Directive relative aux signatures électroniques a été suivie d'un texte plus général, Directive CE/2000/31 du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, en particulier le commerce électronique, sur le marché interne, qui a trait à des divers aspects de la fourniture de services informatiques et des contrats électroniques, (*Journal officiel des Communautés européennes*, No. L 178, 17 juillet 2000).

[9] Fin janvier 2007, des lois d'application des dispositions de la Loi type de la CNUDCI sur le commerce électronique avaient été adoptées par au moins les pays suivants: Afrique du Sud *(Loi de 2002 relative aux communications et aux transactions électroniques)*; Australie (*Loi de 1999 relative aux transactions électroniques)*; Chine *(Loi de 2004 relative aux signatures électroniques*); Colombie (*Loi relative au commerce électronique);* Équateur (*Loi de 2002*

relatives au commerce électronique des États fédéraux comme le Canada[10] et les États-Unis.[11] À quelques rares exceptions près,[12] les pays qui ont promulgué des textes

---

relative au commerce électronique, aux signatures électroniques et aux messages de données); France (*Loi No 2000-230 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*); Inde *(Loi No. 21 de 2000 relative aux technologies de l'information);* Irlande *(Loi de 2000 relative au commerce électronique);* Jordanie *(Loi No. 85 de 2001 relative aux transactions électroniques);* Maurice (*Loi de 2000 relative aux transactions électroniques*); Mexique (*Décret de 2000 portant réforme de différentes dispositions du Code civil du District fédéral en matière fédérale, du Code fédérakl de procédure civile et de la loi fédérale relative à la protection du consommateur)*; Nouvelle-Zélande (*Loi de 2002 relatives aux transactions électroniques*); Pakistan (*Ordonnance de 2002 relative aux transactions électroniques*); Panama (*Loi de 2001 relative aux signatures numérique*); Philippines (*Loi de 2000 relative au commerce électronique*); République de Corée (*Loi-cadre de 2001 relative au commerce électronique*); République dominicaine (*Loi de 2002 relative au commerce électronique et aux documents et signatures numériques*); Singapour (*Loi de 1998 relative aux transactions électroniques*)*;* Slovénie (*Loi de 2000 relative au commerce et aux signatures électroniques*); Sri Lanka (*Loi de 2006 relative auxx transactions électroniques*); Thaïlande (*Accord relatif aux transactions électroniques*); Venezuela (République bolivarienne du) (*Décret de 2001 relatif aux messages de données et aux signatures électroniques*) et Viet Nam (*Loi de 2006 relative aux transactions électroniques*). La Loi type a également été adoptée par Guernsey (*Electronic Transactions (Guernsey) Law 2000),* Jersey (*Electronic Communications (Jersey) Law 2000)* et l'île de Man (*Electronic Transactions Act 2000)*, dépendances de la Couronne britannique; dans le territoire britannique d'outre-mer des Bermudes (*Electronic Transactions Act 1999*); les îles Cayman (*Electronic Transactions Act 2000*); les îles Turques-et-Caïques (*Electronic Transactions Ordinance 2000*); et la Région administrative spéciale chinoise de Hong Kong (*Ordonnance No. 1 de 2000 relative aux transactions électroniques*). Sauf indication contraire, les références qui sont faites ci-après à la législation des pays indiqués se rapporte aux dispositions des textes énumérés ci-dessus.

[10] Au Canada, le texte d'application de la Loi type est la *Loi uniforme relative au commerce électronique* (UECA), adoptée en 1999 par la Conférence canadienne sur l'uniformalisation du droit (disponible, avec un commentaire officiel, à l'adresse http://www.chlc.ca/en/poam2/index.cfm?sec=1999&sub=1999ia, consulté le 12 avril 2007). L'UECA a depuis lors été promulguée par plusieurs provinces et territoires, dont l'Alberta, la Colombie britannique, le Manitoba, le Nouveau Brunswick, Terre-Neuve, le Labrador, la Nouvelle-Écosse, l'Ontario, l'île du Prince Edward, Saskatchewan et le Yukon. La Province du Québec a adopté une loi spécifique (*Loi de 2001 portant création d'un cadre juridique pour les technologies de l'information*) qui, bien que de portée plus générale et de libellé très différent, répond à bien des égards aux mêmes objectifs que l'UECA et est généralement conforme à la Loi type de la CNUDCI. L'on trouvera les dernières informations disponibles concernant la promulgation de l'UECA à l'adresse http://www.chlc.ca/en/cls/index.cfm?sec=4&sub=4b> (consulté le 7 février 2007).

[11] Aux États-Unis d'Amérique, la National Conference of Commissioners on Uniform State Law s'est fondée sur la Loi type de la CNUDCI sur le commerce électronique pour élaborer la Loi uniforme relative aux transactions électroniques (UETA), qu'elle a adoptée en 1999 (le texte de l'UETA, avec le commentaire officiel, est disponible à l'adresse http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm, consulté le 7 février 2007). L'UETA a depuis lors été promulguée par le District de Columbia et les 46 États suivants: Alabama, Alaska, Arizona, Arkansas, Californie, Caroline du Nord, Caroline du Sud, Colorado, Connecticut, Dakota du Nord, Dakota du Sud, Delaware, Floride, Hawaï, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiane, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, Nouveau Mexique, Ohio, Oklahoma, Oregon, Pennsylvanie, Rhodes Island, Tennessee, Texas, Utah, Vermont, Virginie, Virginie occidentale, Wisconsin et Wyoming. Les autres États adopteront probablement des textes d'application dans un proche avenir, dont l'Illinois, qui a déjà incorporé les dispositions de la Loi type de la CNUDCI par le biais de la loi de 1998 relative à la sécurité

d'application de la Loi type ont préservé son approche technologiquement neutre et n'ont ni prescrit, ni privilégié l'utilisation d'une méthode spécifique. Aussi bien la Loi type de la CNUDCI sur les signatures électroniques[13], qui a été adoptée en 2001, que la plus récente Convention des Nations Unies sur l'utilisation des communications électroniques dans les contrats internationaux[14] (qui a été adoptée par l'Assemblée des Nations Unies le 23 novembre 2005 et a été ouverte à la signature le 16 janvier 2006) suivent la même approche, bien que la Loi type de la CNUDCI sur les signatures électroniques contienne quelques dispositions supplémentaires (voir ci-dessous les paragraphes (…)-(…).

11. Lorsque la loi suit l'approche minimaliste, la question de savoir si l'équivalence de la signature électronique a été prouvée relève habituellement du pouvoir d'appréciation du juge, de l'arbitre ou de l'autorité publique, agissant généralement sur la base du principe dit de la "fiabilité appropriée". Selon ce principe, tous les types de signatures électroniques qui satisfont aux conditions fixées sont considérés comme valables; ce principe reflète par conséquent le principe de neutralité technologique.

