Nations Unies A/CN.9/630/Add.4

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: 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 (deuxième partie, chapitre II, sections A et B1) d'un document de référence général consacré aux aspects juridiques de l'utilisation internationale des méthodes d'authentification et de signature électroniques.

V.07-82266 (F) 250607 260607

Annexe

Table des matières

Deuxième partie

Méthodes d'authentification et de signature électroniques

[…]

II. Méthodes et critères d'établissement de l'équivalence juridique

1. Comme indiqué ci-dessus, il ressort de l'enquête entreprise par le Groupe de travail sur la sécurité et la confidentialité de l'information (GTSCI) de l'Organisation de coopération et eu développement économiques (OCDE) que la plupart des cadres législatifs étaient, en principe, exempts de discrimination à l'égard des méthodes de signature et d'authentification électroniques étrangères, aussi longtemps que celles-ci répondaient aux normes locales ou à leur équivalent, en ce sens qu'ils ne refusaient pas de reconnaître effet juridique aux signatures relatives à des services provenant de pays étrangers, à condition que lesdites signatures aient été créées dans les mêmes conditions que celle reconnues par la législation interne.[1] Cependant, le GTSCI de l'OCDE a également relevé que les mécanismes mis en place pour faciliter la reconnaissance des services étrangers d'authentification n'étaient généralement pas bien développés et a considéré qu'il s'agissait d'un domaine dans lequel il pourrait être utile de poursuivre les travaux. Étant donné que toute étude à ce sujet serait étroitement liée à la question plus générale de l'interopérabilité, le GTSCI a été d'avis que les deux thèmes pourraient être combinés, il a suggéré de mettre au point une série de pratiques optimales ou de lignes directrices.

2. Les sections ci-après contiennent un exposé des mécanismes et arrangements juridiques établis pour faciliter l'interopérabilité au plan international ainsi que des éléments qui déterminent l'équivalence des régimes de responsabilité. Elles traitent principalement des questions découlant de l'utilisation au plan international de méthodes de signature et d'authentification électroniques étayées par des certificats délivrés par un prestataire de services de certification fiable, et en particulier des signatures numériques créées dans le cadre d'une infrastructure à clé publique (ICP), étant donné que les difficultés juridiques risquent d'être plus nombreuses dans le contexte de l'utilisation transfrontière de méthodes de signature et d'authentification électroniques qui exigent l'implication de tierces parties dans le processus de signature ou d'authentification.

A. Types et mécanismes de reconnaissance croisée

3. La charge supplémentaire que représente pour les prestataires de services de certification étrangers la nécessité de se conformer à des normes technologiques nationales risque de devenir un obstacle au commerce international.[2] Par exemple,

---

[1] Voir note […] [*The Use of Authentication across Borders in OECD Countries*].

[2] Voir Alliance for Global Business, "A discussion paper on trade-related aspects of electronic commerce in response to the WTO's e-commerce work programme", avril 1999, http://www.biac.org/statements/iccp/AGBtoWTOavril1999.pdf, consulté le 5 février 2007, p. 29.

les lois qui réglementent les moyens par lesquels les autorités nationales reconnaissent les signatures électroniques et certificats étrangers risquent d'opérer une discrimination à l'égard des entreprises étrangères. À ce jour, tous les législateurs qui ont évoqué cette question ont inclus dans leur législation interne, sous une forme ou sous une autre, une règle relative aux normes que doit respecter le prestataire de services de certification étrangers de sorte que la question est indissociablement liée à celle, plus générale, des conflits de normes nationales. Simultanément, la législation peut également imposer d'autres limitations géographiques ou de procédure qui empêchent la reconnaissance transfrontière des signatures électroniques.

4. En l'absence d'ICP internationales, la reconnaissance des certificats émis par des autorités de certification étrangères peut soulever différents problèmes. La reconnaissance des certificats étrangers est fréquemment assurée par une méthode appelée “certification croisée”. En pareil cas, il faut que des autorités de certification essentiellement équivalentes (ou bien des autorités de certification disposées à assumer certains risques en ce qui concerne les certificats établis par d'autres autorités de certification) reconnaissent respectivement les services qu'elles fournissent, de sorte que leurs usagers puissent communiquer ensemble plus efficacement et en pouvant mieux se fier à la fiabilité des certificats établis. Des difficultés juridiques peuvent surgir dans le contexte de la certification croisée ou de l'enchaînement des certificats lorsqu'interviennent de multiples politiques de sécurité, par exemple s'agissant de déterminer la partie dont la faute a causé un préjudice et sur les déclarations desquelles l'usager a fait fond.

1. Reconnaissance croisée

5. La reconnaissance croisée est un dispositif d'interopérabilité selon lequel la partie se trouvant dans la zone couverte par une ICP peut utiliser des informations fournies par l'autorité d'une autre ICP pour authentifier une question relevant de la région de cette dernière.[3] Un tel arrangement résulte habituellement d'un processus formel d'agrément ou d'accréditation dans la région de l'autre ICP ou d'un processus formel d'audit du prestataire de services de certification de la région couverte par l'ICP.[4] La question de savoir s'il est possible de se fier à une ICP étrangère relève de la partie intéressée ou du propriétaire de l'application ou du service plutôt que du prestataire de services de certification auquel la partie intéressée s'en remet directement.

6. La reconnaissance croisée intervient habituellement au niveau de l'ICP plutôt qu'à celui du prestataire de services de certification. Ainsi, lorsqu'une ICP reconnaît une autre ICP, elle reconnaît automatiquement tous les prestataires de services de certification agréés par celle-ci. La reconnaissance est fondée sur une évaluation du processus d'agrément de l'autre ICP plutôt que sur une analyse de chaque prestataire

---

[3] Le concept de reconnaissance croisée a été élaboré en 2000 par ce qui était alors le Groupe de travail sur les télécommunications et l'information de l'Asia-Pacific Economic Cooperation, Electronic Authentication Task Group, voir publication No. 202-TC-01.2, *Electronic authentication: issues relating to its selection and use* (APEC, 2002), disponible à l'adresse http://www.apec.org/apec/publications/all_publications/telecommunications.html, consulté le 7 février 2007.

[4] Définition fondée sur le Groupe de travail sur les télécommunications et l'information de l'APEC, Electronic Authentication Task Group.

de services de certification accrédité par l'autre ICP. Lorsque des ICP délivrent plusieurs catégories de certificats, le processus de reconnaissance croisée exige d'identifier une catégorie de certificats jugée acceptable pour l'utilisation dans les deux régions, sur la base d'une évaluation de cette catégorie de certificats.

7. La reconnaissance croisée soulève des questions d'interopérabilité technique au niveau de l'application seulement: autrement dit, l'application doit pouvoir traiter le certificat étranger et avoir accès au système de répertoire de la région de l'ICP étrangère pour confirmer le statut du certificat étranger. Il y a lieu de noter que, dans la pratique, les prestataires de services de certification délivrent des certificats assortis de divers degrés de fiabilité, selon les fins auxquelles les certificats sont censés être utilisés par leurs clients. Selon leur degré respectif de fiabilité, les certificats et les signatures électroniques peuvent produire des effets juridiques divers, aussi bien au plan interne qu'à l'étranger. Dans certains pays, par exemple, même des certificats parfois appelés certificats de "faible valeur" peuvent dans certaines circonstances (par exemple lorsque les parties sont contractuellement convenues d'utiliser de tels instruments) produire un effet juridique (voir ci-dessous les paragraphes [42 à 50]). L'équivalence qui doit être établie est par conséquent entre certificats fonctionnellement comparables.

8. Comme indiqué ci-dessus, en matière de reconnaissance croisée, c'est à la partie intéressée qu'il incombe de décider si elle peut se fier à un certificat étranger, et non à son prestataire de services de certification. Cela ne suppose pas nécessairement l'existence d'un contrat ou d'un accord entre deux domaines ICP. Il n'est pas nécessaire non plus de recenser en détail les politiques applicables en matière de certificats[5] ni les affirmations faites au sujet des pratiques d'établissement des certificats,[6] dans la mesure où c'est la partie intéressée qui détermine si elle acceptera le certificat étranger après s'être attaché à déterminer si celui-ci a été délivré par un prestataire de services de certification étrangers fiable. Le prestataire de services est considéré comme fiable s'il a été agréé ou accrédité par un organe officiel ou s'il a fait l'objet d'un audit de la part d'une tierce partie indépendante réputée. La partie intéressée prend elle-même sa décision à la lumière des politiques stipulées touchant l'établissement des certificats dans le domaine ICP étranger.

