Nations Unies A/CN.9/630/Add.3

Assemblée générale

Distr.: Générale
16 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: chapitre type sur l'utilisation internationale des méthodes d'authentification et de signature électroniques

Note du secrétariat

Additif

L'annexe à la présente note contient une partie (deuxième partie, chap. premier, sections A et B) d'un chapitre type d'un document de référence général qui traite des aspects juridiques de l'utilisation internationale des méthodes d'authentification et de signature électroniques.

V.07-82260 (F) 170507 180507

Annexe

Table des matières

Deuxième partie

Utilisation internationale des méthodes de signature et d'authentification électroniques

I. Reconnaissance juridique des méthodes étrangères d'authentification et de signature électroniques

1. Les incompatibilités juridiques et techniques sont les deux principales sources de difficultés dans l'utilisation internationale des méthodes d'authentification et de signature électroniques, surtout lorsque celles-ci sont destinées à remplacer une signature juridiquement valable. Les incompatibilités techniques affectent l'interopérabilité des systèmes d'authentification. Des incompatibilités juridiques peuvent provenir du fait que les différentes législations imposent des exigences différentes en matière d'utilisation et de validité des méthodes d'authentification et de signature électroniques.

A. Incidences internationales des législations internes

2. Lorsque les législations internes autorisent des équivalents électroniques des méthodes d'authentification sur papier, les critères de validité de ces équivalents peuvent être inconciliables. Par exemple, si la législation ne reconnaît que les signatures numériques, d'autres formes de signatures électroniques ne seront pas acceptées. D'autres incohérences dans les critères de reconnaissance des méthodes d'authentification et de signature électroniques n'empêcheront peut-être pas, en principe, leur utilisation à l'échelle internationale, mais le coût et les difficultés engendrés par la nécessité de respecter les contraintes imposées par divers pays risquent de réduire les gains de rapidité et d'efficacité que l'on attend de l'utilisation des communications électroniques.

3. Les sections suivantes examinent les incidences de diverses approches juridiques de la technologie sur le développement de la reconnaissance internationale. Elles font également brièvement le point sur le consensus international qui se dégage à propos des mesures susceptibles de faciliter l'utilisation internationale des méthodes d'authentification et de signature électroniques

1. Obstacles internationaux engendrés par des approches internes contradictoires

4. Les approches techniquement neutres, notamment celles qui intègrent un "critère de fiabilité", permettent en général de résoudre les incompatibilités juridiques. La Loi type de la CNUDCI sur le commerce électronique, paragraphe 1 b) de l'article 7[1], et la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux, paragraphe 3 de l'article 9[2], font partie des instruments juridiques internationaux qui adoptent une telle approche. En vertu de cette dernière, une méthode d'authentification ou de

[1] Voir note [...] [publication des Nations Unies, numéro de vente: F.99.V.4].
[2] Voir note [...] [résolution 60/21 de l'Assemblée générale, annexe].

signature électronique qui permet à la fois d'identifier le signataire et d'indiquer la volonté de ce dernier concernant l'information contenue dans la communication électronique satisfait aux exigences de signature, dans la mesure où elle remplit plusieurs critères. Compte tenu de toutes les circonstances, y compris tout accord entre l'expéditeur et le destinataire du message de données, la méthode d'authentification ou de signature doit démontrer qu'elle est aussi fiable qu'il convient au vu de l'objet pour lequel le message de données a été créé ou communiqué. À défaut, elle peut également démontrer qu'elle a rempli ces objectifs, par elle-même ou en conjonction avec d'autres éléments.

5. Certes, l'approche minimaliste facilite l'utilisation internationale des signatures et de l'authentification électroniques, puisque toute méthode d'authentification ou de signature électronique peut être utilisée valablement pour signer ou authentifier un contrat ou une communication, dans la mesure où elle remplit les conditions générales susmentionnées. Cette approche a toutefois pour conséquence que lesdites conditions sont en général uniquement confirmées a posteriori, et il n'est pas garanti qu'un tribunal reconnaisse l'utilisation d'une méthode en particulier.