12. Une très large gamme de facteurs juridiques, techniques et commerciaux peuvent intervenir lorsqu'il s'agit de déterminer si, dans les circonstances, telle ou telle méthode d'authentification offre un degré de fiabilité approprié, et notamment: a) le degré de perfectionnement du matériel utilisé par chacune des parties; b) la nature de leur activité commerciale; c) la fréquence avec laquelle les parties réalisent des opérations commerciales; d) la nature et l'importance de la transaction; e) les conditions auxquelles doit répondre la signature à l'application de la législation ou de la réglementation applicable; f) la capacité des systèmes de communication; g) le respect des procédures d'authentification imposées par les intermédiaires; h) la gamme de procédures d'authentification offertes par un intermédiaire; i) le respect des pratiques et des usages commerciaux; j) l'existence de mécanismes d'assurance couvrant les messages non autorisés; k) l'importance et la valeur de l'information contenue dans le message de données; l) la disponibilité d'autres méthodes d'identification et leur coût; m) le degré d'acceptation ou de non acceptation de la méthode d'identification employée dans secteur considéré à la fois au moment où la méthode a été convenue et au moment où le message de données a été communiqué.

2. Approche technospécifique

13. Le souci de promouvoir la neutralité technologique soulève d'autres questions importantes. L'impossibilité de garantir une sécurité absolue contre la fraude et les erreurs de transmission n'est pas limitée au monde du commerce électronique et s'applique aussi au monde des documents sur support papier. Lorsqu'ils sont appelés à formuler des règles en matière de commerce électronique, les législateurs sont fréquemment enclins à rechercher le degré de sécurité le plus élevé qu'offre la technologie existante.[15] Il n'est pas

---

du commerce électronique. L'on trouvera les dernières informations disponibles sur l'application de l'UETA à l'adresse http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp, consulté le 7 février 2007.

[12] Afrique du Sud, Colombie, Équateur, Inde, Maurice, Panama et République dominicaine.

[13] Voir note […] (Publication des Nations Unies, numéro de vente: F.02.V.8).

[14] Voir note […] (résolution 60/21 de l'Assemblée générale, annexe).

[15] L'un des premiers exemples a été la Loi relative aux signatures numériques promulguée par l'État de l'Utah, adoptée en 1995, mais abrogée à compter de mai 2006 par le projet de loi No. 20 disponible à l'adresse: http://www.le.state.ut.us/~2006/htmdoc/sbillhtm/sb0020.htm, consulté le 28 mars 2007. L'orientation technologique de la loi de l'Utah se retrouve dans un certain nombre de pays dont la législation ne reconnaît que les signatures numériques créées au

douteux que, dans la pratique, il faut appliquer les mesures de sécurité les plus rigoureuses possibles pour éviter tout accès non autorisé aux données, assurer l'intégrité des communications et protéger les systèmes informatiques et l'information. Toutefois, du point de vue du droit privé des affaires, il peut être mieux approprié de graduer les normes de sécurité par étape, comme cela est fait dans le monde des documents sur support papier. Dans ce dernier cas, en effet, les hommes d'affaires sont généralement libres de choisir parmi une large gamme de méthodes pour garantir l'intégrité et l'authenticité de leur communication (on peut en citer comme exemple les degrés différents d'authentification des signatures manuscrites selon qu'il s'agit d'un seing contrat privé ou d'un acte notarié). Selon une approche technospécifique, la réglementation applicable indiquerait quelle est la technologie à utiliser pour qu'une signature électronique soit juridiquement valable. Tel est le cas, par exemple, lorsque la loi, dans le but d'assurer une plus grande sécurité, exige des applications ICP. Les approches qui imposent l'utilisation d'une technologie spécifique sont également appelées "prescriptives".

14. Les inconvénients de l'approche technospécifique sont qu'en privilégiant des types déterminés de signatures électroniques, elle "risque d'exclure d'autres technologies pouvant être meilleures".[16] Plutôt que de faciliter le développement du commerce électronique et l'utilisation de techniques d'authentification électronique, une telle approche pourrait ainsi avoir l'effet opposé. En outre, en imposant une technologie déterminée, la législation risque de cristalliser les règles applicables avant qu'une technologie déterminée ne parvienne à son état de pleine maturité.[17] Il se peut alors que la législation empêche l'évolution ultérieure de cette technologie ou condamne rapidement celle-ci à l'obsolescence par suite de l'évolution de la technique. Un autre aspect est que toutes les applications n'exigent peut-être pas le même degré de sécurité que celui qu'offrent certaines techniques spécifiées, comme les signatures numériques. Il se peut également que la rapidité et la facilité des communications ou d'autres considérations soient plus importantes pour les parties que la nécessité de garantir l'intégrité de l'information électronique communiquée par tel ou tel moyen. Imposer l'utilisation de moyens d'authentification inutilement sûrs pourrait entraîner des gaspillages d'argent et d'efforts et ainsi entraver la diffusion du commerce électronique.

---

moyen d'une infrastructure à clé publique (IPC) comme seul moyen valable d'authentification électronique, ce qui est le cas, par exemple, en Allemagne (Loi de 1997 relative aux signatures numériques, promulguée comme article 3 de la Loi relative aux services d'information et de communication du 13 juin 1997); en Argentine (Loi No. 25.506 relative aux signatures numériques et Décret No. 2628/2002 relatif aux signatures numériques portant application de la loi No. 25.506); en Estonie (Loi de 2000 relative aux signatures numériques); en Fédération de Russie (Loi fédérale No. 1-FZ) du 10 janvier 2002) relative aux signatures numériques électroniques); en Israël (Loi de 2001relative aux signatures électroniques); en Inde (Loi de 2000 relative à l'information technologique); au Japon (Loi de 2001 relative aux signatures électroniques et aux services de certification); en Lituanie (Loi de 2000 relative aux signatures électroniques); en Malaisie (Loi de 1997 relative aux signatures numériques); et en Pologne (Loi de 2001 relative aux signatures électroniques).

[16] Stewart Baker et Matthew Yeo, document d'information « Background and Issues Concerning authentication and the ITU » en collaboration avec le Secrétariat de l'Union internationale des télécommunications, présenté à la réunion d'experts de l'Union internationale des télécommunications sur les signatures électroniques et les autorités de certification: incidences pour l'Union internationale des télécommunications, Genève, 9 et 10 décembre 1999, document No.2 www.itu.int/osg/spu/ni/esca/meetingdec9-101999/briefingpaper.html, consulté le 12 avril 2007.

[17] Étant donné cependant que l'IPC est aujourd'hui une technologie assez mûre et bien établie, certaines de ces craintes ne s'appliqueraient sans doute pas avec la même force.

15. Les législations qui reposent sur l'approche technospécifique privilégient habituellement l'utilisation de signatures numériques à l'intérieur d'une infrastructure à clé publique (IPC). La façon dont les IPC sont structurées, à son tour, varie d'un pays à l'autre selon le degré d'intervention des pouvoirs publics. Dans ce cas également, on peut identifier essentiellement trois modèles:

a) **Autorégulation**. Selon ce modèle, les moyens d'authentification sont laissés totalement libres. Il se peut que l'État adopte pour sa propre administration plusieurs systèmes d'authentification, mais le secteur privé reste libre d'adopter les mécanismes d'authentification, commerciaux ou autres, qu'il juge appropriés. Il n'est pas désigné d'autorité supérieure investie d'une autorité obligatoire, et les prestataires de services d'authentification sont ceux qui ont la responsabilité d'assurer l'interopérabilité avec les autres prestataires de services nationaux et internationaux, selon les objectifs du système d'authentification. En outre, les technologies et les prestataires de service d'authentification n'ont pas à être agréés (sous réserve, le cas échéant, de l'application des dispositions relatives à la protection des consommateurs.[18]

b) **Intervention limitée des pouvoirs publics**. L'État peut décider d'établir une autorité supérieure d'authentification, de compétence volontaire ou obligatoire. Dans pareil cas, il pourra être nécessaire pour les prestataires de service d'authentification de se tenir en rapport avec ladite autorité pour que leurs marques d'authentification soient acceptées en dehors de leurs propres systèmes. Les spécifications techniques et les modalités de gestion des prestataires de service d'authentification devront alors être publiées aussi rapidement que possible de sorte qu'aussi bien les services publics que le secteur privé puissent s'organiser en conséquence. Les prestataires de services d'authentification peuvent également être sujets à agrément.[19]

c) **Mécanisme public**. Il se peut que l'État décide de créer au plan central un prestataire de services d'authentification à compétence exclusive. Des prestataires de service d'authentification à des fins spéciales peuvent également être établis avec l'autorisation de l'État.[20] Les systèmes de gestion de l'identité (voir ci-dessus les paragraphes […] à […] constituent pour l'État un autre moyen de diriger indirectement le processus de signature numérique. Quelques pays ont déjà lancé des programmes en vue de délivrer à la population des documents d'identité à lecture machine équipés de signatures numériques.