2. Certification croisée entre infrastructures à clé publique

9. Par certification croisée, l'on entend la pratique consistant à reconnaître la clé publique d'un autre prestataire de services de certification jusqu'à un degré convenu de fiabilité, normalement par contrat. Elle résulte essentiellement de la fusion totale ou partielle de deux domaines ICP en un seul domaine plus vaste. Pour les usagers d'un prestataire de services, les usagers de l'autre sont simplement des signataires relevant de l'ICP élargie.

10. Une certification croisée suppose l'interopérabilité technique et l'harmonisation des politiques et pratiques relatives à l'établissement des certificats.

---

[5] Les politiques concernant les certificats sont une série déterminé de règles qui indiquent l'applicabilité d'un certificat à une communauté déterminée et/ou une catégorie d'applications caractérisées par des règles de sécurité communes.

[6] Les affirmations en question sont celles que fait un prestataire de services de certification concernant les pratiques qu'il suit lorsqu'il établit un certificat.

L'harmonisation des politiques et pratiques est indispensable pour faire en sorte que les domaines ICP soient compatibles pour ce qui est aussi bien de leurs opérations de gestion des certificats (c'est-à-dire délivrance, suspension et révocation des certificats) que de leur application de normes opérationnelles et de règles de sécurité similaires. L'étendue de la couverture de la responsabilité est pertinente aussi. Il s'agit là d'une question hautement complexe dans la mesure où les documents en question sont habituellement volumineux et traitent de questions extrêmement diverses.

11. La certification croisée se prête le mieux à des modèles commerciaux relativement fermés, par exemple si les deux domaines ICP partagent une série d'applications et de services, comme courriels ou applications financières. Elle peut se trouver considérablement facilitée par l'existence de systèmes techniquement compatibles, de politiques convergentes et de structures juridiques identiques.

12. La certification croisée unilatérale (un domaine ICP se fiant à un autre mais pas inversement) est peu commune. Le domaine ICP qui fait confiance à l'autre doit veiller, de manière unilatérale, à ce que ses politiques soient compatibles avec celles du domaine ICP auquel il se fie. Son utilisation paraît être limitée aux applications et services dans le cas desquels la confiance qu'exige la transaction dont il s'agit est unilatérale, par exemple une application selon laquelle le commerçant doit prouver l'identité du client avant que celui-ci ne soumette des informations confidentielles.

B. Équivalence des normes de conduite et des régimes de responsabilité

13. Lorsque l'utilisation au plan international de méthodes de signature et d'authentification électroniques est fondée sur un système de reconnaissance ou de certification croisée, il faut, pour pouvoir décider de reconnaître l'ensemble d'une ICP ou un ou plusieurs prestataires de services de certification étrangers, ou pour établir des niveaux d'équivalence entre catégories de certificats établis dans le contexte d'ICP différentes, évaluer l'équivalence entre les pratiques de certification et les certificats nationaux et étrangers.[7] Du point de vue juridique, il faut pour cela évaluer l'équivalence entre essentiellement trois éléments: équivalence de valeur juridique; équivalence des obligations juridiques; et équivalence de responsabilité.

14. L'équivalence de valeur juridique signifie qu'il est attribué à une signature et à un certificat étrangers le même effet juridique que leur équivalent national. L'effet juridique national qui en résulte sera déterminé essentiellement sur la base de la valeur que le droit interne accorde aux méthodes de signature et d'authentification électroniques, comme on l'a déjà vu (voir ci-dessus par. […]-[…]). Pour reconnaître l'équivalence des obligations juridiques et des régimes de responsabilité, il faut déterminer que les obligations imposées sur les parties qui opèrent dans le cadre d'un régime d'ICP correspondent essentiellement à celles que prévoit le régime

[7] Le Certificate Policy Working Group de la Federal Public Key Infrastructure Policy Authority des États-Unis, par exemple, a mis au point une méthode pour porter une appréciation sur l'équivalence des éléments des politiques applicables (sur la base de cadres appelés RFC (“Request for Comments”) 2527). Cette méthode peut être utilisée pour l'analyse de différentes ICP ou d'une ICP déterminée au regard des lignes directrices en question (voir http://www.cio.gov/fpkipa, consulté le 20 février 2007).

national et que la responsabilité en cas de violation desdites obligations est essentiellement la même.

15. La responsabilité, dans le contexte des signatures électroniques, peut soulever des questions différentes selon la technologie et l'infrastructure de certification utilisées. Des problèmes complexes peuvent surgir, spécialement lorsque le certificat est fourni par une tierce partie spécialisée, comme un prestataire de services de certification. En pareil cas, il y a essentiellement trois parties en présence, à savoir le prestataire de services de certification, le signataire et la tierce partie qui se fie à la signature. Dans la mesure où leurs actes ou omissions causent un préjudice à une quelconque des autres ou contreviennent à leurs obligations expresses ou tacites, chacune peut voir sa responsabilité engagée ou perdre le droit de se retourner contre une autre partie. Différentes approches législatives ont été adoptées en ce qui concerne la responsabilité liée à l'utilisation de signatures numériques:

a) **Absence de dispositions spécifiques concernant les normes de conduite ou la responsabilité**. La loi peut demeurer muette sur ce point, ce qui peut être une autre formule pouvant être envisagée. Aux États-Unis d'Amérique, la loi de 2000 relative aux signatures électroniques dans le commerce national et international[8] ne contient aucune disposition concernant la responsabilité de l'une quelconque des parties qui interviennent dans le service de certification. Généralement parlant, c'est cette approche qui a été adoptée par la plupart des autres pays qui s'en tiennent à une approche minimaliste des signatures électroniques, comme l'Australie;[9]

b) **Normes de conduite et règles de responsabilité applicables uniquement aux prestataires de services de certification**. Une autre approche est celle qui consiste pour la loi à ne réglementer que la responsabilité du prestataire de services de certification. Tel est le cas en vertu de la Directive 1999/93/CE de l'Union européenne portant établissement d'un cadre communautaire pour les signatures électroniques,[10] dont le vingt-deuxième alinéa du préambule stipule que “les prestataires de services de certification qui fournissent des services de certification publics sont sujets à la réglementation nationale concernant la responsabilité”, comme l'indique l'article 6 de la Directive. Il y a lieu de noter que l'article 6 ne s'applique qu'aux "signatures qualifiées", ce qui, pour l'instant, signifie des signatures numériques basées sur ICP exclusivement;[11]

---

[8] Voir note […] [Article 7031 du chapitre 96 du titre 15 du Code des États-Unis (Principes régissant l'utilisation des signatures électroniques dans les transactions internationales)].

[9] Il a été considéré, par exemple, que les mécanismes de droit privé reconnus par le droit australien, comme les dispositions contractuelles relatives aux exclusions, dérogations et dénis de responsabilité, ainsi que les limites imposées à leur fonctionnement par la *common law*, étaient mieux adaptés à la réglementation de la responsabilité que des dispositions légales (voir Mark Sneddon, Legal liability and e-transactions: a scoping study for the National Electronic Authentication Council (National Office for the Information Economy, Canberra, 2000), http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf, consulté le 7 février 2007, pp. 43-47).

[10] Voir note […] [*Journal officiel des communautés européennes,* L 13/12].

[11] Les législations adoptées dans l'Union européenne suivent cette approche; par exemple, la loi allemande relative aux signatures électroniques (SignaturGesetz – SigG) et l'ordonnance connexe (SigV) de 2001, la Loi fédérale autrichienne sur les signatures électroniques (SigG) et

c) **Normes de conduite et règles de responsabilité applicables aux signataires et aux prestataires de services de certification**. Dans certains pays, la loi stipule qu'aussi bien le signataire que le prestataire de services de certification peuvent voir leur responsabilité engagée, mais n'établit pas de normes de diligence en ce qui concerne la partie qui fait fond sur le certificat. Tel est le cas en Chine en vertu de la loi de 2005 relative aux signatures électroniques. Il en va de même à Singapour conformément à la loi de 1998 relative aux transactions électroniques;

d) **Normes de conduite et règles de responsabilité applicables à toutes les parties**. Enfin, la loi peut prévoir des normes de conduite et un régime de responsabilité pour toutes les parties en cause. C'est cette approche qui a été adoptée par la loi type de la CNUDCI sur les signatures électroniques,[12] qui définit les obligations en ce qui concerne la conduite du signataire (article 8), du prestataire de services de certification (article 9) et de la partie qui fait fond sur le certificat (article 11). L'on peut dire que la loi type a posé les critères au regard desquels peut être évaluée la conduite des parties en question. Toutefois, elle laisse au droit interne le soin de déterminer les conséquences de l'inexécution des différentes obligations et le régime de responsabilité qui peut affecter les différentes parties en présence dans le contexte des systèmes de signatures électroniques.