6. L'utilisation internationale des signatures et de l'authentification électroniques pose véritablement problème dans les systèmes qui prescrivent ou favorisent une technique en particulier. La complexité de la situation s'accroît proportionnellement au niveau de réglementation administrative des signatures et de l'authentification électroniques et au degré de sécurité juridique que la loi confère à telle ou telle méthode ou technique. Les raisons en sont simples: lorsque la loi n'attache aucune valeur ou présomption juridique particulière à certains types de signature ou d'authentification électronique et se contente de prévoir leur équivalence générale aux signatures manuscrites ou à l'authentification sur papier, les risques liés à l'utilisation de la signature électronique sont les mêmes que pour une signature manuscrite en vertu de la législation en vigueur. Par contre, lorsque davantage de présomptions juridiques sont conférées par la loi à une signature électronique particulière (généralement celles qui sont considérées comme "sécurisées" ou "avancées"), le niveau supérieur de risque est déplacé d'une partie à l'autre. Une hypothèse fondamentale de la législation spécifique à une technique est que ce transfert général a priori des risques juridiques peut se justifier par le niveau de fiabilité offert par une technique donnée, lorsque certaines normes et procédures sont respectées. L'inconvénient de cette approche est que, une fois que la fiabilité a priori est liée à l'utilisation (entre autres conditions) d'une technique particulière, toutes les autres techniques – voire la même si elle est utilisée dans des conditions légèrement différentes – deviennent a priori peu fiables, ou du moins sont soupçonnées a priori d'être peu fiables.

7. L'incompatibilité entre les législations nationales spécifique à une technique risque donc d'entraver l'utilisation des signatures électroniques dans le commerce international plutôt que de l'encourager. Cela pourrait se produire de deux manières différentes mais étroitement liées.

8. Premièrement, si les signatures électroniques et les prestataires de services de certification qui les authentifient sont soumis à des exigences techniques et juridiques contradictoires dans différents pays, l'utilisation des signatures électroniques risque d'être entravée ou empêchée dans de nombreuses opérations

internationales si la signature électronique ne peut pas remplir simultanément les diverses conditions.

9. Deuxièmement, une législation spécifique à une technique, notamment si elle favorise les signatures numériques, ce qui est également le cas de l'approche en deux temps, risque d'engendrer un ensemble disparate de normes techniques et de conditions d'autorisation contradictoires qui rendront l'utilisation internationale des signatures électroniques très difficile. Un système dans lequel chaque pays prescrit ses propres normes empêchera peut-être aussi les parties de conclure des accords de reconnaissance mutuelle et de certification croisée[3]. En effet, un problème important non résolu en relation, notamment, avec les signatures numériques, est celui de la reconnaissance transfrontière. Le Groupe de travail sur la sécurité de l'information et la vie privée de l'Organisation de coopération et de développement économiques (OCDE) (ci-après le GTSIVP de l'OCDE) a noté que, même si l'approche adoptée par la plupart des pays semblait non discriminatoire, les différences entre les exigences nationales continueraient à engendrer des problèmes d'interopérabilité[4]. Pour les besoins de la présente étude, les points faibles ci-après, relevés par le GTSIVP de l'OCDE, peuvent présenter un intérêt.

a) **Interopérabilité**. On a constaté de nombreux obstacles et limitations à l'interopérabilité. Au niveau technique, malgré l'abondance des normes, l'absence de normes de base communes applicables à certaines technologies était considérée comme un problème. Au niveau juridique et administratif, les difficultés des parties prenantes à comprendre leur cadre de confiance respectif et, en particulier, l'attribution des responsabilités juridiques et financières, étaient considérées comme des obstacles au progrès. Selon le GTSIVP de l'OCDE, "il semble que ce secteur requiert un examen plus étroit et minutieux si l'on veut essayer d'élaborer des outils communs pour aider les juridictions à mettre en œuvre le niveau d'interopérabilité souhaité pour une application technologique ou un système particulier";

b) **Reconnaissance des services d'authentification étrangers**. Selon le GTSIVP de l'OCDE, les efforts se sont concentrés sur la mise en place de services d'authentification au niveau national; c'est pourquoi les mécanismes destinés à reconnaître les services d'authentification étrangers "ne sont en général pas encore très développés". Le GTSIVP de l'OCDE laisse donc entendre que c'est "un secteur dans lequel il serait utile de poursuivre les travaux. Étant donné que toute activité dans ce domaine est étroitement liée à la question plus générale de l'interopérabilité, ces thèmes pourraient être traités conjointement";