3. Approche dualiste

16. Selon cette approche, la loi fixe un seuil minimum de conditions auxquelles doivent répondre les méthodes d'authentification électronique pour avoir un certain statut juridique minimum et accorde un effet juridique plus large à certaines méthodes d'authentification électronique (parfois appelées signatures électroniques sécurisées, avancées ou renforcées ou certificats qualifiés).[21] Au niveau le plus élémentaire, les

---

[18] Asia-Pacific Economic Cooperation. *Assessment Report on Paperless Trading of APEC Economies* (Beijing, Secrétariat de l'APEC, 2005), p. 63 et 64, où les États-Unis sont cités comme exemple d'application de ce modèle.

[19] Singapour est cité comme exemple.

[20] La Chine et la Malaisie sont citées comme exemples.

[21] Babette Aalberts et Simone van der Hof, Digital Signature Blindness – Analysis of

législations qui reposent sur une approche dualiste reconnaissent généralement aux signatures électroniques l'équivalence fonctionnelle des signatures manuscrites sur la base de critères technologiquement neutres. Des signatures reflétant un niveau de sécurité plus élevé, auquel s'appliquent certaines présomptions valables jusqu'à preuve du contraire, sont requises dans des conditions spécifiques liées à l'utilisation d'une technologie déterminée. À l'heure actuelle, les législations de ce type définissent habituellement de telles signatures sécurisées sur la base des technologies IPC.

17. Cette approche est habituellement celle qui est retenue par les pays qui considèrent que leur législation doit fixer un certain nombre de normes technologiques tout en laissant libre cours aux progrès de la technologie. Elle peut offrir un moyen terme entre flexibilité et certitude dans le contexte des signatures électroniques en laissant aux parties le soin de décider, à la lumière de leurs usages commerciaux, si le coût et la gêne que suppose l'utilisation d'une méthode plus sûre sont justifiés par leurs besoins. Ces textes donnent également des indications concernant les critères de reconnaissance des signatures électroniques dans le contexte du modèle d'autorité de certification retenu. Il est généralement possible de combiner l'approche dualiste et n'importe quel type de modèle de certification (autorégulation, accréditation volontaire ou mécanisme public), comme c'est essentiellement le cas pour l'approche technospécifique (voir plus haut, par. ...). Ainsi, si certaines règles peuvent être suffisamment flexibles pour rendre possible l'utilisation de différents modèles de certification des signatures électroniques, certains systèmes ne reconnaissent que les prestataires de services de certification agréés comme émetteurs possibles de certificats "sécurisés" ou "qualifiés".

18. Les premiers à adopter des textes reposant sur l'approche dualiste ont notamment été Singapour[22] et l'Union européenne,[23] qui ont été suivis par plusieurs autres pays.[24] La

---

Legislative Approaches to Electronic Authentication, novembre 1999, http://rechten.uvt.nl/simone/Digsigbl.pdf>, 3.2.2.

[22] L'article 8 de la loi de 1998 relative aux transactions électroniques reconnaît toute forme de signature électronique, mais les présomptions énumérées à l'article 18 (à savoir, entre autres, que la signature est celle de la personne à laquelle elle se rapporte et que la signature a été apposée par ladite personne dans l'intention de signer ou d'approuver le contenu électronique du message) ne s'appliquent qu'aux "signatures électroniques sécurisées" qui répondent aux conditions de l'article 17 (autrement dit, la signature doit: a) être propre à la personne qui l'utilise, b) pouvoir identifier ladite personne, c) avoir été créée par l'utilisation d'un moyen soumis au contrôle exclusif de la personne qui l'a employée, et d) être liée au document électronique auquel elle se rapporte de sorte que la signature serait privée de validité si le document était modifié. Les signatures numériques étayées par un certificat fiable conforme à l'article 20 sont automatiquement considérées comme des "signatures électroniques sécurisées" aux fins de la loi.

[23] Comme la loi singapourienne relative aux transactions électroniques, la Directive de l'Union européenne sur les signatures électroniques (voir supra, note 1) établit une distinction entre la "signature électronique" (définie au paragraphe 1 de l'article 2 comme étant "une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification") et la "signature électronique avancée" (définie au paragraphe 2 dudit article comme étant une signature électronique satisfaisante aux exigences suivantes: "a) être liée uniquement au signataire, b) permettre d'identifier le signataire, c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif, et d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable". Aux termes du paragraphe 2 de l'article 5 de la Directive, les États Membres de l'UE doivent veiller à ce que "l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que la signature se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat qualifié, ou qu'elle ne repose pas

Loi type de la CNUDCI sur les signatures électroniques permet à l'État ayant décidé d'appliquer ce texte de mettre en place un système dualiste, même si elle ne l'encourage pas activement.[25]

19. S'agissant du deuxième niveau, il a été proposé que les pays n'exigent pas l'utilisation de signatures du deuxième niveau dans le cas des conditions de forme des transactions commerciales internationales et que les signatures électroniques "sécurisées" soient limitées aux domaines d'application du droit qui n'ont guère d'impact sur le commerce international (par exemple fiducie, droit de la famille, transactions immobilières, etc.).[26] Il a été suggéré en outre que les lois envisageant deux niveaux de signatures reconnaissent expressément effet aux accords contractuels touchant l'utilisation de la reconnaissance des signatures électroniques, pour que les modèles mondiaux d'authentification de type contractuel n'aillent pas à l'encontre des réglementations nationales.

B. Valeur probante des signatures électroniques et des méthodes d'authentification

20. L'un des principaux objectifs de la Loi type de la CNUDCI sur le commerce électronique et de la Loi type de la CNUDCI sur les signatures électroniques était d'éviter le manque de cohérence et le risque de sur-régulation en proposant des critères généraux en vue d'établir une équivalence fonctionnelle entre les signatures et les méthodes d'authentification électroniques et sur support papier. La Loi type de la CNUDCI sur le commerce électronique a été très largement acceptée et de plus en plus d'États l'ont utilisée comme modèle pour promulguer leurs lois relatives au commerce électronique, mais l'on ne peut pas encore tenir pour acquis que les principes reflétés dans la Loi type sont d'application universelle. L'attitude adoptée par divers pays en ce qui concerne les signatures électroniques et l'authentification reflète habituellement l'approche suivie pour ce qui est de l'exigence d'un écrit et de la valeur probante des documents électroniques.