16. Les différences entre régimes nationaux de responsabilité peuvent constituer un obstacle à la reconnaissance transfrontière des signatures électroniques. Il y a essentiellement à cela deux raisons. Premièrement, il se peut que les prestataires de services de certification hésitent à reconnaître les certificats étrangers ou les clés employées par les prestataires de services de certification étrangers, dont la responsabilité ou les normes de diligence peuvent être moins rigoureuses que celles qui leur sont applicables. Deuxièmement, il se peut que les usagers de méthodes de signatures et d'authentification électroniques craignent eux aussi que des limites de responsabilité ou des normes de diligence inférieures, dans le cas d'un prestataire de services de certification étranger, ne restreignent les recours qui leur sont ouverts, par exemple dans le cas de falsifications ou d'informations erronées. Pour les mêmes raisons, lorsque la législation réglemente l'utilisation des méthodes de signature et d'authentification électroniques ou les activités des prestataires de services de certification, elle subordonne habituellement leur reconnaissance des certificats ou l'agrément des prestataires de services de certification étrangers à une évaluation des équivalences, pour ce qui est du fond, de la fiabilité offerte par les certificats et les prestataires de services nationaux. Les normes de diligence et les niveaux de responsabilité auxquels sont soumis les diverses parties constituent, en droit, le principal critère de référence au regard duquel est évaluée l'équivalence. De plus, la possibilité pour un prestataire de services de certification de limiter sa responsabilité ou de s'en exonérer ne manquera pas on plus d'avoir un impact sur le niveau d'équivalence reconnu à ses certificats.

---

l'article 4 du Décret de 2002 relatif aux signatures électroniques du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord.

[12] Voir note […] [publication des Nations Unies, numéro de vente: F.02.V.8].

1. Fondement de la responsabilité dans un cadre d'infrastructure à clé publique

17. L'allocation de responsabilité dans un cadre d'ICP se fait essentiellement de deux façons: par le biais de dispositions contractuelles ou par l'effet de la loi (précédent, loi écrite ou les deux). Les relations entre le prestataire de services de certification et de signataire ont habituellement un caractère contractuel, de sorte que la responsabilité sera généralement fondée sur une violation des obligations contractuelles de l'une ou l'autre des parties. Les relations entre le signataire et la tierce partie dépendront de la nature de la transaction qui les lie. Elles pourront, mais pas nécessairement, être fondées sur un contrat. Enfin, les relations entre le prestataire de services de certification et la tierce partie qui fait fond sur le certificat ne sont généralement pas fondées sur un contrat.[13] Dans la plupart des systèmes juridiques, le fondement de la responsabilité (qu'elle soit contractuelle ou quasi-délictuelle) aura des conséquences significatives pour le régime de responsabilité, en particulier en ce qui concerne les éléments suivants: a) le degré de faute qui pourrait engager la responsabilité d'une partie (autrement dit, quelle est la "norme de négligence" imposée à une partie à l'égard de l'autre); b) les parties qui peuvent réclamer réparation et l'étendue du préjudice dont elles peuvent demander réparation; et c) la question de savoir si une partie défaillante peut ou non limiter ou exclure sa responsabilité.

18. Il découle de ce qui précède non seulement que le régime de responsabilité variera d'un pays à l'autre mais aussi qu'il dépendra, à l'intérieur d'un même pays, de la nature de la relation entre la partie tenue pour responsable et la partie lésée. En outre, différentes règles et théories juridiques peuvent avoir un impact sur tel ou tel aspect de la responsabilité, que celle-ci soit contractuelle, qu'elle soit fondée sur la *common law* ou qu'elle soit régie par la loi, ce qui a parfois pour effet d'atténuer les différences entre les deux régimes. La présente étude ne saurait tenter d'offrir une analyse complète et détaillée de ces questions de caractère général. Elle portera plutôt sur les questions spécifiquement évoquées dans un contexte d'ICP et exposera brièvement comment elles ont été réglées par les législations nationales.

a) Norme de diligence

19. Bien que les divers systèmes juridiques se réfèrent à des systèmes de classement et des théories différents, il a été tenu pour acquis, aux fins de la présente étude, que la responsabilité des parties en présence, dans un cadre d'ICP, aurait essentiellement trois fondements possibles: la négligence ordinaire ou faute; la présomption de négligence (ou faute avec inversion de la charge de la preuve); et la responsabilité objective.[14]

---

[13] Steffen Hindelang, dans “No remedy for disappointed trust: the liability regime for certification authorities towards third parties outwith the EC Directive in England and Germany compared”, *Journal of Information, Law and Technology*, 2002, No. 1, (http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/hindelang, consulté le 6 février 2007), 4.1.1, a discuté en détail la possibilité de créer une relation contractuelle entre le prestataire de services de certification et la tierce partie au regard du droit anglais, et est parvenu à une conclusion négative. Il y a néanmoins des pays où une relation contractuelle pourrait prendre naissance.

[14] Pour une discussion du système de responsabilité dans ce contexte, voir Balboni, “Liability of certification service providers …” (voir note […]), p. 232 et suivantes.

i) Négligence ordinaire

20. Selon cette norme générale, une personne est juridiquement tenue de réparer les conséquences négatives de ses actes, à condition que sa relation avec la personne lésée donne naissance, en droit, à une obligation de diligence. En outre, la norme de diligence généralement requise est une “diligence raisonnable”, laquelle doit être définie simplement comme le degré de diligence qu'un bon père de famille exercerait dans des circonstances semblables. Dans les pays de *common law*, c'est ce que l'on appelle souvent la norme de la “personne raisonnable” tandis que dans les pays de tradition romaniste, l'on parle souvent de norme de “bon père de famille” (*bonus pater familias*). Envisagée spécifiquement du point de vue des affaires, l'on entend par diligence raisonnable le degré de diligence qu'une personne habituellement prudente et compétente se livrant à la même catégorie d'activité exercerait dans des circonstances similaires. Lorsque la responsabilité, d'une manière générale, est fondée sur la négligence ordinaire, il incombe à la partie lésée d'apporter la preuve que le préjudice subi a été causé par le manquement par l'autre partie à ses obligations.

21. La diligence raisonnable (ou la négligence ordinaire) est la norme générale de diligence exigée par la loi type de la CNUDCI sur les signatures électroniques. Cette norme de diligence s'applique aux prestataires de services de certification en ce qui concerne la délivrance et la révocation de certificats et la divulgation d'informations.[15] On peut avoir recours à plusieurs éléments pour évaluer la mesure dans laquelle le prestataire de services de certification se conforme à cette norme générale de diligence.[16] La même norme s'applique également au signataire, qui doit éviter toute utilisation non autorisée et toute divulgation de ses données afférentes à la création de signature.[17] La loi type étend la même norme générale de diligence

---

[15] Voir note […] [publication des Nations Unies, numéro de vente: F.02.V.8]. Le paragraphe 1 de l'article 9 de la loi type stipule ce qui suit: “a) Lorsqu'un prestataire de services de certification fournit des services visant à étayer une signature électronique qui peut être utilisée pour produire des effets juridiques en tant que signature, ce prestataire (…) b) prend les dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il faits concernant le certificat durant tout son cycle de vie ou figurant dans le certificat sont exactes et complètes; (…); “d) fournit à toute partie se fiant au certificat des moyens raisonnablement accessibles de déterminer, s'il y a lieu, à partir de ce certificat ou de toute autre manière (…)”.

[16] Voir note […] [*Loi type sur les signatures électroniques et Guide d'application 2001*]. Le paragraphe 146 du Guide se lit notamment comme suit: “Pour évaluer la responsabilité du prestataire de services de certification, il y a lieu de tenir compte, entre autres, des éléments suivants: a) le coût de l'obtention du certificat; b) la nature des informations certifiées; c) l'existence et l'étendue de toute restriction concernant les fins auxquelles le certificat peut être utilisé; d) l'existence de toute affirmation limitant la portée ou l’étendue de la responsabilité du prestataire de services de certification; et e) les actes de la partie se fiant au certificat ayant pu contribuer à la création du préjudice. Lors de la rédaction de la loi type, il a été généralement convenu que, pour déterminer le montant du préjudice pouvant donner lieu à réparation dans l'État adoptant, il convient de tenir compte des règles régissant la limitation de responsabilité dans l'État où est établi le prestataire de services de certification ou dans tout autre État dont la législation serait applicable en vertu des règles pertinentes de conflits de lois.”