---

[3] Stewart Baker et Matthew Yeo, en collaboration avec le secrétariat de l'Union internationale des télécommunications, "Background and issues concerning authentication and the ITU", document d'information présenté à la réunion d'experts sur les signatures électroniques et les autorités de certification: enjeux pour les télécommunications, Genève, 9 et 10 décembre 1999, document n° 2.

[4] Organisation de coopération et de développement économiques, Groupe de travail sur la sécurité de l'information et la vie privée, *L'usage transfrontalier de l'authentification dans les pays de l'OCDE* (DSTI/ICCP/REG(2005)4/FINAL), http://www.oecd.org/dataoecd/15/59/35883416.pdf, accès le 2 février 2007.

c) **Acceptation des certificats**[5]. Dans certains cas, l'acceptation des certificats délivrés par d'autres entités a été citée comme un obstacle à l'interopérabilité. Le GTSIVP de l'OCDE suggère par conséquent que l'on examine la possibilité d'élaborer un ensemble de bonnes pratiques ou de lignes directrices pour délivrer des certificats à des fins d'authentification. Des travaux sont peut-être déjà en cours dans plusieurs pays sur ce thème et ils pourraient être utiles à toute initiative du GTSIVP de l'OCDE dans ce domaine;

d) **Une large palette de méthodes d'authentification**. Le GTSIVP de l'OCDE a constaté que, dans presque tous les États membres de l'OCDE, une large palette de méthodes d'authentification était déjà utilisée. Ces méthodes vont des mots de passe, d'une part, aux certificats d'authentification (*token*), à la signature numérique et à la biométrie, d'autre part. Selon la technologie utilisée et les contraintes qu'elle impose, ces méthodes peuvent être utilisées individuellement ou être combinées. Nombreux sont ceux qui pourraient juger cette diversité positive, mais si l'on se réfère aux informations contenues dans les réponses au questionnaire du GTSIVP de l'OCDE, l'éventail des possibilités est tel que fournisseurs et utilisateurs de services d'authentification risquent d'être complètement désorientés lors du choix de la méthode la plus adaptée à leurs besoins. Selon le GTSIVP de l'OCDE, il serait donc peut-être utile d'adopter un outil de référence pour évaluer les différentes méthodes d'authentification et pour définir dans quelle mesure leurs caractéristiques répondent aux attentes des fournisseurs ou des utilisateurs.

10. La confiance dans l'utilisation des méthodes d'authentification et de signature électroniques dans les opérations internationales pourrait être renforcée par une large adoption de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux et la mise en œuvre de son approche techniquement neutre en matière de signatures et d'authentification électroniques. Toutefois, il ne serait pas réaliste de s'attendre à ce que cela rende inutile l'élaboration d'une solution harmonisée pour faire face à des normes techniques et juridiques incompatibles. De nombreux pays continueront peut-être à prescrire l'utilisation de méthodes d'authentification précises pour certains types d'opérations. De plus, certains pays estimeront peut-être que des orientations plus concrètes sont nécessaires pour évaluer la fiabilité des méthodes d'authentification et de signature, en particulier les méthodes étrangères, et leur équivalence avec celles qu'ils utilisent, ou du moins qu'ils connaissent.

---

[5] Un certificat sert à prouver qu'un particulier ou un dispositif précis est passé par un processus d'authentification. Les certificats liés à l'utilisateur sont essentiels à des fins d'identification. Les certificats au porteur peuvent être suffisants pour certaines formes d'autorisation. On mentionnera comme exemple un permis de conduire valable, un numéro de sécurité sociale ou un autre numéro d'identification, ou une carte à puce. Centre pour la démocratie et la technologie, "Privacy principles for authentication systems", http://tprc.org/papers/2003/183/CDTauthenticationTPRC.pdf, accès le 12 avril 2007; voir aussi Centre pour la démocratie et la technologie, groupe de travail sur l'authentification et les principes de confidentialité, "Interim report on privacy principles for authentication systems", http://www.cdt.org/privacy/authentication/030513interim.pdf, accès le 12 avril 2007.