---

sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature. Cependant, seules les signatures électroniques avancées "basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature" sont considérées comme répondant "aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites imprimées "sur papier" et étant "recevables comme preuves en justice".

[24] Par exemple Maurice et Pakistan (ibid.). Pour plus amples détails sur les législations respectives, voir la note [9] ci-dessus.

[25] Le paragraphe 3 de l'Article 6 de la Loi type de la CNUDCI sur les signatures électroniques (voir note [...]) stipule qu'une signature électronique est considérée comme fiable si; a) les données afférentes à la création de signature sont, dans le contexte dans lequel elles sont utilisées, liées exclusivement au signataire, b) les données afférentes à la création de signature étaient, au moment de la signature, sous le contrôle exclusif du signataire, c) toute modification apportée à la signature électronique après le moment de la signature est décelable, et d) dans le cas où l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte, toute modification apportée à cette information après le moment de la signature est décelable.

[26] Baker et Yeo, “Background and Issues Concerning Authentication and the ITU”, voir note 16.

1. “Authentification” et attribution des enregistrements électroniques

21. L'utilisation de méthodes électroniques d'identification soulève deux questions qui méritent d'être examinées dans le présent contexte. La première a trait à celle, générale, de l'attribution d'un message à son expéditeur supposé et la deuxième est de savoir si la méthode d'identification utilisée par les parties est propre à satisfaire aux conditions légales de forme, en particulier en ce qui concerne 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'authentification.

22. La Loi type sur le commerce électronique 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,[27] 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 été 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 la paternité d'un message de données ou d'établir l'identité des parties 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 est considéré comme émanant de l'expéditeur.

23. 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.

24. 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.[28] La législation 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

---

[27] Publication des Nations Unies, numéro de vente: F.99.V.11 disponible à l’adresse: http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf>.

[28] Colombie (art. 17); Équateur (art. 10); Jordanie (art. 15); Maurice (par. 2 de l'article 12); Philippines (par. 3 de l'article 18); République de Corée (par. 2 de l'article 7); Singapour (par. 3 de l'article 13); Thaïlande (article 16) et Venezuela (article 9). L'on trouve des règles semblables dans la législation de Jersey (Dépendance de la Couronne britannique) (article 8) et des territoires britanniques d'outre-mer des Bermudes (par. 2 de l'article 16) et des îles Turques-et-Caïques (article 14). Pour plus amples détails, voir note 9 ci-dessus.

d'attribution du message.[29] 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.[30]

25. 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.[31] Enfin, quelques pays qui ont incorporé la Loi type sur le commerce électronique dans leur droit interne n'ont pas prévu de dispositions particulières fondées sur l'article 13.[32] Ces pays sont partis du principe qu'aucune règle particulière n'était nécessaire et qu'il valait mieux utiliser les mêmes moyens de preuve ordinaire pour l'attribution des messages que pour l'attribution de 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.”[33]

26. D'autres pays ont néanmoins préféré séparer les dispositions de la Loi type concernant l'attribution et celles qui ont trait aux signatures électroniques. Cette approche est basée sur l'idée que, dans un contexte documentaire, l'attribution a essentiellement pour objectif de constituer une présomption et peut reposer sur des moyens plus larges que ceux qui servent exclusivement à identifier une personne. Les législations de certains pays, comme la loi uniforme des États-Unis relative aux transactions électroniques, mettent en relief ce principe en stipulant par exemple 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", ce qui “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."[34] Cette règle générale d'attribution n'affecte pas l'utilisation d'une signature

---

[29] Mexique (voir note 9 ci-dessus) par. I de l'article 90).

[30] Par exemple, la Loi uniforme des États-Unis sur les opérations électroniques (UETA) (voir note 10) prévoit à 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 imputable". 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 toute autre manière prévue par la loi ”.

[31] Australie (par. 1 de l'article 15); des règles essentiellement identiques sont prévues dans la législation des pays suivants: Inde (article 11); Pakistan (2002, par. 2 de l'article 13); Slovénie (article 5); île de Man (Dépendance de la Couronne britannique) (article 2) et Région administrative spéciale chinoise de Hong Kong (article 18).

[32] Par exemple, Afrique du Sud, Canada, France, Irlande et Nouvelle-Zélande.

[33] Canada, *Loi uniforme annotée sur le commerce électronique (*voir note 10*),* commentaire officiel de l'article 10.

[34] États-Unis, Loi uniforme 1999 relative aux transactions électroniques) (voir note 11, article 9). Le paragraphe 1 du commentaire officiel de l'article 9 offre les exemples suivants d'attribution aussi bien de l'enregistrement que d'une signature électronique: la personne "tape son nom dans une commande par courrier électronique"; "l'employé de la personne, conformément au pouvoir qui lui a été donné, tape le nom de la personne dans une commande

comme moyen d'attribuer un enregistrement à une personne mais est fondée sur la reconnaissance du fait que "une signature n'est pas la seule méthode d'attribution."[35] Selon le commentaire officiel de cette loi, par conséquent,

> "4. Un environnement électronique peut contenir certaines informations qui ne semblent pas attribuer un enregistrement particulier à une personne ou qui lient clairement les deux. Les codes numériques, les numéros d'identification personnels et les paires de clés publique et privée servent à établir la part 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 moyens 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. La mention des procédures de sécurité ne veut pas dire que d'autres formes de preuves 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."[36]

27. 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

---

par courrier électronique"; ou "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".

[35] Ibid.: Le paragraphe 3 du commentaire officiel de l'article 9 se lit comme suit : "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 indique la machine à partir de laquelle il été envoyé. De même, le document transmis peut contenir l'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'identifier 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."

[36] Ibid. commentaire officiel de l'article 9.

circonstances, y compris toute convention éventuelle des parties" ainsi qu'en fonction "d'autres conditions légales envisagées à la lumière de ce contexte."[37]

28. Selon cette conception flexible de l'attribution, les tribunaux des États-Unis d'Amérique semblent faire preuve de souplesse en ce qui concerne la recevabilité des enregistrements électroniques, y compris des messages électroniques, comme élément de preuve en matière civile.[38] Des tribunaux américains ont rejeté les arguments selon lesquels les messages électroniques n'étaient pas recevables du fait qu'ils n'étaient pas authentifiés et constituaient une preuve testimoniale.[39] Ils ont estimé au contraire que les messages électroniques obtenus du demandeur pendant la procédure de divulgation des pièces s'authentifiaient eux-mêmes car "la production pendant la procédure de divulgation de documents détenus par les parties est un motif suffisant pour considérer ces documents comme s'auto-authentifiant."[40] Les tribunaux prennent généralement en considération tous les éléments de preuve disponibles et ne rejettent pas les enregistrements électroniques comme étant en principe irrecevables.

29. Dans les pays qui ont adopté la Loi type sur le commerce électronique, 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 signatures électroniques. Les craintes exprimées au sujet du risque de manipulation des enregistrements électroniques, par exemple, ont conduit les tribunaux de certains de ces pays à refuser de considérer des courriels comme élément de preuve recevable, faisant valoir que les courriels ne comportent de garanties adéquates d'intégrité.[41] Il existe aussi d'autres exemples de cette approche plus restrictive, dont plusieurs récentes affaires de ventes aux enchères sur Internet, dans lesquelles les tribunaux ont appliqué une règle stricte pour l'attribution de messages de données. Ces affaires concernaient le plus souvent des allégations de contravention au contrat fondées sur le défaut de paiement de biens prétendument achetés aux enchères sur Internet, le demandeur soutenant chaque fois que le défendeur était l'acheteur, étant donné 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 tribunaux 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. Ils 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

---

[37] Ibid. paragraphe 6 du commentaire officiel de l'article 9.