[17] Voir note […] [publication des Nations Unies, numéro de vente: F.02.V.8]. L'article 8 de la loi type se lit en partie comme suit: “Lorsque des données afférentes à la création de signature peuvent être utilisées pour créer un signature ayant des effets juridiques, chaque signataire: a) prend des dispositions raisonnables pour éviter toute utilisation non autorisée de ses donnés afférentes à la création de signature; b) sans retard injustifié, utilise les moyens fournis par le prestataire de services de certification (…), ou fait d'une autre manière des efforts raisonnables

raisonnable à la partie qui se fie au certificat, laquelle est censée adopter des mesures raisonnables pour vérifier à la fois la fiabilité d'une signature électronique et la validité, la suspension ou la révocation du certificat, ainsi qu'observer toute limitation concernant celui-ci.[18]

22. Quelques pays, habituellement des pays ayant incorporé à leur droit interne la loi type de la CNUDCI sur le commerce électronique,[19] ont adopté la norme générale de "diligence raisonnable" pour définir les normes de conduite applicables au prestataire de services de certification.[20] Dans quelques pays, il apparaît que le prestataire de services de certification "soit généralement tenu par une norme générale de diligence raisonnable", bien que le fait que, par leur nature même, les prestataires de services de certification seront des parties dotées de compétences spécialisées en lesquelles les profanes placent une confiance allant au-delà de celle qu'ils accordent aux acteurs qui interviennent normalement sur les marchés "pourra éventuellement déboucher sur l'acquisition d'un statut professionnel ou, de quelque autre manière, les soumettre à une obligation de diligence plus élevée, les prestataires de services devant faire ce qui est raisonnable à la lumière de leurs compétences spécialisées."[21] En fait, comme indiqué ci-dessous (voir par. 29), telle paraît être la situation dans la plupart des pays.

23. En ce qui concerne le signataire, certains pays qui ont adopté la loi type de la CNUDCI sur les signatures électroniques prévoient une norme générale de "diligence raisonnable".[22] Dans plusieurs d'entre eux, la législation donne une liste plus ou moins détaillée d'obligations positives, sans pour autant décrire la norme de diligence ou indiquer les conséquences de l'inobservation desdites obligations.[23]

---

pour aviser toute personne dont il peut raisonnablement penser qu'elle fie à la signature électronique ou qu'elle fournit des services visant à étayer la signature électronique si: i) il sait que les données afférentes à la création de signature ont été compromises; ou ii) il estime, au regard des circonstances connues de lui, qu'il y a un risque important que les données afférentes à la création de signature aient été compromises". En outre, le signataire doit prendre "des dispositions raisonnables pour assurer que toutes les déclarations qu'il fait concernant le certificat durant tout son cycle de vie ou devant figurer dans le certificat sont exactes et complètes".

[18] Loi type de la CNUDCI sur les signatures électroniques (voir note […]), alinéa a), b) i) et b) ii) de l'article 11.

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

[20] Par exemple, l'article 28 de la loi de 2000 relative aux transactions électroniques des îles Caïmanes; et l'article 28 de la loi de 2000 sur les transactions électroniques de la Thaïlande.

[21] "Certification authority: liability issues", étude établie pour l'American Bankers Association par Thomas J. Smedinghoff, février 1998 (http://www.bakernet.com/ecommerce/CA-Liability-Analysis.doc), consulté le 5 février 2007, section 1.1.

[22] Par exemple, article 27 de la loi de 2001 sur les transactions électroniques de la Thaïlande.

[23] Par exemple, article 25 de la loi de 2001 sur les signatures numériques de l'Argentine; article 24 de la loi de 2002 sur les documents électroniques, les signatures électroniques et les services de certification desdites signatures du Chili; article 17 de la loi relative au commerce électronique, aux signatures électroniques et aux messages de données de l'Équateur; article 31 de la loi de 2000 sur les transactions électroniques des îles Caïmanes; articles 40 à 42 de la loi de 2000 sur les technologies de l'information de l'Inde; articles 33 à 36 de la loi de 2000 relative aux transactions électroniques de Maurice; article 17 de la loi relative aux signatures et certificats numériques du Pérou; article 21 de la loi relative aux échanges et au commerce électroniques de la Tunisie; article 15 de l'Ordonnance relative aux procédures et principes applicables à la mise en œuvre de la loi de 2005 relative aux signatures électroniques de la Turquie; et article 19 de la loi relative aux messages de données et aux signatures électroniques de la République

Dans certains pays, cependant, la loi complète expressément la liste d'obligations par une règle générale de responsabilité du signataire en cas de violation de ses obligations,[24] responsabilité qui peut même, dans un cas, avoir un caractère pénal.[25] Certes, il n'y a peut-être pas de norme de diligence unique, mais un système échelonné, la règle applicable par défaut aux obligations du signataire étant une norme générale de diligence raisonnable, norme qui est cependant relevée pour acquérir le statut de garantie dans le cas de certaines obligations spécifiques, habituellement celles qui ont trait à l'exactitude et à la véracité des affirmations faites.[26]

24. La situation de la partie qui se fie au certificat est particulière car il est peu probable qu'un acte ou une omission de sa part puisse causer un préjudice au signataire ou au prestataire de services de certification. Le plus souvent, si la partie qui fait fond sur le certificat manque à exercer la diligence requise, elle supporte les conséquences de ses actes mais n'encourt pas de responsabilité à l'égard du prestataire de services de certification. Il n'est donc pas surprenant que les législations nationales relatives aux signatures électroniques, lorsqu'elles traitent du rôle des parties qui se fient aux certificats, prévoient rarement autre chose qu'une liste générale d'obligations essentielles. Tel est généralement le cas dans les pays qui ont adopté la loi type de la CNUDCI sur les signatures électroniques, qui recommandent une norme de “diligence raisonnable” en ce qui concerne la conduite de la partie qui se fie au certificat.[27] Dans certains cas, cependant, cette règle n'est

---

bolivarienne du Venezuela.

[24] Article 27 de la loi relative aux signatures électroniques de la Chine, promulguée en 2004; article 40 de la loi 527 relative au commerce électronique de la Colombie; article 12 de la loi fédérale de 2002 sur les signatures électroniques numériques de la Fédération de Russie; article 99 du Code de commerce du Mexique: décret de 2003 relatif aux signatures électroniques; articles 37 et 39 de la loi de 2001 sur les signatures numériques du Panama; articles 53 et 55 de la loi de 2002 sur le commerce électronique, les documents et les signatures numériques de la République dominicaine; article 19 de la loi sur les messages de données et les signatures électroniques de la République bolivarienne du Venezuela; et article 25 de la loi relative aux transactions électroniques du Viet Nam.

[25] Pakistan, Electronic Transactions Ordinance, 2002, section 34.

[26] Par exemple, chapitre 88 de la Loi relative aux transactions électroniques de Singapour. Le paragraphe 2 de l'article 37 de cette loi stipule qu'en acceptant un certificat, le signataire "certifie à tous ceux qui se fient raisonnablement aux informations contenues dans le certificat que: a) le signataire détient légalement la clé privée correspondant à la clé publique indiquée dans le certificat; b) toutes les affirmations faites par le signataire à l'autorité de certification et qui revêtent de l'importance pour l'exactitude des informations figurant dans le certificat sont véridiques; et c) toutes les informations figurant dans le certificat sont véridiques pour autant que le sache le signataire." Le paragraphe 1 de l'article 39, en revanche, n'envisage qu'une "obligation de faire preuve d'une diligence raisonnable pour conserver le contrôle de la clé privée correspondant à la clé publique indiquée dans ledit certificat et empêcher qu'elle ne soit divulguée à une personne non autorisée à créer la signature numérique du signataire." Tel paraît également être le cas en République bolivarienne du Venezuela, où l'article 19 de la Loi relative aux messages de données et signatures électroniques qualifie expressément de "due diligence" (*"actuar con diligencia"*) l'obligation d'éviter toute utilisation non autorisée du dispositif de création de signature, tandis que les autres obligations sont exprimées en termes catégoriques.