2. Émergence d'un consensus

11. Les divergences entre politiques relevées au plan international s'expliquent probablement par une combinaison de facteurs à des degrés divers. Comme on l'a vu plus haut (voir par. [...]-[...] ci-dessus), certains pays ont tendance à avoir des exigences de forme plus sévères et spécifiques en ce qui concerne les signatures et les documents, alors que d'autres se concentrent sur l'intention du signataire, et autorisent un large éventail de moyens pour prouver la validité de la signature. Ces différences d'ordre général transparaissent habituellement dans la législation qui traite des méthodes d'authentification et de signature électroniques (voir par. [...]-[...] ci-dessus). Une autre source de disparités résulte du degré variable d'intervention des pouvoirs publics dans les aspects techniques de ces méthodes. Certains pays ont tendance à jouer un rôle direct dans la définition des normes applicables aux nouvelles technologies, dans l'idée, peut-être, que cela conférera un avantage concurrentiel à leur industrie[6].

12. Il est également possible que les différentes politiques reflètent différentes hypothèses quant à l'évolution des techniques d'authentification. Un scénario, le système d'authentification universelle[7], suppose que l'objectif principal des techniques d'authentification sera de vérifier l'identité et les caractéristiques de personnes qui n'ont aucune relation préexistante entre elles, et qui utilisent en commun une technique n'ayant pas fait l'objet d'un accord contractuel. Dès lors, la technique d'authentification ou de signature devrait confirmer l'identité ou les autres caractéristiques d'une personne à un nombre potentiellement illimité de personnes et pour un nombre potentiellement illimité d'objets. Ce modèle souligne l'importance des normes techniques et des exigences opérationnelles des prestataires de services de certification lorsque des tiers de confiance sont concernés. Un autre scénario, celui du système de l'authentification liée, recommande que les techniques d'authentification et de signature servent principalement à vérifier l'identité et les caractéristiques de personnes qui utilisent en commun une technique en vertu d'un accord contractuel[8]. La technique d'authentification devrait donc confirmer l'identité ou d'autres caractéristiques du titulaire du certificat uniquement pour un ensemble défini d'objets, au sein d'une communauté définie de parties susceptibles de se fier aux certificats, qui sont soumises à des conditions communes d'utilisation de la technique. Conformément à ce modèle, l'accent est mis sur la reconnaissance juridique des accords contractuels.

13. Malgré ces divergences, qui subsistent en partie, les conclusions du GTSIVP de l'OCDE[9] montrent qu'un consensus international semble se dégager sur les principes fondamentaux qui devraient régir le commerce électronique, en particulier les signatures électroniques. Les conclusions suivantes sont particulièrement intéressantes du point de vue de la présente étude:

a) **Approche non discriminatoire des signatures et des services "étrangers"**. Les cadres législatifs reconnaissent la valeur juridique des signatures certifiées par des services situés dans d'autres pays si celles-ci ont été créées dans les mêmes conditions que les signatures certifiées au niveau national. Dans ces

---

6 Voir note [...] "Background and issues concerning authentication and the ITU".
7 Ibid.
8 Ibid.
9 Voir note [...] [*L'usage transfrontalier de l'authentification dans les pays de l'OCDE*].