[38] *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; and *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.

[39] *Sea-Land Service, Inc. v. Lozen International, LLC.*, United States Court of Appeals for the Ninth Circuit, 3 avril 2002, Federal Reporter, 3rd series, vol. 285, p. 808.

[40] *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.

[41] Amtsgericht (Tribunal de district) Bonn, Affaire No. 3 C 193/01, 25 octobre 2001, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 332/2002 (http://www.jurpc.de/rechtspr/20020332.htm, consulté le 11 septembre 2003).

participer à la vente aux enchères en se servant de son nom.[42] Ce risque a été jugé "très élevé" par certains tribunaux au vu des avis d'experts concernant des menaces d'atteinte à la sécurité des réseaux de communication par Internet, en particulier par l'utilisation de "chevaux de Troie" permettant de "voler" le mot de passe d'une personne.[43] 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.[44] Une telle présomption pouvait éventuellement être attachée à une "signature électronique avancée", telle que définie par la loi, mais le détenteur d'un "mot de passe" ne devait pas assumer le risque que celui-ci soit détourné par des personnes non autorisées.[45]

2. Satisfaction des exigences prévues par la loi concernant les signatures

30. Dans certains pays, les tribunaux ont été enclins à interpréter de façon souple les exigences légales en matière de signature. Comme indiqué plus haut (voir introduction, par. (…) - (…), tel a habituellement été le cas, dans certains pays de tradition romaniste, dans le contexte des dispositions des lois anti-fraude qui stipulent que certaines transactions, pour être valables, doivent être établies par écrit et porter une signature. Aux États-Unis, les tribunaux ont également accueilli favorablement la reconnaissance par le législateur des signatures électroniques, admettant leur utilisation dans des situations qui n'étaient pas expressément prévues dans la loi d'habilitation, par exemple dans le cas des mandats judiciaires.[46] Fait plus important, dans le domaine contractuel, les tribunaux 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, les tribunaux ont estimé que le nom dactylographié de l'expéditeur figurant dans un message électronique satisfaisait à l'exigence légale de signature.[47] 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.[48] Le fait que les

---

[42] Amtsgericht (Tribunal de district) Erfurt, Affaire No. 28 C 2354/01, 14 septembre 2001, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 71/2002 (www.jurpc.de/rechtspr/20020071.htm>; 25 août 2003); see also Landgericht (Tribunal du Land) Bonn, Affaire No. 2 O 472/03, 19 décembre 2003, *JurPC—Internet Zeitschrift für Rechtsinformatik,* JurPC Web-Dok. 74/2004, (http://www.jurpc.de/rechtspr/20040074.htm, consulté le 2 février 2007).

[43] Landgericht (Tribunal du Land) Konstanz, Affaire No. 2 O 141/01 A, 19 avril 2002, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 291/2002 (http://www.jurpc.de/rechtspr/20020291.htm, consulté le 25 août 2003).

[44] Landgericht (Tribunal du Land) Bonn, Affaire No. 2 O 450/00, 7 août 2001, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 136/2002 (http://www.jurpc.de/rechtspr/20020136.htm, consulté le 25 août 2003).

[45] Oberlandesgericht (Cour d'appel) Cologne, Affaire No. 19 U 16/02, 6 septembre 2002, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 364/2002 (http://www.jurpc.de/rechtspr/20020364.htm, consulté le 25 août 2003).

[46] *Department of Agriculture & Consumer Services c. Haire*, Fourth Distrcit, Court of Appeal of Florida, Affaire Nos. 4D02-2584 & 4D02-3315, 15 janvier 2003 (http://www.4dca.org/Jan2003/01-15-03/4D02-2584op.pdf, consulté le 12 septembre 2003).

[47] *Cloud Corporation v. Hasbro, Inc.*, United States Court of Appeals for the Seventh Circuit, 26 décembre 2002, Federal Reporter, 3rd series, vol. 314, p. 296.

[48] *Jonathan P. Shattuck c. David K. Klotzbach*, Superior Court of Massachusetts,

tribunaux américains se montrent disposés à considérer que les courriels et les noms qui y sont dactylographiés peuvent satisfaire aux exigences de l'écrit[49] reflète une interprétation extensive de la notion de "signature" qui est entendue comme englobant "tout symbole apposé ou adopté par une partie dans l'intention d'authentifier un écrit" de sorte que, dans certains cas, "un nom dactylographié ou un en-tête sur un document suffit à satisfaire à l'exigence de signature".[50] Lorsque les parties ne contestent pas avoir expédié ou reçu des communications par courriel, les exigences légales de signature se trouveraient satisfaites étant donné que les tribunaux reconnaissent depuis longtemps "qu'une signature liant son auteur peut revêtir la forme de toute marque ou désignation jugée appropriée par la partie qui entend être liée", aussi longtemps que celle-ci "a l'intention de s'engager".[51]

31. Les tribunaux britanniques ont suivi une démarche semblable, considérant généralement la forme d'une signature comme moins importante que sa fonction. Ainsi, les tribunaux tiennent compte habituellement de l'adéquation du moyen utilisé aussi bien s'agissant d'attribuer un message à une personne déterminée ainsi que d'indiquer l'intention de la personne en ce qui concerne le message. Un courriel peut par conséquent constituer un "document" et le nom dactylographié sur un courriel une "signature".[52] Quelques tribunaux ont déclaré n'avoir "aucun doute que si une partie crée et expédie un message électronique, elle sera considérée comme l'ayant signé tout comme si elle avait apposé sa signature manuscrite sur le même document sur papier" et que "le fait que le document est créé électroniquement plutôt que sur un support papier ne peut faire aucune différence."[53] À l'occasion, les tribunaux ont refusé d'admettre, dans le contexte de la législation anti-fraude, qu'un courriel constituait un contrat signé, essentiellement parce que l'intention des parties d'être liées par la signature faisait défaut. Cependant, il ne paraît pas y avoir de cas dans lequel les tribunaux ont refusé *a priori* de considérer qu'un courriel et les noms qui y étaient dactylographiés pouvaient satisfaire aux exigences légales en matière d'écrit et de signature. Dans certains cas, les tribunaux ont considéré que les conditions fixées par la législation anti-fraude n'étaient pas satisfaites car les courriels en question reflétaient simplement les négociations en cours et non un accord final, par exemple parce que, lors des négociations, l'intention de l'une des parties était qu'un contrat liant l'une et l'autre serait conclu après la signature d'un "mémorandum d'accord" et pas avant. [54] Dans d'autres cas, les tribunaux ont fait savoir qu'ils auraient peut-être été enclins à admettre comme signature "le nom ou les initiales" de son auteur "à la fin du courriel" ou "en tout autre

---

11 décembre 2001, 2001 Mass. Super. LEXIS 642.

[49] *Central Illinois Light Company v. Consolidation Coal Company*, United States District Court for the Central District of Illinois, Peoria Division, 30 décembre 2002, Federal Supplement, 2nd Series, vol. 235, p. 916.