[27] Article 21 de la Loi de 2000 relative aux transactions électroniques des îles Caïmanes; article 107 du Code de commerce du Mexique: Décret de 2003 relatif aux signatures électroniques; et article 30 de la Loi de 2001 relative aux transactions électroniques de la Thaïlande.

pas prévue expressément.[28] Il y a lieu de noter que les obligations expresses ou tacites de la partie qui se fie au certificat ne sont pas sans importance pour le prestataire de services de certification. En fait, tout manquement de sa part à son obligation de diligence peut permettre au prestataire de services de certification de l'invoquer pour dégager sa responsabilité à l'égard de la partie qui se fie au certificat, par exemple lorsqu'il peut prouver que le préjudice subi par cette dernière aurait pu être évité ou atténué si elle avait pris des mesures raisonnables pour s'assurer de la validité du certificat ou des fins auxquelles il pouvait être utilisé.

ii) Présomption de négligence

25. La deuxième possibilité est un régime fondé sur la faute avec inversion de la charge de la preuve. Selon ce système, une partie est présumée être en faute dès lors qu'un acte qui lui est imputable a causé un préjudice. Le fondement d'un tel système est généralement l'hypothèse que, dans certaines circonstances, il ne peut normalement se produire de préjudice que si une partie a manqué à ses obligations ou ne s'est pas conformée aux normes de conduite attendues d'elle.

26. En droit civil, il peut y avoir présomption de faute en cas de violation du contrat,[29] ainsi que dans divers cas de responsabilité quasi-délictuelle. L'on peut en citer comme exemples la responsabilité encourue du fait des actes d'employés, de préposés, d'enfants ou d'animaux, la responsabilité découlant de telle ou telle activité commerciale ou industrielle (dommages environnementaux, dommages à des biens adjacents, accidents de la circulation). Les théories qui justifient l'inversion de la charge de la preuve et les cas spécifiques dans lesquels elle est admise varient d'un pays à l'autre

27. Dans la pratique, un tel système débouche sur un résultat semblable à celui de la norme renforcée de diligence attendue des professionnels en *common law*. Les professionnels doivent posséder un minimum de connaissances et d'aptitudes spéciales nécessaires pour agir comme membres de la profession et ont l'obligation d'agir comme le ferait dans des circonstances semblables tout membre raisonnable de la profession.[30] Cela ne signifie pas nécessairement que la charge de la preuve

---

[28] Article 16 de l'Ordonnance de 2005 relative aux procédures et principes applicables à la mise en œuvre de la Loi relative aux signatures électroniques de la Turquie; et article 26 de la Loi relative aux transactions électroniques du Viet Nam.

[29] Le paragraphe 1 de l'article 280, du Code civil allemand, par exemple, considère que le débiteur est responsable de tout préjudice causé par la violation d'une obligation contractuelle, à moins que cette violation ne lui soit pas imputable (*"Verletzt der Schuldner eine Pflicht aus dem Schuldverhältnis, so kann der Gläubiger Ersatz des hierdurch entstehenden Schadens verlangen. Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat"*). Le paragraphe 1 de l'article 97 du Code des obligations de la Suisse expose ce principe en termes encore plus clairs: si le créancier n'obtient pas l'exécution en nature, le débiteur doit réparer le préjudice qui en résulte à moins de pouvoir prouver qu'aucune faute ne lui est imputable (*"Lorsque le créancier ne peut obtenir l'exécution de l'obligation ou ne peut l'obtenir qu'imparfaitement, le débiteur est tenu de réparer le dommage en résultant, à moins qu'il ne prouve qu'aucune faute ne lui est imputable"*). Une règle semblable figure à l'article 1218 du Code civil italien. En droit français, la négligence est toujours présumée si le contrat prévoit une obligation de résultat, mais l'existence d'une faute doit être établie si le contrat prévoyait une obligation de moyens plutôt que de résultat (voir Gérard Légier, "Responsabilité contractuelle", *Répertoire de droit civil Dalloz*, août 1989, No. 58-68).

[30] W. Page Keeton et al., *Prosser and Keeton on the Law of Torts*, 5th ed., (Saint Paul, Minnesota,

est inversée, mais la norme plus élevée de diligence attendue d'un professionnel signifie, en pratique, que celui-ci est réputé être capable d'éviter de causer un préjudice aux personnes qui ont recours à leurs services ou dont le soin leur est confié s'ils agissent conformément auxdites normes. Dans certaines circonstances, cependant, la doctrine dite *res ipsa loquitur* permet aux tribunaux de présumer, jusqu'à preuve du contraire, que la survenance d'un dommage "dans des circonstances normales" n'est possible que si une personne ne fait pas preuve de diligence raisonnable.[31]

28. Si cette règle est appliquée aux activités des prestataires de services de certification, cela signifierait que dans tous les cas où une partie qui se fie à un certificat ou à un signataire subit un préjudice pour avoir utilisé une signature électronique ou un certificat et si ledit préjudice peut être imputé au fait que le prestataire de services de certification n'a pas agi conformément à ses obligations contractuelles ou légales, le prestataire de services de certification est présumé fautif.

29. La présomption de négligence paraît être la norme généralement applicable en vertu des législations nationales. Selon la Directive de l'Union européenne relative aux signatures électroniques, par exemple, le prestataire de services de certification peut voir sa responsabilité engagée à l'égard de toute entité qui fait fond sur le certificat qualifié, à moins que le prestataire de services n'apporte la preuve qu'il n'a pas commis de faute.[32] Autrement dit, la responsabilité du prestataire de services de certification est fondée sur la faute avec inversion de la charge de la preuve: il doit prouver que ses actes n'ont pas été négligents, étant donné que c'est lui qui est le mieux placé pour se faire, disposant des compétences techniques nécessaires et ayant accès aux informations pertinentes (qu'aussi bien des signataires que des tierces parties qui se fient au certificat risquent de ne pas avoir).

30. Tel est également le cas en vertu de la législation de divers pays non membres de l'Union européenne qui établit une liste détaillée des obligations des prestataires de services de certification et qui, de manière générale, stipulent qu'ils sont responsables de tout préjudice causé par tout manquement à leurs obligations légales.[33] Il est difficile de dire si toutes ces lois ont véritablement pour effet

---

West Publishing Co., 1984), section 32 p. 187.

[31] "Il faut qu'une négligence soit raisonnablement établie. Lorsque la chose est sous le contrôle du défendeur ou de ses préposés et l'accident est tel que, normalement, il ne surviendrait pas si la personne ayant la garde de la chose faisait preuve d'une diligence raisonnable, il est raisonnablement établi, en l'absence d'explication du défendeur, que l'accident a été imputable à un manque de diligence." (C. J. Erle dans l'affaire *Scott c. The London and St. Katherine's Docks Co.*, Ex. Ch., 3 H & C 596, 601, 159 Eng. Rep. 665, 667 (1865)).

[32] Voir note […] [*Journal officiel des communautés européennes*, L 13/12]. L'article 6 de la Directive pose une norme minimum de responsabilité. Les États ont la latitude de renforcer la responsabilité du prestataire de services de certification, par exemple en introduisant un régime de responsabilité objective ou en étendant leur responsabilité aux certificats non qualifiés. Cependant, tel n'a pas été le cas jusqu'à présent et il est peu probable que cela advienne étant donné que cela placerait les prestataires de services de certification établis dans un pays dans une situation désavantagée par rapport à ceux d'autres pays de l'Union européenne. (Balboni "Liability of certification service providers …" (voir note […]), p. 222).

[33] Article 38 de la loi de 2001 relative aux signatures numériques de l'Argentine; article 14 de la loi de 2002 sur les documents électroniques, les signatures électroniques et les services de certification de ces signatures du Chili; l'article 13 de la loi relative au commerce extérieur, aux

d'inverser la charge de la preuve, mais plusieurs d'entre elles le prévoient expressément, soit d'une manière générale,[34] soit dans le contexte d'obligations spécifiques.[35]

31. La préférence manifestée pour un régime fondé sur la présomption de faute résulte sans doute de la crainte qu'une responsabilité fondée sur la négligence ordinaire ne constitue pas un régime équitable pour la partie qui se fie au certificat, laquelle peut ne pas avoir les connaissances technologiques ni l'accès à l'information nécessaires pour pouvoir prouver la négligence du prestataire de services de certification.

iii) Responsabilité objective

32. La responsabilité objective est une règle utilisée dans divers systèmes juridiques pour fonder la responsabilité d'une personne (habituellement du fait des produits) sans qu'il soit nécessaire d'établir l'existence d'une faute ou d'un manquement à l'obligation de diligence. La personne est réputée responsable simplement pour avoir lancé un produit défectueux sur un marché ou pour avoir fabriqué un matériel dysfonctionnel. Comme la responsabilité est déduite du simple fait qu'il y a eu perte ou dommage, les divers éléments juridiques requis pour qualifier un acte, comme négligence, manquement à une garantie ou conduite délibérée, n'ont pas à être établis.