conditions, l'approche est non discriminatoire, tant que les exigences locales ou des exigences équivalentes sont satisfaites. Cette information recoupe les conclusions des examens précédents du GTSIVP de l'OCDE sur l'authentification;

b) **Neutralité technologique**. La quasi-totalité des répondants ont indiqué que leur cadre législatif et réglementaire régissant les services d'authentification et les signatures électroniques était technologiquement neutre. Cependant, lorsqu'il s'agit d'applications concernant la cyberadministration ou lorsqu'un niveau maximum de sécurité est requis pour la signature électronique, la majorité des répondants ont indiqué que l'utilisation d'une infrastructure à clef publique (ICP) était spécifiée. À partir de ces éléments d'information, on constate que si les cadres législatifs peuvent être technologiquement neutres, la technologie doit être spécifiée lorsqu'il s'agit de décisions concernant l'administration publique;

c) **Importance de l'ICP**. Selon le GTSIVP de l'OCDE, l'ICP semble la méthode d'authentification privilégiée lorsqu'on recherche une preuve forte de l'identité et un niveau élevé de sécurité juridique pour la signature électronique. Généralement, elle est utilisée par des "communautés d'intérêts" spécifiques dont tous les membres ont eu préalablement des liens professionnels sous une forme ou une autre. L'adoption de cartes à puce à clef publique et l'intégration de fonctions de certification numérique dans les logiciels d'application ont simplifié l'utilisation de cette méthode pour les utilisateurs. Cependant, il est généralement admis que l'ICP n'est pas nécessaire pour toutes les applications et que les méthodes d'authentification devraient être sélectionnées en fonction de leur adéquation aux objectifs poursuivis.

14. De plus, le GTSIVP de l'OCDE a relevé que tous les pays étudiés disposaient, sous une forme ou une autre, d'un cadre législatif ou réglementaire qui conférait des effets juridiques aux signatures électroniques au niveau national. Il a constaté que, même si dans le détail les législations différaient d'un pays à l'autre, une approche cohérente semblait se dessiner, car la plupart d'entre elles s'inspiraient de cadres internationaux ou transnationaux existants (par exemple la Loi type de la CNUDCI sur les signatures électroniques ou la Directive 1999/93/CE du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques[10]).

B. Critères pour la reconnaissance des méthodes étrangères d'authentification et de signature électroniques

15. Comme mentionné plus haut, l'un des principaux obstacles à l'utilisation internationale des signatures et de l'authentification électroniques a été le manque d'interopérabilité dû à des normes incompatibles ou divergentes, ou à leur mise en œuvre incohérente. De nombreuses instances ont été établies pour promouvoir une ICP interopérable fondée sur des normes pouvant servir de cadre à des opérations sécurisées dans les applications du commerce électronique. Ces instances comprennent aussi bien des organisations intergouvernementales[11] que des organisations mixtes publiques/privées[12], à l'échelle mondiale[13] ou régionale.

---

[10] *Journal Officiel des Communautés européennes*, n° L 13/12, 19 janvier 2000.

[11] Dans la région Asie-Pacifique, le forum de l'Association de coopération économique Asie-Pacifique a élaboré des principes directeurs applicables aux mécanismes d'émission de

16. Ces activités techniques visent en partie à élaborer des normes techniques en vue de fournir les informations nécessaires pour répondre à certaines exigences juridiques[14]. Toutefois, elles portent dans une large mesure davantage sur les questions techniques que sur les questions juridiques et n'entrent pas dans le cadre de la présente étude. Les sections suivantes se concentrent donc surtout sur les

---

certificats pouvant être utilisés dans le commerce électronique transfrontière (groupe spécial sur la sécurité électronique, groupe de travail sur les télécommunications et l'information, décembre 2004), http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf, accès le 12 avril 2007. Ces principes directeurs visent à aider à élaborer des mécanismes potentiellement interopérables et à faire le point de l'interopérabilité des mécanismes existants. Ils couvrent des catégories ou types de certificats qui sont uniquement utilisés dans le commerce électronique international. Ils ne s'étendent pas à d'autres certificats et n'ont pas pour objet de limiter les mécanismes à la seule émission des certificats auxquels ils s'appliquent.