[50] Ibid., p. 919. “Des documents internes, factures et courriels peuvent être utilisés comme éléments de preuve aux fins de l'application de la Loi relative à la fraude de l'Illinois. En l'espèce, cependant, le tribunal a considéré que le contrat allégué ne répondait pas aux conditions prévues par la Loi relative à la fraude, non pas parce que les courriels en tant que tels ne pouvaient pas valablement documenter les conditions d'un contrat, mais plutôt parce que rien n'indiquait que les auteurs des courriels et les personnes qui y étaient mentionnées étaient des employés du défendeur.

[51] *Roger Edwards LLC c. Fiddes & Son Ltd*, United States District Court for the District of Maine, 14 février 2003, Federal Supplement, 2nd Series, vol. 245, p. 251.

[52] Hull Industrial Tribunal, *Hall v. Cognos Limited* Affaire No 1803325/97, non publié.

[53] High Court (Chancery Division), *Mehta c. J Pereira Fernandes SA* [2006] EWHC 813 (Ch), [2006] 2 Lloyd's Rep 244.

[54] Queen’s Bench Division, *Pretty Pictures Sarl c. Quixote Films Ltd*, 30 janvier 2003 ([2003] EWHC 311 (QB), [2003] All ER (D) 303 (Jan)).

endroit dans le corps même du courriel", considérant cependant que "l'insertion automatique de l'adresse électronique d'une personne après que le document a été transmis par le prestataire de services Internet d'expédition et/ou de réception" n'était pas "censée constituer une signature".[55] Bien que les tribunaux britanniques paraissent interpréter les dispositions de la législation anti-fraude concernant l'exigence d'un écrit plus rigoureusement que leurs homologues américains, ils tendent généralement à admettre l'utilisation de tout type de signature électronique ou de méthode d'authentification, même en l'absence d'autorisation expresse du législateur, aussi longtemps que la méthode en question remplit les mêmes fonctions qu'une signature manuscrite.[56]

32. Dans les pays de tradition romaniste, les tribunaux ont généralement tendance à suivre une approche plus restrictive, sans doute parce que, pour beaucoup de ces pays, la notion de "document" implique d'ordinaire l'usage d'une forme ou d'une autre d'authentification, ce qui le rend difficile à distinguer d'une "signature". Dans des 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.[57] Une approche un peu plus souple, cependant, se reflète dans un certain nombre de décisions judiciaires qui ont accepté 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.[58]

33. 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'acceptation 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 identifier des fax contenant des déclarations d'appels transmis directement par modem depuis l'ordinateur à un télécopieur d'un tribunal. Dans les premières affaires jugées, les cours d'appel[59] et la Cour fédérale de justice (*Bundesgerichtshof*)[60] avaient

---

[55] *Mehta c. J Pereira Fernandes SA* (voir note 53).

[56] *Mehta c. J Pereira Fernandes SA* (*supra*, note 55). No. 25 "Il y a lieu de noter, dans le texte de la Directive de l'Union européenne concernant le commerce électronique, que la Commission des lois estime qu'il n'y a pas lieu d'apporter de modifications significatives aux lois qui exigent une signature car la question de savoir si les exigences prévues par lesdites lois ont été satisfaites peut être réglée de manière fonctionnelle en se demandant si la conduite du signataire apparent reflète, pour une personne raisonnable, une intention d'authentifier le message […] Ainsi, comme je l'ai déjà dit, si une partie ou l'agent d'une partie qui expédie un courriel et dactylographie son nom ou le nom de son mandant comme exigé ou autorisé par la jurisprudence dans le corps même d'un courriel, cela constituerait à mon avis une signature suffisante aux fins de la Loi relative à la fraude]".

[57] La Cour de Cassation a jugé irrecevable une requête en appel signée électroniquement attendu qu'il existait des doutes sur l'identité de la personne ayant créé la signature et que la requête avait été signée électroniquement avant l'entrée en vigueur de la loi du 13 mars 2000 reconnaissant l'effet juridique des signatures électroniques (Cour de Cassation, Deuxième Chambre civile, 30 avril 2003, *Société Chalets Boisson*, disponible a l'adresse www.juriscom.net/jpt/visu.php?ID=239, consulté le 12 septembre 2003).

[58] Conseil d'État, 28 décembre 2001, N° 235784, *Élections municipales d'Entre-Deux-Monts* (disponible à l'adresse www.rajf.org/article.php3?id_article=467**,** consulté le 12 septembre 2003).

[59] Par exemple, Oberlandesgericht Karlsruhe (Cour d'appel), Affaire No. 14 U 202/96, 14 novembre 1997, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 09/1998

estimé qu'une image numérisée d'une signature manuscrite ne satisfaisait pas aux exigences 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 législation allemande. Toutefois, il incombait généralement au législateur et non au juge d'établir les conditions d'équivalence entre les écrits et communications dématérialisés par transferts de données.[61] 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.[62]

34. Il est intéressant de noter que les tribunaux, même dans certains pays de tradition romaniste qui ont promulgué une législation reconnaissant l'utilisation de signatures numériques basées sur l'ICP, comme la Colombie,[63] ont eux aussi adopté une approche souple et ont confirmé, par exemple, qu'une procédure judiciaire pouvait être menée entièrement au moyen de communications électroniques. Les pièces échangées pendant une telle procédure étaient valables même si elles n'étaient pas revêtues d'une signature numérique étant donné que les communications électroniques utilisaient des méthodes permettant d'identifier les parties.[64]

35. La jurisprudence concernant les signatures électroniques demeure rare et les quelques décisions judiciaires rendues jusqu'à présent ne constituent pas une base suffisante pour tirer des conclusions fermes. Néanmoins, un bref examen des précédents

---

(disponible à l'adresse www.jurpc.de/rechtspr/19980009.htm, consulté le 12 septembre 2003).

[60] Allemagne, Bundesgerichtshof (Cour fédérale de justice), Affaire No. XI ZR 367/97, 29 septembre 1998, *JurPC—Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 291/2002 (http://www.jurpc.de/rechtspr/19990005.htm, consulté le 12 septembre 2003).

[61] Ibid.

[62] Dans une décision rendue au sujet d'une affaire que lui avait soumise la Bundesgerichtshof de l'Allemagne (Cour fédérale de justice) (voir la note 62 ci-dessus), le Gemeinsamer Senat der obersten Gerichtshöfe des Bundes (Sénat commun des cours suprêmes de la Fédération) 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 évolué de manière à tenir compte des récentes innovations technologiques, telles que le télex ou la télécopie. 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 (http://www.jurpc.de/rechtspr/20000160.htm, consulté le 12 septembre 2003).

[63] La Colombie, par exemple, a adopté la Loi type de la CNUDCI sur le commerce électronique, y compris les dispositions générales de son article 7, mais a établi une présomption juridique d'authenticité seulement pour les signatures numériques (Article 28 de la Loi relative au commerce électronique).