33. La responsabilité objective constitue une règle exceptionnelle dans la plupart des systèmes juridiques et n'est généralement pas présumée, à moins que la loi ne l'impose. Dans le contexte des méthodes de signature et d'authentification électroniques, la responsabilité objective peut imposer une charge excessive au prestataire de services de certification, ce qui risque à son tour d'entraver la viabilité commerciale de ce secteur à un stade embryonnaire de son développement. À l'heure actuelle, aucun pays ne paraît imposer une responsabilité objective aux prestataires de services de certification ou autres parties qui interviennent dans le processus de signature électronique. Il est vrai que, dans les pays qui ont établi un

---

signatures électroniques et aux messages de données de l'Équateur; l'article 51 de la loi de 2001sur les signatures numériques du Panama; et l'article 22 de la loi relative aux échanges et au commerce électronique de la Tunisie.

[34] Article 28 de la loi relative aux signatures électroniques de la Chine, promulguée en 2004 "Si l'auteur d'une signature électronique ou une personne qui se fie à une signature électronique subit un préjudice pour s'être fiée au service fourni par un prestataire de services électroniques de certification dans le contexte d'une transaction civile, et si ledit prestataire de services n'apporte pas la preuve que le préjudice ne lui est pas imputable, il en est responsable"; voir également l'article 13 de la loi de 2004 sur les signatures électroniques de la Turquie: “Le prestataire de services électroniques de certification est responsable des dommages subis par des tiers du fait de la violation des dispositions de la présente loi ou de son ordonnance d'application. Le prestataire de services électroniques de certification est exonéré de responsabilité s'il apporte la preuve que le dommage n'est pas imputable à une faute de sa part".

[35] L'article 20 du titre 308B de la loi de 1998 relative aux transactions électroniques de la Barbade: “Un prestataire de services de certification agréé n'est pas responsable des erreurs figurant dans un certificat accrédité si a) les informations en question ont été fournies par la personne identifiée dans le certificat accrédité ou en son nom; et b) si le prestataire de services de certification peut apporter la preuve qu'il a pris toutes les mesures raisonnablement possibles pour vérifier cette information.”; voir également le paragraphe 2 b) de l'article 23 de la loi de 1999 sur les transactions électroniques des Bermudes.

répertoire des obligations positives des prestataires de services de certification, la norme de diligence exigée de ces derniers est habituellement très élevée et parfois même proche d'un régime de responsabilité objective, mais le prestataire de services peut néanmoins dégager sa responsabilité s'il peut apporter la preuve qu'il a agi avec la diligence voulue.[36]

b) Parties en droit de réclamer réparation et étendue de celle-ci

34. Une question importante, pour déterminer l'étendue de la responsabilité des prestataires de services de certification et des signataires, a trait aux groupes de personnes pouvant être en droit de demander réparation du préjudice subi du fait d'un manquement par une autre partie à ses obligations contractuelles ou légales. Une autre question connexe est celle de savoir quelle est l'étendue de l'obligation de réparer et quels sont les types de préjudices qui doivent donner lieu à réparation.

35. D'une manière générale, la responsabilité contractuelle découle de la contravention à une obligation contractuelle. Dans un contexte d'ICP, il y a habituellement un contrat entre le signataire et le prestataire de services de certification. Les conséquences d'un manquement par une des parties à ses obligations contractuelles à l'égard de l'autre sont déterminées par le libellé du contrat, tel qu'il est régi par le droit contractuel applicable. Dans le cas des signatures et certificats électroniques, une responsabilité sortant du cadre contractuel habituel peut prendre naissance lorsqu'une personne a subi un préjudice pour s'être raisonnablement fiée aux informations fournies par le prestataire de services de certification ou par le signataire si lesdites informations se sont avérées fausses ou inexactes. Normalement, la tierce partie qui a fait fond sur le certificat n'est pas contractuellement liée au prestataire de services de certification et n'a probablement aucun rapport avec celui-ci, sauf à faire fond sur ses services de certification. Cela peut susciter des questions difficiles qui n'ont pas toujours reçu de réponse complète dans certains pays.

36. Dans la plupart des systèmes de tradition romaniste, il y a lieu de supposer que le prestataire de services de certification est responsable du préjudice subi par la partie qui s'est fiée au certificat pour avoir fait fond sur des informations inexactes ou fausses, même si la législation concernant les signatures électroniques ne contient pas de disposition spécifique à cet effet. Dans plusieurs pays, cette responsabilité peut découler de la disposition générale relative à la responsabilité quasi-délictuelle qui a été introduite dans la législation de la plupart des pays de tradition romaniste,[37] sous réserve de certaines exceptions.[38] Dans quelques pays, on peut établir une analogie entre les activités des prestataires de services de

---

[36] Par exemple, Chili, Équateur et Panama.

[37] L'article 1382 du Code civil de la France stipule que quiconque cause un dommage à autrui est tenu de le réparer. Cette règle générale de responsabilité a inspiré des dispositions semblables dans plusieurs autres pays, comme l'article 2043 du Code civil italien et l'article 483 du Code civil portugais.

[38] Le Code civil allemand contient trois dispositions de caractère général (sections 823 I, 823 II et 826) ainsi qu'un petit nombre de règles spécifiques touchant plusieurs situations quasi-délictuelles définies de manière passablement restrictive. La principale disposition est la section 823 I, qui s'écarte du Code civil français dans la mesure où elle se réfère expressément aux dommages causés “à la vie, à l'organisme, à la santé, à la liberté, aux biens ou à d'autres droits” d'une autre personne.

certification et des notaires, lesquels sont généralement tenus pour responsables du préjudice causé par toute négligence dans l'accomplissement de leurs obligations.

37. Dans les pays de *common law*, cependant, il se peut que la situation ne soit pas aussi claire. Lorsqu'un acte quasi-délictuel est commis dans le contexte de l'exécution d'un contrat, les pays de *common law* ont traditionnellement requis un élément de proximité contractuelle entre l'auteur de l'acte préjudiciable et la partie lésée. Comme la tierce partie ayant fait fond sur le certificat n'est pas liée par contrat avec le prestataire de services de certification et n'a probablement aucun rapport avec celui-ci, sauf pour ce qui est de faire fond sur le certificat faussement établi, il peut être difficile dans certains pays (faute de dispositions légales expresses) pour la partie lésée d'établir son droit d'agir contre le prestataire de services de certification.[39] En l'absence de proximité contractuelle, il faut pour pouvoir agir en invoquant une responsabilité quasi-délictuelle, en *common law*, établir un manquement à l'obligation de diligence de l'auteur de l'acte préjudiciable à l'égard de la partie lésée. Il est parfois difficile de dire si une telle obligation existe, pour le prestataire de services de certification, à l'égard de toutes les parties pouvant être appelées à faire fond sur ses certificats. Généralement, la *common law* répugne à soumettre une personne à une "responsabilité d'un montant indéterminé, pendant une durée indéterminée, à l'égard d'une catégorie non déterminée de personnes"[40] du fait d'affirmations négligentes, à moins que celles-ci "soient faites directement, sachant qu'elle s'y fiera, à une personne à laquelle l'auteur est lié par une obligation quelconque d'agir avec diligence découlant d'une disposition légale, d'un contrat ou de quelque autre facteur".[41]

38. En l'occurrence, la question en jeu est de déterminer quelle est la gamme de personnes envers lesquelles le prestataire de services de certification (ou d'ailleurs le signataire) a une obligation de diligence. Il existe essentiellement trois normes pouvant être utilisées pour définir la catégorie de personnes qui, en pareille situation, peuvent valablement intenter une réclamation contre le prestataire de services de certification:[42]

a) **Norme de prévisibilité**. Il s'agit de la norme de responsabilité la plus large. Selon ce système, le signataire ou le prestataire de services de certification est responsable à l'égard de toute personne dont il était raisonnablement prévisible qu'elle se fierait aux affirmations erronées;

---

[39] Dans le cas de la *common law* anglaise, par exemple, l'auteur est parvenu à la conclusion qu'"en l'absence de législation, la responsabilité du prestataire de services de certification à l'égard de la tierce partie est loin d'être certaine, même s'il est à prévoir que celle-ci subira un préjudice du fait de sa négligence. De plus, l'on voit difficilement comment la tierce partie pourrait se protéger. S'il n'y a pas de responsabilité, l'on se trouve en présence tout au moins d'une lacune, et la négligence de la part du prestataire de services de certification, en particulier, crée une lacune manifeste. La *common law* peut combler des lacunes, mais le processus est incertain et peu sûr" (Paul Todd, *E-Commerce Law* (Abingdon, Oxon, Cavendish Publishing Limited, 2005, p. 149-150). Des conclusions similaires ont été tirées en ce qui concerne le droit australien; voir Sneddon, *Legal liability and e-transactions* … (voir note [11]), p. 15.