12 Au sein de l'Union européenne, l'Initiative européenne de normalisation des signatures électroniques (EESSI) a été créée en 1999 par l'enceinte de coordination des activités de normalisation pour les technologies de l'information et de communication (ICT Standards Board) afin de coordonner les activités de normalisation à l'appui de la mise en œuvre de la Directive 1999/93/CE de l'Union européenne sur les signatures électroniques. Le ICT Standards Board est une initiative du Comité européen de normalisation, lequel a été créé par des organisations nationales de normalisation et par deux organisations à but non lucratif: le Comité européen de normalisation électrotechnique et l'Institut européen des normes de télécommunication. L'EESSI a élaboré diverses normes pour promouvoir l'interopérabilité, mais leur mise en œuvre a été lente, en raison semble-t-il de leur complexité (Paolo Balboni, "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information and Communications Technology Law*, vol. 13, n° 3, 2004), p. 211 à 242, 214.

13 Par exemple, l'OASIS (Organization for the Advancement of Structured Information Standards), consortium international à but non lucratif fondé en 1993 pour promouvoir l'élaboration, la convergence et l'adoption de normes pour le commerce électronique. L'OASIS a créé un comité technique sur l'ICP constitué d'utilisateurs, de vendeurs et d'experts chargés de traiter de certains aspects de la mise en place de la technologie des certificats numériques. Ce comité a élaboré un plan d'action en vue, notamment, de définir des profils ou des principes directeurs spécifiques décrivant comment les normes devraient être utilisées dans certaines applications pour permettre l'interopérabilité des ICP; de créer de nouvelles normes si nécessaire; et de prévoir des tests d'interopérabilité (OASIS, comité technique sur l'ICP, plan d'action de février 2004), http://www.oasis-open.org/committees/pki/pkiactionplan.pdf; accès le 12 avril 2007).

14 L'Institut européen des normes de télécommunication (ETSI), par exemple, a élaboré une norme (TS 102 231) pour créer une structure non hiérarchisée qui pourra notamment traiter de la reconnaissance croisée des domaines ICP et, partant, de la validité des certificats. En résumé, la spécification technique TS 102 231 prévoit la fourniture d'informations sur le statut des prestataires de services de certification (appelé "prestataires de services de confiance"). Ces informations sont présentées sous la forme d'une liste signée. Cette liste prévue par l'ETSI répond à l'exigence de preuves sur le point de savoir si le prestataire d'un service de confiance opère ou opérait avec l'approbation d'un mécanisme reconnu, au moment où le service a été fourni, ou au moment où une transaction faisant appel à ce service a été effectuée. Pour se conformer à cette exigence, la liste doit contenir des informations permettant de déterminer si le service du prestataire était connu par l'opérateur du mécanisme au moment de la transaction, et dans l'affirmative, quel était le statut de ce service (c'est-à-dire s'il était approuvé, suspendu, supprimé ou annulé). Sur la liste prévue par la spécification technique TS 102 231 doivent donc figurer non seulement le statut actuel du service, mais également son historique. La liste renferme ainsi un ensemble de services valides ("liste blanche") et de services supprimés ou annulés ("liste noire") (voir http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231v010201p&RGW.doc, accès le 4 mars 2007).

exigences juridiques de forme et de fond de la reconnaissance internationale des signatures électroniques.

1. Lieu d'origine, réciprocité et validation au niveau local

17. Le lieu d'origine est un élément généralement lié à l'attribution de la reconnaissance juridique à un document ou à un acte étranger. Cela se fait en général sur la base de la réciprocité, ce qui signifie que les signatures et certificats d'un pays donné se voient reconnaître un effet au plan national dans la mesure où il y a effectivement réciprocité. Un autre élément connexe consiste à soumettre la reconnaissance au niveau national d'une signature ou d'un certificat étranger à une forme quelconque de validation ou de reconnaissance par un prestataire de services de certification, une autorité de certification ou un organisme de réglementation à l'échelle nationale. Certains pays conjuguent tous ces éléments[15].