[64] Colombie, Juzgado Segundo Promiscuo Municipal Rovira Tolima, *Juan Carlos Samper v. Jaime Tapias*, 21 juillet 2003, Rad. 73-624-40-89-002-2003-053-00. Le tribunal a considéré que la procédure menée par les moyens électroniques était valable alors même que les courriels n'étaient pas revêtus d'une signature juridique étant donné: a) que l'expéditeur des messages de données pouvait être pleinement identifié; b) que l'expéditeur des messages de données avait confirmé le contenu du message envoyé; c) que les messages de données étaient conservés en lieu sûr au Tribunal; et d) que les messages pouvaient être consultés à tout moment (disponible à l'adresse http://www.camara-e.net/_upload/80403--0-7-diaz082003.pdf, consulté le 2 février 2007).

existants fait apparaître plusieurs tendances. Il semble que l'approche adoptée par le législateur en matière de signatures électroniques et d'authentification ait influencé l'attitude des tribunaux dans ce domaine. L'accent mis par le législateur sur les "signatures" électroniques, en l'absence de règle générale concomitante d'attribution, a peut-être conduit à accorder une attention excessive à la fonction d'identification des méthodes d'authentification, ce qui, dans certains pays, a suscité une certaine méfiance à l'égard des méthodes d'authentification qui ne répondent pas à la définition légale d'une "signature" électronique. 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 de la validité des contrats. 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.

3. Efforts visant à établir des équivalents électroniques de formes spéciales de signatures

a) Apostilles*

36. Il a été dit que l'esprit et la lettre de la Convention supprimant l'exigence de la légalisation des actes publics étrangers, faite à La Haye le 5 octobre 1961, ne faisaient pas obstacle à l'usage des technologies modernes.[65] Le Premier Forum international sur la notarisation et l'apostille électroniques a souscrit à cette conclusion et a relevé que l'application et le fonctionnement de la Convention pourraient être améliorés par le recours à de telles technologies.[66] Si la Convention est interprétée à la lumière du principe d'équivalence fonctionnelle, les autorités compétentes pourraient à la fois tenir des registres électroniques et délivrer des apostilles électroniques et faciliter ainsi l'entraide judiciaire et la fourniture de services gouvernementaux.

37. En avril 2006, la Conférence de La Haye de droit international privé et la National Notary Association (NNA) des États-Unis ont lancé le programme pilote d'apostilles électroniques (e-APP), dans le cadre duquel la Conférence de La Haye et la NNA, avec tout État intéressé, s'emploient à mettre au point, promouvoir et faciliter l'application de logiciels pour a) la délivrance et l'utilisation d'apostilles électroniques et b) l'établissement de registres électroniques d'apostilles.[67]

---

* Cette section serait développée davantage dans la version finale du document de référence général.

[65] Conférence de La Haye de droit international privé "Conclusions and recommendations adopted by the Special Commission on the practical operation of The Hague Apostille, Evidence and Service Conventions: 28 octobre au 4 novembre 2003 (La Haye, 2003).

[66] Conclusions adoptées lors du Premier Forum international sur la notarisation et l'apostille électroniques, tenu à Las Vegas (États-Unis les 30 et 31 mai 2005) (disponible à l'adresse http://www.hcch.net/upload/concl_forum.pdf, consulté le 7 février 2007).

[67] Le Programme pilote d'apostilles électroniques (e-APP) est conçu de manière à utiliser les technologies existantes, déjà largement répandues. La technologie suggérée est le support PDF avec XML incorporé. L'on trouvera des informations plus détaillées à l'adresse http://hcch.e-vision.nl/index_en.php?act=text.display&tid=37, sous la rubrique “Deuxième Forum international sur la notarisation et l'apostille électroniques", tenu à Washington (États-Unis) du 27-29 mai 2006).

b) Sceaux

38. Quelques pays ont déjà éliminé l'exigence du sceau, l'apposition d'un sceau n'apparaissant plus comme pertinente dans le contexte contemporain. Le sceau a été remplacé par une signature attestée (c'est-à-dire donnée en présence d'un témoin).[68] Les législations d'autres pays considèrent que des signatures électroniques sécurisées répondent aux exigences du sceau. L'Irlande, par exemple, a promulgué des dispositions spécifiques concernant les signatures électroniques sécurisées selon lesquelles celles-ci peuvent, sous réserve d'être certifiées comme il convient, être utilisées en lieu et place d'un sceau, avec l'assentiment de la personne ou de l'organisme public auquel peut ou doit être remis le document revêtu d'un sceau.[69] Au Canada, l'exigence que la signature d'une personne soit accompagnée d'un sceau prévu par certaines lois fédérales se trouve satisfaite par une signature électronique sécurisée identifiant celle-ci comme étant le sceau de l'intéressé.[70]

39. Plusieurs pays ont également lancé des initiatives envisageant l'utilisation de documents et de signatures électroniques dans le cadre des transactions faisant intervenir des titres de propriété immobilière. Le modèle utilisé dans l'État de Victoria, en Australie, envisage l'utilisation de signatures numériques sécurisées via Internet au moyen de cartes numériques délivrées par une autorité de certification. Au Royaume-Uni, le modèle prévoit qu'un avocat pourra signer un titre de propriété immobilière au nom de son client via Internet. Dans certains pays, la loi reconnaît la possibilité d'utiliser des "sceaux électroniques", par opposition à des "sceaux manuels", laissant aux règlements d'application le soin de déterminer séparément les aspects techniques de la forme que doit revêtir le sceau électronique.[71]

40. Aux États-Unis, la Loi uniforme sur l'enregistrement électronique des biens immobiliers[72] stipule expressément qu'une signature électronique n'a pas à être

---

[68] Au Royaume-Uni, par exemple, la Law of Property Act (Miscellaneous Provisions) Acte de 1989, qui a mis en oeuvre le Rapport de la Commission de réforme des lois sur les “Deeds and Escrows” (Law Com. No.143, 1987).

[69] Irlande, article 16 de la Loi relative au commerce électronique. Cependant, lorsque le document revêtu d'un sceau peut ou doit être remis à un organisme public ou à une personne agissant en son nom, l'organisme public qui accepte l'utilisation d'une signature électronique peut néanmoins exiger qu'elle soit donnée conformément à une technologie et à des formalités de procédures spécifiques.

[70] Canada, article 39 du Titre de 2 de la Loi de 2000 relative à la protection de l'information personnelle et aux documents électroniques. Les lois fédérales en question sont la Loi relative aux biens immobiliers et fédéraux et son Règlement d'application.

[71] L'on peut en citer comme exemples les règles relatives à la validation de documents par des professionnels agréés ou accrédités; tel est le cas notamment de la Loi du Manitoba relative aux professions techniques et aux géoscientifiques, qui définit un "sceau électronique" comme étant la forme d'identification délivrée par l'association professionnelle aux fins de la validation électronique des documents à lecture machine (voir http://apegm.mb.ca/keydocs/act/index.html; consulté le 4 avril 2007).