[40] Les propos du juge Cardozo, dans l'affaire *Ultramares Corporation c. George A. Touche et al*, Cour d'appel de New York, 6 janvier 1931, 174 N.E. 441, p. 445.

[41] Ibid., p. 447.

[42] Smedinghoff, "Certification authority: liability issues" (voir note [23]), section 4.3.1.

b) **Norme fondée sur l'intention et la connaissance**. Il s'agit ici d'une norme plus étroite qui limite la responsabilité au préjudice subi par un membre du groupe de personnes dans l'intérêt desquelles l'on entend fournir l'information ou l'on sait que l'intéressé a l'intention de la fournir;

c) **Norme de proximité**. Cette norme est la plus limitée et donne naissance à une obligation à l'égard exclusivement du client ou de la personne à laquelle le fournisseur de l'information est spécifiquement lié.

39. La Loi type de la CNUDCI sur les signatures électroniques n'essaie pas de circonscrire le groupe de personnes pouvant relever de la catégorie des "parties qui se fient au certificat", laquelle peut comprendre "toute personne ayant ou non une relation contractuelle avec le signataire ou avec le prestataire de services de certification."[43] De même, selon la Directive de l'Union européenne relative aux signatures électroniques, le prestataire de services de certification est responsable du préjudice causé à toute entité ou toute personne physique ou morale qui se fie raisonnablement au certificat qualifié. La Directive de l'Union européenne est manifestement structurée sur la base d'un système ICP étant donné qu'elle ne s'applique qu'aux signatures numériques (certificats qualifiés). La notion d'entité est habituellement interprétée comme englobant les tierces parties qui se fient au certificat, et c'est ainsi que la Directive a été appliquée par tous les États membres sauf deux.[44]

40. Comme la Loi type de la CNUDCI sur les signatures électroniques, la Directive de l'Union européenne ne rétrécit pas les catégories de personnes pouvant être considérée comme parties ayant fait fond sur un certificat. Aussi a t-il été suggéré que, même en common law, "il est évident, dans le contexte de la fourniture de services de certification, qu'un prestataire de services est lié par une obligation de diligence à l'égard de quiconque peut être appelé à faire fond sur ses certificats pour déterminer d'accepter une signature électronique déterminée dans une transaction donnée vu que l'objet même de la délivrance du certificat est d'encourager une telle pratique."[45]

41. Une autre question intéressante a trait à la nature du préjudice pouvant donner lieu à réparation par le signataire ou le prestataire de services de certification. Dans certains pays de *common law*, par exemple, les demandes d'indemnisation d'un préjudice purement économique causé par des produits défectueux ne peuvent pas être fondées sur une responsabilité quasi-délictuelle. Cependant, en cas de fraude délibérée, dans certains pays, même des affirmations dont l'inexactitude est due à la négligence sont considérées comme des exceptions à la règle.[46] Il est intéressant de noter à ce propos que le Décret de 2002 sur les signatures électroniques du Royaume-Uni ne reprend pas les dispositions relatives à la responsabilité de la Directive de l'Union européenne concernant les signatures électroniques. Ce sont par conséquent des règles usuelles de responsabilité qui s'appliquent, lesquelles sont

---

[43] *Loi type de la CNUDCI sur les signatures électroniques et Guide d'application 2001*. (Voir note […]), par. 150.

[44] Des exceptions sont le Danemark et la Hongrie (Balboni, "Liability of certification service providers …" (voir note […]), p. 220.

[45] Lorna Brazell, *Electronic Signatures: Law and Regulation* (London, Sweet and Maxwell, 2004), p. 187.

[46] Smedinghoff, "Certification authority: liability issues" (voir note [23]), section 4.5.

en l'occurrence fondées sur le critère de proximité du préjudice.[47] Le montant du préjudice pouvant donner lieu à réparation est une question réglée par le droit général de la responsabilité contractuelle ou quasi-délictuelle. Certaines législations font aux prestataires de services de certification l'obligation expresse de contracter une assurance pour couvrir leur responsabilité ou d'indiquer à tous les signataires potentiels, entre autres informations, quelles sont les garanties financières existantes visant à couvrir une éventuelle responsabilité.[48]

c) Possibilité de limitation ou d'exonération contractuelles de responsabilité

42. Les prestataires de services de certification essaient, aussi systématiquement que possible, de limiter leur responsabilité contractuelle et quasi-délictuelle à l'égard du signataire et des parties qui se fient à leurs certificats. En ce qui concerne le signataire, les clauses de limitation de responsabilité figurent habituellement dans le dossier contractuel, comme l'exposé des pratiques applicables. De telles clauses peuvent imposer un plafond de responsabilité par incident, par série d'incidents ou par période de temps ou d'exclure certaines catégories de dommages. Une autre méthode consiste à indiquer dans les certificats la valeur maximum des transactions pour lesquelles ils peuvent être utilisés, ou à limiter l'utilisation des certificats à certaines fins exclusivement.[49]

43. Si la plupart des systèmes juridiques reconnaissent généralement le droit des parties à un contrat de limiter ou d'exclure leur responsabilité par le biais de dispositions contractuelles, ce droit est habituellement soumis à différentes limitations et conditions. Dans la plupart des pays de tradition romaniste, par exemple, il n'est pas possible pour une personne d'exclure totalement sa responsabilité du chef d'actes qui lui sont directement imputables[50], ou bien une telle exclusion est sujette à des limitations clairement stipulées.[51] De plus, si les conditions du contrat ne sont pas librement négociées mais s'il s'agit plutôt d'un contrat d'adhésion, certains types de clauses de limitation et responsabilité peuvent être jugés “abusifs” et par conséquent frappés de nullité.

---

[47] Dumortier et al, “The legal and market aspects of electronic signatures” (voir note [...]), p. 215.

[48] Article 21 a) 1) de la loi de 2001 relative aux signatures numériques de l'Argentine; et article 13 de la loi de 2004 sur les signatures électroniques de la Turquie; voir également l'article 104 (III) du Code de commerce du Mexique: Décret de 2003 relatif aux signatures électroniques.

[49] Voir Smedinghoff, “Certification authority: liability issues” (voir note [23]), section 5.2.5.4; et Hindelang, “No remedy for disappointed trust …” (voir note [15]), section 4.1.1.

[50] En France, il est en principe possible d'exclure la responsabilité découlant d'un manquement au contrat. Dans la pratique, cependant, les tribunaux tendent à annuler de telles clauses d'exonération de responsabilité lorsqu'ils considèrent qu'elles ont eu pour effet de dégager la partie intéressée des conséquences d'un manquement à une obligation contractuelle "fondamentale" (voir Légier, “Responsabilité contractuelle” (voir note […]), No. 262 et 263).

[51] Dans la plupart des pays de tradition romaniste, la loi interdit les clauses d'exonération de responsabilité dans le cas de faute lourde ou de violation d'une obligation imposée par une règle d'ordre public. Certains pays ont promulgué des règles expresses à cet effet, comme le par. II de l'article 100 du Code des obligations de la Suisse et l'article 1229 du Code civil italien. D'autres pays, comme le Portugal, n'ont pas promulgué de règle légale similaire mais parviennent essentiellement au même résultat que l'Italie (voir António Pinto Monteiro, *Cláusulas Limitativas e de Exclusão de Responsabilidade Civil* (Coimbra, Faculdade de Direito de Coimbra, 1985), p. 217).

44. Dans les pays de *common law*, plusieurs théories peuvent conduire à un résultat semblable. Aux États-Unis, par exemple, les tribunaux ne reconnaissent généralement pas la validité des dispositions contractuelles jugées “inadmissibles”. Bien que ce concept dépende habituellement des circonstances de l'espèce, il désigne habituellement des conditions contractuelles “que, d'un côté, aucune personne dotée de raison et en pleine possession de ses facultés n'imposerait, et, d'un autre côté, aucune personne juste et honnête n'accepterait”[52] et qui sont caractérisées par “une absence de choix authentique de la part de l'une des parties et par des conditions léonines en faveur de l'autre.”[53] Comme le concept de droit civil de contrat d'adhésion, cette doctrine a été appliquée pour empêcher les parties se trouvant dans une position de négociation dominante de se livrer à des “pratiques commerciales abusives”.[54] Cependant, les conditions contractuelles de cette catégorie ne sont pas toutes jugées nulles. Bien que, d'une façon générale, les tribunaux reconnaissent la validité des contrats standards ou des contrats d'adhésion dont les conditions ne donnent pas lieu à négociation, il arrive qu'un tribunal, même dans le cas de contrats à la consommation, refuse de reconnaître la validité d'une clause d'un contrat standard si son insertion constitue une surprise injustifiée.[55]

45. Enfin, dans les pays aussi bien de tradition romaniste que de *common law*, les règles relatives à la protection du consommateur peuvent beaucoup réduire la possibilité pour un prestataire de services de certification de limiter sa responsabilité à l'égard du signataire lorsque cette limitation de responsabilité aurait dans la pratique pour effet de priver le signataire d'un droit ou d'un recours reconnu par la législation applicable.