18. Il est rare que les législations nationales refusent expressément la reconnaissance juridique à des signatures ou certificats étrangers, ce qui peut, en apparence, confirmer leur caractère non discriminatoire. Dans la pratique, toutefois, de nombreux régimes de reconnaissance auront probablement certains effets discriminatoires, même si cela n'est pas intentionnel. La directive de l'Union européenne sur les signatures électroniques, par exemple, interdit de manière générale toute discrimination à l'égard des certificats qualifiés étrangers (c'est-à-dire les signatures numériques fondées sur l'ICP). Toutefois, cela bénéficie surtout aux certificats émis par des prestataires de services de certification établis sur le territoire des États membres de l'Union européenne. Pour les autres, il existe trois options pour obtenir la reconnaissance d'un certificat dans l'Union européenne: remplir les conditions visées dans la directive européenne sur les signatures électroniques et être accrédité dans le cadre d'un régime d'accréditation établi dans un État membre; instaurer une certification croisée avec un prestataire de services de certification établi dans un État membre de l'Union européenne; ou opérer dans le cadre d'une reconnaissance générale en application d'un accord international[16]. Il ressort de la manière dont la directive réglemente les aspects internationaux que l'un des objectifs qu'elle poursuit consiste à garantir l'accès des marchés extérieurs aux prestataires européens de services de certification[17]. En

---

[15] En Argentine, par exemple, les certificats et les signatures électroniques étrangers sont reconnus s'il existe un accord de réciprocité avec le pays d'origine de l'autorité de certification étrangère, ou s'il y a "reconnaissance par une autorité de certification agréée en Argentine et validée par l'organisme chargé d'appliquer la réglementation" (voir *Ley de firma digital* (2001), art. 16).

[16] En fait, en vertu de l'article 7 de la directive, les États membres de l'Union européenne doivent uniquement veiller à ce que les certificats délivrés par un prestataire de service de certification établi dans un pays tiers soient reconnus équivalents, sur le plan juridique, aux certificats délivrés par un prestataire de services de certification établi dans la Communauté: a) si le prestataire de services de certification remplit les conditions visées dans la directive et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un État membre; ou b) si un prestataire de services de certification établi dans la Communauté, qui satisfait aux exigences visées dans la présente directive, garantit le certificat; ou c) si le certificat ou le prestataire de services de certification "est reconnu en application d'un accord bilatéral ou multilatéral entre la Communauté et des pays tiers ou des organisations internationales".

[17] L'objectif tendant à assurer l'accès des marchés étrangers aux prestataires européens de services de certification apparaît clairement dans la formulation du paragraphe 3 de l'article 7 de la directive, qui dispose que: "Lorsque la Commission est informée de l'existence de difficultés rencontrées par des entreprises communautaires pour obtenir l'accès au marché de pays tiers,

cumulant, d'une part, l'exigence de l'équivalence fonctionnelle avec les normes de l'Union européenne et, d'autre part, l'obligations d'être "accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un État membre", la directive européenne sur les signatures électroniques exige en fait des prestataires de services de certification étrangers qu'ils respectent à la fois leur régime et celui de l'Union européenne, c'est-à-dire plus que ce qui est demandé aux prestataires accrédités dans un État membre de l'Union européenne[18].

19. L'article 7 de la directive européenne sur les signatures électroniques a été mis en œuvre avec quelques variantes[19]. Ainsi, l'Irlande et Malte reconnaissent les signatures numériques étrangères (certificats qualifiés selon la terminologie européenne) en tant qu'équivalent des signatures internes, sous réserve que d'autres exigences juridiques soient remplies. Dans d'autres pays, la reconnaissance est soumise à une vérification interne (Autriche, Luxembourg), ou à la décision d'une autorité nationale (Estonie, Pologne, République tchèque). Cette tendance à exiger une forme quelconque de vérification interne, si elle se justifie en général par un souci légitime quant au niveau de fiabilité des certificats étrangers, entraîne dans les faits une forme de discrimination à l'égard de ces derniers en fonction de leur origine géographique.

2. Équivalence fonctionnelle

20. Fidèle à une tradition de longue date, la CNUDCI n'a pas voulu tenir compte de considérations géographiques lorsqu'elle a proposé des critères pour la reconnaissance des certificats et des signatures électroniques étrangers. En effet, le paragraphe 1 de l'article 12 de la Loi type de la CNUDCI sur les signatures électroniques prévoit expressément que, pour déterminer si, ou dans quelle mesure, un certificat ou une signature électronique produit légalement ses effets, il n'est tenu compte ni du lieu dans lequel le certificat est émis ou la signature électronique créée ou utilisée, ni du lieu dans lequel l'émetteur ou le signataire a son établissement.