[72] La loi uniforme sur l'enregistrement électronique des biens immobiliers (The Uniform Real Property Electronic Recording Act) des États-Unis a été rédigée par la National Conference of Commissioners on Uniform State Laws et est disponible à l'adresse http://www.law.upenn.edu/bll/ulc/urpera/URPERA_Final_Apr05-1.htm, consulté le 7 février 2007). La Loi uniforme a été adoptée par les États de l'Arizona, de la Caroline du Nord, du Delaware, du District of Columbia, du Kansas, du Texas, de la Virginie et du Wisconsin (voir http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-urpera.asp,

accompagnée d'un timbre, d'une impression ou d'un sceau physique ou de son image électronique. Essentiellement, ce n'est que l'information figurant sur le sceau, plutôt que celui-ci, qui est requise. Une signature électronique répond à l'exigence d'un timbre, d'une impression ou d'un sceau personnel ou social. Ces indices physiques ne sont pas applicables à un document totalement électronique, mais cette loi stipule que les informations qui figureraient autrement sur le timbre, l'impression ou le sceau doivent être jointes au document ou à la signature électronique ou y être logiquement associées.[73] Ainsi, le timbre ou le sceau notarial qu'exige la législation de certains États n'est pas nécessaire, conformément à cette loi, pour une notarisation électronique. Le timbre ou le sceau de la société qui doit être apposé conformément à la législation de certains États pour authentifier l'acte d'un fondé de pouvoir d'une société n'est pas nécessaire non plus.

c) Notarisation*

41. Aux États-Unis, il existe essentiellement trois lois concernant la notarisation: la Loi uniforme relative aux transactions électroniques, la Loi relative aux signatures électroniques dans le commerce national et international[74] et la Loi uniforme relative à l'enregistrement des biens immobiliers.[75] L'effet combiné desdites lois est que l'exigence légale d'un écrit ou l'exigence d'une signature sur un document devant être notarié ou sur un document sous serment se trouve satisfaite si la signature électronique de la personne autorisée, ainsi que toutes les autres informations requises par la législation applicable, sont jointes au document ou y sont logiquement associées.

42. En Autriche, l'archive de documents électroniques CyberDOC, administré par une société indépendante créée conjointement par la Chambre autrichienne des notaires et Siemens AG, met à la disposition des notaires des archives électroniques qui comportent des fonctions d'authentification.[76] Les notaires autrichiens sont tenus par la loi de verser à ces archives tous les actes notariaux établis après le 1er janvier 2000.

d) Attestation

43. On a fait valoir que les processus classiques de vérification par un témoin, comme les attestations, ne se prêtent pas entièrement à la signature électronique de documents étant donné que nul ne peut avoir l'assurance que l'image qui apparaît sur l'écran est en fait le document sur lequel sera apposée la signature électronique. Tout ce que peuvent voir le signataire et le témoin est une représentation sur l'écran, visible à l'œil nu, de ce qui se trouve prétendument en mémoire. Lorsque le témoin voit le signataire taper des touches sur le clavier, il ne peut pas être certain de ce qui se passe effectivement. Il ne serait par conséquent possible d'avoir la certitude que ce qui apparaît à l'écran correspond au contenu de la mémoire et que les touches

---

consulté le 7 février 2007).

[73] Ces critères sont semblables à ceux prévus par la Loi uniforme relative aux transactions électroniques des États-Unis.

* Cette section serait développée davantage dans la version finale du document de référence général.

[74] Articles 7001 à 7031 du chapitre 96 du Titre 15 du Code des États-Unis.

[75] Voir note 74.

[76] Voir *Österreichische Notariatskammer* (Chambre autrichienne des notaires), disponible à l'adresse http://www.notar.at/de/portal/einrichtungen/cyberdocgmbhcokg/, consulté le 7 février 2007).

utilisées par le signataire correspondent à son intention que si l'ordinateur a été vérifié au moyen de critères d'évaluation fiables.[77]

44. Toutefois, une signature électronique sécurisée pourrait jouer le même rôle que le témoin en identifiant la personne apparaissant comme l'auteur de la signature de l'acte. En utilisant une signature électronique sécurisée sans témoin humain, l'on peut vérifier l'authenticité de la signature, l'identité de la personne à laquelle appartient la signature, l'intégrité du document et probablement même la date et l'heure de la signature. En ce sens, la signature électronique sécurisée peut même être plus certaine qu'une signature manuscrite ordinaire. L'avantage de faire attester par un témoin une signature numérique sécurisée serait vraisemblablement minime, à moins que le caractère volontaire de la signature ne soit mis en question.[78]

45. La législation existante n'est pas allée jusqu'au point de remplacer totalement les règles d'attestation par des signatures électroniques, mais elle permet simplement au témoin d'utiliser une signature électronique. En Nouvelle-Zélande, la Loi relative aux transactions électroniques stipule que la signature électronique d'un témoin répond aux exigences légales de la signature ou du sceau qui doit être attesté. La technologie à employer aux fins de la signature électronique n'est pas spécifiée, aussi longtemps qu'elle "identifie dûment le témoin et indique comme il convient que la signature ou le sceau a été attesté" et qu'elle "est aussi fiable que nécessaire étant donné le but dans lequel et les circonstances dans lesquelles la signature du témoin est requise".[79]

46. La Loi canadienne relative à la protection de l'information personnelle et aux documents électroniques dispose que, lorsque la législation fédérale prévoit qu'une signature doit être attestée par un témoin, cette exigence est satisfaite, dans le cas d'un document électronique, si chaque signataire et chaque témoin signe le document électronique au moyen de sa propre signature électronique sécurisée.[80] Lorsque la législation fédérale exige, comme cela est parfois le cas, qu'un témoin déclare ou certifie que l'information fournie par une personne est véridique, exacte ou complète, cette exigence se trouve satisfaite dès lors que la personne en question appose sa signature électronique sécurisée.[81] Toute déclaration sous serment ou déclaration solennelle exigée par la législation fédérale peut être faite sous forme

---

[77] C'est ce qui est parfois appelé le problème "What You See Is What You Sign" (WYSIWYS) (Ce que vous voyez est ce que vous signez). Voir V. Liu *et al.*, "Visually sealed and digitally signed documents", Association of Computing Machine, *ACM International Conference Proceeding Series, vol. 56, Proceedings of the Twenty-seventh Australian Conference on Computer Science,* vol. 26 (Dunedin, Nouvelle-Zélande, 2004), p. 287, voir également pour une discussion des Trusted Display Controllers.

[78] Voir la discussion figurant dans Joint Infocomm Development Authority of Singapore and the Attorney – General's Chambers, *Joint IDA-AGC Review of Electronic Transactions Act* Stage II: *Exclusions under Section 4 of the ETA*, document de travail LRRD No. 2 /2004 (Singapour, 2004), parties 5 et 8, disponible à l'adresse www.agc.gov.sg, sous la rubrique “Publications”.

[79] Nouvelle-Zélande, Loi relative aux transactions électroniques (voir la note 9, article 23), disponible à l'adresse http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes, consulté le 4 avril 2007).

[80] Canada, Loi relative à la protection des informations personnelles et aux documents électroniques (voir note 72), partie 2, article 46.

[81] Ibid, article 45.

électronique si son auteur la signe au moyen de sa signature électronique sécurisée et si la personne devant laquelle la déclaration est faite ou qui est habilitée à recevoir des déclarations sous serment ou des déclarations solennelles la signe au moyen de sa signature électronique sécurisée.[82] Une autre formule qui a été suggérée pour donner une assurance supplémentaire est que la signature électronique soit apposée par un professionnel fiable, comme un avocat ou un notaire, ou en sa présence.[83]

---

[82] Ibid, article 44.

[83] Le notaire devra obtenir l'authentification de la signature électronique par une autorité de certification agréée. Il se peut que l'acheteur et le vendeur doivent autoriser le notaire à signer par procuration écrite. Voir E-conveyancing: strategy for the implementation of E–conveyancing in England and Wales (Royaume-Uni, Land Registry, 2005), disponible à l'adresse http://www.landregistry.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc, consulté le 7 avril 2007). Ce projet doit être discuté par étapes entre 2006 et 2009.