46. La possibilité pour le prestataire de services de certification de limiter sa responsabilité potentielle à l'égard de la partie qui se fie au certificat est normalement sujette, le plus souvent, à des restrictions encore plus rigoureuses. Indépendamment des modèles commerciaux fermés dans lesquels la partie faisant fond sur un certificat est tenue d'adhérer à des clauses contractuelles établies,[56] il arrive très fréquemment que ladite partie ne soit pas liée par contrat au prestataire de services de certification ni même au signataire. Ainsi, dans la mesure où cette partie peut demander réparation sur la base d'une responsabilité quasi-délictuelle au prestataire de services de certification ou au signataire, ces derniers peuvent n'avoir à leur disposition aucun moyen de limiter leur responsabilité étant donné que, dans la plupart des systèmes juridiques, ils devraient pour cela informer comme il

---

[52] *First Financial Ins. Co. c. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), citant *Hume c. U.S.*, 132 U.S. 406, 410 (1975), cité dans Smedinghoff, “Certification authority: liability issues” (voir note [23]), section 5.2.5.4.

[53] Ibid., citant l'affaire *Williams c. Walker-Thomas Furniture Co.,* 350 F.2d 315, 320 (D.C. 1965), cité dans in Smedinghoff, “Certification authority: liability issues” (voir note [23]), section 5.2.5.4.

[54] *First Financial Ins. Co. c. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), cité dans Smedinghoff, “Certification authority: liability issues” (voir note [23]), section 5.2.5.4.

[55] Raymond T. Nimmer, *Information Law*, section 11.12[4][a], p. 11 à 37, cité dans Smedinghoff, “Certification authority: liability issues” (voir note [23]), section 5.2.5.4.

[56] Comme envisagé pour la E-Authentication Federation administrée par la Administration of the United States Government (voir E-Authentication Federation, Interim Legal Document Suite, version 4.0.7, disponible à l'adresse http://www.cio.gov/eauthentication/documents/LegalSuite.pdf, consulté le 8 février 2007).

convient la partie qui se fie au certificat de la limitation de leur responsabilité. La méconnaissance de l'identité de la partie appelée à se fier au certificat avant la survenance du préjudice peut empêcher le prestataire de services de certification (et sans doute encore plus le signataire) de mettre en place un système efficace de limitation de sa responsabilité. Ce problème est typique des systèmes ouverts dans lesquels des inconnus traitent entre eux sans avoir eu de contacts antérieurs et laissent le signataire exposé à des conséquences potentiellement dévastatrices.[57] Beaucoup, en particulier parmi les représentants de l'industrie de la certification, ont considéré qu'il s'agissait là d'un obstacle majeur à une plus large utilisation des méthodes de signature et d'authentification électroniques étant donné la difficulté pour les prestataires de services de certification d'évaluer l'étendue potentielle de leur responsabilité.

47. Le désir d'élucider le droit dans ce domaine a conduit plusieurs pays à reconnaître expressément le droit des prestataires de services de certification de limiter leur responsabilité. La Directive de l'Union européenne sur les signatures électroniques, par exemple, fait aux États membres de l'Union l'obligation de faire en sorte que le prestataire de services de certification indique sur un certificat qualifié les limitations applicables à l'utilisation dudit certificat, aussi longtemps que ces limitations sont reconnaissables par des tiers.[58] Ces limitations peuvent habituellement être rangées en deux catégories: il peut y avoir des limites concernant les types de transactions pour lesquelles peuvent être utilisés des certificats ou catégories de certificats déterminés; et il peut aussi y avoir des limites à la valeur des transactions pour lesquelles le certificat ou la catégorie de certificats en question peut être utilisé. Dans l'une ou l'autre hypothèse, le prestataire de services de certification est expressément exonéré de responsabilité du chef de préjudices découlant de l'utilisation d'un certificat qualifié dépassant les limitations qui lui sont imposée.[59] En outre, la Directive de l'Union européenne relative aux signatures électroniques impose aux États membres de l'Union l'obligation de veiller à ce qu'un prestataire de services de certification puisse indiquer sur le certificat qualifié une limite de la valeur des transactions pour lesquelles le certificat peut être utilisé, aussi longtemps que ladite limite est reconnaissable par des tiers.[60] En pareil cas, la responsabilité du prestataire de services de certification ne dépasse pas cette limite maximum.[61]

48. La Directive de l'Union européenne n'établit pas de plafond à la responsabilité que peut encourir le prestataire de services de certification. Elle n'en autorise pas moins ledit prestataire de services à limiter la valeur maximum de la transaction pour laquelle un certificat peut être utilisé, l'exonérant ainsi de responsabilité au-delà de ce plafond de valeur.[62] Il est fréquent aussi, dans la pratique commerciale,

---

[57] Sneddon, "*Legal liability and e-transactions* ..." (voir note [11]), p. 18.

[58] Directive de l'Union européenne relative aux signatures électroniques (voir note […]), article 6, paragraphe 2.

[59] Ibid.

[60] Ibid., article 6, paragraphe 3.

[61] Ibid.

[62] Dumortier et al. "The legal and market aspects of electronic signatures" (voir note […]), p. 55, avec une discussion dans Hindelang, "No remedy for disappointed trust …" (voir note [15]), section 4.1.1. Balboni, "Liability of certification service providers …" (voir note […]), p. 230, va plus loin et affirme que "… en vertu du paragraphe 4 de l'article 6, il est possible uniquement de limiter la valeur de la transaction (...), ce qui n'a rien à voir avec une limitation de la valeur

que les prestataires de services de certification introduisent par le biais de dispositions contractuelles un plafond global de leur responsabilité.

49. La législation interne de plusieurs autres pays appuie ces pratiques contractuelles en reconnaissant la limite de la responsabilité du prestataire de services de certification à l'égard de toute partie potentiellement lésée. Habituellement, ces pays autorisent les limitations spécifiées dans l'énoncé des pratiques applicables par le prestataire de services de certification et, dans certains cas, exonèrent expressément celui-ci de responsabilité lorsqu'un certificat a été utilisé à une fin autre que celle pour laquelle il a été délivré.[63] En outre, certains pays reconnaissent le droit des prestataires de services de certification d'émettre des certificats de catégories différentes et d'établir des degrés de fiabilité recommandés différents,[64] ce qui entraîne habituellement des niveaux différents de limitation (et de sécurité) selon l'honoraire payé. Cependant, la législation de certains pays interdit expressément toute limitation de responsabilité autre que celle résultant d'une limitation de l'utilisation ou de la valeur des certificats.[65]

50. Les pays qui ont adopté une approche minimaliste, quant à eux, ont considéré une intervention du législateur comme généralement déconseillable et ont préféré laisser aux parties le soin de régler la question dans leur contrat.[66]

---

potentielle du préjudice pouvant résulter de la transaction."

[63] Article 39 de la loi de 2001 relative aux signatures numériques de l'Argentine, article 20 du titre 308B de la loi de 1998 sur les transactions électroniques de la Barbade; paragraphes 3 et 4 de l'article III de la loi de 1999 sur les transactions électroniques des Bermudes; article 14 de la loi de 2002 sur les documents électroniques, les signatures électroniques et les services de certification de telles signatures du Chili; et paragraphes 7 et 8 (dans ce dernier cas, cependant, sans exonération expresse de responsabilité) de l'article 29 de la loi relative aux transactions électroniques du Viet Nam.

[64] Articles 38 et 39 de la loi de 2000 relative aux transactions électroniques de Maurice, et titre 88 de la loi de 1998 sur les transactions électroniques de Singapour.

[65] Article 13 de la loi de 2004 sur les signatures électroniques de la Turquie.

[66] Voir, pour l'Australie, Sneddon, *Legal liability and e-transactions* (voir note [11]), pp. 44-47; et, pour les États-Unis, Smedinghoff, "Certification authority: liability issues" (voir note [23]), section 5.2.51.