21. Le paragraphe 1 de l'article 12 de la Loi type vise à traduire le principe fondamental selon lequel le lieu d'origine ne doit, en aucun cas, être par lui-même un facteur permettant de déterminer si et dans quelle mesure des certificats ou des signatures électroniques étrangers devraient être reconnus comme susceptibles de produire légalement des effets. Cette détermination ne doit pas dépendre du lieu dans lequel le certificat ou la signature électronique a été émis, mais de sa fiabilité technique. On trouve également des dispositions non discriminatoires similaires à l'article 12 de la Loi type dans d'autres législations nationales, notamment la loi intitulée "United States Electronic Signatures in Global and National Commerce Act 2000" (loi des États-Unis sur les signatures électroniques dans le commerce mondial et national, 2000)[20]. Ces dispositions prévoient que le lieu d'origine ne doit

---

elle peut, au besoin, soumettre au Conseil des propositions en vue d'obtenir le mandat nécessaire pour négocier des droits comparables pour les entreprises communautaires dans ces pays tiers."

[18] Jos Dumortier *et al.*, "The legal and market aspects of electronic signatures", étude réalisée pour la Direction générale Société de l'information de la Commission européenne (Katholieke Universiteit Leuven, 2003), p. 58.

[19] Ibid., p. 92 à 94.

[20] Voir note [...] [Code des États-Unis, titre 15, chapitre 96, article 7031 (principes régissant l'utilisation des signatures électroniques dans les opérations internationales)].

pas être par lui-même un facteur permettant de déterminer si et dans quelle mesure des certificats ou des signatures électroniques étrangers devraient être reconnus comme susceptibles de produire légalement des effets dans un État adoptant. Elles reconnaissent que la valeur légale d'un certificat ou d'une signature électronique doit dépendre de sa fiabilité technique[21].

22. Plutôt que de tenir compte de facteurs géographiques, la Loi type établit un critère d'équivalence substantielle entre les niveaux de fiabilité offerts par les certificats et signatures en question. Si, en conséquence, le certificat étranger offre "un niveau de fiabilité substantiellement équivalent" à celui d'un certificat émis dans l'État adoptant, il a "les mêmes effets juridiques". De la même manière, une signature électronique créée ou utilisée en dehors du pays "a les mêmes effets juridiques" qu'une signature électronique créée ou utilisée dans le pays "à condition qu'elle offre un niveau de fiabilité substantiellement équivalent". L'équivalence entre les niveaux de fiabilité offerts par les certificats et signatures internes et étrangers doit être déterminée en accord avec des normes internationales reconnues et tout autre facteur pertinent, notamment une convention entre les parties portant sur l'utilisation de certains types de certificats ou de signatures électroniques, à moins que cette convention soit invalide ou sans effets en vertu de la loi applicable.

23. La Loi type n'exige ni n'encourage les dispositions relatives à la réciprocité. En fait, elle "ne contient aucune proposition particulière" pour ce qui est des "techniques juridiques que pourrait utiliser un État adoptant pour reconnaître a priori la fiabilité de certificats et de signatures conformes à la loi d'un État étranger (par exemple une déclaration unilatérale ou un traité)"[22]. Parmi les méthodes permettant d'obtenir ce résultat qui ont été mentionnées durant l'élaboration de la Loi type figure, notamment, la reconnaissance automatique des signatures respectant les lois d'un autre État si les lois de l'État étranger exigent un niveau de fiabilité au moins équivalent à celui requis pour des signatures internes équivalentes. D'autres techniques juridiques que pourrait utiliser un État adoptant pour reconnaître a priori la fiabilité de certificats et de signatures étrangers pourraient inclure les déclarations unilatérales ou les traités[23].

---

[21] Voir *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation*, deuxième partie, par. 83.

[22] Ibid., par. 157.

[23] Voir le rapport du Groupe de travail sur le commerce électronique sur les travaux de sa trente-septième session (A/CN.9/483), par. 39 et 42.